CAHIER DU RETEX

RECHERCHE

LES FORCES TERRESTRES ET LE CYBERESPACE COMME NOUVEAU CHAMP DE BATAILLE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA DÉFENSE
Armée de Terre
CDEF Centre de Doctrine d'Emploi des Forces
DREX Division Recherche et Retour d'Expérience

MAI 2014

Les cahiers du RETEX contribuent à la réflexion sur les grandes problématiques qui intéressent aujourd'hui l'armée de Terre française et viennent nourrir les travaux de doctrine.

Ils se déclinent en quatre collections complémentaires :

La collection « opérations »

Elle regroupe les synthèses thématiques liées à un théâtre d'opération ou à une fonction opérationnelle, ainsi que les recueils d'enseignement tactiques au format poche.

La collection « exercices »

Elle publie les rapports d'analyse après action (3A) des exercices de niveau corps à brigade.

La collection « recherche »

Elle publie des travaux à caractère historique ou exploratoire qui visent à éclairer une problématique particulière de l'emploi des forces. Ils suivent le plus souvent une méthodologie de recherche universitaire. Confiés à des officiers de réserve ou des stagiaires, ils ne constituent pas un document officiel.

La collection « rapports »

Elle publie des études notamment celles menées à partir de témoignages de chefs en opérations suivant la technique de l'interview d'autorité.

Illustration de couverture :
Exercice TOLL. Canjuers. VAB SAEC (Station d'appui électronique de contact) du 54e Régiment de Transmission de Oberhoffen.
M. Klein©armée de Terre

LES FORCES TERRESTRES ET LE CYBERESPACE COMME NOUVEAU CHAMP DE BATAILLE

ÉTAT DES LIEUX ET PERSPECTIVES

Élodie SIMON, étudiante à l'Institut des Hautes Études Internationales,
Université Paris 2 Panthéon – Assas.

AVERTISSEMENT

Cette nouvelle livraison des « Cahiers du RETEX » propose un état des lieux sur le « Cyberespace ». Ce travail de chercheur s'inscrit dans l'esprit de la collection des « cahiers du RETEX », dont la vocation est de susciter la réflexion et d'apporter des éléments nouveaux pouvant faire l'objet d'études ultérieures plus approfondies. Il permet ainsi aux lecteurs non-initiés de progresser dans la connaissance d'un milieu complexe et « nouveau ».

Les propos tenus n'engageant que leur auteur, ce travail ne peut être assimilé à un document de doctrine. Il ne préjuge pas des études doctrinales ultérieures, ni de la définition militaire officielle qui sera adoptée pour le cyberespace.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA DÉFENSE

ARMEE DE TERRE

Paris, le 6 mai 2014

CENTRE DE DOCTRINE D'EMPLOI DES FORCES

Division recherche et retour d'expérience

« Le cyberespace est désormais un champ de confrontation à part entière. Dans le cadre des opérations militaires, il doit être considéré comme un milieu, au même titre que l'air, la mer, la terre et l'espace extra-atmosphérique ». C'est en ces termes que débute la doctrine interarmées sur la cyberdéfense qui vient d'être publiée (DIA 3.40, 2014).

Dans cet esprit, l'auteur de ce ***document de recherche*** *explore les vulnérabilités propres aux forces terrestres et les apports de la guerre cybernétique à un affrontement conventionnel. Elle vise aussi à s'interroger sur les opportunités que ce nouvel espace peut engendrer pour l'armée de Terre. Il ne s'agit pas d'un document de doctrine mais d'une étude, qui vient « labourer » un champ nouveau et nourrir la réflexion.*

Après avoir défini les acteurs de ce nouvel espace de bataille, ce document décrit les menaces pouvant peser sur les forces terrestres et fait l'état des lieux des réponses militaires qui y ont déjà été apportées.

Général Jean-François PARLANTI

1, place Joffre – Case 53 – 75700 PARIS SP 07 – Tél. : 01.44.42.81.52 - Fax : 01.44.42.44.66
michel.goya@intradef.gouv.fr

AVANT-PROPOS

Les forces terrestres et le cyberespace comme nouveau champ de bataille. État des lieux et perspectives

En temps de paix comme en temps de guerre, les attaques cybernétiques sont d'ores et déjà une réalité pour les États, pour leurs structures civiles et militaires. Face à ces menaces qui pèsent sur les réseaux informatiques, considérant le développement de la numérisation du champ de bataille et de l'évolution des technologies de l'information, le cyberespace constitue désormais une dimension importante dans les conflits actuels. Pour les forces armées, il s'agit dorénavant d'être capable de maîtriser les réseaux, c'est-à-dire de gérer l'information, de la sécuriser et d'assurer la capacité à opérer.

Or, même s'il n'existe pas encore actuellement de consensus sur la définition de la cyberguerre – résumée pour le moment à l'ensemble des actions militaires visant à la maîtrise du cyberespace –, on considère généralement qu'elle englobe la sécurité des systèmes d'information, la lutte informatique active et la guerre électronique tout en comprenant des zones de recouvrement avec le renseignement, les opérations psychologiques et les opérations d'information.

En France plus spécifiquement, le concept de cyberdéfense regroupe trois piliers : la défense active en profondeur des systèmes d'information, la capacité de gestion de crise cybernétique et enfin la capacité de lutte et de conduite d'opérations dans le cyberespace.

Depuis l'adoption d'un schéma directeur, d'un concept interarmées définissant le cadre général de la cyberdéfense et une doctrine interarmées détaillant les fonctions et moyens de la cyberdéfense la France considère la cyberdéfense comme l'une de ses priorités en matière de Défense. Il est donc nécessaire de réfléchir à la place et aux prérogatives des forces terrestres dans ce maillage.

Cette **étude** vise ainsi à s'interroger sur les vulnérabilités propres aux forces terrestres dans le contexte de la montée en puissance de la conduite d'opérations militaires dans le cyberespace, sur la position des forces armées françaises vis-à-vis des menaces cybernétiques, sur le rôle des apports de la guerre cybernétique à un affrontement conventionnel. En résumé, quel rôle l'armée de Terre peut-elle ou doit-elle jouer dans le cadre la guerre cybernétique ?

FOREWORD

The land forces and cyberspace: a new battleground. Overview and perspectives

In peacetime and wartime alike, cyber attack is now a reality for every State, both in their civilian and their military structures. Confronted with threats that already pose a risk to their computer networks, in terms of battlespace digitization and developments in information technology, cyberspace now represents a significant portion of current conflicts. The armed forces must be capable of controlling their networks, which means managing information, ensuring it is secure and thereby enabling them to operate.

However, even if there is no consensus as yet on the definition of cyberwar – briefly defined as "military action that aims to control cyberspace" – it is generally considered to cover the securing of information systems, active cyber combat and electronic war, including the areas that overlap with intelligence, PSYOPS and information operations.

In France in particular, the concept brings together three mainstays: active, in-depth defense of our information systems, the capacity to handle a cyber crisis and lastly the capacity to combat and conduct operations in cyberspace.

Since adopting a master plan in the form of a joint concept defining the general context of cyber defense and a joint doctrine detailing cyber defense functions and assets, France considers cyber defense as a priority in terms of defense. It is therefore necessary to question the role and prerogatives of the land forces in this system.

This study aims to raise questions on the vulnerabilities specific to the land forces in relation to the build-up of military operations conducted in cyberspace, the position of the French armed forces in terms of cyber threat and the elements cyber war adds to conventional battle. To sum up, what role can or should the French Army play in cyber war?

SOMMAIRE

LISTE DES SIGLES UTILISÉS

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CALID	Centre d'Analyse de Lutte Informatique Défensive
CCD CoE	Centre d'excellence pour la cyberdéfense de Tallinn
CDMA	*Cyber Defence Management Authority*
CERT	*Computer Emergency Response Team*
CHAMP	*Counter-electronics High-powered Microwave Advanced Missile Project*
CICDE	Centre Interarmées de concepts, de doctrines et d'expérimentations
CNO	*Computer Network Operations*
COSMIC	Commandant des systèmes d'information et de communication
CPCO	Centre de Planification et de Conduite des Opérations
DAS	Délégation aux Affaires Stratégiques
DCS	*Distributed Control Systems*
DGA	Direction Générale de l'Armement
DGSIC	Direction Générale des Systèmes d'Information et de Communication
DICoD	Délégation à l'Information et à la Communication de la Défense
DDoS	Attaque par déni de service distribué
DoD	*United States Department of Defense*
DoS	Attaque par déni de service
ENISA	*European Network and Information Security Agency*
FELIN	Fantassin à Équipement et Liaisons Intégrés
GNSS	*Global Navigation Satellite System*
GPS	*Global Positionning System*
IED	Engins explosifs improvisés
I2Os	*Information and Infrastructure Operations*
JIM LR	*Jumelle Infrarouge Multifonctions Long Range*
LBDSN	Livre Blanc Défense et Sécurité Nationale
LID	Lutte Informatique Défensive
LIO	Lutte Informatique Offensive
NCW	*Network Centric Warfare*
NEB	Numérisation de l'Espace de Bataille
NSA	*National Security Agency*
OG Cyber	Officier Général Cyber
OIV	Organismes d'Intérêt Vital
OTAN	Organisation du Traité de l'Atlantique Nord
PESD	Politique Européenne de Sécurité et de Défense
RMA	*Revolution in Military Affairs*
SCADA	*Supervisory Control And Data Acquisition*
SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale
SIC	Systèmes d'Information et de Communication
SSI	Sécurité des Systèmes d'Information
TRADOC	*U.S Army Training and Doctrine Command*
U.S CyberCom	*U.S Cyber Command*

INTRODUCTION

« Potential enemy states are no longer on the other side of the ocean
But just behind the firewall[1] ».

Roger DARBY[2]

« Le cyberespace est donc désormais un champ de confrontation à part entière[3] ».
« [Les cyberattaques] constituent une menace majeure, à forte probabilité et à fort impact potentiel[4] ».

Livre Blanc Défense et Sécurité Nationale 2013

Samedi 12 janvier 2013 : vingt-quatre heures après le déclenchement de l'opération Serval au Mali, deux sites Internet du Ministère de la Défense sont la cible d'une attaque par déni de service. Celle-ci est déjouée par l'hébergeur des sites, Prosodie[5]. Le nombre d'attaques traitées par le Ministère de la Défense est en augmentation : 196 attaques ont été recensées par le Centre d'Analyse de Lutte Informatique Défensive (CALID[6]) en 2011, 420 en 2012[7]. À titre de comparaison sur la même année 2012, selon l'U.S. CyberCom, les réseaux du *Department of Defense* américain ont été attaqués en moyenne 250 000 fois par heure, notamment par des services de renseignement étrangers[8].

La numérisation du champ de bataille et l'évolution des technologies de l'information ont conféré au cyberespace une importance déterminante : il s'agit pour les forces armées de maîtriser les réseaux, c'est-à-dire de gérer l'information transitant, de la sécuriser, et d'assurer la capacité à opérer dans ce domaine. Certains parlent de « cyberguerres » menées par et à l'encontre des États. S'il n'existe pas de consensus sur les définitions, la cyberguerre est ici comprise comme l'ensemble des actions militaires visant à la maîtrise du cyberespace afin d'y conduire des opérations spécifiques ou de préparer l'exploitation vers un autre espace de conflit (terre, air, mer, espace ; avec le cyberespace, ces domaines d'opération constituent les cinq *global commons*) en servant de démultiplicateur de force[9]. Ainsi, la cyberguerre

---

1 Un *firewall* est un logiciel qui empêche l'accès non-autorisé à un ordinateur ou à un réseau tout en permettant les communications autorisées.

2 Roger Darby, "Cyber Defense in Focus : Enemies Near and Far – or Just Behind the Firewall : The Case for Knowledge Management", *Defense Studies, Journal of Military and Strategic Studies*, vol. 12 n° 4, December 2012, p. 523.

3 Livre Blanc Défense et Sécurité Nationale 2013, p. 45.

4 Livre Blanc Défense et Sécurité Nationale 2013, p. 48.

5 Il s'agissait notamment du site Internet de la Délégation à l'Information et à la Communication de la Défense, Dossier « La Cyberguerre est déclarée », Courrier international, N° 1165, 28 février – 6 mars 2013, p. 30-37. Voir également http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/20130111trib000742055/cyberguerre-comment-la-france-se-protege.html

6 Le Centre d'Analyse de Lutte Informatique Défensive assure des missions de veille, d'analyse et d'alerte des réseaux informatiques du Ministère de la Défense, il garantit la réaction rapide des forces armées françaises face aux menaces cybernétiques. Le CALID assure sa fonction de protection des systèmes d'information en parallèle de la chaîne « Sécurité des systèmes d'information » des forces armées, et en collaboration avec d'autres entités ministérielles en charge de la sécurité informatique. Source : http://www.defense.gouv.fr/actualites/dossiers/sept-2011-cyberdefense-enjeu-du-21e-siecle/france/voir-les-articles/le-calid-l-expert-technique-en-securite-informatique-du-ministere

7 Discours prononcé par le M. Jean-Yves Le Drian, Ministre de la Défense, en ouverture du colloque « Cybersécurité : un enjeu mondial, une priorité nationale, des réponses régionales », Rennes, 3 juin 2013, http://www.defense.gouv.fr/ministre/prises-de-parole-du-ministre/prises-de-parole-de-m.-jean-yves-le-drian/discours-du-ministre-de-la-defense-au-colloque-sur-la-cyberdefense

8 James G. Stavridis, Elton C. Parker III, "Sailing the cyber sea", JFQ, Issue 65, 2nd Quarter 2012, p. 61.

9 Bertrand Boyer, *Cyberstratégie - l'art de la guerre numérique*, Paris, Nuvis, 2012, p. 82.

englobe la lutte informatique active, la sécurité des systèmes d'information et la guerre électronique, tout en comprenant des zones de recouvrement avec le renseignement, les opérations psychologiques, et les opérations d'information[10]. Les champs d'action dans le cyberespace sont multiples : une attaque cybernétique peut avoir pour cible le réseau informatique de la force afin de gêner les communications du niveau stratégique au niveau opératif, elle peut également viser le compte officiel du Ministère sur un réseau social dans le but de délégitimer son action dans le cadre d'une guerre de l'information. L'Otan (plus précisément le groupe d'expert du Centre d'excellence de Tallinn[11]) définit une attaque cybernétique comme une opération cybernétique, défensive ou offensive, dont on peut raisonnablement attendre qu'elle blesse ou tue des personnes, ou entraîne des dommages ou la destruction de biens[12]. Le concept de cyberdéfense tel que défini par la France regroupe trois piliers : la défense active en profondeur des systèmes d'information, la capacité de gestion de crise cybernétique, et enfin la capacité de lutte et de conduite d'opérations dans le cyberespace[13].

En temps de paix comme en temps de guerre, les attaques cybernétiques sont une réalité pour les États, pour leurs structures civiles et militaires. De nombreux États ont fait de la maîtrise du cyberespace un outil d'action militaire : ils conduisent des opérations de cyberespionnage, mettent en place des capacités de lutte informatique défensive et offensive dans un environnement sans frontières établies où la distinction entre cible civile et cible militaire est floue (comment s'assurer qu'un virus informatique n'atteindra que des réseaux militaires et ne se propagera pas sur des réseaux civils ?). Par ailleurs, les États adoptent des stratégies et doctrines en matière d'opérations dans le cyberespace. À titre d'exemple, les États-Unis ont adopté en 2011 une stratégie selon laquelle ils se disent prêts à répondre militairement à tout acte hostile dans le cyberespace[14]. Le *Capstone Concept for Joint Operations,* pierre angulaire de la doctrine militaire américaine, définit les opérations dans le cyberespace[15] comme un domaine de projection du pouvoir militaire au même titre que les quatre autre *global commons*. En France, si le Ministère de la Défense a adopté un concept interarmées définissant le cadre général de la cyberdéfense, une doctrine interarmées détaillant les fonctions et moyens de la cyberdéfense, et enfin un schéma directeur[16], il est intéressant de s'interroger sur la place et les prérogatives des forces terrestres dans ce maillage.

Dans cette logique, trois problématiques sont explorées dans cette étude :

- Quelles sont les vulnérabilités propres aux forces terrestres dans le contexte de la montée en puissance de la conduite d'opérations militaires dans le cyberespace ?

- Quelle position les forces armées françaises et les principales puissances militaires étrangères ont-elles adopté vis-à-vis des menaces cybernétiques : moyens financiers, technologiques, humains, quelles ambitions pour leurs forces armées (et terrestres le cas échéant) ?

- Quels peuvent être les apports de la guerre cybernétique à un affrontement conventionnel ? Quel rôle l'armée de Terre peut-elle jouer ?

Si les attaques cybernétiques sont sources de menaces nouvelles pour l'ensemble des forces armées françaises, l'attention est ici portée sur

[10] Bertrand Boyer, *Cyberstratégie - l'art de la guerre numérique,* Paris, Nuvis, 2012, p. 81.

[11] L'OTAN a réuni un groupe d'experts pour étudier l'applicabilité du droit international à la guerre cybernétique dans le cadre du Centre d'excellence pour la cyberdéfense (CCD CoE) de Tallinn. Le fruit de ces travaux est le Manuel de Tallinn, publié en mars 2013.

[12] The International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, *Tallinn Manual on the international law applicable to cyber warfare,* (ci-après appelé « Manuel de Tallinn »), General editor Michael N. Schmitt, Cambridge University Press, p. 106. La règle 30 dispose : *« A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects ».*

[13] Philippe Bougeret (Col), OSSI-Terre, « Le défi de la cyberdéfense pour l'armée de Terre », Transmetteurs, 1er semestre 2013, n° 6, p. 22.

[14] The White House, "International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World", Mai 2011, disponible à l'adresse suivante : http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[15] Joint Chiefs of Staff, "Capstone Concept for Joint Operations : Joint Force 2020", 10 septembre 2012, p. 2. http://www.dtic.mil/futurejointwarfare/concepts/ccjo_2012.pdf

[16] Interview du contre-amiral Arnaud Coustillière, Officier Général cyberdéfense, « La cyberdéfense est l'une des priorités de la Défense », *Armées d'aujourd'hui,* décembre 2012 – janvier 2013, n° 376, p. 38.

l'émergence de menaces non conventionnelles pesant sur les systèmes utilisés par les forces terrestres, plus particulièrement les systèmes de commandement et de contrôle, les systèmes d'armes et les systèmes de communication. En outre, le non-respect des règles assurant la sécurité des systèmes d'information et la montée en puissance de l'utilisation d'Internet et des réseaux sociaux par les hommes de la force en opérations et en métropole constituent une nouvelle source de vulnérabilités pour les forces armées.

Dans un contexte où un acteur isolé peut atteindre par une attaque cybernétique des infrastructures critiques et menacer la sécurité de l'État, il est nécessaire d'étudier quels moyens financiers, technologiques et humains les principales puissances militaires accordent à leurs forces armées, et en particulier leurs forces terrestres, jusqu'au plus petit échelon ; ces éléments varient d'une puissance à l'autre.

Les opérations menées dans le cyberespace ont pour finalité de gêner, rendre confus, démoraliser, désorganiser, distraire l'ennemi et diminuer ses capacités de réaction. La combinaison d'actions dans le cyberespace avec des opérations militaires conventionnelles est une nouvelle forme de combat dans laquelle la guerre cybernétique doit servir de démultiplicateur de force. En France, la doctrine interarmées en matière d'opérations militaires dans le cyberespace existe et évolue. Deux chaînes distinctes existent : d'une part, la chaîne sécurité des systèmes d'information, en charge de mettre en place des systèmes sécurisés ; l'armée de Terre, comme chaque armée, possède sa propre chaîne SSI. Il s'agit de mettre en place la défense passive de nos systèmes. D'autre part, une chaîne opérationnelle cyber intégrée au Centre de Planification et de Conduite des Opérations, conduit les opérations de cyberdéfense. C'est le volet dynamique de la cyberdéfense. Ces opérations sont centralisées et interarmées. L'armée de Terre y concourt notamment en apportant ses compétences particulières, par exemple par la contribution aux GIR (groupes d'intervention rapide).

À partir de sources ouvertes exclusivement, ce travail dresse un état des lieux au 1er semestre 2013 de l'implication de l'armée de Terre dans le cyberespace comme nouveau champ de bataille. Après avoir distingué la guerre cybernétique de la guerre de l'information (chapitre introductif), les acteurs et moyens d'actions susceptibles d'agir et d'être employés dans un contexte de conflit cybernétique sont présentés (chapitre 1). Le chapitre 2 explore les menaces pesant sur les forces terrestres à plusieurs niveaux, il s'agit des menaces pesant sur les systèmes exploités (systèmes d'armes par exemple) ainsi que de l'impact que peuvent avoir une utilisation négligente d'Internet ou le non-respect des règles d'hygiène cybernétique par le personnel. Il est nécessaire de dresser un état des lieux des réponses apportées aux niveaux interalliés et nationaux à l'échelon des forces armées – et des forces terrestres – face à la réalité des attaques cybernétiques (chapitre 3). Enfin, des pistes de réflexion sur la combinaison de la guerre numérique avec le champ de bataille traditionnel seront étudiées (chapitre 4).

CHAPITRE INTRODUCTIF

DISTINCTION ENTRE GUERRE CYBERNÉTIQUE ET GUERRE DE L'INFORMATION

Distinguer guerre cybernétique (ou guerre numérique, ou cyberguerre) et guerre de l'information est un préalable nécessaire à l'étude des forces terrestres et du cyberespace comme nouveau champ de bataille. Le terme « cyberguerre » est quotidiennement employé pour faire référence à un large spectre d'actions. L'introduction du virus informatique Stuxnet dans une centrale nucléaire iranienne, l'intrusion dans les réseaux du *Department of Defense* américain et le vol de documents confidentiels relatifs à des systèmes d'armes par des services étatiques étrangers, ou encore la conduite d'un programme de surveillance électronique de collecte de renseignement mis en place par la *National Security Agency* américaine ont été qualifiés de « cyberguerre » dans les médias. Ce terme renvoie aussi bien à des situations de conflit symétrique (entre deux ou plusieurs États) qu'asymétrique (entre un État et un ou plusieurs acteurs non-étatiques).

Selon Eric Filiol, expert en sécurité informatique, la cyberguerre est un **conflit « classique dont au moins une des composantes, dans la réalisation, les motivations et les outils (armes au sens large du terme) s'appuie sur le champ informatique ou numérique »**[17]**.** Bertrand Boyer, ingénieur de formation et transmetteur, entend la cyberguerre (ou guerre numérique) comme « l'ensemble des actions militaires visant à la maîtrise du cyberespace afin, soit d'y conduire des opérations spécifiques, soit de préparer l'exploitation vers un autre espace de conflit (terre, air, mer)[18] ». La cyberguerre regroupe ainsi plusieurs activités : lutte informatique active, sécurité des systèmes d'information, et elle comprend des zones de recouvrement avec le renseignement, la guerre électronique, les opérations psychologiques et les opérations d'information. L'étude des forces terrestres dans le cyberespace est fondée sur cette conception de la guerre cybernétique incluant différentes activités.

La guerre de l'information couvre un spectre plus large que la guerre cybernétique. Elle désigne « l'ensemble des actions menées par les forces armées, dirigé et coordonné au plus haut niveau, visant à utiliser ou à défendre l'information, les systèmes d'information et les processus décisionnels, pour appuyer une stratégie d'influence et contribuer, dans le cadre des opérations, à l'atteinte de l'état final recherché, en respectant les valeurs défendues[19] ». Daniel Ventre, ingénieur au CNRS et titulaire de la chaire « Cyberdéfense et cybersécurité » Saint-Cyr Sogeti Thalès, définit la guerre de l'information comme « toute activité destinée à acquérir données et connaissances (et à en priver l'adversaire) dans une finalité stratégique, soit par des systèmes (vecteurs et moyens de traitement de l'information), soit par le contenu, en assurant une domination informationnelle »[20]. Selon la Doctrine de l'OTAN relative aux opérations d'information (ou opérations de renseignement)[21], la guerre de l'information repose sur cinq capacités[22] :

---

17 Grégoire Chaumeil, Anne-Lise Llouquet et Nelly Moussu, « Cyberespace le 5ème champ de bataille », *Armées d'aujourd'hui,* novembre - décembre 2011, n° 365, p. 52.

18 Bertrand Boyer, *Cyberstratégie - l'art de la guerre numérique,* Paris, Nuvis, 2012, p. 82.

19 *Défense et Sécurité nationale, Le Livre Blanc,* La documentation française, éditions Odile Jacob, 2008, p. 58.

20 Daniel Ventre (dir.), *Cyberguerre et guerre de l'information : stratégies, règles, enjeux,* Lavoisier, Paris, 2010.

21 NATO Allied Joint Publication (AJP) 3.10, *Allied Joint Doctrine for Information Operations,* 23 novembre 2009. Accessible à l'adresse suivante : http://info.publicintelligence.net/NATO-IO.pdf

22 NB : les traductions de l'anglais au français ont été réalisées à l'aide du Glossaire OTAN de termes et de définitions, AAP-6 (2008), http://www.fas.org/irp/doddir/other/nato2008.pdf

- Les **opérations psychologiques** (opérations menées pour susciter la réaction souhaitée de la part de l'audience-cible) ;

- Les **mesures militaires visant à induire l'ennemi en erreur** grâce à des truquages, des désinformations de la réalité ou des falsifications en vue de l'inciter à réagir d'une manière préjudiciable à ses propres intérêts *(military deception)* ;

- La **sécurité des opérations** (ensemble des mesures qui donnent à une opération ou à un exercice militaires la sécurité adéquate par des moyens actifs ou passifs, afin d'interdire à l'ennemi la connaissance du dispositif, des moyens et des intentions des forces amies) ;

- Les **opérations sur les réseaux informatiques** *(computer network operations)* ;

- La **guerre électronique** (action militaire destinée à exploiter le spectre électromagnétique, qui englobe la recherche, l'interception et l'identification des émissions électromagnétiques, l'emploi de l'énergie électromagnétique, y compris l'énergie dirigée, pour diminuer ou prévenir l'emploi par l'ennemi du spectre électromagnétique, et mesure pour s'assurer de son emploi efficace par les forces amies).

Dans toutes ces composantes, le renseignement et la maîtrise de l'information sont centraux. Les opérations de renseignement peuvent être menées dans le cyberespace ainsi que dans d'autres domaines. Les opérations cybernétiques peuvent recouper le champ des opérations de renseignement dès lors que la guerre cybernétique est conçue comme une action ayant pour finalité d'influencer la volonté et les capacités décisionnelles de l'ennemi sur le plan politique et militaire par le moyen de *Computer Network Operations*[23].

[23] Joint Staff, U.S Department of Defense, *Joint Publication 3-13 Information Operations*, 13 février 2006, http://www.carlisle.army.mil/DIME/documents/jp3_13.pdf

CHAPITRE 1

DIVERSITÉ DES ACTEURS ET DES MOYENS D'ACTION DANS LE CYBERESPACE

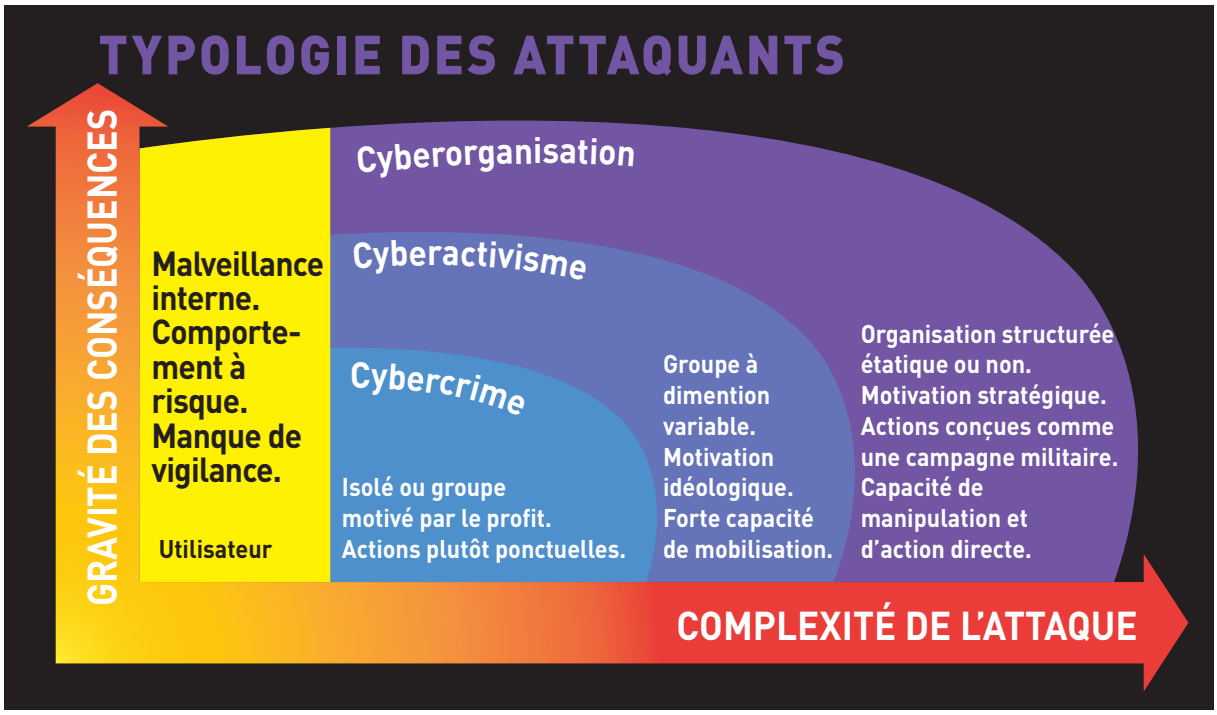
Le monde numérique a élargi le champ des possibles pour le monde civil comme le monde militaire. La dépendance de nos sociétés aux systèmes informatiques a entraîné l'émergence de nouvelles menaces ainsi que des moyens d'action nouveaux dans le cadre de ce que certains appellent cyberguerre. Le cyberespace est devenu un champ d'affrontement dans des domaines variés politique, économique, et militaire. L'emploi du terme cyberguerre est répandu, il renvoie à des réalités différentes allant de la conduite d'opérations d'espionnage, de reconnaissance, de recueil d'information dans le cyberespace menées par les États grâce à des capacités de lutte informatique défensive et offensive, au coup d'éclat de *hackers* étant parvenus à défacer[24] la page d'accueil d'un site Internet officiel. Ce premier chapitre a pour objet de poser le cadre nécessaire à la compréhension du cyberespace comme nouveau champ de bataille en présentant la diversité des acteurs susceptibles d'interagir avec les forces armées dans le cyberespace (section 1) ainsi que les moyens d'action dans le 5e milieu (section 2). Enfin, trois types d'attaques affectant directement ou indirectement les forces armées sont détaillées afin d'en comprendre le processus (section 3).

11 – LES ACTEURS : DE L'INDIVIDU ISOLÉ À L'ACTEUR ÉTATIQUE

Agir dans le cyberespace nécessite de posséder les infrastructures et outils technologiques ainsi que le savoir-faire technique. Dans les pays développés, les individus possèdent dans leur majorité ces éléments et peuvent agir dans le cyberespace. Dans les pays en voie de développement, l'action dans le cyberespace est souvent réservée aux acteurs étatiques disposant majoritairement de la technologie et des compétences. Le spectre des acteurs pouvant agir dans le cyberespace est étendu, il est donc nécessaire d'établir une typologie afin d'identifier les auteurs des menaces potentielles pesant sur les forces terrestres. La typologie présentée dans l'analyse suivante est non exhaustive et ne présente que les grandes familles d'acteurs susceptibles d'interagir avec les forces armées dans le cyberespace (ainsi, la cybercriminalité[25] est jugée hors champ dans la mesure où

[24] Le défacement (aussi appelé défiguration)consiste à modifier la page d'un site web en altérant son contenu, en modifiant par exemple sa page d'accueil pour y faire figurer son message.

[25] Selon l'Agence Nationale de la Sécurité des Systèmes d'Information, la cybercriminalité renvoie aux actes contrevenant aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible (ANSSI, « Défense et sécurité des systèmes d'information : Stratégie de la France », SGDSN, Février 2011, p. 21 http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf). Concrètement, la cybercriminalité recouvre des actes tels que l'escroquerie sur Internet, la fraude à la carte bancaire ou encore la pédopornographie sur Internet.



Source : Grégoire Chaumeil, Anne-Lise Llouquet et Nelly Moussu, « Cyberespace le 5ème champ de bataille », *Armées d'aujourd'hui,* novembre-décembre 2011, n° 365, p. 43. POUR BIBLIO : p. 32-52.

ses finalités ne sont pas politiques – elles ne visent pas des cibles militaires ou un État – mais relèvent de la cupidité). Pour une typologie précise, le lecteur pourra se référer à l'ouvrage « Cyberespace et acteurs du cyberconflit » de Daniel Ventre[26].

La typologie ci-dessus établie par le Ministère de la Défense[27] identifie trois grandes catégories d'attaquants dans le cyberespace : les cybercriminels, les cyberactivistes et les cyberorganisations. De nombreux auteurs s'accordent à dire que deux types d'acteurs sont susceptibles de mener des actions de guerre cybernétique : les acteurs étatiques et les organisations terroristes ou extrémistes[28]. Aussi, l'étude se concentre sur ces derniers. Enfin, les vulnérabilités liées aux utilisateurs des systèmes d'information et de communication internes au Ministère de la Défense seront analysées car elles constituent une préoccupation importante pour le Ministère et pour les forces terrestres.

111 – Acteurs non-étatiques

À la différence de la guerre conventionnelle, la guerre dans le cyberespace n'est pas menée par un acteur physique présent sur le champ de bataille, mais par un acteur virtuel et potentiellement anonyme. Un individu isolé ou un groupe d'individus auteur d'une attaque cybernétique s'arrogent des pouvoirs disproportionnés par rapport à leurs pouvoirs réels dans un schéma d'affrontement dans les quatre milieux traditionnels (les *global commons*). En juin 2013, le Ministre de la Défense déclarait ainsi :

> « *[…] le cyber est aussi investi par des groupes non-étatiques, qui y trouvent une arme idéale. Que leurs motivations soient politiques, idéologiques ou mafieuses, ils développent ainsi la capacité d'affronter à distance un État, avec une facilité qui leur était auparavant interdite*[29] ».

[26] Daniel Ventre, *Cyberespace et acteurs du cyberconflit*, éditions Lavoisier, Paris, 2011, p. 103-118.

[27] Cette typologie est extraite du dossier « Cyberespace le 5ème champ de bataille » du magazine mensuel *Armées d'aujourd'hui.*

[28] Voir par exemple l'étude de Paul Cornish, David Livingstone, Dave Cemente, Claire Yorke, "On Cyber Warfare", *Chatham House report*, novembre 2010, p. 10.

[29] Discours prononcé par M. Jean-Yves Le Drian, Ministre de la Défense, en ouverture du colloque organisé par le Centre de Recherche des Écoles de Saint-Cyr Coëtquidan intitulé « Cybersécurité : un enjeu mondial, une priorité nationale, des réponses régionales », Rennes, 3 juin 2013.

Trois grands types d'acteurs non-étatiques sont susceptibles de conduire des actions hostiles à l'encontre d'un État et de ses forces armées : les *hackers*, les cyberactivistes et les cyberorganisations.

Hackers[30]

Les *hackers*, également appelés pirates informatiques, peuvent être regroupés en trois familles déterminées en fonction de leurs motivations. Les « chapeaux blancs » (*white hats*) sont des individus à la recherche de vulnérabilités et de failles dans la sécurité des systèmes informatiques ou logiciels afin de les communiquer à leurs propriétaires dans le but de renforcer leur sécurité. Il s'agit souvent de consultants en sécurité informatique. Les « chapeaux gris » (*grey hats*) recherchent les failles et vulnérabilités sans y être autorisés, dans le but de démontrer leur compétence et leur habilité, ou afin d'alerter l'institution ou entreprise visée des vulnérabilités de ses systèmes. Enfin, les « chapeaux noirs » (*black hats*) sont des criminels, cyberespions ou cyberterroristes procédant à des attaques informatiques. Leurs motivations sont personnelles, il s'agit pour la majorité d'entre eux de gagner de l'argent en menant des opérations d'espionnage économique ou en travaillant avec des organisations criminelles.

Cyberactivistes

Les cyberactivistes, également appelés hacktivistes (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), utilisent Internet dans le but faire valoir leurs motivations. Celles-ci sont principalement d'ordre idéologique, politique, religieux ou économique[31]. Ces groupes d'hacktivistes sont de taille variable, ils sont caractérisés par une forte capacité à mobiliser sans nécessairement posséder de structure. Leur action peut potentiellement avoir un impact direct sur les affaires internes d'un État ou d'une organisation internationale. Ainsi, en 2011, en réponse à un rapport publié par l'OTAN à son sujet, le groupe Anonymous a annoncé qu'il avait pénétré les sites Internet de l'OTAN et dérobé des documents dont certains ont été mis en ligne à titre de preuve[32].

Anonymous est un groupe d'hacktivistes rassemblant une communauté d'individus à travers le monde. Ceux-ci mènent régulièrement des actions de défacement (changement de la page d'un site Internet), des attaques par déni de service distribué, ils piratent également des comptes de messagerie[33]. Ils agissent pour des raisons idéologiques : ils dénoncent les atteintes à la liberté d'expression sur Internet et défendent un Internet libre et accessible à tous (leur lutte pour une plus grande transparence est traduite par la publication de documents confidentiels). Leurs actions peuvent également revêtir un aspect politique, ils œuvrent parfois directement auprès d'opposants à un régime en contribuant au partage de vidéos en ligne et en les aidant à dissimuler leur identité, comme ce fut le cas en Tunisie en 2010-2011 et actuellement en Syrie[34]. Ainsi, le groupe Anonymous influence directement les affaires d'un pays en situation de conflit armé ou non. Il est considéré comme une menace réelle : récemment, le gouvernement suisse a simulé une attaque cybernétique sur les infrastructures critiques du pays afin de s'entraîner à les défendre contre une « cyber-attaque massive menée contre la Suisse pour des raisons politiques[35] » (sites Internet des banques inaccessibles, réseau ferroviaire immobilisé, etc.). Le scénario identifiait les *hackers* d'Anonymous comme auteur des attaques, ces derniers souhaitant que la Suisse

---

30 La typologie retenue est celle présentée dans le rapport du Sénateur Jean-Marie Bockel, « La cyberdéfense : un enjeu mondial, une priorité nationale », Rapport d'information fait au nom de la Commission des affaires étrangères, de la défense et des forces armées du Sénat n° 681, enregistré à la Présidence du Sénat le 18 juillet 2012, p. 32-33.

31 Yannick Chatelain, Loïck Roche, *Hackers ! Le 5e pouvoir*, éditions Maxima, Paris, 2002, p. 57. Dans une thèse parue en 2004, Alexandra SAMUEL propose la définition suivante : "hacktivismis the non violent use of illegal or legally ambiguous digital tools in pursuit of political ends" *(Hacktivism and the Future of Political Participation*, thèse de l'Université. de Harvard, Cambridge Massachusetts, septembre 2004, p. 2).

32 Alain Esterle, Bruno Gruselle et Bruno Tertrais, « Cyber Dissuasion », Fondation pour la Recherche Stratégique, 2012, n° 3, p. 50.

33 Récemment, des hackers d'Anonymous ont piraté le compte de messagerie de Bachar El-Assad et ont transmis ses correspondances aux opposants du régime qui n'ont pas tardé à les rendre publics. Olivier Danino, « L'utilisation stratégique du cyber au Moyen-Orient », p. 24-25, étude confiée à M. Danino par la Délégation aux Affaires Stratégiques (disponible à l'adresse suivante : http://www.defense.gouv.fr/das/reflexion-strategique/etudes-prospectives-et-strategiques).

34 Olivier Danino, « L'utilisation stratégique du cyber au Moyen-Orient », p. 24, étude confiée à M. Danino par la Délégation aux Affaires Stratégiques (disponible à l'adresse suivante : http://www.defense.gouv.fr/das/reflexion-strategique/etudes-prospectives-et-strategiques).

35 http://www.01net.com/editorial/595985/la-suisse-attaquee-par-lesanonymous-dans-un-exercice-de-cyber-defense/

dévoile l'identité des évadés fiscaux[36]. Dans la réalité, de tels groupes ont déjà influé sur le cours des relations internationales et diplomatiques : la publication de près de 250 000 câbles diplomatiques des ambassades américaines en 2011 par Wikileaks, une communauté de *hackers*, témoigne du poids de ces organisations[37]. On peut ainsi s'interroger sur le potentiel de nuisance/d'hostilité d'un groupe d'individus utilisant des méthodes informatiques avec une forte capacité de mobilisation a des fins hostiles à l'encontre des États et/ou des organisations internationales.

Cyberorganisations

Le champ des cyberorganisations est vaste, il couvre à la fois des organisations indépendantes et des organisations liées à des États sans leur être officiellement rattachées. Ces acteurs se distinguent de la catégorie précédente par leur organisation plus structurée et bénéficient de moyens financiers importants. Les cyberorganisations reposent moins sur une capacité de mobilisation large que sur une structure à laquelle il est difficile d'accéder et qui reste la propriété d'un groupe bien défini. Enfin, leurs motivations sont souvent politiques ou idéologiques, mais peuvent revêtir d'autres dimensions (religieuse notamment).

De nombreuses cyberorganisations agissent en dehors de toute structure étatique. On peut citer l'*International Muslim's Cyber Army*, ou encore la *Muslim Liberation Army*, deux groupes d'idéologie islamiste et dont les actions s'inscrivent dans le cadre de ce que certains appellent le « Jihad cybernétique », le « cyber Jihad » ou encore le « e-Jihad »[38]. En effet, les groupes armés prônant le Jihad se sont tournés vers l'Internet et en ont fait un outil de communication pour gagner les cœurs et les esprits des musulmans dans le monde[39]. On peut parler de cyberterrorisme lorsque des groupes terroristes utilisent l'Internet à des fins de propagande et de prosélytisme[40] ou mènent des attaques cybernétiques à des fins de perturbation à grande échelle[41]. Le terme renvoie également au fait de conduire des attaques contre des ordinateurs et/ou réseaux – et les données qu'ils contiennent – afin d'intimider une instance officielle ou une population[42]. Internet permet en effet à des groupes dispersés de s'unir, de partager leurs actions, de diffuser leur message, de communiquer sur leurs succès ou au contraire de désinformer la population sur ceux de l'adversaire[43]. En un mot, Internet est davantage un outil de communication pour ces organisations qu'une plateforme pour mener des attaques cybernétiques. Récemment, les Somaliens d'Al-Shebab ont utilisé Internet, et en particulier les réseaux sociaux, pour publier les photos d'un soldat français tué au cours de l'opération de libération de l'otage Denis Allex[44]. Autre exemple : en réponse à l'intervention française au Mali, AQMI a conçu un jeu vidéo en ligne dont le but est de détruire virtuellement l'aviation de l'armée française ; dans ce jeu d'arcade, les « cyber-djihadistes » doivent détruire les avions français ou mourir en martyr[45]. Néanmoins, il faut noter qu'aucune attaque cybernétique terroriste importante n'a été répertoriée aujourd'hui, aucun élément ne permet d'affirmer qu'un groupe tel qu'Al Qaïda a les capacités ou les ressources pour lancer une attaque cybernétique majeure. L'Internet permet essentiellement à ces groupes terroristes de bénéficier d'un outil d'information pour diffuser leur message et mobiliser des partisans[46].

---

[36] http://www.bk.admin.ch/themen/07664/07670/index.html?lang=fr

[37] Fred Schreier, "The Report on Cyberwarfare", DCAF, 2012, p. 9.

[38] Olivier Danino, « L'utilisation stratégique du cyber au Moyen-Orient », p. 19, étude confiée à M. Danino par la Délégation aux Affaires Stratégiques (disponible à l'adresse suivante : http://www.defense.gouv.fr/das/reflexion-strategique/etudes-prospectives-et-strategiques).

[39] Wael Adhami, « The strategic importance of the Internet for armed insurgent groups in modern warfare », *Revue internationale de la Croix-Rouge*, Volume 89, n° 868, décembre 2007, p. 857.

[40] Jean-Marie Bockel, « Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense », n° 681, enregistré à la Présidence du Sénat le 18 juillet 2012, p. 35.

[41] Observatoire du Monde Cybernétique, *DAS*, Trimestriel septembre 2012, p. 15.

[42] Myriam Dunn Cavelty, "Cyberwar: Concept, Status Quo, and Limitations", Center for Security Studies, *Analysis in Security Policy*, n° 71, avril 2010, p. 1. La note est disponible à l'adresse suivante : http://www.css.ethz.ch/publications/pdfs/CSS-Analyses-71.pdf (consulté le 3 février 2013).

[43] Marc Hecker (chercheur au centre des études de sécurité de l'IFRI), « Armées contre insurgés : à qui profite le web ? », entretien réalisé par Joseph HENROTIN, *DSI* n° 51, septembre 2009, p. 28-31.

[44] http://www.franceinfo.fr/monde/comment-les-djihadistes-se-servent-du-web-2-0-906347-2013-02-28

[45] Dans ce jeu, lorsque le joueur clique sur « play », le message suivant (en arabe) apparaît sur son écran : « Frère musulman, vas-y et repousse l'invasion française contre le Mali musulman » (source : http://www.france24.com/fr/20130313-djihad-jeu-video-mali-armee-francaise-avion-al-qaida-forum-islamiste consultée le 31 mars 2013).

[46] Paul Cornish, David Livingstone, Dave Clemente, Claire Yorke, "On Cyber Warfare", *Chatham House report*, novembre 2010, p. 8.

Certaines cyberorganisations sont liées à un parti politique ou un État. C'est le cas de l'*Iran Cyber Army*, et de la *Syrian Electronic Army* (SEA). Cette dernière a vocation à diffuser les messages du régime syrien. Si l'organisation affirme qu'elle est totalement indépendante, Bachar El-Assad a néanmoins approuvé ses actions, ce qui souligne l'ambigüité du lien qui les unit (la SEA apparaît comme un bras armé du régime syrien)[47]. De telles organisations ne sont pas officiellement liées à un État mais exécutent de fait la volonté d'un gouvernement en agissant dans le cyberespace. Sans engager la responsabilité de l'État dont elles émanent si l'attaque était découverte et révélée par la victime, elles peuvent mener des opérations offensives de lutte informatique.

Certains auteurs, dont Nicolas Arpagian, parlent de « cyber-guerrilla » dans la mesure où il n'y a pas de conflit ouvert entre deux nations, mais plutôt une succession d'actions offensives à un certain degré menées en permanence et en dessous d'un certain seuil d'intensité[48]. Concernant l'intégration de la dimension cybernétique dans le fonctionnement de partis politiques, il faut noter que le Hezbollah s'est doté d'une unité cybernétique dès les années 2000, celle-ci a agi pour la première fois lors du survol du territoire israélien par un drone du Hezbollah[49].

112 – Acteurs étatiques

Les États ont développé des capacités d'action dans le cyberespace (les capacités propres des acteurs étatiques majeurs concernant la cyber seront étudiées dans le chapitre 3 de cette étude), certains États revendiquent ouvertement leur capacité à agir dans ce nouveau milieu[50]. Aujourd'hui, concevoir une opération militaire implique de prévoir et mettre en œuvre des actions sur les systèmes d'information sur le plan défensif comme offensif[51]. Deux éléments sont à noter en ce sens : d'une part, de nombreux États – parmi lesquels les États-Unis et la France – ont fait de la protection des systèmes d'information une priorité nationale[52], d'autre part les dépenses en armement dans le domaine informatique sont les seules à rester en constante augmentation malgré les restrictions budgétaires impactant la majorité des États, et donc les industries de défense[53] : le marché de la cyberdéfense serait évalué à cinquante milliards de dollars[54]. D'une manière générale, en reprenant

[47] Olivier Danino, « L'utilisation stratégique du cyber au Moyen-Orient », p. 20-21, étude confiée à M. Danino par la Délégation aux Affaires Stratégiques (disponible à l'adresse suivante : http://www.defense.gouv.fr/das/reflexion-strategique/etudes-prospectives-et-strategiques).

[48] Les 5 à 7 du CICR, « Cyberguerre : défi du futur pour l'humanitaire ? », débat organisé le 18 décembre 2012 à Paris. Nicolas Arpagian est directeur scientifique du Cycle « Sécurité Numérique » à l'Institut des Hautes Études de la Sécurité et de la Justice. La vidéo de ce débat est accessible sur le lien http://www.youtube.com/watch?v=26tW4OPCWvY. Bertrand Boyer emploie la terminologie de « guérilla numérique », il estime que le cyberespace « redonne toute sa place à l'action d'unités spécialisées pratiquant une nouvelle forme de guérillas [...] il convient de penser une réponse adaptée à ce type de combat « irrégulier » sous peine de demeurer dans l'aveuglement de l'attente d'une confrontation majeure qui demeure improbable à moyen terme » (voir *Cyberstratégie - l'art de la guerre numérique,* Paris, Nuvis, 2012, p. 126).

[49] Olivier Danino, « L'utilisation stratégique du cyber au Moyen-Orient », p. 21, étude confiée à M. Danino par la Délégation aux Affaires Stratégiques (disponible à l'adresse suivante : http://www.defense.gouv.fr/das/reflexion-strategique/etudes-prospectives-et-strategiques).

[50] À titre d'exemple, les États-Unis développent des règles d'engagement dans le cyberespace (Observatoire du monde cybernétique, Lettre mensuelle n° 5, mai 2012, p. 3).

[51] Jean-Marie Bockel, « Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense », n° 681, enregistré à la Présidence du Sénat le 18 juillet 2012, p. 36.

[52] La Maison Blanche a nommé en décembre 2009 un conseiller spécial sur la menace cybernétique *(Special Assistant to the President and Cybersecurity Coordinator,* Michael Daniel a succédé à Howard Schmidt et occupe actuellement ce poste) ; en juillet 2011, le Pentagone a publié une stratégie concernant le cyberespace (Department of Defense, "Strategy for Operating in Cyberspace", juillet 2011). Quant au Royaume-Uni, les attaques cybernétiques par des États, cyberorganisations ou cyberactivistes ont été déterminées comme l'une des quatre menaces de première importance à la sécurité nationale, les trois autres étant le terrorisme international, une crise militaire interétatique et un accident majeur ou une catastrophe naturelle (HM Government, "A Strong Britain in an Age of Uncertainty: The National Security Strategy", 2010). Enfin, la France a adopté en 2011 une stratégie nationale en matière de défense et sécurité des systèmes d'information (SGDSN, « Défense et sécurité des systèmes d'information : la stratégie de la France », février 2011).

[53] Les segments du renseignement-surveillance-reconnaissance et la cyber seraient en forte croissance, tandis que le marché de l'armement stagnerait. Observatoire du monde cybernétique (DAS), Lettre n° 7, juillet 2012, p. 2. (Accessible à l'adresse suivante : http://www.defense.gouv.fr/das/reflexion-strategique/observatoires/observatoire-du-monde-cybernetique).

[54] Anonyme, « La cyberdéfense, un marché en plein boom ? », 24 mai 2012, billet publié sur le blog cyber-défense.fr accessible à l'adresse suivante : http://cyber-defense.fr/blog/index.php?post/2012/05/24/La-cyberdefense%2C-un-marché-en-plein-boom

la typologie établie par Thomas Rid[55], les États conduisent dans le cyberespace des attaques cybernétiques qui s'apparentent à des modes d'action bien connus : le sabotage, l'espionnage et la subversion (entendue comme action de communication)[56]. Ils développent à ces fins des arsenaux d'armes informatiques dont les capacités sont classifiées[57].

Les États peuvent trouver des intérêts divers au combat dans le cyberespace. Tout d'abord, la cyberconflictualité nécessite peu de troupes, des matériels relativement faciles d'accès (ordinateur, connexion Internet), et n'exige pas l'engagement des forces sur le théâtre. En outre, des attaques cybernétiques peuvent permettre à un État de parvenir à un but politique ou stratégique sans recourir à la force conventionnelle dans le cadre d'un conflit armé. Enfin, les opérations cybernétiques permettent une réactivité, voire une anticipation (dans la mesure où l'avantage est à l'attaquant) dont les opérations conventionnelles bénéficient moins facilement. Ce point est d'ailleurs souligné dans le Livre Blanc de 2013 :

> « *Les opérations ciblées conduites par les forces spéciales et les frappes à distance, le cas échéant cybernétiques, pourraient devenir plus fréquentes, compte tenu de leur souplesse d'emploi dans un contexte où les interventions classiques continueront d'être politiquement plus difficiles et parfois moins efficaces*[58] ».

[55] Thomas Rid, chercheur au King's College de Londres, est l'auteur d'un article considéré par la communauté scientifique comme une référence concernant l'étude du cyberespace comme nouveau champ de conflictualité : "Cyber War Will Not Take Place", *Journal of Strategic Studies,* 2012, Vol. 35, Issue 1, p. 5-32.

[56] Thomas Ridécrit : "All politically motivated cyber attacks are merely sophisticated versions of three activities that are as old as warfare itself: sabotage, espionnage, and subversion" ("Cyber War Will Not Take Place", *Journal of Strategic Studies,* 2012, Vol. 35, Issue 1, p. 5).

[57] Ellen Nakashima, "List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare", *The Washington Post,* 31 mai 2011, disponible à l'adresse suivante : http://articles.washingtonpost.com/2011-05-31/national/35264250_1_cyber-computer-warfare-stuxnet. La journaliste rapporte les propos d'un haut gradé de l'armée américaine qui aurait déclaré au sujet des armes informatiques approuvées par le Pentagone : « peu importe qu'il s'agisse d'un tank, d'un M-16 ou d'un virus informatique, [l'arme] suit les mêmes règles afin que l'on comprenne comment l'utiliser, quand l'utiliser ou quand c'est impossible, ce dont on peut et ne peut pas se servir » (traduction personnelle).

[58] SGDSN, *Livre Blanc Défense et Sécurité Nationale 2013,* p. 30.

Aux menaces provenant des acteurs étatiques et non-étatiques, il faut ajouter la menace représentée par les acteurs internes au Ministère de la Défense.

113 – Acteurs internes

Ce sujet est peu traité dans les études et ouvrages déjà parus alors qu'il est partie intégrante de l'étude du cyberespace comme nouveau champ de bataille pour les forces terrestres. Les acteurs internes sont les individus opérant au sein du Ministère de la Défense – civils ou militaires –, ils constituent une menace réelle pour les systèmes des forces terrestres et plus généralement pour le Ministère de la Défense. Leurs intentions sont rarement hostiles ou malveillantes, néanmoins le manque de connaissance et le non-respect des principes de sécurité des systèmes d'information et de communication (SSIC) et des procédures peuvent conduire ces individus à adopter un comportement à risque, à être négligents.

Alors que, dans un schéma conventionnel, le risque d'un soldat retournant son arme contre ses frères d'arme est très faible, dans le cyberespace il est réel dès lors que le risque n'est pas lié à l'intention de nuire. En ouvrant une pièce jointe, en insérant une clé USB sans passer par une station blanche, le civil et le militaire peuvent contribuer, sans en être conscients, à une attaque visant les systèmes informatiques du Ministère. Ainsi, ils constituent directement ou indirectement une menace portant sur les forces armées françaises.

Étatiques ou non, de multiples acteurs sont susceptibles d'agir dans le cyberespace à l'encontre des forces armées. Leurs motivations peuvent être politiques, idéologiques ou religieuses. Ils disposent de plusieurs modes d'actions pour procéder à une attaque cybernétique.

12 – MODES D'ACTION DANS LE CYBERESPACE

Après avoir présenté les différents acteurs susceptibles d'interagir avec les forces armées dans le cyberespace, il convient de préciser les différents modes d'actions auxquels ils peuvent avoir recours : quelles sont les armes du combat dans le cyberespace ?

Cette section a pour finalité de présenter les méthodes exploitables dans le 5ème champ de bataille et auxquelles les forces armées françaises, et en particulier l'armée de Terre peuvent être confrontées et avoir recours : attaque par armes informatiques, attaques par déni de service et neutralisation physique des réseaux. La typologie des modes d'action dans le cyberespace retenue ici est inspirée de celle établie par Bertrand Boyer[59], le lecteur pourra se référer à une analyse plus détaillée dans son ouvrage *Cyberstratégie - l'art de la guerre numérique*[60].

121 – Attaque par armes informatiques

Avant de présenter divers outils permettant de mener des attaques cybernétiques, il est nécessaire de préciser ce que l'on appelle « arme informatique » ou « cyberarme ». Les armes ne sont normalement pas létales dans le cyberespace, néanmoins elles permettent potentiellement de neutraliser des systèmes d'armes adverses. Selon Thomas Rid et Peter McBurney, une cyberarme est un sous-ensemble d'armes, et plus généralement un code informatique utilisé ou conçu pour être utilisé dans le but de causer des dommages physiques, fonctionnels ou psychologiques à des structures, systèmes ou êtres vivants[61]. Michel Baud[62] propose une définition semblable : « 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[63] ». Les attaques par arme informatique, ou attaques cybernétiques, consistent à mettre en œuvre des outils développés spécifiquement pour nuire à une cible identifiée dans le cyberespace ou dans un espace physique. Plusieurs armes informatiques peuvent être utilisées : virus, vers, chevaux de Troie.

Catégories d'armes informatiques

Un **virus** est un type de maliciel introduit dans un système informatique qui se propage d'un ordinateur à l'autre en se fixant sur un document[64]. Il est souvent activé par inadvertance par l'utilisateur (par exemple en téléchargeant un fichier infecté ou en ouvrant un document infecté transmis en pièce jointe dans un courriel). Lorsqu'il est activé, un virus peut corrompre, altérer ou détruire des données, ou encore transférer des informations. Conficker est un exemple de virus informatique, il a visé des structures sensibles parmi lesquelles celles du Ministère de la Défense français, notamment le réseau interne de la Marine nationale[65].

Un **ver** est un maliciel qui se propage à l'intérieur d'un réseau, souvent de façon autonome, sans nécessairement se fixer sur un autre programme (comme le fait un virus). À l'inverse des virus, les vers ont la capacité de se propager sur les réseaux. Ils sont d'autant plus nocifs qu'ils peuvent se répandre par leurs propres moyens. Stuxnet est un exemple de ver informatique, il a été créé pour modifier la vitesse de rotation des centrifugeuses iraniennes et ainsi ralentir le programme nucléaire iranien.

Enfin, un **cheval de Troie** est un programme comportant une fonction cachée, connue seulement de l'attaquant. Un cheval de Troie permet à son auteur de prendre le contrôle de l'ordinateur compromis

---

59 Bertrand Boyer est officier des Troupes de marine, Saint-Cyrien et breveté de l'École de Guerre. Ingénieur de formation, il a orienté son parcours vers la sécurité des systèmes d'information après ses temps de commandement. Il a suivi une scolarité à Télécom ParisTech dans le cadre de l'enseignement supérieur scientifique et technique.

60 Bertrand Boyer, *Cyberstratégie - l'art de la guerre numérique,* Paris, Nuvis, 2012. La typologie des moyens d'action dans le cyberespace est développée aux pages 132-149.

61 « [...] a cyber-weapon is seen as a subset of weapons more generally: as computer code that is used, designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings », Thomas RID, Peter McBURNEY, "Cyber-weapons", *RUSI Journal,* février-mars 2012, vol. 157, n° 1, p. 7. Le **Manuel de Tallinn** pose une définition plus précise d'une « cyberarme » : le terme désigne la partie d'un système permettant de causer des dommages à des biens ou de les détruire, ou de provoquer des blessures ou la mort ; il inclut tous les matériels, instruments, mécanismes, équipements ou logiciels utilisés, conçus ou dont on entend se servir pour mener une attaque cybernétique au sens de la Règle 30. Voir Manuel de Tallinn, CCD CoE, Règle 41, p. 141 et suivantes.

62 Le chef de bataillon (TA) Michel BAUD est officier de l'armée de Terre, transmetteur. Il est diplômé de l'enseignement militaire supérieur, du Cours Supérieur d'État-Major ainsi que de l'École de Guerre, et est détaché comme chercheur au sein du Laboratoire de Recherche sur la Défense de l'Institut Français des Relations Internationales (IFRI).

63 Michel Baud, « Cyberguerre – en quête d'une stratégie », *Focus stratégique,* n° 44, IFRI, mai 2013, p. 11.

64 Fred Schreier, "The Report on Cyberwarfare", DCAF, 2012, p. 57.

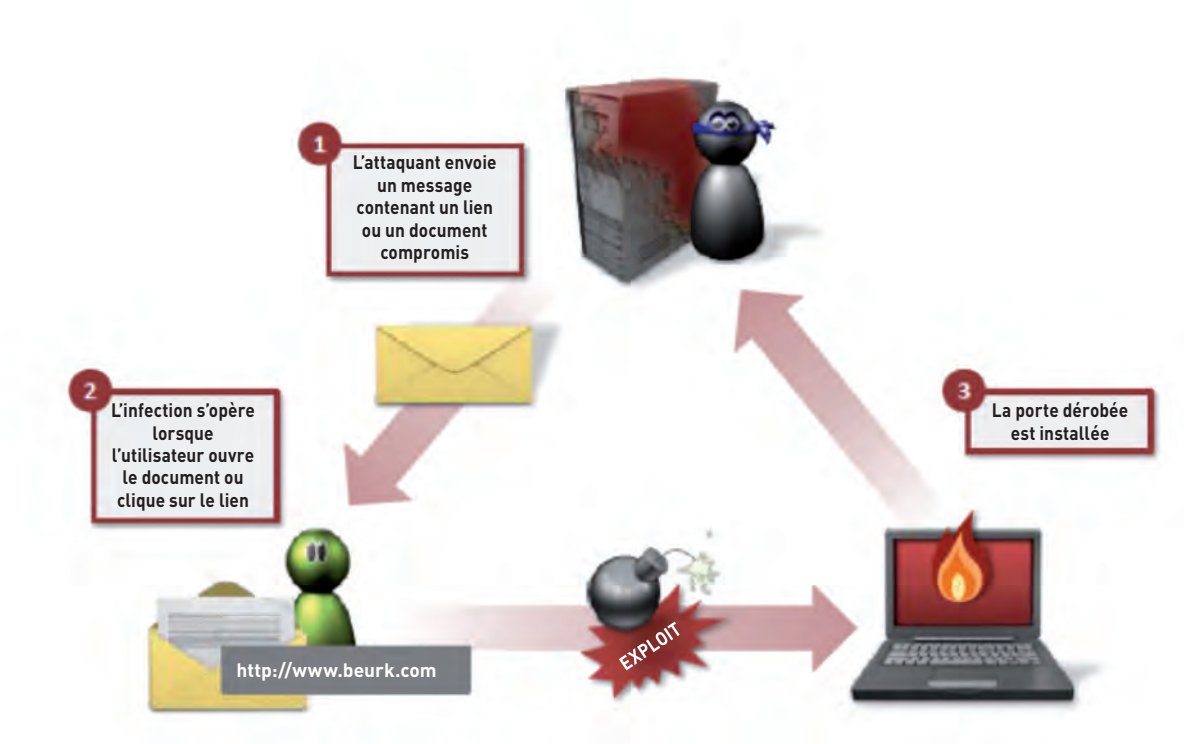
65 Jean-Dominique Merchet, « Les armées attaquées par un virus informatique », billet publié le 5 février 2009 (http://secret-defense.blogs.liberation.fr/defense/2009/02/les-armes-attaq.html).

et de s'en servir à l'insu de son propriétaire. Les chevaux de Troie sont souvent utilisés pour mener des attaques ciblées, les programmes sont développés et adaptés pour des cibles spécifiques[66]. Les « portes dérobées » (également appelées *backdoors*) sont les chevaux de Troie les plus répandus, elles consistent à surveiller les activités d'un logiciel à distance et éventuellement à en prendre le contrôle. Une porte dérobée introduite par un développeur ou un tiers dans un logiciel peut ainsi lui permettre de contourner une authentification normale en sécurisant l'accès à distance à un ordinateur tout en restant non détecté[67]. Le concepteur du cheval de Troie peut ainsi prendre le contrôle à distance d'un système informatique qu'il a infecté (un ordinateur, et potentiellement les ordinateurs reliés au même réseau que la machine infectée).

Mise en œuvre des armes informatiques et finalités

Les codes malveillants peuvent être transmis de différentes façons : par intrusion physique dans le réseau (port USB, câble), ou encore par « *social engineering* ». Le *social engineering* est l'exploitation de la confiance, de l'ignorance ou de la crédulité d'une personne afin d'obtenir quelque chose que cette dernière n'aurait pas consciemment consenti à donner (un identifiant, un mot de passe par exemple). Le *phishing*[68] et le démarchage par courrier sont considérés comme des formes de *social engineering*. Le schéma ci-dessous représente le processus d'une attaque par *spearphishing* (on parle de *spearphishing* lorsque l'hameçonnage vise précisément une ou plusieurs personnes, il s'agit d'une attaque ciblée) :

"Spear Phishing"



Source : Symantec, conférence « Stuxnet, Duqu, Flame et autres maliciels : nouvelles armes informatiques ? », 21 mars 2013, Paris.

[66] Jean-Marie Bockel, « La cyberdéfense : un enjeu mondial, une priorité nationale », Rapport d'information fait au nom de la Commission des Affaires étrangères, de la Défense et des forces armées, du Sénat n° 681, enregistré à la Présidence du Sénat le 18 juillet 2012, p. 27.

[67] Fred Schreier, "The Report on Cyberwarfare", DCAF, 2012, p. 52.

[68] Le *phishing*, également appelé « hameçonnage », consiste à obtenir des renseignements personnels en faisant croire à une personne qu'elle s'adresse à quelqu'un de confiance. Le *phishing* repose sur l'envoi de messages génériques à un grand nombre de destinataires.

Dans le cas de l'intrusion dans les réseaux de l'Élysée en mai 2012, les conseillers de Nicolas Sarkozy auraient été contactés *via* le réseau social[69] Facebook par un faux profil les invitant à entrer leurs identifiants et mots de passe sur une fausse page Intranet de l'Élysée. Les *hackers* auraient ensuite injecté un ver ayant les mêmes fonctionnalités que Flame[70] afin de récupérer des fichiers confidentiels[71]. De tels procédés ont déjà été utilisés directement contre les forces armées : en Israël, le cas « Zukerman » a connu une résonnance importante. Des membres du Hezbollah ont créé un profil Facebook sous les traits d'une jeune femme fictive, Reut Zukerman ; ils sont entrés en contact avec des soldats israéliens par l'intermédiaire de ce profil et auraient réussi à obtenir des informations de divers degrés d'importance auprès de 200 soldats israéliens[72]. Début 2012, l'amiral James G. Stavridis, Commandant suprême des forces alliées en Europe, a été victime d'une attaque semblable : des internautes ont usurpé son identité en créant un faux profil Facebook. Sur le réseau social, ces derniers ont réussi à collecter des données personnelles concernant des officiers supérieurs de plusieurs armées occidentales[73]. Cet exemple illustre la menace interne pesant sur les forces armées, notamment en raison de l'utilisation des réseaux sociaux à des fins professionnelles. Dans le cas de l'amiral Stavridis, les officiers ciblés ont communiqué des données sensibles *via* Facebook malgré l'absence de sécurisation de la communication sur le réseau. Aussi, il est nécessaire de sensibiliser tous les utilisateurs du Ministère et des forces armées, civils et militaire, du plus bas au plus haut niveau de la hiérarchie, au respect de certaines règles parmi lesquelles l'interdiction de l'utilisation des réseaux sociaux comme outil de travail (en particulier comme messagerie professionnelle).

[69] Le terme réseau social est défini comme « un site Internet permettant à l'internaute de s'inscrire et d'y créer une carte d'identité virtuelle appelée le plus souvent "profil" » (voir Laurent SUPLY, « Définition : réseau social », Suivez le Geek, 1er janvier 2008, http://blog.lefigaro.fr/hightech/2008/01/definition-reseau-social.html).

[70] Le virus Flame a été conçu pour voler de l'information (son et vidéo inclus).

[71] Observatoire du monde cybernétique (DAS), Lettre n° 11, novembre 2012, p. 2 (accessibles à l'adresse suivante : http://www.defense.gouv.fr/das/reflexion-strategique/observatoires/observatoire-du-monde-cybernetique).

[72] Marc Hecker et Thomas Rid, « Les armées françaises doivent-elles craindre les réseaux sociaux ? », *Politique étrangère* 2, 2012, p. 319.

[73] Marc Hecker et Thomas Rid, « Les armées françaises doivent-elles craindre les réseaux sociaux ? », *Politique étrangère* 2, 2012, p. 319.

122 – Attaques par déni de service

Une attaque par déni de service (DoS) consiste à détourner les moyens existant afin de rendre indisponible ou de ralentir l'accès au serveur ciblé pendant un certain temps en envoyant un nombre de requêtes instantanées supérieur à ses capacités de traitement. Cette attaque peut être lancée depuis une source unique, ou depuis une multitude d'ordinateurs : un opérateur prend le contrôle de plusieurs ordinateurs grâce auxquels il formule des requêtes sur le serveur cible et provoque ainsi sa saturation. On parle alors d'attaque par déni de service distribué (DDoS). Les machines infectées le sont sans que leur propriétaire en ait nécessairement connaissance. Les attaques par déni de service ont largement été utilisées à l'encontre de l'Estonie en 2007 : on a dénombré jusqu'à 85 000 ordinateurs envoyant des requêtes à des serveurs de façon continuelles durant trois semaines[74].

123 – Neutralisation physique des réseaux ou de moyens électroniques terminaux

Les réseaux existent grâce à des supports physiques (câbles sous-marins ou terrestres) et des structures indispensables à leur fonctionnement (centrales électriques, systèmes de climatisation, centres de données – *data centers*). Neutraliser physiquement ces structures pourrait permettre à un attaquant d'endommager voire de rendre inopérant un réseau et donc les systèmes informatiques qui en dépendent pendant un certain temps. De telles actions ne sont pas dans le champ de guerre cybernétique au sens strict, néanmoins le risque existe même si aujourd'hui, aucune neutralisation physique des réseaux n'est recensée (cette méthode a été envisagée par le passé : en 1999, l'OTAN avait étudié cette option dans le cadre de son intervention au Kosovo[75]).

La neutralisation de moyens électroniques terminaux est également un moyen d'action dans le cyberespace, même si elle relève de la guerre électronique

[74] Thomas Rid, Peter McBurney, « Cyber-weapons », *RUSI Journal*, février-mars 2012, vol. 157, n° 1, p. 9.

[75] Assemblée européenne de sécurité et de défense, « La guerre informatique », document C/2022, 5 novembre 2008, par. 68, p. 11.

et n'est pas une attaque cybernétique. Elle consiste à détruire les systèmes électroniques adverses en produisant une impulsion électromagnétique. De nouvelles armes sont développées dans ce domaine : le projet CHAMP (*Counter-electronics High-powered Microwave Advanced Missile Project*) mené par Boeing consiste à doter un missile d'un canon à impulsion micro-ondes capable de causer une surtension dans les cibles et ainsi de les neutraliser[76].

13 – ÉTUDES DE CAS

Deux types d'attaques cybernétiques sont survenues dans le cadre de conflits armés ces dernières années : d'une part des attaques relevant de la guerre de l'information, et d'autre part des attaques cybernétiques visant des matériels militaires. En outre, on peut recenser certaines attaques de grande ampleur qui ont été conduites en dehors d'une situation de conflit armé. De façon non exhaustive, cette section présente des cas avérés afin de comprendre divers processus d'attaques dans le cyberespace et leurs conséquences. Les cas développés ci-dessous ont été retenus car ils sont un aperçu des conflits militaires tels qu'ils sont déjà et seront vraisemblablement conduits désormais, c'est-à-dire en associant des attaques cybernétiques à l'usage conventionnel de la force, en visant en particulier les systèmes d'information.

131 – Attaques relevant de la guerre de l'information : Kosovo, Israël/Hezbollah, Géorgie/Russie, Corée du Sud

La guerre de l'information couvre un spectre d'activités plus large que la guerre cybernétique, néanmoins la maîtrise de l'information est un outil clé dans la conduite d'actions dans le cyberespace. Selon Michel Baud, « dans cette Cyberguerre, la maîtrise de l'information est le centre de gravité du conflit[77] ».

Tchétchénie, 1994 et 1999-2001

La Tchétchénie est l'un des premiers théâtres de conflit où l'on a pu constater l'utilisation du cyberespace par les parties en conflit, en parallèle des opérations militaires sur le terrain. Ce fut le cas au cours des deux guerres de Tchétchénie entre les forces armées de la Fédération de Russie et les indépendantistes tchétchènes : la première de 1994 à 1996 et la seconde de 1999 à 2001[78]. Les indépendantistes tchétchènes sont considérés comme des précurseurs dans l'utilisation d'Internet à des fins de propagande : ils étaient notamment parvenus à mettre en place un fonds de soutien à la guerre, à en communiquer les coordonnées bancaires afin de rassembler des fonds pour leur mouvement et d'unifier la diaspora tchétchène[79]. Si les deux parties en conflit utilisaient Internet afin de transmettre leurs messages relatifs au conflit, la guerre de l'information semble avoir tourné à l'avantage des indépendantistes tchétchènes : en 1999, les images d'un char russe ouvrant le feu sur un bus transportant des civils près du village de Chervlyonnaya et faisant vingt-huit victimes fut mise en ligne, tandis que les autorités russes niaient l'incident[80]. La publication de cette vidéo contredisant la position officielle russe aurait fait pencher l'opinion publique en faveur des indépendantistes.

Kosovo

La guerre du Kosovo (1998-1999) est le théâtre sur lequel l'OTAN et les membres de l'Alliance ont pour la première fois envisagé et mené des attaques cybernétiques. Des intrusions et tentatives de perturbation des sites gouvernementaux, parmi lesquels celui des forces armées serbes, ont été recensées[81].

[76] Michel Baud, « Cyberguerre – en quête d'une stratégie », *Focus stratégique n° 44,* IFRI, mai 2013, p. 13.

[77] Michel Baud, « La Cyberguerre n'aura pas lieu, mais il faut s'y préparer », IFRI, *Politique étrangère* 2, 2012, p. 308.

[78] Le site Internet de la Documentation française propose une chronologie des deux guerres de Tchétchénie : http://www.ladocumentationfrancaise.fr/dossiers/d000076-la-deuxieme-guerre-de-tchetchenie-1999-2006/chronologie

[79] Fred Schreier, "The Report on Cyberwarfare", DCAF, 2012, p. 107. Voir également Kenneth GEERS, "Cyberspace and the Changing Nature of Warfare", accessible à l'adresse suivante : http://www.carlisle.army.mil/DIME/documents/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf

[80] Fred Schreier, "The Report on Cyberwarfare", DCAF, 2012, p. 108. Voir également Robyn DIXON, "Russia to Pour Money Into Chechen Fight", *Los Angeles Times,* 7 octobre 1999 (http://articles.latimes.com/1999/oct/07/news/mn-19719).

[81] Assemblée européenne de sécurité et de défense, « La guerre informatique », document C/2022, 5 novembre 2008, par. 68, p. 18.

Néanmoins, le cyberespace comme nouveau champ de bataille a dès cette époque soulevé des interrogations : le général Wesley Clark, Commandant Suprême des Forces Alliées en Europe, aurait critiqué la stratégie américaine en déclarant que la Force aurait pu faire beaucoup mieux afin d'isoler électroniquement le président Slobodan Miloševic en réponse au refus des États-Unis d'engager des attaques informatiques contre la Serbie[82]. Deux raisons furent avancées pour justifier cette position : officiellement, les États-Unis auraient redouté les conséquences légales d'attaques informatiques ainsi que le risque encouru de voir leurs actions qualifiées de crimes de guerre ; officieusement, la première puissance militaire au monde aurait préféré ne pas révéler ses capacités d'action dans le cyberespace et conserver une avance technologique certaine sur ses ennemis[83].

Dans l'autre camp, face aux opérations aériennes menées par l'OTAN sur la Serbie, de nombreuses communautés de *hackers* pro-Serbes et/ou anti-occident conduisirent des attaques cybernétiques à l'encontre des sites officiels de l'OTAN, notamment par déni de service et défacement[84]. Ils saturèrent également le serveur de messagerie de l'Organisation[85]. L'une d'entre elles, les « *Black Hands* », un groupe de *hackers* serbes[86] fut très active.

Israël/Palestine

Entre 2000 et 2002, un conflit cybernétique eut lieu entre Israël et les territoires palestiniens. Il fut déclenché par de jeunes *hackers* israéliens après qu'ils eurent lancé des attaques par déni de service à l'encontre de six sites Internet du Hezbollah et du Hamas[87]. En réponse, les Palestiniens ainsi que des organisations islamiques appelèrent au *Cyber Holy War*, c'est-à-dire à la Guerre Sainte cybernétique[88]. Des *hackers* pro-palestiniens parvinrent à atteindre les sites Internet du Parlement israélien, du Ministre des Affaires étrangères et du site d'information des forces armées israéliennes ; en janvier 2001, les attaques avaient atteint 160 sites israéliens et 35 sites palestiniens[89].

Israël est depuis devenu le leader régional en termes de capacité défensive et offensive dans le cyberespace. L'État israélien a fait de la maîtrise de la communication dans le cyberespace – et en particulier sur les réseaux sociaux – un outil militaire fondamental, au même titre que les moyens militaires conventionnels. Lors de l'opération « Plomb Durci » en 2008-2009, Israël a créé une chaîne officielle[90] sur la plateforme de partage de vidéos You Tube et a mis en ligne de nombreuses vidéos des opérations menées dans la bande de Gaza.

Crédits : IsraeliDefense Forces

[82] Julian Borger, "Pentagonkept the lid on cyberwar in Kosovo", *The Guardian,* 9 novembre 1999, http://www.theguardian.com/world/1999/nov/09/balkans

[83] *Idem.*

[84] Jason Healey, Leendert Van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today and Tomorrow", Atlantic Council Issue Brief, février 2012, p. 2. Voir également l'article d'Ellen MESSMER, "Kosovo cyber-war intensifies", *Network World Fusion,* 5 décembre 1999, http://www.networkworld.com/news/1999/0512kosovo.html

[85] Michel Baud, « La Cyberguerre n'aura pas lieu, mais il faut s'y préparer », IFRI, *Politique étrangère* 2, 2012, p. 309.

[86] Chantale Quesney, *Kosovo : les mémoires qui tuent, la guerre vue sur Internet,* éditions L'Harmattan, Les Presses de l'Université de Laval, 2001, p. 49-51.

[87] Patrick D. Allen, COL, U.S Army Reserve, Chris DEMCHAK, LCL, U.S Army, "The Palestinian-Israeli Cyberwar", *Military Review,* mars-avril 2003, p. 52-53, accessible en suivant le lien http://usacac.leavenworth.army.mil/CAC/milreview/download/English/MarApr03/allen.pdf

[88] Fred Schreier, "The Report on Cyberwarfare", DCAF, 2012, p. 108.

[89] Fred Schreier, "The Report on Cyberwarfare", DCAF, 2012, p. 109.

[90] Il s'agit de la chaîne « Israel Defense Forces », http://www.youtube.com/user/idfnadesk

Cette stratégie a été renouvelée en novembre 2012 à l'occasion de l'opération « Pilier de défense » en utilisant en outre le réseau social Twitter afin de communiquer instantanément sur les opérations menées par les forces israéliennes. Le 14 novembre, 29 raids aériens sont lancés sur la bande de Gaza[91]. Alors qu'il venait de tuer Ahmed al-Jaabari, chef des Brigades Ezzedines Al-Qassam (branche armée du Hamas), Tsahal a publié deux twitts : « *the IDF has begun a wide spread campaign on terror sites &operatives in the #Gaza Strip, chief among them #Hamas &Islamic Jihad targets*[92] », suivi de « *the first target, hit minutes ago, was Ahmed Al-Jabari, head of the #Hamas military wing*[93] ». Parallèlement, le Hamas n'a pas laissé le champ des réseaux sociaux aux Israéliens et les a également fortement investis. Le conflit de novembre 2012 témoigne de l'importance que les parties au conflit accordent au cyberespace comme champ de communication. Il illustre la volonté des belligérants de délégitimer l'adversaire et son action en communiquant presque instantanément sur les dommages collatéraux dont il est à l'origine, afin de nourrir ou au contraire d'entamer le soutien de l'opinion et d'infléchir la motivation de l'ennemi[94].

Géorgie/Russie

En août 2008, la Géorgie fut victime d'attaques par armes informatiques de grande ampleur dans le cadre de la crise contre la Russie. Dans la nuit du 7 au 8 août, l'armée géorgienne avait donné l'assaut contre l'Ossétie du Sud, et la Russie était intervenue en faveur de la région séparatiste[95]. Lors de la campagne militaire russe contre la Géorgie, l'emploi d'armes informatiques fut pour la première fois ouvertement intégré à une stratégie militaire : en parallèle des opérations terrestres, navales et aériennes, des opérations dans le cyberespace furent menées[96]. Trois méthodes furent employées à grande échelle : le défacement des sites officiels des institutions géorgiennes, les attaques par déni de service contre les sites Internet d'institutions à la fois publiques et privées, et enfin la distribution de maliciels et la diffusion auprès du grand public – parmi lesquels des *hackers* – de procédés pour mener des actions contre la Géorgie sur des forums[97].

L'un des objectifs recherchés par les auteurs des attaques cybernétiques était de limiter la capacité de son adversaire à communiquer et d'introduire de fausses informations. Néanmoins, le conflit russo-géorgien illustre également les limites de la guerre de l'information puisque quelques heures après la neutralisation des sites officiels des institutions géorgiennes, ceux-ci ont été délocalisés aux États-Unis et en Pologne afin de permettre la continuité des services de l'État géorgien[98].

Corée du Sud

L'exemple le plus récent en matière d'attaques cybernétiques en situation de conflit armé est celui de la Corée du Nord et de la Corée du Sud. Le conflit, qui a éclaté en 1950, est aujourd'hui mené sur un nouveau front : le front cybernétique. En mars 2013, l'éditeur de solutions informatiques de sécurité Symantec a détecté une nouvelle arme informatique, le cheval de Troie « Jokra », présentant une caractéristique inédite : il est capable d'atteindre les systèmes exploités par Linux[99]. Jokra a atteint plusieurs cibles en Corée du Sud, dont trois chaînes de télévision, deux banques et un opérateur télécom[100]. 32 000 ordinateurs auraient été infectés par le cheval de Troie[101]. Séoul serait parvenu à identifier l'origine des attaques menées contre la Corée du Sud et a officiellement dénoncé l'implication de la Chine et de la Corée du Nord dans les attaques cybernétiques conduites[102].

---

91 Romain Mielcarek, « Guerre et communication 2.0 », *DSI*, n° 93, juin 2013, p. 57.

92 https://twitter.com/IDFSpokesperson/status/268722403989925888

93 https://twitter.com/IDFSpokesperson/status/268722815300169729

94 Olivier Danino, « L'utilisation stratégique du cyber au Moyen-Orient », p. 29, étude confiée à M. Danino par la Délégation aux Affaires Stratégiques.

95 Florence Mardirossian, « Géorgie-Russie, les enjeux de la crise », *Le Monde Diplomatique*, 15 août 2008, http://www.monde-diplomatique.fr/carnet/2008-08-15-Georgie

96 Rosemary M. Carter, Brent Feick, Roy C. Undersander, "Offensive Cyber for the Joint Force Commander; it's Not That Different", *Joint Force Quarterly*, Issue 66, 3rd Quarter 2012, p. 22. Voir également Thomas RID, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, 2012, Vol. 35, Issue 1, p. 13.

97 Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, 2012, Vol. 35, Issue 1, p. 13-14. Voir aussi Assemblée européenne de sécurité et de défense, « La guerre informatique », document C/2022, 5 novembre 2008, par. 94, p. 14.

98 Assemblée européenne de sécurité et de défense, « La guerre informatique », document C/2022, 5 novembre 2008, par. 71, p. 11.

99 http://www.symantec.com/security_response/writeup.jsp?docid=2013-032014-2531-99

100 Anonyme, "South Korea on alert for cyber-attacks after major network goes down", *The Guardian*, 20 mars 2013, http://www.theguardian.com/world/2013/mar/20/south-korea-under-cyber-attack

101 http://www.bbc.co.uk/news/world-asia-23042334

102 Sébastien Seibt, « Cyber-attaque contre la Corée du Sud : la balle est dans le camp chinois », *France 24*, http://www.france24.com/fr/20130321-ip-adresse-coree-sud-nord-chine-cyber-attaque-piratage-hacking-decouverte

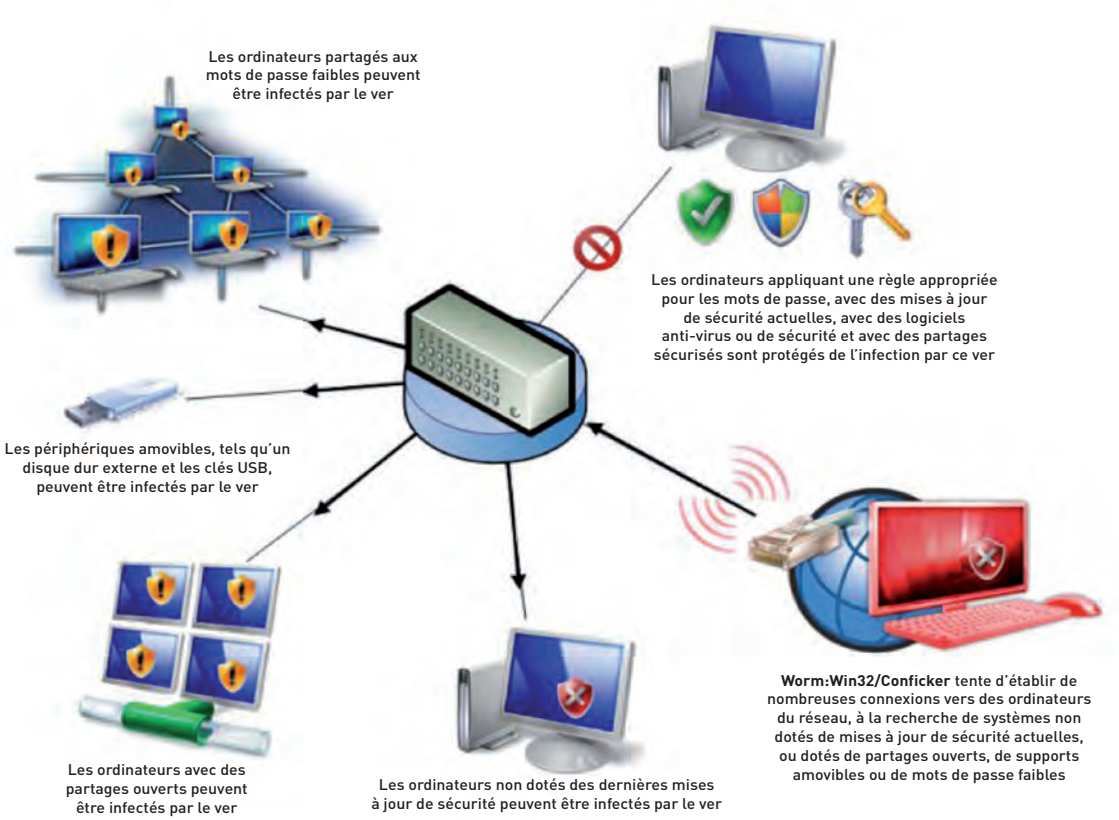
Les attaques de mars 2013 se sont déroulées dans un contexte diplomatique difficile entre la Corée du Nord et la Corée du Sud : au début du mois, le *leader* nord-coréen Kim Jong-Un avait déclaré que son armée était prête à mener une guerre totale, après avoir menacé la Corée du Sud et les États-Unis d'une frappe nucléaire préventive[103]. Dans ce contexte, le cyberespace apparaît comme un champ diplomatique à part entière que les États utilisent afin d'affirmer leur position et leur discours sur la scène internationale.

132 – Attaques cybernétiques visant des matériels militaires et les forces armées

La Guerre du Golfe fut, selon plusieurs auteurs, la première guerre au cours de laquelle des attaques cybernétiques furent menées sur les matériels militaires. En effet, les Américains ont lancé des attaques cybernétiques contre les infrastructures irakiennes dans la phase 1 de l'Opération « Tempête du Désert » en parallèle de la campagne aérienne[104]. Plus récemment, deux maliciels ont été particulièrement préoccupants pour certaines forces armées ces trois dernières années : Sofacy et Conficker ; le premier est un cheval de Troie, le second est un ver informatique.

Sofacy

Ce cheval de Troie[105] a visé plusieurs organisations militaires européennes, il avait pour finalité de voler des informations (identifiants utilisateurs, mots de passe, frappes clavier, copies d'écrans). Les données étaient ensuite exfiltrées par mail ou par Internet.



Crédits : *Microsoft*[106]

[103] Anonyme, « La Corée du Nord rompt son pacte de non-agression avec la Corée du Sud », *Le Huffington Post*, 8 août 2013, http://www.huffingtonpost.fr/2013/03/08/coree-du-nord-larmee-est-prete-mener-guerre-totale_n_2834765.html

[104] Fred SCHREIER, "The Report on Cyberwarfare", DCAF, 2012, p. 107.

[105] Voici la fiche Symantec sur le cheval de Troie « Sofacy » : http://www.symantec.com/security_response/writeup.jsp?docid=2011-090714-2907-99

[106] http://www.zdnet.fr/actualites/securite-la-marine-victime-du-virus-conficker-downadup-39387036.htm

Win 32 Conficker

Win 32 Conficker est un ver informatique exploitant une vulnérabilité du service Serveur Windows (système exploité par le Ministère de la Défense) qui permet une exécution de code à distance. Il se propage sur d'autres ordinateurs par le réseau, grâce aux interconnexions ou par le moyen des supports amovibles tels que les clés USB.

Le schéma qui précède illustre le fonctionnement du ver Conficker :

Le ver Conficker a attaqué les forces armées françaises, il aurait notamment infiltré le réseau interne de la Marine (Intramar) ainsi que certains ordinateurs du 8e Régiment des Transmissions[107]. Les conséquences auraient pu être lourdes : le ver aurait infecté le système de contrôle aérien, en conséquence et les avions Rafales de la Force d'Action Navale auraient été dans l'impossibilité de décoller pendant plusieurs heures[108].

133 – Attaques cybernétiques conduites en dehors d'un conflit armé

Dans la mesure où elles peuvent affecter directement ou indirectement les forces armées, les attaques cybernétiques conduites en temps de paix entrent dans le champ de cette étude. Les événements les plus emblématiques d'attaques cybernétiques conduites en dehors d'un conflit armé sont les attaques survenues en Estonie et l'attaque de la centrale nucléaire iranienne de Natanz.

Estonie

Les événements survenus en Estonie en avril et mai 2007 sont considérés comme le premier cas de conflit cybernétique en raison des cibles visées par les attaques (les infrastructures de l'État estonien : sites gouvernementaux et secteur économique public et privé) et de l'ampleur des dysfonctionnements consécutifs[109]. Les attaques s'inscrivaient dans un contexte politique compliqué entre l'Estonie et la Russie : elles sont survenues après que les autorités estoniennes eurent décidé de déplacer le monument érigé en souvenir des combattants de l'armée soviétique qui avaient contribué à mettre fin à l'occupation allemande en 1944 (le monument devait quitter le centre de Tallinn pour être érigé à nouveau dans un cimetière de la ville). Le gouvernement russe ainsi que la communauté russophone d'Estonie s'étaient vivement opposés à cette décision[110]. Le 27 avril 2007, les premières attaques informatiques par déni de service distribué saturaient les sites gouvernementaux et bancaires. L'ampleur des attaques était sans précédent : le 9 mai, 58 sites Internet furent attaqués et rendus inaccessibles[111].

Les autorités estoniennes ainsi que les experts de l'OTAN et de la Commission européenne ne parvinrent pas à identifier un acteur étatique derrière les attaques, bien que l'ampleur et l'intensité laissent penser que seul un État pouvait être en mesure de coordonner et conduire de telles attaques[112]. En revanche, il ne fait aucun doute que ce sont des *hackers* pro-russes qui ont massivement participé aux attaques cybernétiques menées contre l'Estonie. Sur les forums Internet russes, les autorités estoniennes trouvèrent des appels à la mobilisation accompagnés d'instructions spécifiques expliquant comment participer aux attaques par déni de service. Les sites gouvernementaux recevaient habituellement 1 000 visites quotidiennes, soudainement ils en reçurent 2 000 par seconde[113]. En parallèle des sites Internet gouvernementaux, les banques estoniennes furent visées : dans un pays où 95 % des transactions bancaires sont effectuées en ligne, la fermeture des banques causée par les attaques par déni de service a provoqué des pertes économiques très importantes[114].

---

107 Jean-Dominique Merchet, « Les armées attaquées par un virus informatique (actualisé) », *Secret Défense*, 5 février 2009, http://secretdefense.blogs.liberation.fr/defense/2009/02/les-armes-attaq.html ; voir également http://www.zdnet.fr/actualites/securite-la-marine-victime-du-virus-conficker-downadup-39387036.htm

108 Michel Baud, « La Cyberguerre n'aura pas lieu, mais il faut s'y préparer », IFRI, *Politique étrangère* 2, 2012, p. 310.

109 Assemblée européenne de sécurité et de défense, « La guerre informatique », document C/2022, 5 novembre 2008, par. 1, p. 5. Voir également Michel BAUD, « La Cyberguerre n'aura pas lieu, mais il faut s'y préparer », IFRI, *Politique étrangère* 2, 2012, p. 309.

110 Jean-Marie Bockel, « La cyberdéfense : un enjeu mondial, une priorité nationale », Rapport d'information fait au nom de la Commission des affaires étrangères, de la défense et des forces armées du Sénat n° 681, enregistré à la Présidence du Sénat le 18 juillet 2012, p. 12.

111 *Idem*.

112 Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, 2012, Vol. 35, Issue 1, p. 12.

113 Fred Schreier, "The Report on Cyberwarfare", DCAF, 2012, p. 109.

114 Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, 2012, Vol. 35, Issue 1, p. 11.

Les équipes d'experts en sécurité informatique dépêchées par les États-Unis et l'OTAN afin d'aider les autorités estoniennes à stabiliser la situation furent frappées par la durée de ces attaques – plusieurs semaines – et par leur intensité[115]. Certains experts qualifient les attaques cybernétiques menées contre l'Estonie d'actes de guerre au sens clausewitzien dans la mesure où l'intention de leurs auteurs était de créer un sentiment de panique au sein de la société[116]. Dans une logique prospective, le Sénateur Bockel estime que le cas de l'Estonie illustre l'utilisation qui peut être faite de l'Internet, et plus particulièrement des attaques par déni de service afin d'intimider ou de conduire des représailles dans un contexte de tensions politiques entre deux ou plusieurs États[117].

Stuxnet[118]

Le ver Stuxnet a été conçu dans le cadre de l'opération « Olympic Games » mise en place par le gouvernement américain et ayant associé des experts israéliens de l'unité 8200[119]. Celle-ci avait pour but d'atteindre la centrale nucléaire iranienne de Natanz et de ralentir le programme nucléaire iranien : Stuxnet modifiait la vitesse de rotation des centrifugeuses enrichissant l'uranium tout en neutralisant les montées d'alerte et provoqua l'endommagement de plus de mille centrifugeuses, réalisant ainsi les objectifs de ses concepteurs[120]. Le ver Stuxnet fut découvert en 2010, il illustre la menace que constituent les attaques cybernétiques pour les forces armées, y compris en situation de paix : si le virus Stuxnet a été conçu pour infecter le système informatique de la centrale nucléaire iranienne, il a également eu des conséquences pour les forces armées françaises en infectant le réseau Intradef sur le théâtre afghan en 2010[121].

Outre ces situations caractérisées par l'ampleur des dommages causés et l'intensité rare des attaques menées, d'autres événements *a priori* moins significatifs pour les forces armées doivent néanmoins être pris en compte dans ce cadre. L'intrusion des réseaux informatiques de l'Élysée en mai 2012, mentionnée plus haut[122], peut sembler moins préoccupante pour les forces armées que celle perpétrée contre le réseau Intradef sur le théâtre afghan, néanmoins elle visait le Président de la République, chef des armées[123]. Aussi est-il nécessaire d'intégrer l'importance quantitative et qualitative de ce type d'attaques dans l'appréciation de la menace cybernétique pesant sur les forces armées et sur la nation.

---

115 Fred Schreier, "The Report on Cyberwarfare", DCAF, 2012, p. 110.

116 Paul Cornish, David Livingstone, Dave Clemente, Claire Yorke, "On Cyber Warfare", *Chatham House report*, novembre 2010, p. 10.

117 Jean-Marie Bockel, « La cyberdéfense : un enjeu mondial, une priorité nationale », Rapport d'information fait au nom de la Commission des affaires étrangères, de la défense et des forces armées, du Sénat n° 681, enregistré à la Présidence du Sénat le 18 juillet 2012, p. 13.

118 Pour une étude détaillée du ver Stuxnet, le lecteur pourra se référer à l'article de Brian Weeden, ancien officier de l'US Air Force : Brian Weeden, "Cyber offense and defense as mutually exclusive national policy priorities", UNIDIR, *Confronting Cyberconflict,* Geneva, 2011, p. 19-30. L'article disponible à l'adresse suivante : http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=143274. Dans la même logique que le ver Stuxnet, en mai 2012 un ver vingt fois plus puissant a été découvert : **Flame.** Ce maliciel, conçu pour pénétrer les réseaux et voler des informations (y compris le vol de fichiers son et vidéo), serait contrôlé à partir de serveurs de commande & contrôle ainsi que Windows Update. Il aurait infecté un nombre relativement faible d'ordinateurs, principalement en Iran, Syrie, Israël, Liban, Soudan, Cisjordanie, et en Égypte.

119 Nicolas Caproni, « Stuxnet : le retour de Flame », note publiée sur le site www.cyber-securite.fr, 4 juin 2012 (accessible en suivant le lien http://www.cyber-securite.fr/2012/06/04/stuxnet-le-retour-de-flame/). Voir également Dominique Pignon, « La prospective du caractère stratégique du cyberespace », Délégation aux Affaires Stratégiques, Ministère de la Défense, 2012, p. 36-38 et 40.

120 Stuxnet est un code malveillant exploitant des vulnérabilités dans le système *Microsoft Windows* et le logiciel de SCADA *WinCC* de *Siemens*. Il a infecté plus de 40 000 adresses IP uniques, le ver comportait quatre vulnérabilités 0-day (vulnérabilités identifiées pour la première fois ; en moyenne, les experts de la sécurité informatique trouvent une dizaine de vulnérabilités 0-day par an), deux vulnérabilités peu connues, sept méthodes de propagation, et deux vols de signature numérique. Un code malveillant « classique » représente en moyenne 15-20 kilo-octets. Stuxnet représentait 600 kilo octets. Source : Laurent HESLAULT (Directeur des stratégies de sécurité – Symantec Europe du sud), « Stuxnet, Duqu, Flame et autres maliciels : nouvelles armes informatiques ? », conférence tenue le 21 mars 2013 à Paris et organisée par l'Association Nationale des Auditeurs Jeunes de l'IHEDN. Voir la vidéo Symantex « *Stuxnet 0.5 – the missing link* » expliquant le Stuxnet (http://www.youtube.com/watch?v=hPR-08_RPAs).

121 Colonel Philippe Bougeret, OSSI-Terre, « Le défi de la cyberdéfense pour l'armée de Terre », *Transmetteurs,* 1er semestre 2013, n° 6, p. 22.

122 Voir le paragraphe « mise en œuvre des armes informatiques et finalités » dans la sous-section « attaques par armes informatiques ».

123 L'article 15 de la Constitution du 4 octobre 1958 (à jour de la révision constitutionnelle du 23 juillet 2008) stipule que *« Le Président de la République est le chef des armées. Il préside les conseils et les comités supérieurs de la défense nationale ».*

Le cyberespace est un nouveau champ d'action pour les forces armées, il est caractérisé par une multitude de moyens d'actions qui permettent d'agir du niveau tactique jusqu'au niveau stratégique. De nombreux acteurs, hackeurs ou cyberterroristes, sont susceptibles d'agir dans le cyberespace à l'encontre des forces armées au même titre qu'un État possédant un arsenal d'armes informatiques et des ressources humaines importantes. Les attaques contre la Géorgie en 2008 illustrent la façon dont des opérations militaires peuvent être menées dans le cyberespace en parallèle des opérations militaires terrestres, aériennes et navales. L'effet psychologique de ces opérations est déterminant : en plus d'affecter stratégiquement la capacité des autorités à réagir, les attaques cybernétiques peuvent atteindre le moral de la population en soulignant l'incapacité des autorités à maîtriser la situation[124]. Le conflit géorgien de 2008, premier exemple d'attaques cybernétiques coïncidant avec des opérations militaires conventionnelles, semble avoir amorcé une nouvelle ère dans la conduite de la guerre. En ce sens, le Sénateur Bockel estime « [qu']il semble acquis [...] que l'on ne peut guère concevoir désormais de conflit militaire sans qu'il s'accompagne d'attaques sur les systèmes d'information[125] ». Le chapitre suivant étudie les vulnérabilités potentielles des systèmes d'information à la fois civils et militaires pour les forces terrestres.

[124] Fred Schreier, "The Report on Cyberwarfare", DCAF, 2012, p. 112.

[125] Jean-Marie Bockel, « La cyberdéfense : un enjeu mondial, une priorité nationale », Rapport d'information fait au nom de la Commission des affaires étrangères, de la défense et des forces armées, du Sénat n° 681, enregistré à la Présidence du Sénat le 18 juillet 2012, p. 36.

CHAPITRE 2

MENACES PESANT SUR LES FORCES TERRESTRES

Du drone envoyant aux troupes au sol son flux ininterrompu d'images, De la remontée automatique des positions des mobiles par GPS couplé aux réseaux (*Blue Force Tracking*) au système FELIN (fantassin à équipement et liaisons intégrés), l'efficacité des forces terrestres repose sur la mise en réseau. La sécurité et la protection des systèmes d'information et de communication (SIC) sont fondamentales. Dans ce cadre, ce chapitre explore la question de la vulnérabilité des forces terrestres liée au cyberespace.

Néanmoins, la vulnérabilité des SIC de l'armée de Terre ne doit pas être isolée du sujet plus large de la vulnérabilité des systèmes d'information à l'échelle interarmées, interalliés et interministériel. Une attaque visant une entreprise, une industrie de défense ou un système allié interconnecté peut en effet atteindre les forces terrestres françaises. Bertrand Boyer souligne la porosité de la frontière entre le militaire et le civil et précise :

> « *Le militaire, détenteur légitime de la force, doit [...] agir sur l'ensemble des réseaux et des infrastructures existantes (propriétés d'entreprises privées) dont dépendent non seulement sa chaîne de commandement mais également les principales fonctions régaliennes. La frontière entre le monde militaire et le civil devient poreuse, de nouvelles interactions sont à définir, encadrer et contrôler afin de garantir un meilleur niveau de coopération*[126] ».

Dans cette logique, les menaces portant sur les systèmes civils et duals (section 21) ainsi que la question des vulnérabilités potentielles des systèmes militaires utilisés par les forces terrestres (section 22) seront développées. Une réflexion sur la menace représentée par le personnel de la Force sera également menée à travers les questions de l'hygiène cybernétique et de l'utilisation d'Internet en opérations (section 23).

21 – MENACES PORTANT SUR LES SYSTÈMES CIVILS ET LES SYSTÈMES DUALS

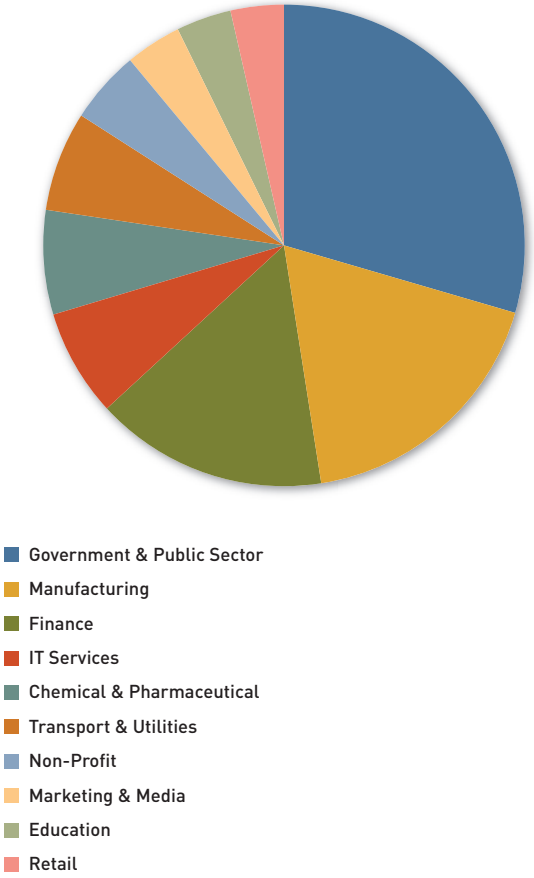
> « *La récurrence actuelle de ces intrusions, notamment par des États, donne à penser que des informations sont méthodiquement collectées pour rendre possible, dans une situation de conflit, une attaque de grande envergure. Une telle attaque serait susceptible de paralyser des pans entiers de l'activité du pays, de déclencher des catastrophes technologiques ou écologiques, et de faire de nombreuses victimes. Elle pourrait donc constituer un véritable acte de guerre*[127] ».
>
> Livre Blanc sur la Défense
> et la Sécurité Nationale 2013

Tous les secteurs d'activité sont concernés par les attaques informatiques, néanmoins le secteur public et gouvernemental est de loin le plus ciblé (plus d'un tiers des attaques recensées par l'éditeur de solutions informatiques de sécurité Symantec visait ce secteur en 2012).

[126] Bertrand Boyer, *Cyberstratégie - l'art de la guerre numérique*, Paris, Nuvis, 2012, p. 86.

[127] Livre Blanc Défense et Sécurité Nationale 2013, p. 49.

Attaques ciblées par secteur d'activité



Source : Symantec, conférence « Stuxnet, Duqu, Flame et autres maliciels : nouvelles armes informatiques ? », 21 mars 2013, Paris.

Les menaces portant sur les systèmes civils, et les systèmes duals seront présentées successivement. Néanmoins, le lecteur pourra se référer à une analyse plus complète dans le rapport du Sénateur Bockel sur la cyberdéfense[128], ou encore aux ouvrages de Bertrand Boyer[129] ou de Stéphane Dossé et Olivier Kempf[130].

211 – Menaces sur les infrastructures critiques civiles

Dans les sociétés hautement numérisées, les attaques cybernétiques peuvent causer des effets majeurs en visant des systèmes industriels, de régulation du trafic aérien, ferroviaire ou routier, ou encore des réseaux de distribution d'eau ou d'électricité. L'OTAN, cible de centaines d'attaques cybernétiques quotidiennes[131], considère la menace cyber comme un nouveau défi de sécurité pour les 900 millions de ressortissants de ses pays membres. L'organisation précise, dans son nouveau concept stratégique :

> « *Les cyberattaques augmentent en fréquence, sont mieux organisées et causent des dommages plus coûteux aux administrations, aux entreprises, aux économies, voire aux réseaux de transport et d'approvisionnement ou autres infrastructures critiques ; elles risquent d'atteindre un seuil auquel la prospérité, la sécurité et la stabilité des États et de la zone euro-atlantique pourraient être mises en danger*[132] ».

L'Alliance met ainsi en évidence la nécessité de prendre en compte les menaces cybernétiques pesant sur les systèmes civils, en particulier sur les Opérateurs d'Importance Vitale (OIV) (ou *critical infrastructures* dans la littérature anglo-saxonne). Dans cette même approche, le Livre Blanc sur la Défense et la Sécurité Nationale (LBDSN) 2013 mentionne les « activités d'importance vitale pour le fonctionnement normal de la Nation[133] » et considère comme relevant de la sécurité nationale « les tentatives de pénétration de réseaux numériques à des fins d'espionnage, qu'elles visent les systèmes d'information de l'État ou ceux des entreprises[134] ». Cinq années plus tôt, le LBDSN de 2008 avait qualifié de stratégique la cyber-menace, le dysfonctionnement ou l'indisponibilité de certaines infrastructures critiques hautement dépendantes de l'informatique pouvant entraîner l'arrêt de services

[128] Jean-Marie Bockel, « La cyberdéfense : un enjeu mondial, une priorité nationale », Rapport d'information fait au nom de la Commission des affaires étrangères, de la défense et des forces armées, du Sénat n° 681, enregistré à la Présidence du Sénat le 18 juillet 2012.

[129] Bertrand Boyer, *Cyberstratégie - l'art de la guerre numérique*, Paris, Nuvius, 2012.

[130] Stéphane Dossé et Olivier Kempf (dir.), *Stratégies dans le cyberespace*, Paris, L'esprit du livre, 2011.

[131] OTAN, « Briefing : l'OTAN face aux nouveaux défis de sécurité » (Référence BRIEF11TNSFRE - 0527-11 NATO Graphics & Printing), 2011, p. 9.

[132] Concept stratégique pour la défense et la sécurité des membres de l'Organisation du Traité de l'Atlantique Nord adopté par les chefs d'État et de gouvernement au sommet de l'OTAN à Lisbonne, les 19 et 20 novembre 2010, p. 12-13, par. 12.

[133] Livre Blanc Défense et Sécurité Nationale 2013, p. 106.

[134] Livre Blanc Défense et Sécurité Nationale 2013, p. 45.

essentiels à la vie quotidienne ou à la sécurité des citoyens[135]. Leurs conséquences peuvent indirectement peser sur les forces terrestres. Parallèlement, les attaques cybernétiques visant un système militaire atteignent souvent de nombreux systèmes civils. La question de la cyberdéfense doit donc dépasser le seul angle militaire.

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), créée en 2009, est une autorité au service des pouvoirs publics et des entreprises chargée de la défense et de la sécurité des systèmes d'information. Elle a publié un document de stratégie nationale en février 2011 préconisant comme une priorité le renforcement des infrastructures vitales nationales[136]. La définition des infrastructures vitales nationales n'y est pas donnée, ni leur liste établie publiquement, la France conserve ainsi une indépendance de décision et une souveraineté dans le choix de l'action à mener en réponse à une éventuelle attaque visant une infrastructure critique. En 2011, le site Internet de l'Élysée ou encore les réseaux du Ministère des Finances ont été pénétrés avant la réunion du G20[137] ; ces attaques cybernétiques menées contre des institutions régaliennes peuvent être considérées comme des attaques contre des infrastructures critiques. Les autorités n'ont pas ouvertement communiqué sur la réponse apportée à ces attaques, ni sur les dommages causés.

Une des premières attaques cybernétiques sur une infrastructure critique fut menée pendant la Guerre froide en 1982. Le président Ronald Reagan avait alors approuvé une attaque de la *Supervisory Control and Data Acquisition* sur le système des pipelines russes en Sibérie[138]. L'attaque provoqua une explosion majeure et eut pour conséquence de perturber l'approvisionnement en gaz pendant près d'un an, et par ricochet d'influer sur les échanges commerciaux en énergie de la Russie[139]. En 2008, une autre opération dans le cyberespace a eu des effets majeurs : l'attaque cybernétique menée par la Russie contre les infrastructures Internet de la Géorgie par déni de service rendit inaccessibles les sites gouvernementaux. Cette attaque imposa également à la Banque Nationale du pays la coupure de ses connexions Internet, interrompant toute transaction financière pendant dix jours[140]. Plus récemment, en avril 2013, le piratage du compte *Twitter d'Associated Press* annonçant une explosion à la Maison Blanche et revendiqué par l'Armée Syrienne Libre (soutien du régime de Bashar El-Assad) a directement impacté l'économie américaine sur une courte période[141].

On peut aisément imaginer des effets directs sur les infrastructures, sur leur fonctionnement, jusqu'à leur destruction. Infiltrer une centrale nucléaire, comme dans le cas de la centrale iranienne de Natanz, un réseau de contrôle aérien, pourrait entraîner la paralysie de certains pans d'activité de nos sociétés hautement dépendantes de la technologie. En 2012, une attaque informatique a visé deux entreprises du secteur de l'énergie au Moyen-Orient, dont Aramco, la plus grande entreprise de pétrole saoudienne ; le virus « Shamoon » avait pour but d'acquérir des identifiants et d'exfiltrer des informations. Il a finalement détruit 30 000 postes et serveurs[142].

---

135 Francis DELON, « Infrastructures critiques : le château de cartes numérique », *Défense, Enjeux de défense et de sécurité civils et militaires*, n° 160, janvier - février 2013, p. 4-5.

136 ANSSI, « Défense et sécurité des systèmes d'information : Stratégie de la France », Février 2011, p. 7 (accessible en suivant le lien : http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf).

137 Jean-Marie Bockel, « La cyberdéfense : un enjeu mondial, une priorité nationale », Rapport d'information fait au nom de la Commission des affaires étrangères, de la défense et des forces armées, du Sénat n° 681, enregistré à la Présidence du Sénat le 18 juillet 2012, p. 20.Voir également l'article « Bercy, l'Élysée et le Quai d'Orsay visés par une cyberattaque » du 7 mars 2011 (http://www.lepoint.fr/societe/bercy-l-elysee-et-le-quai-d-orsay-vises-par-une-cyberattaque-07-03-2011-1303652_23.php), ou encore l'article « L'Élysée confirme avoir été la cible d'une cyberattaque au cours des derniers mois » du 12 juillet 2012 (http://www.lemonde.fr/technologies/article/2012/07/12/l-elysee-confirme-avoir-ete-la-cible-d-une-cyberattaque-au-cours-des-derniers-mois_1732517_651865.html).

138 Paul Cornish, David Livingstone, Dave Clemente, Claire Yorke, "On Cyber Warfare", *Chatham House report*, novembre 2010, p. 6.

139 Soren Olson, "Shadow boxing: cyber warfare and strategic economic attack", *JFQ* Issue 66, 3rd Quarter 2012, p. 17.

140 Rosemary M. Carter, Brent Feick, Roy C. Undersander, "Offensive Cyber for the Joint Force Commander; it's Not That Different", *JFQ* Issue 66, 3rd Quarter 2012, p. 22.

141 Selon l'Observatoire du Monde Cybernétique de la Délégation aux Affaires Stratégiques (lettre N° 17 - Mai 2013, p. 2, disponible à l'adresse suivante : http://www.defense.gouv.fr/das/reflexion-strategique/observatoires/observatoire-du-monde-cybernetique), entre 13 h 08 et 13 h 10, le Dow Jones perdait 145 points, soit l'équivalent de 105 milliards d'euros de capitalisation. Voir également l'article « Le piratage du compte Twitter d'AP fait plonger Wall Street » (http://www.lemonde.fr/economie/article/2013/04/24/de main-une-cyberguerre-sur-les-marches_3165087_3234.html).

142 Laurent Heslault (Directeur des stratégies de sécurité – Symantec Europe du sud), « Stuxnet, Duqu, Flame et autres maliciels : nouvelles armes informatiques ? », conférence tenue le 21 mars 2013 à Paris et organisée par l'Association Nationale des Auditeurs Jeunes de l'IHEDN.

212 – Menaces sur les systèmes duals

Les systèmes duals sont des outils utilisés aussi bien dans le monde civil que dans les armées. La question de l'utilisation des systèmes duals par les forces armées est incontournable dans un contexte où nos adversaires « ne manquent pas d'imagination pour utiliser au mieux les produits disponibles. Ces produits sont le plus souvent directement issus du marché civil et au meilleur de la technologie[143] ».

Le système d'exploitation Windows est un système dual par excellence. Le Ministère de la Défense exploite les systèmes informatiques de l'éditeur américain. Or, ce système très utilisé dans le civil (approximativement 85 % du marché des systèmes informatiques exploite Microsoft Windows[144]) est exploitable pour conduire une attaque informatique à l'encontre des forces armées. En janvier 2009, les Rafales de la force d'action navale sont restés cloués au sol en raison d'une attaque informatique : le système de contrôle aérien sous Windows avait été infecté par le ver Win32/Conficker[145]. Le Ministère de la Défense est ainsi confronté au risque d'intrusion dans ses réseaux informatiques exploitant Windows. En avril 2013, le contrat liant le ministère à Microsoft a été remis en cause alors que la Direction Interarmées des Réseaux d'Infrastructures et des Systèmes d'Information de la Défense (DIRISI) était sur le point de reconduire avec lui un accord-cadre d'une durée de 4 ans portant sur le maintien en condition opérationnelle des systèmes informatiques du ministère de la Défense. La presse nationale a révélé les conclusions d'un rapport de la Direction Générale des Systèmes d'Information et de Communication (DGSIC) qui soulignait le risque de perte de souveraineté nationale vis-à-vis des États-Unis en raison de l'introduction de portes dérobées (*backdoors*) par la NSA (*National Security Agency*) dans les logiciels exportés[146]. Ainsi, les réseaux des forces armées françaises seraient depuis de nombreuses années vulnérables à des intrusions de la NSA. Ce rapport recommandait de se tourner vers des logiciels libres (leurs codes sources sont disponibles, contrairement à ceux de Microsoft qui sont confidentiels, notamment pour des raisons commerciales). Le Ministère est dépendant des choix industriels de Microsoft et en assure les coûts (hypothèse d'une migration de Windows XP en Windows 7).

Autre exemple de système dual : les SCADA (*Supervisory Control And Data Acquisition*) et les DCS (*Distributed Control Systems*), également appelés systèmes de contrôle-commande et/ou de supervision, ou systèmes industriels. Ils sont un ensemble de capteurs, de réseaux, de serveurs embarqués et de stations d'administration et permettent la maintenance de systèmes informatiques tout en contrôlant en temps réel des milliers de paramètres dans des domaines variés : sécurité classique, stockage, production électrique, etc. Ils sont utilisés pour la télégestion d'infrastructures à grande échelle telles que des centrales électriques.

Crédits : J.-J. Chatard, DICoD.

Ces systèmes présentent des intérêts pour de potentiels attaquants : d'une part ils protègent des systèmes sensibles, leur altération peut donc entraîner des dommages importants, d'autre part ils sont souvent reliés aux réseaux locaux et Internet et leur accès par un tiers en est facilité. Stuxnet a contourné la difficulté de l'accès et compromis des SCADA

143 Xavier Favreau, Philippe Koffi, Pierre Schanne, Éric Waringhem, « Capacités militaires, innovation et technologies », *Revue Défense Nationale*, juin 2013, n° 761, p. 20.

144 Brian Weeden, "Cyber offense and defense as mutually exclusive national policy priorities", in "Confronting Cyberconflict", UNIDIR, Geneva, 2011, p. 20. biblio : p. 19-30. Article disponible à l'adresse suivante : http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ord587=grp2&ots591=eb06339b-2726-928e-0216-1b3f15392dd8&lng=en&id=143276

145 Michel Baud, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », IFRI, *Politique étrangère,* 2012, n° 2, p. 310.

146 Anonyme, « Un contrat entre Microsoft et le ministère de la Défense fait jaser », 21 avril 2013, accessible en suivant le lien http://www.opex360.com/2013/04/21/un-contrat-entre-microsoft-et-le-ministere-de-la-defense-fait-jaser/

Valise de téléopération du système de jumelles infrarouges multifonctions long range (JIM LR).
Crédit : G. Gesquière, Sirpa Terre

déconnectés d'Internet par une pénétration physique des locaux par des agents de renseignement israéliens[147]. Cela montre que les systèmes informatiques industriels présentent des vulnérabilités dont les conséquences peuvent être importantes[148].

La menace sur les forces terrestres est réelle, prenons l'exemple de jumelles infrarouge. En 2011, la DGA a conclu un contrat avec Sagem portant sur l'acquisition de 1175 jumelles infrarouges multifonctions longue portée (JIM LR 2) dans le cadre du programme JIR-TTA-NG (Jumelles infrarouges toutes armes de nouvelle génération)[149]. Ces jumelles permettent la détection des menaces, la désignation des cibles et le renseignement au profit du commandement et des unités de contact en présentant les fonctionnalités suivantes : vision jour et thermique, télémétrie, pointeur laser, compas, GPS et transmissions de données.

Utilisation d'une jumelle infrarouge multifonctions long range (JIM LR) posée sur une plate-forme motorisée et télécommandable fixée sur trépied.
Crédit : G. Gesquière, Sirpa Terre

L'industriel Thales possède des caméras thermiques similaires (modèle SOPHIE). Ces matériels sont gérés par un service *smartfleet*[150] permettant de choisir les équipements les plus appropriés, et de traiter à distance le niveau de batterie ou encore de constater

147 Observatoire du monde cybernétique (DAS), Lettre n° 6, juin 2012, p. 7.

148 Agence Nationale de la Sécurité des Systèmes d'Information, « Maîtriser la SSI pour les systèmes industriels – La cybersécurité des systèmes industriels », version 1.0, juin 2012, p. 13-14, disponible à l'adresse suivante : http://www.ssi.gouv.fr/IMG/pdf/Guide_securite_industrielle_Version_finale.pdf

149 *DSI*, février 2011, n° 67, p. 11.

150 Interview de Gilles Rousset, directeur Stratégie & Marketing Services, Thales, 29 mai 2013, disponible en suivant le lien http://forcesoperations.com/2013/05/29/fob-interview-gilles-rousset-directeur-strategie-marketing-services-thales/

de dysfonctionnement de chaque équipement. Ce système permet de réduire les coûts de logistique et de maintenance en suivant au plus près le cycle de vie des matériels. Néanmoins, un éventuel attaquant pourrait utiliser ce système de gestion à distance opéré par l'industriel comme support à une attaque cybernétique. Par le biais d'un code informatique, il pourrait en effet modifier les données du système *smartfleet* et indirectement atteindre les forces terrestres déployées (il pourrait par exemple faire recharger les batteries des jumelles à un niveau très inférieur que celui indiqué normalement par le système *smartfleet*).

Les systèmes industriels sont le résultat de projets menés en moyenne sur une vingtaine d'années. Ainsi, lorsque les systèmes sont déployés ils sont souvent déjà vulnérables sur le plan SSI. Olivier Barré, directeur commercial chez Cassidian, l'explique ainsi : « faire simple, c'est très compliqué [...] : le jour où le logiciel est livré, il est déjà potentiellement périmé. Le problème de la mise à jour devient celui de l'industriel[151] ». La solution serait de développer des *packages* de services inclus dans les contrats souscris par le Ministère de la Défense, incluant ainsi dans l'achat de systèmes industriels un volume de conseil et de mises à jour à la charge de l'industriel[152]. Outre atlantique, l'*U.S Army* travaille à la réduction du temps de conception des systèmes IT[153] par les industries de défense (estimé en moyenne sept ou huit ans) pour parvenir à des cycles de développement technologiques classiques d'une à deux années[154].

L'utilisation de systèmes duals dans les forces armées présente des avantages certains. En ce qui concerne l'exploitation du système Windows par le Ministère de la Défense, d'une part l'accord-cadre signé par le Ministère avec Microsoft permet de bénéficier des mises à jour des programmes fournis par Microsoft, d'autre part le Ministère doit investir de façon moins importante dans la formation des utilisateurs des logiciels Microsoft dans la mesure où ils sont habitués à utiliser ces systèmes dans la sphère privée. Ceci ne signifie pas pour autant que les utilisateurs ne doivent pas être informés et sensibilisés aux menaces. Plus généralement, l'utilisation de systèmes civils pour équiper des systèmes militaires (notamment les véhicules et aéronefs) permet de réaliser des économies d'échelle importantes. Quant aux industries de défense, selon Xavier Favreau, Philippe Koffi, Pierre Schanne et Éric Waringhem, travaillant à la DGA[155], une « interaction permanente entre les sphères de l'action opérationnelle, de l'industrie d'armement et de l'innovation technologique constitue l'un des défis permanents d'une puissance militaire moyenne mais complète comme la France qui ne peut se permettre de tout essayer mais dispose de véritables capacités propres pour patrouiller les nouvelles frontières technologiques de l'engagement militaire[156] ».

Les menaces sur les systèmes civils et duals sont essentiellement mises à exécution par le biais d'Internet (déni de service, *phishing*). Il convient donc de maintenir autant que possible un isolement des systèmes militaires vis-à-vis du web.

22 – MENACES PORTANT SUR LES SYSTÈMES MILITAIRES UTILISÉS PAR LES FORCES TERRESTRES

Les SIC ainsi que l'informatique embarquée, les systèmes de préparation des missions et les systèmes d'armes utilisés par les forces terrestres sont interconnectés. Sur le terrain, le réseau *Land War Net* utilisé par les forces armées américaines est indispensable pour des domaines tels que le *command and control*, les communications, l'acquisition de données et la transmission, le renseignement, le *situational awareness*, le ciblage, la logistique, les appels pour évacuation médicale, ou encore pour

[151] Romain Mielcarek, « Transmissions "Do you speak SIC?!" », *DSI*, n° 87, décembre 2012, p. 47.

[152] Romain Mielcareck, « Transmissions "Do you speak SIC?!" », *DSI*, n° 87, décembre 2012, p. 47.

[153] Information technologies.

[154] James G. Stavridis, Elton C. Parker III, « Sailing the cyber sea », *JFQ*, Issue 65, 2nd Quarter 2012, p. 66.

[155] Xavier Favreau est architecte de capacités auprès de l'architecte de système de force Commandement et maîtrise de l'information de la DGA ; Philippe Koffi est architecte de capacités auprès de l'architecte de système de force engagement-combat de la DGA ; Pierre Schanne est chargé de mission innovation auprès du directeur de la stratégie de la DGA ; enfin, Éric Waringhem est le Directeur du centre d'analyse technico-opérationnelle de défense (CATOD) de la DGA.

[156] Xavier Favreau, Philippe Koffi, Pierre Schanne, Éric Waringhem, « Capacités militaires, innovation et technologies », *in Revue Défense Nationale*, juin 2013, n° 761, p. 21.

rester en contact avec les familles[157]. En France, la numérisation de l'espace de bataille (NEB) des forces terrestres devrait être achevée à l'horizon 2020. La NEB correspond à la mise en œuvre sur le champ de bataille de techniques et de procédures garantissant au chef qu'il bénéficiera de la bonne information pour décider et agir plus vite que l'adversaire, en permettant notamment que l'information soit disponible à tous les niveaux de la hiérarchie. Elle concerne – du plus haut au plus bas niveau de commandement – le système d'information et de commandement des forces (planification et conception), le système d'information régimentaire (coordination et mise en œuvre) et le système d'information terminaux (niveau exécution de la manœuvre).

L'ensemble de ces systèmes présente des vulnérabilités sur trois plans : technique, procédural et humain, en gardant néanmoins à l'esprit qu'une vulnérabilité technique ne devient une vulnérabilité qu'à partir du moment où l'ennemi a les capacités opérationnelles de l'exploiter. La section 22 propose un aperçu des menaces éventuelles sur les systèmes de commandement et les capacités de la force.

221 – Menaces sur les systèmes « C2 » (commandement et contrôle)

L'action hostile dans le cyberespace, comme toute action militaire, accordera la priorité à l'attaque d'une cible à haute valeur ajoutée. Attaquer un poste de commandement et ses systèmes de communication permettrait d'interrompre la transmission d'ordres, la logistique d'une mission, et ainsi de paralyser une force pendant un certain temps dépendant de la capacité de réaction cyber de la force ciblée. En effet, les forces exploitent des terminaux d'information tactique qui accueillent un logiciel opérationnel de conduite au combat, ces systèmes permettent par liaison satellite de localiser les combattants sur un *pad*[158] (il s'agit d'un système de commandement type *blue-force tracking*) (certains systèmes permettent de connaître instantanément les capacités opérationnelles des véhicules amis en termes d'armement et de carburant).

Terminal d'information tactique qui accueille le logiciel opérationnel de conduite au combat.
Crédits : P. Hilaire, Sirpa Terre.

Si ces systèmes permettent au chef de faire évoluer son déploiement tactique en optimisant son appréciation de la situation jusqu'au plus petit niveau tactique, et ainsi d'accélérer le processus de décision, ils peuvent constituer un danger : en cas d'infiltration, un ennemi pourrait manipuler les données sur lesquelles le chef fonde sa décision dans le but de l'amener à agir en sa faveur.

Le chef de section est sur le terminal d'accueil du logiciel opérationnel de conduite au combat dans un AMX 10 RC.
Crédits : P. Hilaire, Sirpa Terre.

[157] Susan S. Lawrence, LTG, "Land War Net: Powering America's Army In a Joint, Interagency, Intergovernmental And Multinational Environment", *The Magazine of the Association of the United States Army*, October 2012, p. 185.

[158] Philippe Langloit, « Au cœur de la spatio dépendance : la navigation par satellite », *DSI Hors-Série*, février-mars 2013, n° 28, p. 28.

Un officier met à jour les situations ennemies sur le terminal d'accueil du logiciel opérationnel de conduite au combat dans un VAB.
Crédits : P. Hilaire, Sirpa Terre.

Attaque des réseaux de communication

Les forces communiquent par le moyen de trois supports : radio, ondes hertziennes et liaisons satellites ; elles exploitent tout le spectre radioélectrique. Un adversaire pourrait ainsi attaquer les réseaux de communication des forces terrestres afin de couper la chaîne de commandement entre le poste de contrôle et la force déployée. En infiltrant le système d'information et de commandement des forces (niveau brigade), un intrus pourrait causer le dysfonctionnement de la chaîne de commandement et compromettre le succès de la mission. Autre hypothèse, une attaque par cheval de Troie pourrait permettre à son auteur de voler des informations telles que des noms d'utilisateurs, mots de passe, frappes clavier, copies d'écran et ainsi d'accéder à des informations sensibles ou de manipuler les données. Ceci s'est produit récemment avec le code informatique Sofacy conçu pour attaquer des cibles militaires[159].

La menace d'une attaque des réseaux de communication est vraisemblablement la plus sérieuse en ce qu'elle peut avoir des conséquences directes au niveau tactico-opératif. Cette attaque peut être réalisée par la destruction physique des antennes, des câbles, ou par des actions entreprises dans le cyberespace telles que l'injection d'un virus dans le système informatique, ou enfin par le brouillage électromagnétique. En rendant les communications sur les trois supports inopérantes, l'attaquant aurait le pouvoir de désorganiser la force et de gagner du temps pour obtenir un avantage sur le terrain.

Pour ces raisons, il semble indispensable de préserver un certain nombre de procédures dégradées dans le cadre de la formation de nos forces et des exercices (en incluant des scénarii cyberincident dans les exercices majeurs) pour rendre automatiques les schémas de réponse à une attaque cyber-

[159] Des organisations militaires européennes ont soumis deux documents qui leur semblaient suspects à Symantec. Ces documents utilisaient des « exploits » (morceaux de logiciel exploitant une faille dans le logiciel cible pour pouvoir s'y propager, par exemple message avec une pièce jointe ou un lien, cheval de Troie volant des noms d'utilisateur, des frappes clavier, des mots de passe, des copies d'écran). Les données sont exfiltrées par mail ou internet. Source : Laurent Heslault (Directeur des stratégies de sécurité – Symantec Europe du sud), « Stuxnet, Duqu, Flame et autres maliciels : nouvelles armes informatiques ? », conférence tenue le 21 mars 2013 à Paris et organisée par l'Association Nationale des Auditeurs Jeunes de l'IHEDN.

nétique de la même manière que le fantassin répète les déplacements tactiques par le *drill*. Certains auteurs suggèrent que cet entraînement soit effectif sur le terrain dès le niveau de l'unité, en développant des exercices incluant le soldat afin de remplir la mission même en subissant une attaque cybernétique[160]. Ces schémas de réponse devraient être conçus pour parer une attaque par déni de service de courte durée jusqu'à des menaces persistantes sophistiquées incluant la menace électromagnétique.

Le commandant du *U.S Army Cyber Command*, le Lieutenant-Général Hernandez, souligne la nécessité d'intégrer la dimension cyber dans la formation et l'entraînement des forces. Il insiste sur la capacité d'opposition dans le cyberespace des « unités cybernétiques défendant les réseaux, fournissant un effet de domination dans le cyberespace, rendant possible le commandement de la mission, et assurant un avantage global décisif[161] ».

Infiltration des systèmes de stockage et d'exploitation des données

Infiltrer des sites sécurisés appartenant aux forces armées pourrait permettre à un attaquant de récupérer des données sensibles. Entre 2003 et 2005, des *hackers* ont pénétré des sites sécurisés appartenant aux forces armées américaines et y ont dérobé des informations permettant d'en évaluer les méthodes, procédures et techniques (ces attaques provenaient vraisemblablement de Chine, même si le gouvernement chinois a nié tout lien avec ces actes)[162].

222 – Menaces sur les capacités de la force

Menaces (directes et indirectes) sur les systèmes d'armes

- Menaces directes

Les SIC sont intégrés dans les systèmes d'armes, les outils de maintenance, et plus généralement dans l'environnement proche des plateformes de combat[163]. Les systèmes d'armes intègrent désormais quasi systématiquement de l'informatique, de l'hélicoptère Tigre au système ATLAS. Prenons l'exemple d'un véhicule de l'avant blindé : les calculateurs des différents systèmes (système GPS, système motorisation, système de communication) sont interconnectés. Ils le sont aussi avec les systèmes de préparation des missions et les systèmes de maintenance (qui sont souvent des systèmes industriels, *cf.* l'exemple des jumelles infrarouges multifonctions longue portée[164]) constituant ainsi un point d'entrée pour atteindre un système d'arme exploité par les forces terrestres.

Un radio tireur est sur le terminal d'accueil du LOCC dans un VAB.
Crédits : P. Hilaire, Sirpa Terre

160 Michael J. Lanham, Lieutenant-colonel, « When the network dies », *Armed Forces Journal*, décembre 2012.

161 Rhett A. Hernandez, LTG., "U.S. Army Cyber Command: Cyberspace for America's Force Of Decisive Action", *The Magazine of the Association of the United States Army*, October 2012, p. 208.

162 Assemblée européenne de sécurité et de défense, « La guerre informatique », document C/2022, 5 novembre 2008, par. 141, p. 19.

163 Xavier Favreau, Philippe Koffi, Pierre Schanne, Éric Waringhem, « Capacités militaires, innovation et technologies », in *Revue Défense Nationale*, juin 2013, n° 761, p. 22.

164 Voir *supra* « *212 – Menaces sur les systèmes duals* », relatif aux menaces sur les systèmes de commandement et de contrôle.

- Menaces indirectes : espionnage industriel et intrusions sur sites sensibles

Les menaces sur les systèmes d'armement peuvent également être indirectes. L'espionnage industriel demeure en effet un risque sérieux pour tous les programmes d'armement, les industriels de défense pouvant constituer un point d'entrée pour atteindre les capacités de la force. En 2009, l'industriel Lockheed Martin a subi une intrusion dans ses réseaux, les *hackers* se sont emparés de plus de 24 000 dossiers confidentiels concernant l'avion F-35 *Joint Strike Fighter*[165]. Ils ont obtenu des informations sensibles sur les capteurs et les systèmes informatiques de l'appareil. Cette menace pèse sur les industriels de défense ainsi que sur les sous-traitants moins bien protégés et donc plus vulnérables. La Chine orienterait ainsi vers eux sa stratégie d'espionnage industriel[166]. Aussi, il est indispensable pour les gouvernements d'apporter de l'aide aux entreprises victimes d'attaques cybernétiques et de développer des partenariats public-privé afin de protéger certains intérêts.

En 2013, les autorités américaines ont révélé avoir subi des attaques cybernétiques orchestrées par la Chine, des *hackers* auraient accédé à des réseaux sécurisés et dérobé des documents relatifs au design de systèmes d'armes de haute technologie tels que le THAAD[167], le F/A-18, ou encore l'hélicoptère *Blackhawk*[168]. Pour la première fois, l'administration américaine a publiquement identifié la Chine comme étant responsable de ces intrusions[169].

Crédits : Le Monde.fr[170]

Menaces sur les capteurs

L'auteur de l'attaque informatique peut orienter son action sur les systèmes de capteurs de l'adversaire afin de le rendre sourd et aveugle. Ce résultat pourrait être atteint par le *hacking* de ses systèmes de capteurs (système de défense antiaérienne, système FELIN). C'est la finalité du Programme SUTER développé par les Américains : le programme lance un virus opérant au niveau du système de combat en utilisant le retour des ondes radars que le système adverse émet (il ne s'agirait pas d'une action de guerre cybernétique à proprement parler, mais d'une action de guerre électronique)[171]. Ce programme a

165 Anonyme, "Hype and fear", *The Economist*, 8 décembre 2012, disponible à l'adresse suivante : http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may

166 Ellen Nakashima, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies", *The Washington Post*, 28 mai 2013 (http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html). Un représentant officiel de l'entreprise Lockheed Martin aurait déclaré que l'entreprise « passe plus de temps à solutionner les attaques visant la chaîne d'approvisionnement » de partenaires, sous-contractants et fournisseurs qu'à s'occuper d'attaques visant directement l'entreprise (traduction de l'auteur à partir de l'article d'Ellen Nakashima).

167 *Terminal High Altitude Area Defense*.

168 Ellen Nakashima, « Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies », *The Washington Post*, 28 mai 2013. Voir aussi Sylvain CYPEL, « Les plans des fleurons de la défense américaine aux mains de cyberespions chinois », *LeMonde.fr*, 29 mai 2013, http://www.lemonde.fr/international/article/2013/05/29/les-plans-des-fleurons-de-la-defense-americaine-aux-mains-de-cyberespions-chinois_3420002_3210.html.

169 Ernesto Londono, « Pentagon: Chinese government, military behind cyberspying », *The Washington Post*, 7 mai 2013 (http://www.washingtonpost.com/world/national-security/pentagon-chinese-government-military-behind-cyberspying/2013/05/06/f4851618-b694-11e2-b94c-b684dda07add_story.html)

170 Infographie réalisée par le site Internet du Monde (http://www.lemonde.fr/technologies/infographie/2013/06/08/les-intrusions-informatiques-dont-la-chine-est-accusee_3426462_651865.html).

171 Joseph Henrotin « Conséquences tactiques du hacking radar », *DSI*, février 2013, n° 89, p. 98-103. L'auteur explique que Suter utilise le retour des ondes radars produit par le système de l'adversaire et lance par ce biais un virus opérant au niveau non de l'antenne radar elle-même mais bien du système de combat ; il est alors techniquement possible de réaliser diverses opérations, notamment inventer des plots radars fictifs, manipuler les capteurs, ou encore voir ce que le contrôleur aérien adverse voit.

été mis en œuvre avec succès par les israéliens en septembre 2007 dans l'opération ORCHAD : ces derniers estimaient que la Syrie construisait un réacteur nucléaire à Dayr ez-Zor et ont décidé de lancer une opération visant à détruire les infrastructures. Les avions des forces israéliennes ont pénétré sur le territoire syrien et en sont ressortis sans avoir été détectés par le système de défense aérienne intégré syrien, paralysé par le système SUTER[172].

Il faut noter que l'armée de Terre exploite relativement peu de systèmes de capteurs type sonar (comparé à l'armée de l'Air et la Marine nationale). Néanmoins, elle utilise de nombreux systèmes de capteurs intégrés dans les systèmes d'armes ainsi que des systèmes de renvoi d'images. Aussi, la menace sur les capteurs pèse sur les forces terrestres au même titre que sur les forces armées aériennes et navales.

Par ailleurs, une attaque cybernétique orientée vers les systèmes de capteurs d'appareils tels que des robots terrestres, ou des drones est une hypothèse plausible. En Irak, les drones américains *Predator* ont été infiltrés par les insurgés : à l'aide d'un logiciel gratuit téléchargé depuis Internet pour quelques dollars, ils ont intercepté les données émises par les drones et plus précisément les vidéos qui n'étaient pas cryptées[173]. En 2011, un virus informatique a infecté les postes de commande à distance des drones *Predator* et *Reaper* mis en œuvre par les Américains et effectuant des missions en Afghanistan et sur d'autres théâtres. Le virus aurait été introduit dans les ordinateurs de la base via des disques durs externes[174]. Plus récemment, en 2012, un drone civil aurait été piraté par des chercheurs de l'université du Texas grâce à du matériel d'une valeur de 1 000 $[175]. Ainsi, ces systèmes présentent des vulnérabilités exploitables. Si l'armée de Terre ne met pas en œuvre de drones armés, elle utilise néanmoins plusieurs drones en appui de ses opérations[176], susceptibles de la rendre également vulnérable.

Menaces sur les systèmes de navigation

Les systèmes de navigation par satellite, également appelés GNSS (*Global Navigation Satellite System*) sont une capacité que les armées doivent détenir de façon permanente, autonome et sécurisée. Ils sont presque systématiquement intégrés dans les systèmes militaires : le *blue-force tracking*, la quasi-totalité des systèmes d'armement utilisent le signal GPS pour naviguer et atteindre des cibles avec précision ou donner une référence de temps pour synchroniser les équipes et équipements[177]. C'est la raison pour laquelle l'intégrité, la fiabilité et la continuité des récepteurs sont essentielles pour le succès des opérations militaires.

On pourrait ainsi envisager la volonté d'un adversaire d'altérer les signaux GPS ; en changeant le référentiel coordonnées satellites d'un point, un attaquant pourrait confondre les positions amies et ennemies des forces terrestres déployées. Les conséquences aux niveaux tactique et opérationnel pourraient être considérables et cette menace semble plausible. Toutefois, une telle manœuvre par l'altération des signaux GPS est techniquement complexe, seuls les États-Unis semblent en mesure de réaliser cette procédure à court terme : ils installent actuellement une nouvelle flotte de satellites ayant vocation à émettre un signal uniquement pour leurs forces armées[178] ; on peut déduire de cette politique la capacité des États-Unis à modifier le signal GPS civil (exploité par les autres États et systèmes civils) tout en conservant les coordonnées exactes pour leurs forces armées. Le système de *Nav War* développé par les États-Unis et l'OTAN s'inscrit dans cette logique en

---

172 Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, Vol. 35, n° 1, p. 16-17. Voir également Joseph Henrotin, « Conséquences tactiques du hacking radar », *DSI*, février 2013, n° 89, p. 98-103.

173 Michel Baud, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Politique étrangère*, 2012, n° 2, p. 310-311.

174 Jean-Marie Bockel, « Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense », n° 681, enregistré à la Présidence du Sénat le 18 juillet 2012, p. 31.

175 Observatoire du Monde Cybernétique, *DAS*, lettre N° 7, juillet 2012, p. 3, disponible à l'adresse suivante : http://www.lemonde.fr/technologies/article/2012/07/12/l-elysee-confirme-avoir-ete-la-cible-d-une-cyberattaque-au-cours-des-derniers-mois_1732517_651865.html

176 L'armée de Terre possède actuellement trois types de drones : le SDTI, « système de drone tactique intérimaire » mis en œuvre par le 61e régiment d'artillerie ; le DRAC, « drone de reconnaissance au contact » à disposition des batteries de renseignement de brigades armés, et le DROGEN « drone du génie ».

177 Paul de Geyer d'Orth, Capitaine de frégate, « Les enjeux des systèmes militaires de navigation par satellite », *Les Carnets du Temps*, n° 94, février 2013, p. 10-11. Le Capitaine de frégate de Geyer d'Orth est chef de section position navigation et temps au sein du Commandement interarmées de l'espace.

178 Capitaine de frégate Paul de Geyer d'Orth, « Les enjeux des systèmes militaires de navigation par satellite », *Les Carnets du Temps*, n° 94, février 2013, p. 11.

permettant le brouillage des signaux GNSS ouverts et donc l'interdiction à l'ennemi d'utiliser ces signaux à son profit[179]. Ainsi, en plus de la menace conventionnelle de neutralisation des stations satellites au sol, il existe désormais une menace d'attaque cybernétique sur les données des systèmes GPS.

La menace d'une attaque cybernétique existe d'autant plus dans un contexte de numérisation de l'espace de bataille qui accroît les vulnérabilités techniques et humaines des forces dont les opérations reposent en grande partie sur ce système. Toutefois, ces réseaux informatiques étant fermés – c'est-à-dire internes à la force – les risques de pénétration sont donc limités. Au niveau tactique il faut garder à l'esprit qu'un attaquant aura toujours plus intérêt à attaquer directement un véhicule de l'avant blindé de la force qu'à conduire une attaque cybernétique contre celui-ci. Autrement dit, au niveau tactique, la menace d'une attaque cybernétique est moins prégnante que celle d'une attaque directe, « physique ». En revanche, un ennemi aura toujours intérêt à attaquer des cibles à haute valeur ajoutée au niveau tactico-opératif, voire stratégique. De telles attaques pourraient entraîner une paralysie de la force (en visant notamment les réseaux sur le théâtre d'opération, les points d'énergie, les systèmes de communication, les liaisons satellites, etc.) ; l'attaquant profiterait alors potentiellement d'un avantage militaire sur le plan tactique, opératif, et à court/moyen terme stratégique. La protection des systèmes de communication et de commandement apparaît donc comme une priorité absolue.

23 – MENACES REPRÉSENTÉES PAR LE PERSONNEL DE LA FORCE (cyberhygiène et utilisation Internet par le personnel en opérations)

Assurer l'intégrité, la fiabilité et la continuité des systèmes d'information utilisés par les forces terrestres est indispensable à la supériorité des forces. Il s'agit de limiter les vulnérabilités d'un programme en intégrant des procédures de contrôle et de veille tout au long de sa conception puis de son utilisation dans les forces. En effet, les menaces sur la force provenant du comportement des utilisateurs des systèmes informatiques existent et sont importantes, liées soit à une mauvaise utilisation de systèmes exploités soit à l'utilisation à titre personnel de l'Internet, en particulier des réseaux sociaux.

231 – Le non-respect des règles d'hygiène cybernétique

Il n'existe pas de statistiques en source ouverte concernant l'origine interne ou extérieure des attaques ou des vulnérabilités des systèmes informatiques du ministère de la Défense. Néanmoins dans la grande majorité des cas, les individus et entités malveillantes exploitent des failles ouvertes par un utilisateur n'ayant pas respecté un ou plusieurs principes de sécurité informatique. Les mécanismes les plus sophistiqués de prévention et de détection des menaces seront inopérants si le logiciel de détection des menaces installé sur le poste informatique n'est pas mis à jour, si le mot de passe de la session est par exemple « administrateur » ou si l'utilisateur n'a pas contrôlé sa clé USB dans une station blanche. Selon les experts en cybersécurité, 80 % des attaques informatiques peuvent être bloquées par une bonne hygiène informatique accompagnée de mesures de sécurité préventives. Quant aux 20 % des attaques restantes, les dispositifs de surveillance des réseaux et de détection des agressions (*firewall*, antivirus notamment) peuvent détecter 19 % d'entre elles[180]. Plusieurs employés de la DGA précisent :

« la plus ambitieuse des politiques d'équipements est inutile si l'enseignement de l'hygiène informatique n'est pas conduit : l'usager des systèmes demeurant, spécialement dans ce domaine, sa plus grande vulnérabilité… [181] ».

[179] Capitaine de frégate Paul de Geyer d'Orth, « Les enjeux des systèmes militaires de navigation par satellite », *Les Carnets du Temps*, n° 94, février 2013, p. 11.

[180] Luc-François Salvador, « Vers une approche systémique de la cybersécurité », *Revue de la Gendarmerie Nationale*, 4e trimestre 2012, p. 41. M. Salvador est Président-directeur général de Sogeti, membre du Comité exécutif du groupe Capgemini ; il est par ailleurs colonel de la réserve citoyenne de l'armée de l'Air et auditeur de l'IHEDN (49e session, 1997).

[181] Xavier Favreau, Philippe Koffi, Pierre Schanne, Éric Waringhem, « Capacités militaires, innovation et technologies », *Revue Défense Nationale*, juin 2013, n° 761, p. 23.

Aussi, il est nécessaire de sensibiliser les utilisateurs des systèmes informatiques à tous les niveaux. Le Général Boissan[182], commandant l'École des Transmissions, a identifié le non-respect des règles élémentaires de sécurité des systèmes d'information comme une menace pour les forces armées. Il souligne la nécessité d'une approche par trois niveaux de compétences en ce qui concerne la sensibilisation du personnel aux questions relatives aux cyberespace et cybermenaces[183]. Selon lui, il est nécessaire d'établir :

- un socle de compétences générales, celui-ci implique la mise en place des modules de formation à la sécurité des systèmes d'information pour l'ensemble des forces afin d'adopter un comportement de « cyberhygiène » ;
- un socle de compétences pour les techniciens : les militaires en 2e partie de carrière travaillant en relation avec la SSI doivent acquérir des compétences plus poussées, au niveau de l'armée de Terre aussi bien qu'au niveau interarmées ;
- un socle de compétences spéciales pour les experts : il y a une volonté de détecter et former très tôt des hommes et femmes spécialistes dans l'informatique pour traiter ces questions sur le long terme au sein de l'institution militaire.

Dans le 1er socle de compétences générales, le Ministère a dressé une liste de 10 commandements que tous les utilisateurs des systèmes informatiques du Ministère doivent respecter :

Les 10 commandements cybernétiques[184] :

1. Tu passeras tes supports amovibles sur une station blanche et tu ne connecteras pas de supports personnels sur une station professionnelle
2. Tu effaceras toutes les données sensibles inutiles de tes clés USB avant de voyager
3. Tu rendras compte de toute détection virale aux organismes compétents
4. Tu vérifieras régulièrement qu'aucun équipement anormal n'est connecté sur ta station professionnelle
5. Tu utiliseras des mots de passe robustes
6. Tu ne laisseras pas ton mot de passe accessible
7. Tu ne communiqueras ton adresse mail professionnelle qu'à des personnes de confiance
8. Tu vérifieras l'expéditeur des mails que tu reçois
9. Tu seras vigilant avant d'ouvrir des pièces jointes à un courriel
10. Tu n'enverras pas de fichiers sensibles par Internet sans protection

Crédits : Élodie Simon.

L'acquisition d'un certain niveau d'hygiène informatique par les personnels de la défense est l'une des priorités du Ministère de la Défense. Elle est fondée sur deux piliers : d'une part, il s'agit de rapprocher les formations existantes en matière de SSI, dans ce sens un comité spécialisé dans la formation à la cybersécurité a été mis en place par

[182] Le Général Boissan est officier des Transmissions, Saint-Cyrien et titulaire du Brevet d'Études Militaires Supérieures (1992). Il est par ailleurs ingénieur diplômé de SUPELEC (1991). Le 1er août 2012, il a pris le commandement de l'École des transmissions.

[183] Séminaire organisé par la Chaire de Cyberdéfense et Cybersécurité Saint-Cyr – Sogeti – Thales, « Cyberconflictualité et forces terrestres », 12 février 2013.

[184] Grégoire Chaumeil, Anne-Lise Llouquet et Nelly Moussu, « Cyberespace le 5ème champ de bataille », *Armées d'aujourd'hui*, novembre-décembre 2011, n° 365, p. 47.

le Ministère en février 2013[185] ; d'autre part, ce niveau doit être entretenu de façon continue tout au long de la carrière des membres des forces.

Peu d'informations sont disponibles concernant les socles de compétences propres aux techniciens et aux experts. Le Ministère de la Défense envisage de développer une expertise technique au sein de la filière « systèmes d'information », en s'appuyant sur un pôle d'excellence de la formation en Bretagne auquel la DGA et l'École des Transmissions sont associées (l'École des Transmissions occupe une fonction de référent interarmées)[186].

232 – L'utilisation de l'Internet et des réseaux sociaux à titre personnel

L'utilisation des réseaux sociaux n'est pas une menace cybernétique à proprement parler. Elle constitue une part importante de l'étude du cyberespace comme nouveau champ de bataille. Dans cette partie, seule sera traitée l'utilisation à titre privé de l'Internet et des réseaux sociaux par les hommes de la force. L'étude des réseaux sociaux comme nouvel outil de communication voire comme outil militaire sera présentée dans le chapitre 4 relatif à la combinaison de la guerre numérique avec le champ de bataille conventionnel.

Les évolutions technologiques ont modifié la façon de communiquer et d'interagir. En quelques décennies à peine, nous sommes passés du Web 1.0, où l'internaute visite des pages statiques, au Web 2.0 : l'internaute peut directement contribuer à l'élaboration des contenus et participer à l'animation des réseaux. L'évolution technologique des supports numériques (ordinateurs, tablettes, *smartphones*) ainsi que la libéralisation de l'expression sur les réseaux sociaux[187] permettent un échange instantané d'informations. Nous serions aujourd'hui dans l'ère du Web 3.0 ou 4.0, correspondant respectivement à la montée en puissance des systèmes nomades et à la synchronisation de tous les services du web et des technologiques liées au cyberespace[188].

Les réseaux sociaux personnels (Facebook, Twitter, YouTube, forum « au militaire », etc.) et professionnels (Linkedin, Viadeo, etc.) se sont fortement développés, ils constituent un outil formidable pour les armées (notamment en matière de campagnes de recrutement[189]). Dans le même temps, ces réseaux sont source de vulnérabilités. Le phénomène a récemment fait l'objet d'une attention particulière de la part des armées : en 2012-2013, le Centre Interarmées de Concepts, de Doctrines et d'Expérimentations (CICDE) a publié une réflexion doctrinale interarmées sur les réseaux sociaux[190], tandis que la Délégation aux Affaires Stratégiques a mis en ligne une étude sur la nature et les conséquences des réseaux sociaux pour les forces armées[191]. Cette dernière présente notamment la diversité des réseaux sociaux susceptibles d'être fréquentés par des membres des forces armées.

185 Interview du contre-amiral Arnaud Coustillière, officier général cyberdéfense, état-major des armées, « La cyberdéfense est l'une des priorités de la Défense », propos recueillis par Nelly Moussu, *Armées d'aujourd'hui*, décembre 2012 - janvier 2013, n° 376, p. 38-39.

186 Contre-amiral Arnaud Coustillière, officier général cyberdéfense, État-major des armées, « La cyberdéfense : une priorité pour les armées », *Transmetteurs*, 1er semestre 2013, n° 6, p. 19.

187 Fin 2005, Facebook comptait près de 5 millions de membres dans le monde. En 2011, ils étaient 750 millions. En France, plus de 20 millions de personnes utiliseraient Facebook (http://www.english.rfi.fr/node/73031).

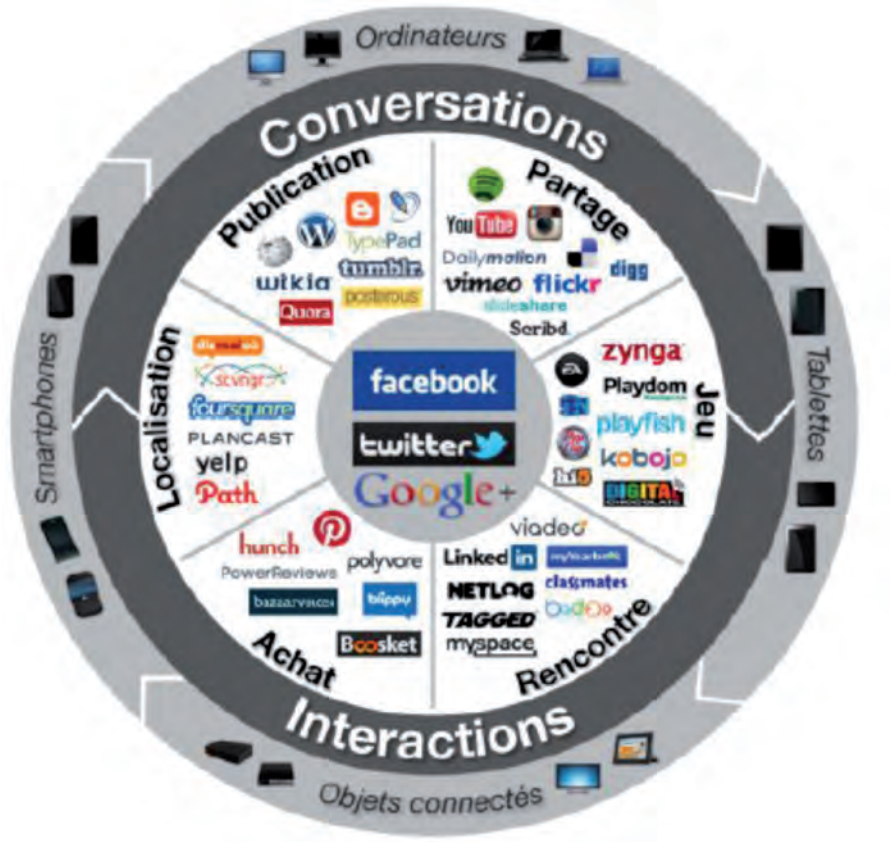
188 CICDE, « Réseaux sociaux. Nature et conséquences pour les forces armées », Réflexion doctrinale interarmées RDIA-2013/001_RS(2013), n° 067/DEF/CICDE/NP du 19 avril 2013, disponible à l'adresse suivante : http://www.cicde.defense.gouv.fr/IMG/pdf/20130423_np_cicde_rdia-reseaux-sociaux.pdf, p. 11-12.

189 En 2013, l'armée de Terre a lancé la campagne de recrutement « pour moi, pour les autres, sengager.fr ». Près de 7 millions de pages Internet ont été visitées, par 1,2 millions internautes ; les candidatures par Internet représentent près de 60 % du total de candidatures déposées auprès de l'armée de Terre. Voir Philippe Chapleau, « La campagne de publicité de l'armée de Terre fait un carton », billet publié le 28 juin 2013 sur le blog Lignes de défense (http://lignesdedefense.blogs.ouest-france.fr/archive/2013/06/28/cocorico-terrien-la-campagne-de-publicite-fait-un-tabac.html).

190 CICDE, « Réseaux sociaux. Nature et conséquences pour les forces armées », Réflexion doctrinale interarmées RDIA-2013/001_RS(2013), n° 067/DEF/CICDE/NP du 19 avril 2013.

191 Marguerite de Durand, Marc Hecker, Thibault Souchet, Nicolas Vanbremeersch, « Nature et conséquences des réseaux sociaux pour les forces armées », IFRI, spintank, septembre 2012, disponible à l'adresse suivante : http://www.defense.gouv.fr/das/reflexion-strategique/etudes-prospectives-et-strategiques/eps-2010-2012. Cette étude fut réalisée au profit du CICDE, de la Délégation à l'information et à la communication de la défense (DICoD) et de la DAS dans le cadre des études prospectives et stratégiques 2010-2012 de l'organisme interarmées.

Représentation des principaux réseaux sociaux et de leurs finalités



Source : Marc HECKER, Nicolas VANBREMEERSCH, Marguerite de DURAND et Thibault SOUCHET, « Nature et conséquence des réseaux sociaux pour les forces armées », septembre 2012, p. 13.

La question de la nature et des conséquences des réseaux sociaux est incontournable pour les forces armées dans un contexte où l'information et la connaissance peuvent permettre de gagner – ou de perdre – une guerre. Ainsi, un *post* précisant un état d'esprit, une localité ou tout autre élément ordinairement anodin peut entraîner des conséquences lourdes pour la force déployée. De retour d'opération en Afghanistan, les soldats français du 3e RIMA de Vannes ont été interrogés sur leurs habitudes concernant les réseaux sociaux. Alors que 67,6 % des militaires affirmaient avoir un compte sur un réseau social comme Facebook, 37,5 % des sondés confiaient utiliser les réseaux sociaux comme un moyen d'échange avec leurs familles pendant un déploiement en opération[192]. Ces chiffres témoignent de la réalité de l'utilisation des réseaux sociaux depuis un théâtre d'opération. Or, plusieurs menaces peuvent se réaliser par le biais des réseaux sociaux, et en particulier du *social engineering* : vol d'identité, atteinte au droit à l'image, ou encore divulgation involontaire d'informations classifiées.

Plus généralement, le facteur Internet par la rapidité de diffusion de l'information qu'il permet doit être pris en compte dans la planification des opérations. Trois risques majeurs liés à l'utilisation des réseaux sociaux par les forces armées peuvent être identifiés : le risque de compromettre le succès de la mission, le risque d'effet « caporal stratégique », et enfin le risque d'atteinte à l'image de l'armée.

Risque de compromettre le succès de la mission

L'utilisation faite par les membres de la force de l'Internet peut remettre en cause le succès de la mission, elle peut en outre constituer un risque vital pour les soldats déployés. En effet, un simple *post* d'humeur sur un réseau social (Twitter, Facebook) ou encore un mail envoyé aux proches peut se révéler être une mine d'informations. En 2010, l'armée israélienne a dû annuler une opération de Tsahal après qu'un soldat a publié sur Facebook : « Mercredi, on nettoie [le village de] Qatana et jeudi, si Dieu veut, on rentre à la maison »[193]. On imagine sans difficulté les conséquences graves que pourraient avoir de tels propos en opération.

[192] Marguerite de Durand, Marc Hecker, Thibault Souchet, Nicolas Vanbremeersch, « Nature et conséquences des réseaux sociaux pour les forces armées », IFRI, spintank, septembre 2012, p. 12-13.

[193] Marc Hecker et Thomas Rid, « Les armées françaises doivent-elles craindre les réseaux sociaux », *Politique étrangère,* n° 2, 2012, p. 319. Voir aussi Olivier Danino, « L'utilisation stratégique du cyber au Moyen-Orient », p. 24-25, étude confiée à M. Danino par la Délégation aux Affaires Stratégiques, p. 30.

Les forces armées françaises ont identifié le risque de captation d'informations opérationnelles engageant la sécurité de la force et/ou la réussite de la mission. La publication interarmées relative à l'utilisation d'Internet à des fins privées dans le cadre de la condition du personnel en opération précise :

> « *[…] toute information (photos ou écrits) relative à des dispositifs de la force, à des départs en mission, à des identités, etc. doit être formellement proscrite dans le cadre de l'utilisation de l'internet de loisir en opération*[194] ».

Le danger que représentait une communication (par réseaux sociaux ou autre support) aux familles d'une activité exceptionnelle pour les forces armées avait bien été pris en compte dans la planification de l'opération de récupération de l'otage Denis Allex en Somalie. Les navires ayant servi d'appui à la mission (dont le Bâtiment de Projection et de Commandement Mistral duquel les hélicoptères ont décollé) avaient été placés en position « Incon rouge », signifiant que les relations Internet de l'équipage, les liaisons téléphoniques avec les familles et l'accès à l'intranet des armées étaient coupés[195].

Risque d'effet « caporal stratégique »

L'effet « caporal stratégique » se produit lorsque des actions entreprises au plus bas échelon de la hiérarchie militaire (ou de façon plus générale au niveau tactique) ont des conséquences au niveau stratégique[196]. Un comportement à risque d'un soldat peut ainsi rendre précaires tous les efforts de stabilisation de la force sur un théâtre d'opérations. Un exemple en Afghanistan permet de prendre conscience de l'effet « caporal stratégique » : en janvier 2012, une vidéo intitulée « *Marines peeing on Taliban* » a été postée sur YouTube[197]. Dans celle-ci, quatre Marines urinaient sur les corps de Talibans morts en faisant des commentaires tels que « *have a great day, budy*[198] ». Le 20 janvier, quatre militaires français sont tués et quinze sont blessés par un soldat afghan ayant retourné son arme contre eux. Il justifie ses actes en mentionnant la vidéo des Marines urinant sur des corps afghans[199]. Suite à ces événements, le Président N. Sarkozy suspend les opérations des forces françaises et envisage leur rapatriement anticipé en déclarant alors : « si les conditions de sécurité ne sont pas clairement rétablies, alors se posera la question d'un retour anticipé de l'armée française en France[200] ». Ainsi une vidéo postée sur un réseau social a eu des répercussions importantes sur le terrain pour les soldats de la force, mais également au plus haut niveau politique et diplomatique.

Il n'existe pas à ce jour de cas similaires concernant les forces armées françaises, aucune vidéo ou photo de soldats français commettant des actes contraires à l'éthique d'une telle gravité à l'encontre de combattants ennemis. On trouve pourtant des vidéos dans lesquelles des soldats français en situation de combat ont un comportement à la limite des valeurs éthiques défendues par les forces armées françaises[201]. Hors situation de conflit armé, l'armée de Terre a dû traiter une situation difficile en août 2010. Un officier coopérant dans un pays africain avait insulté et tenté de faire pression sur un journaliste togolais à qui il ordonnait de retirer des photographies de son appareil. Très vite, une vidéo de l'officier français montrant le comportement critiquable avait été diffusée sur les réseaux sociaux (Facebook, Twitter et YouTube

194 État-Major des Armées, « Utilisation d'Internet à des fins privées dans le cadre de la condition du personnel en opération », Publication interarmées PIA-4.0.1.1_UIFP-CPO(2011), N° D-11-009052/DEF/EMA/SC-SOUT/SLI/SDO/NP du 18 novembre 2011, par. 206. (disponible en suivant le lien http://www.cicde.defense.gouv.fr/IMG/pdf/20111118_np_cicde_pia-4-0-1-1-internet-et-cpo.pdf)

195 Jean Guisnel, « Exclusif. Somalie : le raid pour libérer Denis Allex a été conduit depuis le Mistral », article publié le 13 janvier 2013, http://www.lepoint.fr/editos-du-point/jean-guisnel/exclusif-somalie-le-raid-pour-liberer-denis-allex-a-ete-conduit-depuis-le-mistral-13-01-2013-1613080_53.php. Voir également « Afghanistan : Sarkozy évoque un retrait des troupes », 20 janvier 2012 (http://www.lefigaro.fr/international/2012/01/20/01003-20120120ARTFIG00470-afghanistan-sarkozy-evoque-un-retrait-des-troupes.php).

196 Marc Hecker et Thomas Rid, « Les armées françaises doivent-elles craindre les réseaux sociaux », *Politique étrangère*, n° 2, 2012, p. 319.

197 http://www.youtube.com/watch?v=_TMq3m_Oli4&feature=fvwrel

198 « Passe une bonne journée, mec ».

199 Marguerite de Durand, Marc Hecker, Thibault Souchet, Nicolas Vanbremeersch, « Nature et conséquences des réseaux sociaux pour les forces armées », IFRI, spintank, septembre 2012, p. 46.

200 Propos tenus par N. Sarkozy lors de ses vœux au corps diplomatique. http://www.ambafrance-rsa.org/President-Nicolas-Sarkozy-Voeux-au

201 Dans le documentaire « C'est pas le pied la guerre », un journal filmé clandestinement par deux soldats français en Afghanistan, on peut voir des soldats français se réjouir de l'arrivée de l'appui aérien alors que leur section se trouvait prise en embuscade. Alors que l'aviation bombarde le village d'où proviennent les tirs, les soldats français s'exclament : « il va y avoir de la viande ce soir ! […] À table ! » (voir 9 min 45, http://www.youtube.com/watch?v=Xlnjja3eYho).

notamment) Le lendemain, l'état-major des armées publiait un communiqué dans lequel le comportement de l'officier coopérant serait sanctionné pour « atteinte au renom de l'armée française ». Des faits similaires sur un théâtre de conflit armé où les forces françaises seraient engagées pourraient avoir de graves conséquences en provoquant un effet « caporal stratégique ».

Risque d'atteinte à l'image de l'armée

Le risque d'atteinte à l'image de l'armée est présent au quotidien sur les réseaux sociaux : selon Marc Hecker et Thomas Rid, « il est relativement aisé de trouver des photographies de fêtes trop arrosées ou de scènes s'apparentant à des bizutages et de lire des commentaires désobligeants à l'égard de populations étrangères[202] ». Ce risque peut émaner à la fois des soldats de la force et de personnes extérieures aux forces armées.

En opération ou en France, l'utilisation d'Internet – et en particulier des réseaux sociaux – à titre privé par les militaires peut causer ou contribuer à causer une dégradation de l'image des armées françaises. La mise en ligne de vidéos par des militaires, qu'elles soient de combat ou humoristiques (les *lipdubs*[203] connaissent un succès certain ces dernières années), peuvent en effet dégrader l'image des armées. En 2010, une vidéo dans laquelle six soldats en armes de Tsahal armés dansaient dans une rue d'Hébron sur une chanson de hip-hop a été mise en ligne[204]. Si certains ont accueilli la vidéo avec humour (les grands médias ont majoritairement reçu la vidéo de façon favorable)[205], l'armée israélienne sanctionna les soldats (Tsahal précisa que la situation calme à Hébron et l'ennui des soldats favorisaient ce type de comportements chez les soldats[206]). Quant à la population d'Hébron, elle répondit en mettant en ligne quelques semaines plus tard sa propre vidéo dans laquelle des arrestations de Palestiniens par des soldats israéliens étaient simulées sur une musique populaire[207]. Aujourd'hui, les forces armées françaises, et en particulier l'armée de Terre, semblent être moins concernées par la mise en ligne de vidéos humoristiques que par celles, plus inquiétantes, de vidéos de combats : plusieurs d'entre elles filmées au moyen de caméras fixées sur le casque du soldat peuvent être visionnées sur les réseaux sociaux (en particulier Youtube et Dailymotion). Les risques liés à ces vidéos résident d'une part dans la possibilité d'un effet « caporal stratégique », d'autre part dans les commentaires qui y sont associés : les internautes dénoncent fréquemment les raisons de l'intervention des forces armées françaises tout en dégradant l'image de celles-ci[208].

L'utilisation d'Internet et des réseaux sociaux par les familles et les proches de militaires peut également porter atteinte à l'image des armées. Les proches de militaires ne sont pas soumis au devoir de réserve, et les réseaux sociaux peuvent leur servir de lieu d'expression concernant les dysfonctionnements militaires auxquels ils sont confrontés. En témoigne la réaction suscitée par la mise en œuvre du logiciel Louvois[209] dans l'armée de Terre en 2011, et les impayés qui en ont résulté (13 000 militaires de l'armée de Terre, soit 10 % des effectifs, seraient concernés par les retards de paiement de solde[210]). Des groupes ont été créés par des familles de militaires sur Facebook afin de protester contre les retards de payement, parmi lesquels « Soucis de solde militaire, battons-nous ! » et « Louvois, donne-nous ce que tu nous dois ! »[211]. Le premier groupe,

---

202 Marc Hecker et Thomas Rid, « Les armées françaises doivent-elles craindre les réseaux sociaux », *Politique étrangère,* n° 2, 2012, p. 320.

203 Un *Lipdub* est une vidéo dans laquelle des individus se mettent en scène en faisant du play-back ; dans notre cas, des militaires se mettent en scène, montent une chorégraphie sur une chanson connue. En 2011, pour fêter Noël, l'équipage du porte-avions britannique HMS Ocean a connu un grand succès avec sa reprise de la chanson « All I want for Christmas » de Mariah Carey (http://www.youtube.com/watch?v=SDZcGz4vmJc).

204 Cette vidéo est intitulée « Bataillion 50 Rock the Hebron Casbah », http://www.dailymotion.com/video/xdy5m9_des-soldats-israeliens-dansent-dans_news

205 Marguerite de Durand, Marc Hecker, Thibault Souchet, Nicolas Vanbremeersch, « Nature et conséquences des réseaux sociaux pour les forces armées », IFRI, spintank, septembre 2012, p. 44.

206 Marguerite de Durand, Marc Hecker, Thibault Souchet, Nicolas Vanbremeersch, « Nature et conséquences des réseaux sociaux pour les forces armées », IFRI, spintank, septembre 2012, p. 44.

207 http://www.youtube.com/watch?v=5MGsDlOWJHQ&feature=player_embedded

208 Marguerite de Durand, Marc Hecker, Thibault Souchet, Nicolas Vanbremeersch, « Nature et conséquences des réseaux sociaux pour les forces armées », IFRI, spintank, septembre 2012, p. 52.

209 Logiciel unique à vocation interarmées de la solde.

210 Marguerite de Durand, Marc Hecker, Thibault Souchet, Nicolas Vanbremeersch, « Nature et conséquences des réseaux sociaux pour les forces armées », IFRI, spintank, septembre 2012, p. 95-96.

211 Marguerite de Durand, Marc Hecker, Thibault Souchet, Nicolas Vanbremeersch, « Nature et conséquences des réseaux sociaux pour les forces armées », IFRI, spintank, septembre 2012, p. 98.

ouvert, était consultable par tous ; on y trouvait des contestations contre le retard de paiement de la solde, mais aussi des messages critiquant l'institution militaire, visant directement certains officiers, et enfin des messages à caractère politique. Ainsi, l'expression des proches de militaires sur ce réseau social portait directement atteinte à l'image de l'armée de Terre.

L'armée de Terre n'est pas indifférente à cette question, en 2008 le chef d'état-major de l'armée de Terre a publié une directive relative à la diffusion d'informations militaires sur des sites Internet, blogs ou forums[212]. L'accent est mis sur la sensibilisation de tout le personnel plutôt que sur l'interdiction/sanction. Cette approche diffère de celle retenue outre-Manche, le Royaume-Uni a en effet imposé des règles très strictes afin d'encadrer l'expression des militaires sur Internet et sur les réseaux sociaux[213].

Internet et l'utilisation des réseaux sociaux constituent un nouveau facteur de risques à l'égard des forces armées. Dans le même temps, leur impact positif est réel. Pendant un déploiement en OPEX les réseaux sociaux peuvent permettre au soldat de rester en contact avec ses proches en France, et donc d'avoir davantage de stabilité émotionnelle. Derrière la réalité de la condition du personnel en opération, c'est la question du moral et de l'efficacité du soldat qui est posée. Néanmoins l'utilisation d'Internet à titre privé ne doit pas nuire à la protection des militaires et de leurs familles ni à la sécurité opérationnelle.

Par ailleurs, l'animation de groupes de soutien aux militaires français et les hommages rendus aux soldats tombés pour la France entretiennent le lien armée-Nation. Dans cette logique, les réseaux sociaux sont un outil de communication permettant aux armées d'atteindre un large public et de diffuser ses messages.

[212] Note du chef d'état-major de l'armée de Terre destinée à tous les personnels, 30 juillet 2008, n° 215/DEF/EMAT/PS/BPES/DR. Voir Marc Hecker et Thomas Rid, « Les armées françaises doivent-elles craindre les réseaux sociaux », *Politique étrangère*, n° 2, 2012, p. 322.

[213] La directive 2007DIN03-006 relative à la communication publique des agents du Ministère de la Défense et des forces armées dispose : « les fonctionnaires civils du Ministère de la Défense et les membres des forces armées doivent obtenir une autorisation préalable s'ils veulent écrire, parler ou communiquer publiquement d'une autre manière sur la défense ou des sujets corrélés » (doc 2007DIN03-006).

CHAPITRE 3

ÉTAT DES LIEUX DES RÉPONSES APPORTÉES AUX NIVEAUX INTERALLIÉS ET NATIONAUX POUR LES FORCES ARMÉES FACE AUX VULNÉRABILITÉS LIÉES À L'ACTION DANS LE CYBERESPACE

Les États et organisations internationales ont des perceptions propres des menaces cybernétiques dont ils sont l'objet, ils possèdent en outre des capacités variées afin d'y répondre. Afin de mieux en comprendre les enjeux, ce chapitre propose un état des lieux non exhaustif des mesures prises et des moyens consacrés à la cyberdéfense par différents acteurs. Concernant les réponses étatiques, il s'agit d'envisager la façon dont l'action dans le cyberespace et les menaces qui en émanent sont appréhendées du niveau stratégique au niveau tactico-opératif pour les forces terrestres (lorsque des éléments de réponse sont accessibles) par certains États (section 32). Si l'étude des différents choix nationaux en matière de cyberdéfense est utile à une réflexion propre à la France et à ses forces armées, l'analyse des solutions retenues au niveau international et interalliés est également indispensable dans la mesure où les coopérations multilatérales et bilatérales sont importantes en matière de cyberdéfense (section 31).

31 – NIVEAU INTERALLIÉS ET EUROPÉEN : L'OTAN ET L'UE

En matière de cyberdéfense, le Livre Blanc 2013 favorise une approche coopérative et précise que « toute politique ambitieuse de cyberdéfense passe par le développement de relations étroites entre partenaires internationaux de confiance »[214]. Dans un entretien accordé en mars 2013, le contre-amiral Coustillière, officier général cyberdéfense, soulignait l'importance de la coopération en matière de cyberdéfense, notamment aux niveaux de l'Union Européenne et de l'OTAN[215].

[214] Livre Blanc Défense et Sécurité Nationale 2013, p. 107.

[215] Centre des Hautes Études du Ministère de l'Intérieur, web émission Cyber Talk n° 3, « Le ministère de la Défense dans le cyberespace », mars 2013, http://www.defense-et-strategie.fr/index.php?option=com_content&view=category&id=116:le-cybertalk&Itemid=374

311 – L'Union Européenne

Si la prise en compte du niveau européen semble plus pertinente dans la lutte contre la cybercriminalité qu'en matière de cyberdéfense, elle est pourtant fondamentale. Dans le cadre de la Politique Européenne de Sécurité et de Défense (PESD), l'Union Européenne est directement concernée par les attaques cybernétiques à son encontre et contre ses membres. En 2008, le rapport de la Commission de défense sur la guerre informatique précisait :

> « *La raison d'être de la politique européenne de sécurité et de défense est d'élever le niveau de la défense européenne en développant des concepts, des techniques et des matériels européens. C'est une question d'autonomie politique et opérationnelle, et une affaire technologique et économique d'importance stratégique*[216] ».

Rôle

En amont de la menace cybernétique, l'Union Européenne est un acteur incontournable dans la mesure où elle est compétente dans l'élaboration des règles relatives aux réseaux de communications électroniques. L'UE a donc un rôle à jouer dans l'harmonisation des dispositions techniques au niveau européen dans une logique *top-down* afin d'exiger une meilleure sécurité des réseaux, et de poser les bases nécessaires à la défense et la résilience des réseaux informatiques. Certains auteurs estiment dans ce sens que l'UE pourrait imposer une meilleure sécurité des réseaux et des infrastructures les plus sensibles de tout État membre afin de limiter les failles de leurs SIC et de renforcer la résilience des infrastructures les plus sensibles[217]. La Commissaire européenne chargée des nouvelles technologies travaille sur ce point : Jean-Marie Bockel a ainsi salué la décision de Nelly Kroes de rendre obligatoire la déclaration d'incidents par les opérateurs à leur agence de sécurité des systèmes d'information nationale (l'ANSSI[218] pour la France), mesure inspirée d'une proposition du rapport élaboré par le sénat français[219]. En outre, l'UE est active dans l'élaboration de normes en matière de protection des infrastructures critiques[220].

Structures et actions menées

La Commission européenne a proposé un plan d'action afin de sensibiliser l'ensemble des États membres et de les encourager à acquérir un socle minimum de résilience en matière de cyberdéfense. Celui-ci repose sur quatre piliers : préparation des États à la menace cybernétique (définir un niveau minimum de capacités), développement des capacités de détection de l'Union (développer des systèmes de partage d'information et d'alerte), mise en place de mesures de réaction (les États doivent concevoir des plans nationaux en cas d'alerte), et enfin amélioration de la coopération internationale[221]. Plusieurs dispositions ont été adoptées afin d'assurer une meilleure résilience des réseaux de l'UE et de ses États membres :

- En 2004, l'Agence européenne chargée de la sécurité des réseaux et de l'information a été créée (il s'agit de l'ENISA, *European Network and Information Security Agency*[222]), ce centre d'expertise a notamment pour rôle d'assister la Commission et les États membres « dans leur dialogue avec l'industrie en vue de résoudre les problèmes sécuritaires posés par les matériels et logiciels »[223]. Il est

[216] Grégoire Chaumeil, Anne-Lise Llouquet et Nelly Moussu, « Cyberespace le 5ème champ de bataille », *Armées d'aujourd'hui,* novembre-décembre 2011, n° 365, p. 40.

[217] Emmanuel Dupuy, « Quels enjeux politiques en matière de cyberdéfense ? », *Revue Militaire Suisse,* Numéro 1, janvier-février 2013, p. 20.

[218] Agence Nationale de Sécurité des Systèmes d'Information.

[219] Sénateur Jean-Marie Bockel, « Cyberdéfense : la France a des atouts », *Revue DÉFENSE,* n° 159, novembre-décembre 2012, p. 40. Voir également Jean-Marie Bockel, « La cyberdéfense : un enjeu mondial, une priorité nationale », Rapport d'information fait au nom de la Commission des Affaires étrangères, de la Défense et des forces armées, du Sénat n° 681, enregistré à la Présidence du Sénat le 18 juillet 2012, les recommandations n° 2 à n° 6 visent à renforcer le rôle et les prérogatives de l'ANSSI (p. 122).

[220] Dave Clemente, "Cyber Security and Global Interdependence: What Is Critical?", *Chatham House report,* février 2013, p. 9. Voir plus précisément European Commission, "Proposal amending Council Directive 2008/114/EC (identification and designation of European critical infrastructures)", Version 1, August 2011, http://ec.europa.eu/governance/impact/planned_ia/docs/2012_home_010_directive_critical_infrastructures_en.pdf.

[221] Grégoire Chaumeil, Anne-Lise Llouquet et Nelly Moussu, « Cyberespace le 5ème champ de bataille », *Armées d'aujourd'hui,* novembre-décembre 2011, n° 365, p. 40-41.

[222] Le site officiel de l'ENISA est accessible en suivant le lien http://www.enisa.europa.eu/media/enisa-en-francais

[223] Assemblée européenne de sécurité et de défense, « La guerre informatique », document C/2022, 5 novembre 2008, par. 192, p. 25.

en permanence en contact avec les États membres, notamment par l'intermédiaire des **officiers de liaison détachés**[224]. En juin 2013, le mandat de l'ENISA a été renouvelé pour sept ans[225].

- En 2006, l'UE a établi une liste des infrastructures jugées critiques, elle les définit comme les infrastructures dont la destruction entraînerait des conséquences dans au moins deux États membres[226].

- En 2008, l'Agence Européenne de Défense a travaillé à l'élaboration d'un plan de développement des capacités de l'UE en matière de cyberdéfense, celui-ci prévoit notamment la capacité de mener des opérations en réseau informatique et de mettre en place une « capacité infocentrée européenne »[227].

- En 2011 enfin, l'UE a précisé qu'elle mettrait en place une équipe d'intervention d'urgence en cas d'alerte ou d'attaque à l'encontre des institutions (Commission, Parlement, etc.), cette équipe est susceptible de venir en aide aux États membres victimes d'attaques cybernétiques.

Le Haut Représentant de l'Union aux Affaires étrangères et à la Politique de sécurité a publié en 2013 une communication jointe au Parlement, au Conseil européen, au Comité économique et social européen et au Comité des régions proposant une nouvelle stratégie de cybersécurité pour l'Union européenne[228]. Ce document, intitulé « *Cybersecurity Strategy of the European Union : An Open, Safe and Secure Cyberspace* », propose une stratégie pour l'UE ayant pour finalité de rendre le plus sûr possible le monde européen en ligne[229]. Cette dernière repose sur cinq priorités : parvenir à mettre en place une résilience cybernétique, réduire drastiquement la cybercriminalité, développer des politiques et capacités de cyberdéfense dans le cadre de la PESD, développer les ressources industrielles et technologiques nécessaires à la cybersécurité. La stratégie proposée définit les rôles entre les autorités compétentes et les CERT (*Computer Emergency Response Team*, des centres d'alerte et de réaction aux attaques informatiques), et le soutien apporté par l'UE en cas d'attaque cybernétique majeure. Il s'agit désormais de veiller sur les suites qui seront données par les instances européennes et les États membres de l'Union à cette proposition de stratégie publiée en février 2013.

Limites

Malgré les progrès de la prise en compte des menaces cybernétiques à l'échelle de l'UE, la logique européenne en matière de cyberdéfense rencontre plusieurs obstacles : le premier est la volonté étatique de conserver sa liberté d'action dans le cyberespace. Daniel Ventre note que la « cyberdéfense imposerait de céder une part de ses propres prérogatives, de son pouvoir, de sa souveraineté, le partage d'instruments, d'accès, de réseaux, de moyens, etc. »[230]. Or, tous les États membres de l'Union ne possèdent pas le même niveau de compétences et les mêmes exigences en matière de sécurité des systèmes d'information. Par ailleurs, de nombreux accords bilatéraux sont développés en matière de cyberdéfense, aussi la coopération européenne – collective – peut-elle sembler moins prioritaire aux États que leur sécurité nationale et leur indépendance en matière de protection des infrastructures critiques. Cette coopération en multilatéral large est surtout compliquée par les disparités en matière de moyens consacrés à la cyberdéfense, d'avancées technologiques et de compétences. Ainsi, l'aléa dans la fiabilité de certains partenaires semble poser des difficultés en matière

[224] Assemblée européenne de sécurité et de défense, « La guerre informatique », document C/2022, 5 novembre 2008, par. 193, p. 25.

[225] Observatoire du Monde Cybernétique, *Lettre N° 18* - Juin 2013, p. 2.

[226] CEIS, "Virtual means, actual threats : From cyber security to cyber defense : a new challenge for Europe", Bruxelles, 18 septembre 2009. Alain Esterle, ancien directeur du Département technique de l'ENISA, a participé à ce débat.

[227] Assemblée européenne de sécurité et de défense, « La guerre informatique », document C/2022, 5 novembre 2008, par. 203, p. 27.

[228] Commission européenne, Haut Représentant de l'Union aux Affaires étrangères et à la Politique de sécurité, "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions", 7 février 2013, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[229] En conclusion, le plan précise en effet : "*This proposed cyber-security strategy of the European Union [...] outlines the EU's vision and the actions required, based on strongly protecting and promoting citizens' rights, to make the EU's online environment the safest in the world*", p. 20.

[230] Grégoire Chaumeil, Anne-Lise Llouquet et Nelly Moussu, « Cyberespace le 5ème champ de bataille », *Armées d'aujourd'hui*, novembre - décembre 2011, n° 365, p. 41.

de coopération multilatérale[231]. Enfin, le cadre de réflexion et d'action prééminent en matière de cyberdéfense sur la scène européenne est l'OTAN. L'UE et l'Alliance travaillent ensemble dans le cadre des arrangements dits « *Berlin Plus* » (ils posent le cadre des coopérations entre l'UE et l'OTAN). Les contacts sont fréquents entre les responsables militaires et civils de l'OTAN et leurs interlocuteurs européens (Secrétariat Général du Conseil, Service européen pour l'action extérieure, personnel militaire de l'UE, Agence européenne de Défense, Parlement européen, etc.). Au-delà des contacts, une coopération entre les services est en place : une équipe permanente de liaison de l'OTAN est détachée auprès du personnel militaire de l'UE depuis novembre 2005[232]. Dans une logique complémentaire, le Ministre de la Défense a récemment rappelé la nécessité d'approfondir l'ambition de l'UE en matière de stratégie de cyberdéfense, il a par ailleurs souligné la volonté de la France de « rapprocher l'Union et l'Alliance dans le domaine de la cyberdéfense »[233].

312 – L'OTAN

Bien que la menace cybernétique ait été envisagée dès 2002 (l'agenda politique de l'OTAN mentionne alors la protection des SIC pour la première fois), ce sont les attaques menées en 2007 contre l'Estonie – État membre de l'Alliance – qui ont érigé la cyberdéfense au rang de priorité et accéléré l'élaboration en la matière d'une réponse coopérative. En effet, l'interconnexion des réseaux peut entraîner des conséquences pour l'ensemble des parties connectées en cas d'attaques informatiques. Le Secrétaire Général de l'Otan, Anders Rasmussen, a déclaré en juin 2013 : « Une attaque contre un allié peut nous affecter tous si elle n'est pas combattue rapidement »[234], et a souligné à nouveau la nécessité d'avoir une approche coopérative solide en matière de cyberdéfense dans le cadre de l'Alliance. L'OTAN est l'objet de centaines d'attaques quotidiennes[235] ; en 2012, les experts en sécurité informatique de l'Alliance ont recensé 2 500 cas d'activité anormale ou de tentatives d'intrusion[236]. La lutte contre les attaques cybernétiques des réseaux de l'Alliance – déjà ciblés lors de la guerre du Kosovo en 1999 – est une priorité pour l'OTAN dès lors que ces attaques peuvent remettre en cause son efficacité.

Rôle

L'assurance d'une défense collective – pacte fondateur de l'Alliance – doit être effective aussi bien dans les *global commons* que dans le cyberespace. En 2010, l'Alliance a adopté un concept stratégique mentionnant notamment la nécessité d'adopter une « cyberdéfense en profondeur »[237]. En juin 2011, une politique de cyberdéfense accompagnée d'un plan d'action ont été approuvés. L'Alliance soutient six activités majeures dans le domaine de la cyberdéfense : l'aide aux pays de l'Alliance, l'intégration de la cyberdéfense au processus de planification de défense des pays, la recherche et la formation, la coopération avec les partenaires et organisations internationales ainsi qu'avec l'industrie, et enfin la fourniture d'avis[238] et la coordination de la cyberdéfense entre les pays membres. Le rôle de coordination est fondamental, l'OTAN a une fonction d'harmonisation des mesures et procédures de sécurité des SIC afin de garantir *a minima* la sécurité des systèmes utilisés par les forces armées, en particulier lorsqu'il s'agit de systèmes interopérables et d'interconnexions entre les réseaux des pays et les réseaux de l'Alliance. Dans cette logique, l'Alliance a publié en 2012 un manuel cadre élaboré par son Centre d'excellence pour la cyberdéfense de Tallinn (*Cooperative Cyber Defense Centre of Excellence, Tallinn,* CCD CoE) posant les bases d'une stratégie nationale de cybersécurité et cyberdéfense[239].

---

231 Sénateur Jean-Marie Bockel, « Cyberdéfense : la France a des atouts », *Revue DÉFENSE*, n° 159, novembre-décembre 2012, p. 40-41.

232 Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012, p. 186, accessible à l'adresse suivante : http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

233 Discours prononcé par le M. Jean-Yves Le Drian, Ministre de la Défense, en ouverture du colloque « Cybersécurité : un enjeu mondial, une priorité nationale, des réponses régionales », Rennes, 3 juin 2013.

234 Laurent Lagneau, « Vers la création d'une force de réaction rapide de l'Otan en cas de cyber-attaque », *opex360.com*, 6 juin 2013, http://www.opex360.com/2013/06/06/vers-la-creation-dune-force-de-reaction-rapide-de-lotan-en-cas-de-cyber-attaque/

235 OTAN, « Briefing : l'OTAN face aux nouveaux défis de sécurité » (Référence BRIEF11TNSFRE - 0527-11 NATO Graphics & Printing), 2011, p. 9.

236 Laurent Lagneau, « Vers la création d'une force de réaction rapide de l'Otan en cas de cyber-attaque », *opex360.com*, 6 juin 2013.

237 http://www.nato.int/cps/fr/natolive/official_texts_68580.htm

238 http://www.nato.int/cps/fr/SID-C4621EB1-D3267419/natolive/topics_78170.htm

239 Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE publication, Tallinn 2012, accessible à l'adresse suivante : http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

Structures et actions menées

Depuis 2002, l'Alliance a progressivement mis en place des structures afin de prendre en compte la menace cybernétique :

- À la suite du Sommet de Bucarest, en 2008 l'OTAN a créé la *Cyber Defence Management Authority* (CDMA), une autorité unique chargée de coordonner les réponses des membres à d'éventuelles attaques cybernétiques.

- Le centre technique de la capacité OTAN de réaction aux incidents informatiques (NCIRC) est en charge de la protection et de la défense de tous les réseaux de l'OTAN, il veille à la sécurité des quartiers généraux fixes et déployés[240].

- Le Centre d'excellence pour la cyberdéfense (CCD CoE) de Tallinn[241], créé en mai 2008, est une organisation militaire internationale accréditée par l'OTAN. Le Centre a pour mission de servir d'instance de réflexion, de formation sur les questions liées au cyberespace entre les États membres l'Alliance et ses partenaires. Le centre est une structure incontournable en matière de retour d'expérience pour les forces armées, plusieurs experts – civils et militaires – y travaillent dans l'ensemble des domaines concernés par les questions cyber : géopolitique, juridique, technologique, informatique, etc. L'ouverture de ce centre sur le monde civil est un atout certain. En 2010 le CCD CoE a développé un partenariat avec la société éditrice de solutions informatiques de sécurité Symantec afin de promouvoir la coopération en matière de recherche sur les menaces cybernétiques et les contre-mesures à adopter[242]. Depuis 2013, la France est représentée au Centre par un officier détaché[243].

- En juin 2011, une nouvelle version de la politique de cyberdéfense[244] a été approuvée par les Ministres de la Défense des pays membres de l'Alliance. Le plan d'action validé est fondé sur une approche coordonnée de la cyberdéfense au sein de l'OTAN, il met en avant la nécessité d'acquérir des capacités en matière de prévention des attaques et de résilience des réseaux.

- Dans le cadre de l'établissement d'une capacité de réaction aux incidents informatiques en février 2012, une cellule de veille cybernétique a été mise en place. Le 4 juin 2013, le Secrétaire Général de l'Alliance, A. Rasmussen, a annoncé la création d'une force de réaction rapide chargée de protéger les réseaux informatiques de l'Alliance en cas d'attaque cybernétique avant l'automne 2013[245]. Ces équipes de réaction rapide sont appelées la *Net Force*.

- En avril 2012, l'OTAN a intégré la cyberdéfense dans son processus de planification de défense.

- En juillet 2012, l'Agence OTAN d'information et de communication a été créée, elle a pour fonction de faciliter une protection centralisée pour tous les organismes OTAN.

- En avril 2013, l'infrastructure de gestion de défense et des capacités analytiques du réseau de base a été mise en œuvre, elle est rattachée au Centre technique de la capacité OTAN de réaction aux incidents informatiques.

L'Alliance met par ailleurs en place des exercices interalliés de cyberdéfense chaque année. En 2010, une simulation d'attaque informatique a permis aux agences de l'OTAN ainsi qu'aux forces armées et représentants de 24 pays membres de travailler ensemble à la résolution de la crise[246]. Cet exercice

240 http://www.nato.int/cps/fr/SID-13065477-30924605/natolive/news_85161.htm

241 Le site Internet du Centre d'excellence pour la cyberdéfense de Tallinn est accessible à http://www.ccdcoe.org

242 James G. Stavridis, Elton C. Parker III, « Sailing the cyber sea », *JFQ*, Issue 65, 2nd Quarter 2012, p. 63. Voir également « Symantec et le CCDCOE collaborent sur la recherche des menaces sur Internet » (http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20100111_01)

243 http://www.rpfrance-otan.org/Adhesion-de-la-France-au-Centre-d ; voir également Damien KERLOUET, « La France va participer au Centre de Cyberdéfense de l'OTAN », 3 décembre 2012, http://www.bruxelles2.eu/marches-de-defense/cyber/la-france-va-participer-au-centre-de-recherche-de-cyberdefense-de-lotan.html

244 http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence-fr.pdf

245 Laurent Lagneau, « Vers la création d'une force de réaction rapide de l'Otan en cas de cyber-attaque », *opex360.com*, 6 juin 2013. Cette force devrait être relativement modeste dans un premier temps, le Secrétaire Général a en effet précisé qu'il s'agissait de mettre en place deux équipes de trois personnes.

246 Grégoire Chaumeil, Anne-Lise Llouquet et Nelly Moussu,« Cyberespace le 5ème champ de bataille », *Armées d'aujourd'hui*, novembre-décembre 2011, n° 365, p. 39.

avait pour but de mettre en place une coopération entre organismes civils et militaires de plusieurs pays afin de lutter contre des attaques informatiques visant des moyens de transmission et des systèmes d'information des alliés. En 2012, l'OTAN a organisé l'exercice « *Locked Shields 2012* », il avait notamment pour objectif d'entraîner des spécialistes SIC et des conseillers juridiques afin de développer les capacités de cyberdéfense de l'Alliance[247].

Limites

L'OTAN investit dans les capacités de résilience de l'Alliance aux attaques informatiques. En 2012, elle a dépensé 28 millions d'euros pour améliorer ses capacités de détection et de réaction aux attaques, ainsi que pour mettre en place des équipes spécialisées dotées des dernières technologies[248]. Néanmoins, l'Alliance reste tributaire du niveau de résilience de ses membres. M. Rasmussen a identifié deux phases pour parvenir à un niveau de cyber-résilience acceptable : la protection des réseaux de l'OTAN, et la formulation de réponses adaptées aux demandes d'alliés faisant face à des cyber-attaques[249]. Cette deuxième phase semble plus problématique dès lors que certains États estiment qu'il s'agit d'une prérogative de souveraineté nationale.

La cyberdéfense étant un domaine sensible qui nécessite la construction de relations de confiance avec nos partenaires, le contre-amiral Coustillière souligne la nécessité d'entretenir une approche bilatérale avec des partenaires choisis. Ainsi le Ministère de la Défense travaille également sur des approches franco-britannique et franco-américaine, et même franco-russe[250]. Il semble ainsi indispensable de connaître les capacités de chaque État en matière de cyberdéfense, plus précisément en matière de lutte informatique défensive et offensive. Certains États, tels que la Chine, les États-Unis ou encore le Royaume-Uni ont officiellement annoncé leur volonté de développer des unités militaires à vocation offensive dans le cyberespace[251]. 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'État »[252]. La section suivante propose un état des lieux des structures mises en place par les États au sein de leurs forces armées et des moyens consacrés dans le cadre de la cyberdéfense ; lorsque des informations sont accessibles, le rôle des forces terrestres est détaillé.

32 – NIVEAU NATIONAL : LA FRANCE, LES ÉTATS-UNIS D'AMÉRIQUE, LE ROYAUME-UNI, LA CHINE, L'IRAN, ISRAËL

En matière de lutte informatique défensive et offensive, il est très difficile de connaître la fiabilité des informations disponibles en source ouverte. En effet, le cyberespace est un moyen pour un État de revendiquer et faire valoir sa puissance, il est un outil d'influence. En d'autres termes, le cyberespace revêt une importance en matière de puissance militaire, économique, financière, politique. Les informations révélées par les différents États concernant les ressources financières, humaines, technologiques et industrielles consacrées à la cyberdéfense sont à analyser avec précaution dans la mesure où il est difficile d'établir leur véracité. Néanmoins, elles permettent de dresser un aperçu des moyens consacrés à la cyberdéfense et d'identifier la place et les prérogatives des forces armées et en particulier des forces terrestres dans le dispositif.

247 10http://www.ccdcoe.org/334.html

248 Jason Healey, Leendert Van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today and Tomorrow", Atlantic Council Issue Brief, février 2012, p. 4.

249 http://www.01net.com/editorial/596753/cybersecurite-l-otan-se-dote-d-une-cyberforce-de-reaction-rapide/

250 Centre des Hautes Études du Ministère de l'Intérieur, web émission CyberTalk n° 3, « Le ministère de la Défense dans le cyberespace », mars 2013.

251 Bertrand Boyer, *Cyberstratégie - l'art de la guerre numérique, Paris, Nuvis*, 2012, p. 120.

252 Dans le Livre Blanc sur la Défense et la Sécurité Nationale, il est précisé p. 105 : « *[...] la capacité informatique offensive, associée à une capacité de renseignement, concourt de façon significative à la posture de cybersécurité. Elle contribue à la caractérisation de la menace et à l'identification de son origine. Elle permet en outre d'anticiper certaines attaques et de configurer les moyens de défense en conséquence. La capacité informatique offensive enrichit la palette des options possibles à la disposition de l'État* ».

Dans cette logique, les réponses apportées par différents pays aux menaces cybernétiques seront analysées du niveau stratégique au niveau tactico-opératif lorsque des éléments de réponse ont été identifiés. L'analyse du niveau stratégique est indispensable pour comprendre le cadre général de la perception de cette menace par les États, celle-ci pouvant différer selon les cultures. Cinq approches nationales seront étudiées : la France, les États-Unis, la Chine, l'Iran et Israël.

Toutefois, ce travail se concentrera sur l'angle militaire. Pour une analyse exhaustive des différentes stratégies nationales en matière de cyberdéfense, le lecteur pourra se référer aux travaux réalisés par l'Observatoire du Monde Cybernétique (OMC) de la Délégation aux Affaires Stratégiques (DAS) du Ministère de la Défense en collaboration avec la Compagnie Européenne d'Intelligence Stratégique (CEIS) ; l'OMC effectue un travail de veille et de synthèse pour le Ministère sur les questions relatives au cyberespace, ses travaux sont accessibles sur le site Internet de la DAS[253]. Les éléments de réponse développés ci-dessous s'inspirent également de l'ouvrage de Daniel Ventre intitulé « *Cyber Conflict: Competing National Perspectives* »[254].

321 – La France

En 2009, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) rattachée au Secrétaire Général de la Défense et de la Sécurité Nationale (SGDSN) a été créée. Deux ans plus tard, l'ANSSI a publié une Stratégie de défense et de sécurité des systèmes d'information visant à faire de la France une puissance mondiale de la cyberdéfense[255]. Cet organisme est en charge d'organiser la cyberdéfense au niveau interministériel. Les forces armées détenant des prérogatives spécifiques dans la protection et la défense des infrastructures nationales, l'Agence collabore étroitement avec le Ministère de la Défense, en particulier avec le Centre d'Analyse de Lutte Informatique Défensive (CALID, les deux centres seront d'ailleurs colocalisés à l'horizon 2014[256]) et la section Maîtrise de l'information de la Direction Générale de l'Armement (la DGA est en charge de la composante technologique comprenant l'analyse de la menace, l'expertise technique et la recherche en amont[257]). Le Livre Blanc 2013 souligne la pertinence d'une approche globale de la menace cybernétique :

> « *La doctrine nationale de réponse aux agressions informatiques majeures 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*[258] ».

Le Ministère de la Défense a défini le cadre général de la cyberdéfense (juillet 2011) et élaboré une doctrine détaillant ses fonctions et ses moyens (2012)[259]. La cyberdéfense regroupe trois dimensions : la défense active en profondeur des systèmes d'information, la capacité de gestion de crise cybernétique, et la capacité de lutte et de conduite d'opérations dans le cyberespace[260]. Concernant la structure de commandement, la France a fait le choix de mettre en place une chaîne de commandement unifiée pour la cyberdéfense afin de mieux coordonner les efforts et posséder une vision globale de la situation. Le Livre Blanc 2013 précise :

---

253 La DAS consacre une réflexion importante à la question cyber. Elle travaille conjointement avec la Compagnie Européenne d'intelligence Stratégique dans le cadre de l'Observatoire du Monde Cybernétique, ce dernier publie des lettres mensuelles et trimestrielles de veille sur la cyber (accessibles à l'adresse suivante : http://www.defense.gouv.fr/das/reflexion-strategique/observatoires/observatoire-du-monde-cybernetique). Par ailleurs, la DAS a conduit plusieurs études prospectives et stratégiques sur la cyber, le lecteur pourra notamment se référer à l'étude « L'utilisation stratégique du cyber au Moyen-Orient » réalisée par Olivier Danino (http://www.defense.gouv.fr/das/reflexion-strategique/etudes-prospectives-et-strategiques).

254 Daniel Ventre (dir.), *Cyber Conflict : Competing National Perspectives*, Londres, 2012.

255 ANSSI, « Défense et sécurité des systèmes d'information : Stratégie de la France », Février 2011.

256 Nelly Moussu, « Renforcement de la cyberdéfense au ministère de la Défense », 5 septembre 2011, http://www.defense.gouv.fr/actualites/dossiers/sept-2011-cyberdefense-enjeu-du-21e-siecle/france/voir-les-articles/renforcement-de-la-cyberdefense-au-ministere-de-la-defense

257 Livre Blanc Défense et Sécurité Nationale 2013, p. 94.

258 Livre Blanc Défense et Sécurité Nationale 2013, p. 105.

259 Interview du contre-amiral Arnaud Coustillière, Officier Général cyberdéfense, « La cyberdéfense est l'une des priorités de la Défense », *Armées d'aujourd'hui*, décembre 2012–janvier 2013, n° 376, p. 38.

260 Philippe Bougeret (Col), OSSI-Terre, « Le défi de la cyberdéfense pour l'armée de Terre », *Transmetteurs*, 1er semestre 2013, n° 6, p. 22.

> « *L'organisation opérationnelle des armées intégrera ainsi une chaîne opérationnelle de cyberdéfense, cohérente avec l'organisation et la structure opérationnelles de nos armées, et adaptée aux caractéristiques propres à cet espace de confrontation : unifiée pour tenir compte de l'affaiblissement de la notion de frontière dans cet espace ; centralisée à partir du centre de planification et de conduite des opérations de l'état-major des armées, pour garantir une vision globale d'entrée et une mobilisation rapide des moyens nécessaires ; et spécialisée car demandant des compétences et des comportements adaptés*[261] ».

Cette **chaîne de cyberdéfense opérationnelle** intégrée aux structures de commandement existe depuis juin 2011 et est commandée par un officier général en charge de la cyberdéfense (OG Cyber). L'OG Cyber est rattaché au sous-chef opérations de l'EMA et son mandat porte sur l'ensemble des armées pour la partie transformation et développement des capacités[262].

En plus de la chaîne opérationnelle, une chaîne sécurité des systèmes d'information existe, elle est chargée de fabriquer des systèmes ayant une aptitude à opérer de manière sécurisée dans tous les espaces[263]. Le CALID est un maillon central de la chaîne cyberdéfense, il est chargé de veiller et d'analyser les réseaux informatiques, et d'alerter en cas d'attaque. Il garantit la réaction rapide des forces armées. Le CALID assure sa fonction de protection des systèmes d'information en parallèle de la chaîne « Sécurité des systèmes d'information » des forces armées[264].

Sur un théâtre d'opération

Sur un théâtre d'opération, au **niveau tactico-opératif,** la conduite des opérations inclut une composante cyberdéfense (selon le Livre Blanc 2013, qui regrouperait les domaines d'activité suivants : sécurité des systèmes d'information, lutte informatique défensive, lutte informatique offensive, guerre électronique, renseignement, voir *supra* chapitre 4). Le Commandant de la force est conseillé par deux officiers dont l'expertise porte sur des domaines essentiels en matière d'action dans le cyberespace :

- Le **Commandant des systèmes d'information et de communication interarmées de théâtre (COMSIC IAT),** assisté de l'officier SSI, supervise les réseaux opérationnels. Il est responsable de la mise en place des moyens humains et matériels nécessaires afin d'assurer la sécurité des réseaux et contrôle le respect des règles de sécurité[265]. Il peut dépêcher des techniciens spécialisés en SSI aux ordres d'un officier sécurité des systèmes d'information en liaison avec le CALID afin de limiter les effets d'une attaque éventuelle[266]. Le COMSIC IAT est subordonné au CPCO/J6, et placé sous l'autorité de l'Officier général à la Cyberdéfense,

- L'**officier Lutte Informatique Défensive (OLID)** est chargé de caractériser l'impact d'attaques cybernétiques sur les capacités opérationnelles et d'en rendre compte au commandant de la force. Il est notamment en charge de répertorier les systèmes d'armes affectés par une attaque et en conséquence inutilisables ou représentant un danger pour les hommes de la force.

Le COMSIC IAT assure la fonction d'OLID de théâtre.

Dans l'hypothèse où une force déployée serait l'objet d'attaques cybernétiques de grande ampleur, l'OG Cyber peut ordonner la mise en place d'une cellule de crise au CPCO.

Quelle organisation cyberdéfense pour l'armée de Terre ?

L'armée de Terre possède, comme chaque armée, sa propre chaîne SSI d'une part (le chef d'état-major de l'armée de Terre, autorité organique, est respon-

---

261 Livre Blanc Défense et Sécurité Nationale 2013, p. 94.

262 Grégoire Chaumeil, Anne-Lise Llouquet et Nelly Moussu, « Cyberespace le 5ème champ de bataille », *Armées d'aujourd'hui*, novembre-décembre 2011, n° 365, p. 47. Voir également Michel BAUD, « Cyberguerre – en quête d'une stratégie », *Focus stratégique* n° 44, IFRI, mai 2013, p. 30.

263 Centre des Hautes Études du Ministère de l'Intérieur, web émission CyberTalk n° 3, « Le ministère de la défense dans le cyberespace », mars 2013.

264 Site Internet officiel du Centre d'Analyse de Lutte Informatique Défensive, http://www.defense.gouv.fr/actualites/dossiers/sept-2011-cyberdefense-enjeu-du-21e-siecle/france/voir-les-articles/le-calid-l-expert-technique-en-securite-informatique-du-ministere/(language)/fre-FR#SearchText=CALID#xtcr=1

265 Grégoire Chaumeil, Anne-Lise Llouquet et Nelly Moussu, « Cyberespace le 5ème champ de bataille », *Armées d'aujourd'hui,* novembre-décembre 2011, n° 365, p. 51.

266 Michel Baud, « Cyberguerre – en quête d'une stratégie », *Focus stratégique* n° 44, IFRI, mai 2013, p. 31.

sable de la formation du personnel et de l'emploi des systèmes d'information dans l'armée de Terre), et LID d'autre part.

La chaîne LID des forces terrestres se replace dans la chaîne LID interarmées centralisée.

Dans ce cadre, l'armée de Terre a récemment mis en place une directive (CFT) décrivant la chaîne LID de la composante terrestre en opération. Les structures seront opérantes à court terme. Elle a également mis en place une capacité d'intervention rapide au sein des forces terrestres, à la disposition de la chaîne LID interarmées, ayant vocation à soutenir les théâtres d'opérations en cas d'attaque cybernétique importante[267]. Elle est donc en mesure d'assurer la protection de ces forces, cette protection reste d'abord insérée dans le maillage interarmées. La cyberdéfense s'opère de façon mutualisée, centralisée et unifiée au niveau interarmées sous la responsabilité de l'OG Cyber.

322 – Les États-Unis

Aux États-Unis, les services de la présidence ont publié en 2011 une stratégie internationale concernant le cyberespace, ce document s'intitule « *International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World* » (cette stratégie est l'équivalent de la Stratégie de défense et de sécurité des systèmes d'information publiée par l'ANSSI en 2011)[268]. La stratégie de la Maison Blanche a été déclinée au niveau militaire par un document élaboré par le *Department of Defense* intitulé « *Strategy for operating in cyberspace* »[269]. Celle-ci repose sur cinq piliers[270] :

- considérer le cyberespace comme un domaine opérationnel pour l'action militaire au même titre que la mer, la terre et l'espace, et défendre les réseaux les réseaux du DoD dans cet espace ;
- élaborer et employer de nouveaux concepts opérationnels pour protéger les systèmes d'information, parmi lesquels la lutte informatique défensive ;
- développer des partenariats avec le *Department of Homeland Security* et le secteur privé afin de protéger les infrastructures nationales critiques ;
- établir des relations de confiance et construire un système de sécurité collective dans le cyberespace avec des partenaires internationaux ;
- développer significativement la sécurité des réseaux à travers l'innovation technologique et l'expertise.

Avec près de 15 000 réseaux différents et 7 millions d'interfaces dans 88 pays différents[271], assurer la sécurité et la résilience des systèmes d'information est un défi pour le *Department of Defense* américain (DoD). Sur le plan organisationnel, le DoD a opté pour un commandement décentralisé subordonné à l'*United States Strategic Command* : le *United States*

source : http://www.arcyber.army.mil/org-uscc.html

267 Philippe Bougeret (Col), OSSI-Terre, « Le défi de la cyberdéfense pour l'armée de Terre », *Transmetteurs*, 1er semestre 2013, n° 6, p. 22.

268 The White House, "International Strategy for Cyberspace, Prosperity, Security and Openness in a Networked World", Mai 2011.

269 William Lynn, "Department of Defense strategy for operating in cyberspace", United States' Department of Defense, July 2011.

270 Cheryl Pellerin, "DOD Releases First Strategy for Operating in Cyberspace", U.S Department of Defense, 14 juillet 2011, http://www.defense.gov/news/newsarticle.aspx?id=64686

271 Paul Cornish, David Livingstone, Dave Clemente, Claire Yorke, "On Cyber Warfare", *Chatham House report*, novembre 2010, p. 15.

Cyber Command. Ainsi, chaque armée a ses propres capacités d'action dans le cyberespace et elles sont en partie gérées par le *CyberCom*. Néanmoins, le DoD envisagerait de créer un service cybernétique unifié, un « cyber service », semblable à l'US *Special Operations Command* (SOCOM) qui superviserait des opérateurs spécifiques dans chaque service mais pourrait également planifier et conduire des missions dans le cyberespace (le *Deputy Secretary of Defense* Ashton Carter a émis cette suggestion en juin 2013)[272].

Le commandant du ***U.S Cyber Command,*** identifie trois seuils critiques à atteindre pour maîtriser et gagner les futurs conflits[273] :

- La mise à disposition du commandement d'un panel de capacités d'action dans le cyberespace par le positionnement d'unités cyber à tous les niveaux de la force de façon synchronisée ;
- La conservation indispensable d'une liberté de manœuvre dans le cyberespace pour conserver l'initiative comme sur le terrain ;
- La garantie de la capacité des forces par la défense des systèmes de commandement contre toute attaque cybernétique.

Sur une proposition de budget annuel de 526,6 milliards de dollars pour 2014, le Pentagone consacrerait 4,7 milliards de dollars à la cyberdéfense[274]. Comprenant actuellement 900 personnes (civils et militaires), le *US CyberCom* pourrait voir ses effectifs atteindre 4 900 personnes avant 2015[275].

Le DoD accorde des moyens importants à la recherche sur la cyberdéfense. La DARPA (*Defence Advanced Research Projects Agency*), agence de recherche du DoD sur les technologies dans le secteur de la défense, a développé un projet de recherche intitulé « Plan X »[276]. Il consiste à explorer les possibilités de création de « technologies révolutionnaires pour comprendre, planifier et gérer le combatcyber en temps réel, à grande échelle et dans des environnements dynamiques » et leurs interactions avec les autres domaines (selon Kaigham J. Gabriel, directeur de la DARPA[277]). L'objectif est de fournir aux forces américaines les moyens de dominer le champ de bataille numérique, au même titre que les autres *global commons* : mer, terre, air et espace[278]. Le projet est financé à hauteur de 110 millions de dollars par le DoD.

À l'image des fonds investis par le DoD dans la recherche sur les activités militaires dans le cyberespace, la réflexion doctrinale sur l'acquisition d'une forme de suprématie dans le cyberespace et la conduite d'opérations militaires dans ce milieu est déjà bien avancée outre-atlantique. Elle associe des structures militaires, industrielles, mais aussi universitaires : 72 centres universitaires de recherche traitent de sujets sur le cyberespace, 10 % d'entre eux étudient la lutte informatique offensive et défensive (en incluant les opérations d'information)[279]. Les réflexions menées prévoient déjà les niveaux de compétences et de décisions adéquats pour l'emploi d'armes cybernétiques. Les États-Unis ont annoncé qu'ils se réservent le droit d'engager les moyens diplomatiques, économiques et militaires nécessaires en cas d'attaque cybernétique à leur encontre. Le DoD prépare un éventuel engagement dans le cyberespace en exploitant des systèmes non agres-

---

272 Daniel Wasserbly, "DoDcouldopt for 'cyber service', says Carter", *IHS Jane's Defense Weekly*, vol. 50, Issue 25, 19 juin 2013, p. 10.

273 Rhett A. Hernandez, LTG., "U.S. Army Cyber Command: Cyberspace for America's Force Of Decisive Action", *The Magazine of the Association of the United States Army*, October 2012, p. 205-208.

274 Laurent Lagneau, « Le Pentagone demande un budget de 526,6 milliards de dollars pour 2014 », *opex360.com*, 11 avril 2013, http://www.opex360.com/2013/04/11/le-pentagone-demande-un-budget-de-5266-milliards-de-dollars-pour-2014/

275 Ellen Nakashima, "Pentagon to boost cybersecurity force", *TheWashigtonPost.com*, 27 janvier 2013, http://articles.washingtonpost.com/2013-01-27/world/36583575_1_cyber-protection-forces-cyber-command-cybersecurity

276 Pour une analyse détaillée de ce projet, consulter Guillaume TISSIER, « La nouvelle initiative de défense stratégique américaine dans le cyberespace », *Les notes stratégiques*, CEIS, 2012, p. 18-21.

277 Guillaume Tissier, « La nouvelle initiative de défense stratégique américaine dans le cyberespace », *Les notes stratégiques*, CEIS, 2012, p. 18.

278 Jan Kallaberg, Bhavani Thuraisingham, "Cyber Operations: Bridging from Concept to Cyber Superiority", *Joint Force Quarterly*, Issue 68, 1st Quarter 2013, p. 53.

279 Jan Kallaberg, Bhavani Thuraisingham, "Cyber Operations: Bridging from Concept to Cyber Superiority", *Joint Force Quarterly*, Issue 68, 1st Quarter 2013, p. 57. La NSA a mis en place un système de désignation des centres universitaires de recherche afin de garantir la qualité des travaux d'enseignement et de recherche. Une approche pluridisciplinaire est retenue.

sifs en temps de paix afin d'identifier des failles dans les systèmes leur permettant en cas de conflit d'envoyer des codes informatiques malveillants[280]. Selon un document secret divulgué dans la presse en juin 2013, le Président des États-Unis aurait émis une directive encourageant plusieurs hauts responsables en matière de cyberdéfense à développer des capacités de destruction dans le cyberespace. Il envisagerait leur mise en œuvre contre un ennemi sans mise en garde[281]. Le document prévoirait également l'élaboration d'une liste de cibles potentielles constituées d'infrastructures étrangères vitales[282]. Début 2013, le *US Cyber Command* a officialisé la mise en place d'équipes expertes en lutte informatique offensive, spécialistes de la doctrine, des techniques, tactiques et procédures permettant de protéger les intérêts américains dans le cyberespace. À leur sujet, le commandant du CyberCom a déclaré : « *I would like to be clear that this team, this defend-the-nation team, is not a defensive team* »[283]. Ainsi, 27 équipes ont vocation à assister les commandants de force dans la planification d'attaques cybernétiques.

L'avance acquise par les forces armées américaines en matière de conflit dans le cyberespace ajoutée à ces prises de position confèrent aux États-Unis un poids certain dans les négociations internationales dans ce domaine spécifique (ce fut par exemple le cas dans l'élaboration du Manuel de Tallinn, auquel aucun expert français n'a participé). Aussi semble-t-il nécessaire d'ouvrir le débat doctrinal en France, et d'y associer les acteurs civils – industriels et universitaires tout particulièrement – afin de rayonner et faire valoir les conceptions doctrinales françaises élaborées ou en cours d'élaboration.

Quelles capacités d'action pour l'*U.S.army* dans le cyberepace ?

Les actions menées dans le cyberespace par les forces terrestres sont placées sous l'autorité du *Army Cyber Command*, celui-ci compterait près de 21 000 soldats et civils (contre 4 900 prévus sous peu pour le *US CyberCom*)[284]. Le *U.S Army Training and Doctrine Command* (TRADOC, l'équivalent américain du CDEF) a publié en janvier 2010 un plan d'action dans le cyberespace, le *Cyberspace Operations Concept Capabilities Plan* (CCP)[285]. Celui-ci se concentre sur la conduite d'opérations cybernétiques à l'horizon 2016-2028. La volonté affirmée est de laisser au chef militaire la liberté d'action dans le cyberespace et dans le spectre électromagnétique, tout en altérant cette liberté chez l'adversaire.

323 – La Chine

La communauté des internautes chinois est la première au monde : elle compterait 253 millions d'individus, contre 215 millions aux États-Unis et 273 millions dans l'Union européenne[286]. Les autorités chinoises sont fréquemment dénoncées pour le vol de secrets industriels et gouvernementaux. Le gouvernement américain, en particulier, prend ouvertement position sur l'implication de la Chine dans des opérations de cyberespionnage visant des sites gouvernementaux et certains secteurs de son économie (voir *infra*, chapitre 2). La République populaire de Chine s'appuie dans le cyberespace sur ce qui semble être une logique de guerre de l'information. Selon certains experts, les stratèges militaires chinois conçoivent la maîtrise de l'information comme le gage d'un succès global dans un conflit[287]. Des moyens importants semblent être mis à disposition

[280] Bertrand Boyer, *Cyberstratégie - l'art de la guerre numérique*, Paris, Nuvis, 2012, p. 166.

[281] Il s'agit de la Presidential Policy Directive 20. Robert O'HARROW Jr., Barton GELLMAN, "Secret cyber directive calls for ability to attack without warning", *TheWashingtonPost.com*, 8 juin 2013, http://articles.washingtonpost.com/2013-06-07/world/39817439_1_cyber-tools-president-obama-directive

[282] Glenn Greenwald, Ewen Mac Askill, "Obama orders US to draw up overseas Target list for cyber-attacks", *theguardian.com*, 7 juin 2013, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas

[283] Daniel Wasserbly, "CYBERCOM formulating "offensive teams"", *IHS Jane's Defense Weekly*, 20 mars 2013, Vol. 50, Issue 12, p. 12.

[284] John Reed, "How many cyber troops does the U.S Have?", *Foreign Policy*, 7 mars 2013, http://killerapps.foreignpolicy.com/posts/2013/03/07/how_many_cyber_troops_does_the_military_have

[285] The United States Army, "Cyberspace Operations Concept Capability Plan 2016-2028", TRADOC pamphlet 525-7-8, 22 février 2010, http://www.tradoc.army.mil/tpubs/pams/tp525-7-8.pdf

[286] Dossier « La Cyberguerre est déclarée », *Courrier international*, N° 1165, 28 février – 6 mars 2013, p. 33. Voir également Assemblée européenne de sécurité et de défense, « La guerre informatique », document C/2022, 5 novembre 2008, par. 144, p. 19.

[287] Eleanor Keymer, "The cyber-war", *Jane's Defense Weekly*, 29 septembre 2010, vol. 47, issue 39, p. 24.

de l'armée populaire, les réseaux informatiques publics et privés sont souvent infiltrés et des informations dérobées. La finalité serait de faire peser une menace permanente sur la confidentialité des échanges et des données, et la sécurité des infrastructures[288].

Peu d'information relative aux structures militaires de l'action chinoise dans le cyberespace est disponible. En 2013, une unité de l'Armée populaire de libération dédiée à la lutte informatique offensive aurait été identifiée par la société de sécurité informatique Mandiant. L'Unité 61398 de l'Armée populaire de libération dépendrait de la 2e section de la 3e division de l'état-major de l'armée chinoise. Ses attributions seraient semblables à celles de la NSA américaine et incluraient entre autres la surveillance des messages électroniques, l'analyse des informations recueillies par satellite, et le travail de décodage. L'unité 61398 emploierait 10 000 spécialistes[289]. En mai 2013, les autorités chinoises ont communiqué sur la tenue d'un « exercice digital » pour la première fois, permettant de tester de nouvelles tactiques de combat y compris celles des unités dédiées aux techniques numériques[290].

324 – L'Iran

L'Iran a été victime d'une attaque informatique de grande ampleur avec la propagation du ver Stuxnet dans le système d'une centrale nucléaire. En novembre 2010, suite à la découverte du code, l'Iran a créé le *Cyber Defense Command*. Placé sous l'autorité de l'Organisation de la défense passive iranienne, cette structure est responsable de la défense du pays et de la sécurité de ses infrastructures[291]. Depuis 2010 l'Iran aurait investi 1 milliard de dollars pour renforcer ses capacités de lutte informatique défensive et offensive[292]. Selon la CIA, l'Iran posséderait aujourd'hui l'une des cinq premières « cyberarmées » au monde, dotée d'un budget estimé à 58 millions d'euros, et composée de plus de 2 400 experts et 12 000 réservistes[293].

En matière de lutte informatique offensive, l'Iran semble opter pour une stratégie indirecte en soutenant des organisations non-étatiques – des cyberorganisations – qui défendent ses intérêts dans le cyberespace. L'*Iran Cyber Army*, par exemple, est une cyberorganisation composée de spécialistes informatiques et de hackers. Ces civils sont néanmoins soutenus par le pouvoir[294].

Une structure officielle semble toutefois être rattachée aux forces armées iraniennes : il s'agit d'une unité cybernétique au sein d'une branche des Gardiens de la Révolution appelée « Conseil du cyberespace ». Ce dernier collabore avec des cyberorganisations et a un rôle de formation des *hackers*[295].

325 – Israël

Israël a retenu une stratégie institutionnelle, l'ensemble des efforts en matière de lutte informatique défensive et offensive est organisé par des institutions étatiques et le Ministère de la Défense possède une administration centrale chargée de la question cyber et des unités opérationnelles rattachées au commandement de Tsahal.

---

288 Alain Esterle, Bruno Gruselle et Bruno Tertrais, « Cyber Dissuasion », Fondation pour la Recherche Stratégique, 2012, n° 3, p. 18.

289 Dossier « La Cyberguerre est déclarée », *Courrier international*, N° 1165, 28 février – 6 mars 2013, p. 33. Voir également Sébastian SEIBT, « L'unité 61398, nid de cyber-espions chinois ? », *France24.com*, 19 février 2013, http://www.france24.com/fr/20130219-unite-61398-mandiant-attaque-chine-cyberespionnage-piratage-pcc-armee-shanghai-uglygorilla-dota

290 Anonyme, "China War Games: Army To Conduct Its First Digital Technology Military Exercise", Reuters, 28 mai 2013, http://www.huffingtonpost.com/2013/05/28/china-war-games-digital-technology-exercise-planned_n_3349794.html

291 Olivier Danino, « L'utilisation stratégique du cyber au Moyen-Orient », p. 12, étude confiée à M. Danino par la Délégation aux Affaires Stratégiques.

292 Ehsan Taghadosi, « Pour Téhéran, la meilleure défense c'est l'attaque », *Kheshab.com*, in « La Cyberguerre est déclarée », *Courrier international*, N° 1165, 28 février – 6 mars 2013, p. 34.

293 « La Cyberguerre est déclarée », *Courrier international*, N° 1165, 28 février – 6 mars 2013, p. 34.

294 Nasser Karimi, "Report: Iran's paramilitary launchers cyber attack", *TheWashingtonPost.com*, 14 mars 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/03/14/AR2011031401029.html. Voir également Olivier Danino, « L'utilisation stratégique du cyber au Moyen-Orient », p. 13, étude confiée à M. Danino par la Délégation aux Affaires Stratégiques.

295 Olivier Danino, « L'utilisation stratégique du cyber au Moyen-Orient », p. 14, étude confiée à M. Danino par la Délégation aux Affaires Stratégiques.

L'armée israélienne figure parmi les *leaders* en matière de capacités de lutte informatique défensive et offensive. En 2007, l'opération ORCHAD a démontré le savoir-faire des Israéliens en matière de *hacking radar*. En outre, lors des opérations « Plomb Durci » en 2008-2009 et « Pilier de défense » en 2012, l'utilisation des réseaux sociaux comme outil de communication innovait en matière d'utilisation du champ numérique dans le cadre d'un conflit conventionnel.

Parallèlement à la création d'une industrie solide en matière de SSI, le gouvernement israélien sensibilise dès le plus jeune âge la population aux vulnérabilités liées au cyberespace et à la nécessité d'une hygiène cybernétique.

En termes de structure, le Ministère de la Défense a créé une administration centrale en charge de la cyber en janvier 2012, dont le rôle est de coordonner les efforts des services de sécurité et de soutenir les industries de défense. Concernant l'armée, un centre de cyberdéfense a été créé et surveille les tentatives d'attaques sur les réseaux militaires. Sur le plan militaire, plusieurs structures agissent dans le cyberespace[296] :

- l'Unité 8200[297] est spécialisée dans le renseignement d'origine électromagnétique et le décryptage de codes. Au sein de cette unité, on trouverait :
  - l'unité *Hatzav*, chargée de collecter l'information en open source,
  - une unité projetable sur le terrain ;
- la Direction des Services informatiques est responsable des communications et transmissions au sein de Tsahal. En son sein, on trouve :
  - le *C41 Corps*,
  - une unité opérationnelle (*hayelAhafala*), cette cellule aurait pour rôle d'intervenir auprès des soldats déployés sur le terrain et dont les équipements auraient été atteints par une attaque cybernétique[298],
  - l'unité des télécommunications et des technologies de l'information (*Lotem*).

Deux points sont à souligner en matière de formation : d'une part, Tsahal organise de nombreuses formations pour ses soldats afin de s'assurer un « réservoir de compétences » suffisant, le nombre de militaires spécialisés dans le domaine cybernétique a ainsi augmenté ; d'autre part, en 2012 le *C41 Corps* a mis en place un programme de formation des officiers supérieurs afin de leur enseigner la manière dont le cyberespace affecte les opérations sur le terrain[299].

Les approches nationales en matière de cyberdéfense et d'action dans le cyberespace sont très variées en moyens comme en avancées : alors que les États-Unis conçoivent des règles d'engagement concernant l'action de leurs forces armées dans le cyberespace, certains États, notamment des pays membres de l'OTAN, n'ont toujours pas adopté de stratégie nationale. Dans un domaine d'action où les menaces ne connaissent pas les frontières, il est indispensable d'améliorer les relations de confiance et de privilégier une approche bilatérale sur un sujet très sensible car directement lié à la souveraineté nationale.

296 Olivier Danino, « L'utilisation stratégique du cyber au Moyen-Orient », p. 8-11, étude confiée à M. Danino par la Délégation aux Affaires Stratégiques.

297 « *Yehida Shmoné Matayim* » en hébreu.

298 Anonyme, « Tsahal ouvre sa cellule de guerre contre les cyber-attaques », *Tsahal.fr*, 4 mars 2013, http://tsahal.fr/2013/03/04/tsahal-ouvre-sa-cellule-de-guerre-contre-les-cyber-attaques/

299 Olivier Danino, « L'utilisation stratégique du cyber au Moyen-Orient », p. 10, étude confiée à M. Danino par la Délégation aux Affaires Stratégiques.

CHAPITRE 4

ARMÉE DE TERRE, MANŒUVRE TERRESTRE ET « CYBERGUERRE » : LA COMBINAISON DE LA GUERRE NUMÉRIQUE AVEC LE CHAMP DE BATAILLE CONVENTIONNEL

« Si la dimension opérationnelle [des capacités de lutte informatique active de la France] doit demeurer secrète, on doit s'interroger sur la pertinence d'ouvrir un débat doctrinal comme certains pays l'ont fait[300] *».*

Jean-Marie BOCKEL

« [...] la capacité informatique offensive, associée à une capacité de renseignement, concourt de façon significative à la posture de cybersécurité. Elle contribue à la caractérisation de la menace et à l'identification de son origine. Elle permet en outre d'anticiper certaines attaques et de configurer les moyens de défense en conséquence. La capacité informatique offensive enrichit la palette des options possibles à la disposition de l'État[301] *».*

Livre Blanc Défense et Sécurité Nationale 2013

L'émergence d'un nouveau domaine de combat est une situation rare. Les caractéristiques du cyberespace comme nouveau champ de bataille en font un domaine unique[302] :

1) 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 ;

2) le cyberespace est un espace sans frontières ;

3) 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 ;

4) 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 ;

5) l'évolution permanente des techniques et technologies font du cyberespace un milieu en perpétuelle évolution.

[300] Sénateur Jean-Marie Bockel, « Cyberdéfense : la France a des atouts », *Revue DÉFENSE*, n° 159, novembre-décembre 2012, p. 40.
[301] Livre Blanc Défense et Sécurité Nationale 2013, p. 105.
[302] Fred Schreier, "The Report on Cyberwarfare", DCAF, 2012, p. 93-94.

Dans un contexte où les conflits comportent désormais un volet combat dans le cyberespace, il apparaît indispensable d'intégrer cette nouvelle dimension au cadre conventionnel des opérations. Concernant leurs actions dans le cyberespace, les États-Unis parlent de « *cyber electronic warfare* », et la Chine d'« *integrated network electronic warfare* »[303]. Mais chacun aurait une stratégie propre conjuguant des actions cybernétiques avec le champ de bataille conventionnel, incluant des éléments de sécurité des systèmes d'information, de lutte informatique active et de guerre électronique, tout en recouvrant le champ des opérations de renseignement, des opérations psychologiques, des opérations d'information et de contre-commandement[304].

Après avoir défini le concept de *network centric warfare* (section 1), une proposition de combinaison en temps de guerre des différents domaines identifiés ci-dessus sera explorée en vue d'insérer la guerre numérique au champ de bataille traditionnel (section 2). Les éléments ci-dessous ne sont que des pistes de réflexion et ne témoignent pas des axes explorés et/ou retenus par les forces armées françaises.

41 – GUERRE RÉSEAU-CENTRÉE (*NETWORK CENTRIC WARFARE*) : DE QUOI S'AGIT-IL ?

Le concept de guerre réseau-centrée ou *Network Centric Warfare* (NCW) en anglais fut introduit par la RMA[305] (*the Revolution in Military Affairs*)[306].

Dans ce modèle théorisant les conflits dans le seul cyberespace, l'ennemi est considéré comme un nœud inséré dans un réseau. En parvenant à atteindre les nœuds centraux d'un réseau ennemi, on parvient à atteindre l'ennemi en désorganisant ses systèmes et en le rendant ainsi inopérant en raison de sa dépendance aux systèmes informatiques[307].

Dans les forces armées américaines, la NCW est développée depuis les années 1995 afin de faciliter les échanges d'information entre les différentes armées accélérant ainsi le processus décisionnel pour atteindre une plus grande efficacité militaire. Le concept inclut des technologies interconnectées *via* MILNET (le réseau informatique et de télécommunications militaire américain étendu dans le monde entier). La finalité du NCW est le *knowledge superiority*, c'est-à-dire six fonctions essentielles : commandement, contrôle, communication informatique, renseignement, surveillance, et reconnaissance (C4ISR)[308]. En développant ces capacités au maximum, il s'agit de gérer l'incertitude de façon optimale. L'idée centrale est qu'en assurant la supériorité technologique de la force, on affirme dans le même temps sa supériorité opérationnelle. La NCW repose sur un triptyque :

- en permanence, il s'agit de recueillir des informations sur les structures et données des systèmes adverses ;
- quand elles sont décidées, des attaques cybernétiques visent les systèmes de commandement et les systèmes de navigation ;
- ensuite, les attaques visent la base organisationnelle de l'ennemi, sa logistique et ses appuis, et des structures d'information.

Si le concept de *Network Centric Warfare* a eu un retentissement certain au début des années 2000 dans un contexte où les sociétés civiles aspiraient à une guerre « zéro mort », il est vite apparu limité en raison de l'impossibilité de maîtriser totalement le champ informationnel et électromagnétique. La décision dans l'incertitude reste une dimension réelle de l'action militaire, le Général Desportes le rappelle ainsi : « *Finalement, quelles que soient l'époque ou les technologies disponibles, la clef de l'efficacité du commandement demeurera, au fond, la capacité à traiter*

303 Stéphane Dossé, « Penser opérationnellement la cyberguerre », *in* Stéphane Dossé, Olivier Kempf, Christian Malis (dir.), *Le cyberespace : Nouveau domaine de la pensée stratégique*, Economica, Paris, 2013, p. 117-123.

304 Bertrand Boyer, *Cyberstratégie - l'art de la guerre numérique*, Paris, Nuvis, 2012, p. 81.

305 La RMA est une théorie développée par les forces armées américaines intégrant comme facteurs prépondérants de l'action militaire les nouvelles technologies permettant de nouvelles façons de communiquer, de recueillir, traiter et transmettre l'information. La RMA devait permettre aux forces U.S d'atteindre une parfaite connaissance de leur environnement « *perfect situational awareness* » et une domination complète du spectre (« *full spectrum dominance* »). Le concept semble avoir été abandonné par le Pentagone. Voir Scott Stephenson (LCL), "The Revolution in Military Affairs: Observations on an Out-of-Fashion Idea", *Military Review*, mai-juin 2010, p. 38.

306 Mc Quade Samuel C., III (ed.), E*ncyclopedia of Cybercrime*, Westport, Greenwood Press, 2009, p. 132-133.

307 Grégoire Chamayou, *Théorie du Drone*, La Fabrique éditions, 2013, p. 53.

308 Roger Darby, "Cyber Defense in Focus: Enemies Near and Far – or Just Behind the Firewall: The Case for Knowledge Management", Defense Studies, *Journal of Military and Strategic Studies*, Vol. 12, n° 4, décembre 2012, p. 523-538.

le problème de l'incertitude[309] ». Une réflexion sur la combinaison des opérations dans le cyberespace à une action militaire conventionnelle a été initiée afin de traduire en avantage militaire sur le terrain une certaine maîtrise de l'environnement informationnel.

42 – LA GUERRE CYBERNÉTIQUE COMME COMPOSANTE DE L'ACTION TERRESTRE : COMBINAISON AVEC LE CHAMP DE BATAILLE CONVENTIONNEL

L'emploi d'armes cybernétiques est lié à une inconnue : la résilience des systèmes adverses. En menant une attaque cybernétique contre un système adverse, il est impossible de prévoir avec certitude le succès de l'attaque et difficile de connaître l'étendue exacte des effets : on ne sait pas si le système adverse va être paralysé pendant une heure ou une semaine. En conséquence, l'arme cybernétique ne peut pas avoir une autonomie stratégique, sa fonction reste dans l'appui des missions traditionnelles des forces terrestres et des forces armées en général.

Martin Libicki, chercheur à la RAND Corporation, écrit : « *operational cyberwar cannot win an overall war on its own; it is a support function*[310] ».

421 – La cyberguerre comme composante opérationnelle des forces terrestres : approche américaine

En 2011, l'*U.S Army* a publié un document relatif à la cyberguerre comme composante opérationnelle de l'*U.S Army* pour la période 2016-2028[311]. Ce plan repose sur deux postulats :

- Le premier dispose que dominer le champ cyber-électronique repose sur trois éléments indissociables : gagner l'avantage, protéger cet avantage, et mettre les adversaires en situation de désavantage[312].

- Le second postulat exige pour le chef militaire de conserver sa liberté d'action dans le cyberespace et sur le champ électromagnétique, tout en privant ses adversaires de cette prérogative ; ainsi, il rend possible toute activité dans et par le cyberespace, et en conséquence dans les quatre autres domaines (terre, air, mer, espace)[313]. L'action dans le cyberespace est conçue comme un *force-multiplier*.

L'armée américaine nomme les activités qu'elle mène dans le cyberespace *computer network operations* (CNO), elles s'articulent autour de trois composantes, la défense, l'attaque, et l'exploitation[314] :

- défense des réseaux informatiques : empêcher la pénétration de ses propres réseaux ;

- attaque des réseaux informatiques : observer en pénétrant les réseaux et systèmes adverses afin d'identifier les failles et ou de mener des actions interrompant, altérant ou détruisant l'information ;

- exploitation des réseaux informatiques : exploiter les informations recueillies dans les réseaux et systèmes adverses.

309 Général Vincent Desportes, *Décider dans l'incertitude*, Economica, Paris, 2007, 2e édition, p. 208.

310 Martin C. Libicki, "Cyberdeterrence and cyberwar", RAND, Project Air Force, 2009.

311 The United States Army, "Cyberspace Operations Concept Capability Plan 2016-2028", TRADOC pamphlet 525-7-8, 22 février 2010, http://www.tradoc.army.mil/tpubs/pams/tp525-7-8.pdf

312 The United States Army, "Cyberspace Operations Concept Capability Plan 2016-2028", TRADOC pamphlet 525-7-8, 22 février 2010, p. iv.

313 The United States Army, "Cyberspace Operations Concept Capability Plan 2016-2028", TRADOC pamphlet 525-7-8, 22 février 2010, p. iv. Le second postulat affirme que ces opérations cybernétiques incluent des activités en temps de paix, de façon continue, quotidiennement : *"Commanders seek to retain freedom of action in cyberspace and in the EMS, while denying the same to adversaries at the time and place of their choosing; thereby enabling operational activities in and through cyberspace and consequently the other four domains. CyberOps encompass those actions to gain the advantage, protect that advantage, and place adversaries at a disadvantage in the cyber-electromagnetic contest. CyberOps are not an end to themselves, but rather an integral part of FSO and include activities prevalent in peacetime military engagement, which focus on winning the cyber-electromagnetic contest. CyberOps are continuous; engagements occur daily, most often without the commitment of additional forces"*.

314 Robert A. Miller, Daniel T. Kuehl, Irving Lachow, "Cyber War; Issues in Attack and Defense", *Joint Force Quarterly*, Issue 61, 2nd quarter 2011, p. 18-23.

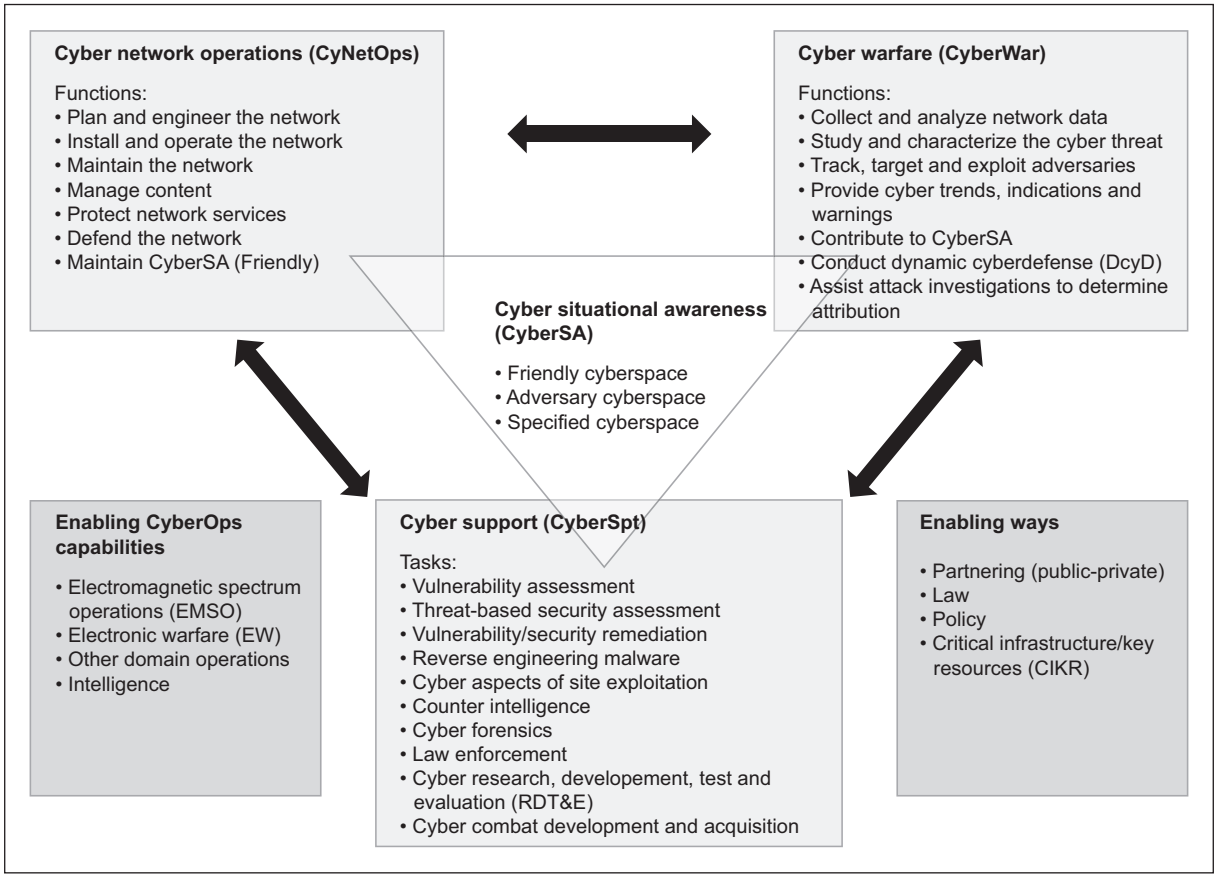
Ainsi, les attaques cybernétiques seraient utilisées afin de déstabiliser la société civile du pays cible et de gêner son action militaire. Certains auteurs parlent d'*information and infrastructure operations* (I^2Os), ayant pour finalité de gêner, rendre confus, démoraliser, distraire l'ennemi et diminuer ses capacités de réaction[315].

Les opérations dans le cyberespace sont regroupées sous l'appellation *CyberOps*. Dans la conception américaine, les *CyberOps* font partie d'un spectre plus large d'opérations qui incluent des activités militaires en temps de paix orientées vers la maîtrise du spectre électromagnétique. Le cadre développé pour la conduite d'opérations militaires dans le cyberespace repose sur quatre composantes : la guerre cybernétique (*CyberWar*), les opérations cybernétiques sur les réseaux (*CyNetOps*), le support cybernétique (*CyberSpt*) et le « *cyber situational awareness* » (*CyberSA*)[316]. Le schéma ci-dessous illustre les possibilités de combinaison des *CyberOps*.

Si ces opérations ne sont pas la compétence exclusive de l'U.S Army, il est intéressant de réfléchir aux capacités des forces terrestres et à l'élaboration de tactiques dans ces domaines.

422 – Les actions dans le cyberespace en appui aux forces terrestres traditionnelles : pistes de réflexion

Conformément aux recommandations du rapport Bockel, le Livre Blanc 2013 souligne la volonté d'accentuer les efforts dans le domaine de la cyberdéfense :



Source : Jason ANDRESS, Steve WINTERFIELD, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Syngress, 2011, p. 41.

[315] Robert A. Miller, Daniel T. Kuehl, Irving Lachow, "Cyber War; Issues in Attack and Defense", *Joint Force Quarterly*, Issue 61, 2nd quarter 2011, p. 18-23.

[316] Jason Andress, Steve Winterfield, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Syngress, 2011, p. 40-41.

« *Le développement de capacités de cyberdéfense fera l'objet d'un effort marqué, en relation étroite avec le domaine du renseignement. 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*[317] ».

Le Livre Blanc 2013 définit trois capacités d'action clés dans le cyberespace :

- la **sécurité des systèmes d'information**[318] qui doit permettre la protection et la résilience des systèmes d'information de l'État, des opérateurs d'infrastructures vitales et des industries stratégiques ;

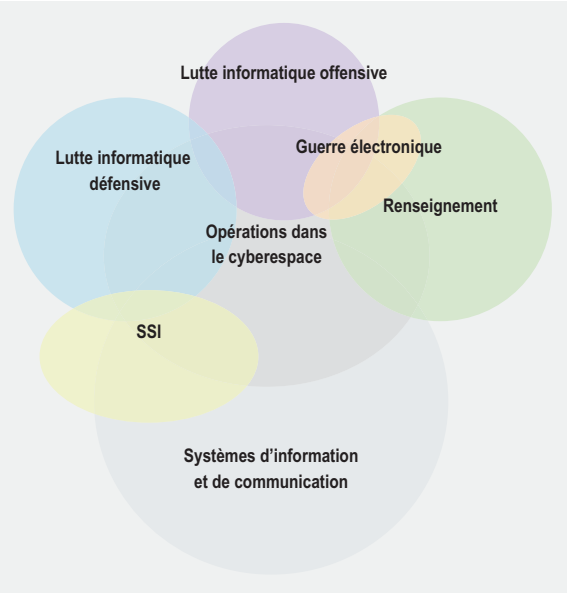
- les **luttes informatiques défensives et offensives**[319], deux domaines qui contribuent à l'identification d'une menace et de son origine, permettent d'anticiper les attaques et améliorent la résilience des systèmes ;

- le **renseignement**[320], c'est-à-dire le traitement d'informations recueillies à travers des sources ouvertes ou des opérations clandestines dans le cyberespace, permettant d'évaluer les dispositifs adverses, de détecter les attaques et d'identifier leur(s) auteur(s).

Les forces armées mettent en œuvre ces capacités au sein de la chaîne de commandement cyber (voir *infra* chapitre 3). Les opérations dans le cyberespace regroupent plusieurs activités (illustration ci-contre).

Les forces terrestres possèdent des capacités d'action dans l'ensemble de ces domaines, deux niveaux d'exploitation existent : en interne (l'armée de Terre possède sa propre chaîne SSI, LID, assure la protection de ses SIC), et en interarmées dans le cadre de la chaîne de commandement « cyber » unifiée.

En utilisant la structure des *Computer Network Attacks* telle qu'elle est conceptualisée par l'*U.S Army* (défense, attaque, surveillance/exploitation), des pistes de réflexion sur la combinaison du cyber-



DAS – OMC, « Observatoire du Monde Cybernétique », Trimestriel juin 2013.

espace avec les forces terrestres conventionnelles peuvent être esquissées. Ces trois niveaux interagissent en permanence, il s'agit de dresser un aperçu de la façon dont ils peuvent se concrétiser aux niveaux stratégique, opératif et tactique. Si le niveau tactico-opératif est d'intérêt principal pour les forces terrestres, il est malgré tout indispensable de voir comment des actions entreprises au niveau stratégique dans le cyberespace peuvent se greffer à l'action des forces terrestres et l'impacter.

Niveau Stratégique

Bien qu'elle soit sujette à controverse, une réflexion doctrinale encourage l'action sur les systèmes adverses d'information et de communications, malgré l'absence de consensus sur la façon d'appliquer le droit international et en particulier le droit des conflits armés, aux opérations militaires dans le cyberespace. Elle repose sur l'idée qu'une attaque cybernétique est moins dangereuse à l'égard des populations civiles qu'une attaque militaire traditionnelle impliquant l'utilisation de la force létale. Dans un contexte où causer des dommages collatéraux peut avoir des répercussions importantes sur la scène internationale[321], une attaque cybernétique présen-

317 Livre Blanc Défense et Sécurité Nationale 2013, p. 94.
318 Livre Blanc Défense et Sécurité Nationale 2013, p. 106.
319 Livre Blanc Défense et Sécurité Nationale 2013, p. 107.
320 Livre Blanc Défense et Sécurité Nationale 2013, p. 107.

321 Brian T. O'Donnell, James C. Kraska, "Humanitarian Law: Developping International Rules for the Digital Battlefield", *Journal of Conflict and Security Law*, 2003, Vol. 8 No. 1 p. 138.

terait un avantage certain. Néanmoins, l'arme cybernétique reste une arme dont on ne maîtrise pas nécessairement les effets et dont les conséquences peuvent être dévastatrices (les effets des attaques menées contre l'Estonie et la Géorgie, eurent des conséquences matérielles importantes, notamment en provoquant le dysfonctionnement d'activités économiques et politiques.

Au niveau stratégique, les opérations relèvent de la chaîne opérationnelle cyberdéfense de niveau interarmées. Néanmoins, dans le cyberespace les frontières entre les trois niveaux ne sont pas aussi clairement définies que dans la science militaire traditionnelle, et des actions entreprises au niveau stratégique dans le cyberespace peuvent directement avoir un impact sur le soldat sur le terrain, et vice versa (*cf.* l'effet caporal stratégique développé en relation avec les réseaux sociaux, *infra* chapitre 2). Le Livre Blanc 2013 a affirmé ouvertement la nécessité de détenir et d'exercer des capacités de lutte informatique offensive afin d'atteindre un état de cybersécurité. Elles contribuent à identifier la menace et son origine, et à anticiper certaines attaques sur les systèmes des forces (voir *infra*).

Niveau opératif

Le niveau opératif, niveau de coopération et de coordination des actions interarmées[322], est déterminant en matière d'actions dans le cyberespace.

La conduite d'attaques cybernétiques en complément d'une action militaire traditionnelle ouvre un nouveau champ des possibles pour les forces armées. La maîtrise du champ cybernétique et électromagnétique peut devenir un démultiplicateur de force. Lors de l'opération ORCHAD, les Israéliens ont conservé l'effet de surprise grâce à des attaques menées contre le système antiaérien syrien et entraînant sa paralysie, alors qu'en parallèle une opération aérienne visant à détruire le réacteur nucléaire syrien de Dayr ez-Zor était lancée (voir *infra* chapitre 2). En Libye, les États-Unis auraient envisagé la conduite d'attaques cybernétiques contre les défenses sol-air libyennes afin de faciliter les opérations aériennes[323].

La maîtrise du champ de l'information est également un élément clé de l'efficacité militaire. Communiquer, recueillir du renseignement en source ouverte ou par les moyens d'attaques cybernétiques, sont essentiels au niveau opératif. Dans le cadre de l'opération en Lybie, des responsables militaires de l'OTAN ont confirmé que Twitter était une source de renseignement pour les forces, des Libyens ayant adressé des *twitts* à la coalition afin de leur communiquer le positionnement en temps réel des troupes du Colonel Kadhafi[324].

Quant à la surveillance, dont la finalité est d'extraire des informations des réseaux numériques adverses explorés, elle se décline aussi bien au niveau stratégique que tactico-opératif[325] par le moyen d'attaques cybernétiques et de guerre électronique.

Niveau tactique

Afin de dominer le cyberespace et démultiplier l'effet des forces de l'armée de Terre, au niveau tactique et sur le plan offensif, les forces terrestres pourraient recourir à plusieurs procédés : la destruction physique des antennes, l'injection d'un ver, virus, ou cheval de Troie dans le système adverse, ou encore le brouillage électromagnétique par impulsions électromagnétiques afin d'interrompre la transmission d'ordres adverses.

Sur le plan défensif, la combinaison du champ de bataille numérique au champ de bataille traditionnel est tout aussi déterminante pour les forces terrestres : la défense de tous les systèmes de protection tels que le brouillage anti-IED et les leurres déjà intégrés dans les véhicules tactiques sont une forme de combinaison entre les deux champs[326].

Un nouvel espace du champ de bataille est apparu avec la montée en puissance des systèmes d'information au sein des forces armées, l'action militaire

322 Armée de Terre, *Tactique générale*, Economica, 2008, p. 11-12.
323 Michel Baud, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », IFRI, *Politique étrangère*, 2012, n° 2, p. 311.
324 Marguerite de Durand, Marc Hecker, Thibault Souchet, Nicolas Vanbremeersch, « Nature et conséquences des réseaux sociaux pour les forces armées », IFRI, spintank, p. 124.
325 Aymeric Bonnemaison, « Vers un "combat cyberélectronique" ? », *in* Stéphane Dossé, Olivier Kempf, Christian Malis, *Le cyberespace : Nouveau domaine de la pensée stratégique*, p. 133-137.
326 Aymeric Bonnemaison, « Vers un "combat cyberélectronique" ? », *in* Stéphane Dossé, Olivier Kempf, Christian Malis, *Le cyberespace : Nouveau domaine de la pensée stratégique*, p. 133-137.

dans le cyberespace unit le spectre électromagnétique à la dimension informatique. On constate que de mêmes modes d'action (guerre électronique, opérations d'information, sécurité des systèmes d'information) sont efficaces à plusieurs niveaux à la fois, c'est très souvent le cas entre le niveau tactique et le niveau opératif. Face à cette interconnexion des niveaux stratégique, opératif et tactique dans l'action cybernétique, Michel Baud défend la mise en place d'unités interarmées au niveau opératif :

« *La réponse cyber développée par les armées, au-delà de son aspect purement défensif, doit donc se faire au niveau opératif grâce à des unités interarmées. C'est en effet le dernier niveau où le chef militaire possède une vue de l'ensemble des opérations menées sur un théâtre, or le champ d'action du cyber est transverse, il irrigue l'ensemble des autres domaines (terre, air, mer et espace)*[327] ».

[327] Baud Michel, « Cyberguerre. En quête d'une stratégie », *Focus stratégique*, n° 44, mai 2013, p. 35.

CONCLUSION

En 2002, Michael N. Schmitt, titulaire de la chaire droit international du *United States Naval WarCollege* et chercheur associé au Centre d'Excellence de Tallinn, écrivait : « *Perhaps equally remarkable will be the maturing of "information warfare" as a tool of combat*[328] ». Le poids de l'information dans nos sociétés en a fait une composante incontournable de l'action des forces terrestres à travers différents domaines. Si les opérations d'information peuvent permettre de « gagner les cœurs et les esprits » et ainsi contribuer à la victoire, la maîtrise des systèmes d'information et de communication et la sécurisation de l'information transitant ou stockée participent du succès militaire. Dominer le spectre électromagnétique et numérique est nécessaire pour conserver sa capacité d'action et contraindre l'adversaire. Néanmoins, les vulnérabilités liées à l'utilisation de systèmes informatiques et numériques par les forces terrestres en opérations (systèmes d'armes, systèmes de commandement, etc.) et dans leur environnement (réseaux sociaux) ainsi que l'aléa concernant les capacités opérationnelles d'ennemis potentiels dans le cyberespace peuvent susciter un climat d'incertitude.

> « *L'imprévu est en voie de transformation et l'imprévu moderne est presque illimité [...]. Au lieu de jouer avec le destin, comme autrefois, une honnête partie des cartes, connaissant les conventions du jeu, connaissant le nombre de cartes et les figures, nous nous trouvons désormais dans la situation d'un joueur qui s'apercevrait avec stupeur que la main de son partenaire lui donne des figures jamais vues et que les règles du jeu sont modifiées à chaque coup* ».
>
> Paul Valéry
> *Regards sur le monde actuel et autres essais,*
> Gallimard, Paris, 2002, p. 195-196

Nouvel espace de combat, le cyberespace ouvre un nouveau champ des possibles aux niveaux stratégique et tactique. Concernant les forces terrestres, au niveau tactico-opératif un contingent engagé sur un théâtre d'opération sera vraisemblablement tout aussi vulnérable à une attaque cybernétique qu'à un missile antichar. Néanmoins, la menace cybernétique pesant sur les forces terrestres en régiment et en opération est non seulement diffuse et permanente (cartographie des réseaux, recueil d'information, etc.), mais encore ponctuelle et ciblée (attaque d'un système de commandement, d'armement, etc.). Il apparaît donc indispensable d'intégrer cette nouvelle dimension au cadre conventionnel des opérations. Cette menace est déjà prise en compte dans la protection et la défense des SI et la gestion de crise au niveau interarmées ainsi que dans les structures SSI et de lutte informatique défensive au niveau armée de Terre, afin d'assurer la continuité des systèmes exploités par les forces. Ainsi, l'armée de Terre s'inscrit dans la chaîne interarmées de cyberdéfense, pilotée par l'OG CYBER. Elle contribue, en interarmées d'abord et en propre ensuite, à la cyberdéfense. La doctrine interarmées est en place. Elle précise l'ensemble du dispositif cyberdéfense des armées.

De son côté, l'armée de terre s'inscrit totalement dans ce dispositif et décline les structures organisationnelles qui prolongent les structures interarmées.

Une réflexion propre à l'armée de Terre est en cours, afin de dresser un panorama des enjeux et opportunités de la cyberconflictualité dans les opérations interarmes

[328] Michael N. Schmitt, "Wiredwarfare : Computer network attack and j*us in bello*", *Revue internationale de la Croix Rouge*, juin 2002, vol. 84, n° 846, p. 365.

GLOSSAIRE

Plusieurs définitions provenant de différentes sources sont recensées pour chaque terme du glossaire dans le but d'illustrer les différences d'interprétation existantes et les difficultés inhérentes à l'absence de consensus sur la terminologie.

Arme informatique, ou cyberarme

Thomas RID, Peter McBURNEY

> Une cyberarme est vue comme un sous-ensemble d'armes et plus généralement un code informatique qui est utilisé ou conçu pour être utilisé avec pour finalité de menacer ou de causer des dommages physiques, fonctionnels ou psychologiques aux structures, systèmes ou organismes vivants[329].

Michel BAUD

> 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[330].

Cyberattaque ou attaque cybernétique

Manuel de Tallinn

> Opération cybernétique, défensive ou offensive, dont on peut raisonnablement attendre qu'elle blesse ou tue des personnes, ou entraîne des dommages ou la destruction de biens[331].

Cyberdéfense

ANSSI

> « Ensemble des mesures techniques et non techniques permettant à un État de défendre, dans le cyberespace, les systèmes d'information jugés essentiels »[332].

Armées françaises

> La cyberdéfense désigne l'ensemble des activités conduites dans le cyberespace pour garantir l'efficacité de l'action des forces armées, leur capacité à opérer en étant soumises à des attaques informatiques, la réalisation des missions confiées et le bon fonctionnement du Ministère. Elle vise à assurer la défense active permanente et en profondeur des systèmes d'information du Ministère en associant des capacités de protection et de défense des systèmes d'information, ainsi qu'une capacité de gestion de crise[333].

US Department of Defense (Joint Chiefs of Staff, « *Joint terminology for cyberspace Operations* », 2010)

> Application intégrée des capacités dans le cyberespace du département de la défense ou du gouvernement américain, et des processus qui permettent de synchroniser en temps réel les moyens permettant de détecter, d'analyser et atténuer les menaces et vulnérabilités, ainsi que de contrer les manœuvres de l'adversaire, afin de défendre les réseaux désignés, protéger les missions critiques et permettre la liberté d'action américaine. La cyberdéfense inclut :

---

329 Thomas Rid, Peter Mc Burney, "Cyber-Weapons", *The RUSI Journal*, vol. 157, n° 1, p. 7.

330 Michel Baud, « Cyberguerre. En quête d'une stratégie », *Focus stratégique*, n° 44, mai 2013, p. 11.

331 The International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, *Tallinn Manual on the international law applicable to cyber warfare*, (ci-après appelé « Manuel de Tallinn »), General editor Michael N. Schmitt, Cambridge University Press, p. 106. La règle 30 dispose : « *A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects* ».

332 ANSSI, « Défense et sécurité des systèmes d'information : Stratégie de la France », SGDSN, Février 2011, p. 21.

333 Il s'agit de la définition cyberdéfense donnée par l'OG cyber, Arnaud Coustillière (Contre-amiral), Officier Général Cyberdéfense, État-major des armées, « La cyberdéfense : une priorité pour les armées », *Transmetteurs*, 1er semestre 2013, n° 6, p. 17.

- les *NetOps proactives* (ex : le contrôle de configuration, les mesures d'information, l'assurance de la sécurité physique, la conception d'architecture sécurisée, la détection d'intrusion...) ;
- les *Defensive Counter Cyber* (inclut la déception militaire par utilisation des pots de miel, redirection, désactivation...) ;
- les contre-mesures défensives.

TRADOC

Actions qui combinent la sécurité de l'information, la défense des réseaux informatiques et la protection des infrastructures critiques par l'utilisation des capacités permettant de prévenir, détecter et contrer les capacités d'un adversaire à manipuler l'information et ou l'infrastructure. La cyberdéfense est intégrée aux aspects défensifs dynamiques de la cyberguerre pour offrir une défense en profondeur.

Cyberdéfense active

CCD CoE (glossaire)

Mesures permettant de détecter ou obtenir des informations par une intrusion, une attaque cybernétique, une menace d'opération cybernétique, pour déterminer l'origine d'une opération impliquant une opération préemptive, préventive ou une opération offensive contre la source.

Cyberdéfense passive

CCD CoE

Mesures permettant de détecter une intrusion cyber et les effets d'une attaque cyber, qui n'implique pas d'atteindre le niveau préemptif, préventif ou d'opération offensive. Exemple : pare-feux, antivirus, etc[334].

[334] CCD CoE, glossaire.

Cyberespace (aussi appelé infrastructure cybernétique)

« Réseau des infrastructures techniques interdépendantes incluant Internet, les réseaux de télécommunication et les systèmes d'ordinateurs, les contrôleurs et les processeurs embarqués dans les industries critiques »[335].

Michel Baud

Espace virtuel rassemblant la communauté des internautes et des ressources d'informations numériques accessibles à travers les réseaux d'ordinateurs[336].

ANSSI

Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement informatisé de données numériques[337].

Monde numérique généré par les ordinateurs et les réseaux informatiques dans lequel hommes et ordinateurs coexistent et qui inclut tous les aspects de l'activité en ligne[338].

Cyberguerre

DoD, *Joint Terminology for Cyberspace Operations*

« Conflit armé conduit totalement ou partiellement par des moyens cyber, [c'est-à-dire] des opérations militaires menées pour interdire à l'ennemi l'utilisation efficace des systèmes du cyberespace et des armes au cours d'un conflit. Cela inclut les cyberattaques, la cyberdéfense et les actions cyber ».

Eric Filiol

Conflit « classique dont au moins une des composantes, dans la réalisation, les motivations et les outils (armes au sens large du terme) s'appuie sur le champ informatique ou numérique »[339].

[335] Joint Chiefs of Staff, "Joint Terminology for Cyberspace Operations", United States Department of Defense, 2010.
[336] Michel BAUD, « Cyberguerre. En quête d'une stratégie », *Focus stratégique*, n° 44, mai 2013, p. 9.
[337] ANSSI, « Défense et sécurité des systèmes d'information : Stratégie de la France », SGDSN, Février 2011, p. 21.
[338] OTAN (AC/322/SC/2-NC3TS L 2007 0002 Cyberwar related definitions, 11 avril 2007).
[339] Grégoire Chaumeil, Anne-Lise Llouquet et Nelly Moussu, « Cyberespace le 5ème champ de bataille », *Armées d'aujourd'hui*, novembre-décembre 2011, n° 365, p. 52.

Cybersécurité

ANSSI

État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Union Internationale des Télécommunications (Recommandation UIT-T X.1205)

« On entend par cybersécurité l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyber environnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication et la totalité des informations transmises et/ou stockées dans le cyber environnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyber environnement. Les objectifs généraux en matière de sécurité sont les suivants : disponibilité, intégrité, qui peut englober l'authenticité et la non-répudiation, confidentialité.

Département de la Défense US

Ensemble des actions organisationnelles requises pour assurer la protection de l'information sous toutes ses formes (électronique, physique) ainsi que des systèmes et des réseaux où l'on accède à l'information, où elle est stockée, traitée, transmise, en prenant des précautions pour les protéger contre le crime, les attaques, le sabotage, l'espionnage, les accidents, les défaillances. Les risques de la cybersécurité incluent ceux qui portent atteinte à la confiance des partenaires, affectent les consommateurs et la croissance, violent l'identité et la vie privée des consommateurs et partenaires et affectent les opérations des infrastructures critiques nationales.

Guerre

Armées françaises

Lutte armée entre groupes sociaux, et spécialement entre États, considérée comme un phénomène social. Elle se traduit par un état de guerre ou de situation de guerre dans la zone d'affrontement. État de guerre est un état juridique qui découle d'une déclaration de guerre ou d'un ultimatum avec déclaration de guerre conditionnelle[340].

Guerre de l'information

Daniel Ventre

« Toute activité destinée à acquérir données et connaissances (et à en priver l'adversaire) dans une finalité stratégique, soit par des systèmes (vecteurs et moyens de traitement de l'information), soit par le contenu, en assurant une domination informationnelle »[341].

Livre blanc 2008

« L'ensemble des actions menées par les forces armées, dirigé et coordonné au plus haut niveau, visant à utiliser ou à défendre l'information, les systèmes d'information et les processus décisionnels, pour appuyer une stratégie d'influence et contribuer, dans le cadre des opérations, à l'atteinte de l'état final recherché, en respectant les valeurs défendues »[342].

Système d'information

ANSSI

« Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information »[343].

340 Glossaire interarmées de terminologie opérationnelle français (PA 0.5.5.2).
341 Daniel Ventre (dir.), *Cyberguerre et guerre de l'information : stratégies, règles, enjeux*, Lavoisier, Paris, 2010.
342 *Défense et Sécurité nationale, Le Livre Blanc*, La documentation française, éditions Odile Jacob, 2008, p. 58.
343 ANSSI, « Défense et sécurité des systèmes d'information : Stratégie de la France », SGDSN, Février 2011, p. 22.

BIBLIOGRAPHIE

Ouvrages

- ANDRESS Jason, WINTERFIELD Steve, *Cyber Warfare : Techniques, Tactics and Tools for Security Practitioners*, Syngress, 2011.
- Armée de terre, *Tactique générale*, Economica, Paris, 2008.
- CHATELAIN Yannick, ROCHE Loïck, *Hackers ! Le 5e pouvoir*, éditions Maxima, Paris, 2002.
- BOYER Bertrand, *Cyberstratégie - l'art de la guerre numérique*, Nuvis, Paris, 2012.
- CARR Jeffrey, *Inside Cyber Warfare*, Sebastopol, O'Reilly 2nd édition, 2011.
- DESPORTES Vincent (Gén), *Décider dans l'incertitude*, Economica, Paris, 2007, 2e édition.
- DOSSÉ Stéphane, KEMPF Olivier, MALIS Christian (dir.), *Le cyberespace : Nouveau domaine de la pensée stratégique*, Economica, Paris, 2013.
- DOSSÉ Stéphane, KEMPF Olivier (dir.), *Stratégies dans le cyberespace*, L'esprit du livre, Paris, 2011.
- The International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, *Tallinn Manual on the international law applicable to cyber warfare*, General editor Michael N. Schmitt, Cambridge University Press, 2013.
- KEMPF Olivier, *Introduction à la cyberstratégie*, Economica, Paris, 2012.
- Mc QUADE Samuel C., III (ed.), *Encyclopedia of Cybercrime*, Westport, Greenwood Press, 2009.
- QUESNEY Chantale, *Kosovo : les mémoires qui tuent, la guerre vue sur Internet*, éditions L'Harmattan, Les Presses de l'Université de Laval, Montréal, 2001.
- VALÉRY Paul, *Regards sur le monde actuel et autres essais*, Gallimard, Paris, 2002.
- VENTRE Daniel, *Cyberattaque et cyberdéfense*, Lavoisier, Paris, 2011.
- VENTRE Daniel, *Cyberespace et acteurs du cyberconflit*, Lavoisier, Paris, 2011.
- VENTRE Daniel (dir.), *Cyber Conflict : Competing National Perspectives*, Wiley, Londres, 2012.

Articles universitaires

- ADHAMI Wael, "The strategic importance of the Internet for armed insurgent groups in modern warfare", *Revue internationale de la Croix-Rouge*, Volume 89, n° 868, décembre 2007, p. 857.
- ALLEN Patrick D. (COL), DEMCHAK Chris (LCL), "The Palestinian-Israeli Cyberwar", Military Review, mars – avril 2003, p. 52-59, http://usacac.leavenworth.army.mil/CAC/milreview/download/English/MarApr03/allen.pdf

- BAUD Michel, « Cyberguerre – en quête d'une stratégie », *Focus stratégique* n° 44, IFRI, mai 2013.
- BAUD Michel, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Politique étrangère*, 2012, n° 2, p. 305-316.
- BAVEREY Lionel (Cdt), « Les opérations réseau-centrées : cheval de bataille ou cheval de troie ? », *Penser les Ailes Française*, 2008, n° 17, p. 23-28.
- BOYER Bertrand, « Cyberdéfense : vers une stratégie numérique indirecte », *RDN*, 2011, n° 745, p. 90-95.
- CLEMENTE Dave, "Cyber Security and Global Interdependance: What Is Critical?", *Chatham House Report*, February 2013.
- CORNISH Paul, LIVINGSTONE David, CLEMENTE Dave, YORKE Claire, "On Cyber Warfare", *Chatham House Report*, Novembre 2010.
- CORNISH Paul, REX Hughes, LIVINGSTONE David, "Cyberspace and the National Security of the United Kingdom: Threats and Responses", *Chatham House Report*, March 2009.
- DUNN CAVELTY Myriam, "Cyberwar: Concept, Status Quo, and Limitations", Center for Security Studies, *Analysis in Security Policy*, n° 71, avril 2010.
- De DURAND Marguerite, HECKER Marc, SOUCHET Thibault, VANBREMEERSCH Nicolas, « Nature et conséquences des réseaux sociaux pour les forces armées », IFRI, spintank, septembre 2012.
- ESTERLE Alain, GRUSELLE Bruno et TERTRAIS Bruno, « Cyber Dissuasion », Fondation pour la Recherche Stratégique, 2012, n° 3.
- FAVREAU Xavier, KOFFI Philippe, SCHANNE Pierre, WARINGHEM Éric, « Capacités militaires, innovation et technologies », *Revue Défense Nationale*, juin 2013, n° 761, p. 19-24.
- GEERS Kenneth, "Cyberspace and the Changing Nature of Warfare", http://www.carlisle.army.mil/DIME/documents/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf
- GEERS Kenneth, "Strategic cyber security", NATO Cooperative Cyber Defence Centre of Excellence, 2011.
- HECKER Marc et RID Thomas, « Les armées françaises doivent-elles craindre les réseaux sociaux », *Politique étrangère* 2, 2012, p. 317-330.
- LIBICKI Martin C., "Cyberdeterrence and Cyberwar", *RAND Corporation monograph series*, 2009, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf
- MELZER Nils, "Cyber operations and *jus in bello*", UNIDIR, *Confronting Cyberconflict*, Geneva, 2011, p. 3-17. http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?lng=en&id=143275
- O'DONNEL Brian T., KRASKA James C., "Humanitarian law: developing international rules for the digital battlefield", *Journal of Conflict and Security Law*, 2003, Vol. 8, N° 1, p. 133-160.
- PETERSON Dale, "Offensive Cyber Weapons: Construction, Development, and Employment", *Journal of Strategic Studies*, 2013, Vol. 36, Issue 1, p. 120-124.
- RID Thomas, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, 2012, Vol. 35, Issue 1, p. 5-32.
- RID Thomas, "More Attacks, Less Violence", *Journal of Strategic Studies*, 2013, Vol. 36, Issue 1, p. 139-142.
- SCHMITT, Michael N., "Wired warfare: Computer network attack and *jus in bello*", *Revue internationale de la Croix Rouge*, juin 2002, vol. 84, n° 846, p. 365-399.

- SCHREIER Fred, "The Report on Cyberwarfare", DCAF, 2012.
- SHARMA Amit, "Cyberwars: a Paradigm Shift from Means to Ends", *Strategic Analysis*, 2010, Vol. 34, N° 1, p. 62-73.
- TISSIER Guillaume, « La nouvelle initiative de défense stratégique américaine dans le cyberespace », *Les notes stratégiques*, CEIS, 2012.
- WEEDEN Brian, "Cyber offense and defense as mutually exclusive national policy priorities", UNIDIR, *Confronting Cyberconflict*, Geneva, 2011, p. 19-30. http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=143274
- WOLF Philippe, « Ambiguïtés et cyberconflits », *in* BOUHADANA Irène et GILLES William (dir.), *Cybercriminalité, cybermenaces et cyberfraudes*, Paris, Imodev, 2012, p. 61-69.
- ZHANG Li, "A Chinese perspective on cyber war", *Revue internationale de la Croix Rouge*, vol. 94, n° 886, juin 2012, p. 801-807.

Articles de magazines

- BOCKEL Jean-Marie, « Cyberdéfense : la France a des atouts », *Revue DÉFENSE*, n°159, novembre-décembre 2012, p. 40-41.
- BOUGERET Philippe (Col), « Le défi de la cyberdéfense pour l'armée de Terre », *Transmetteurs*, 1er semestre 2013, n° 6, p. 22.
- BRUNETAUD Céline (Cne), « Le combat du futur », *Terre Information Magazine*, février 2013, n° 241, p. 40-41.
- CARTER Rosemary M. FEICK Brent, UNDERSANDER Roy C., "Offensive Cyber for the Joint Force Commander: it's Not That Different", *Joint Force Quarterly*, Issue 66, 3rd Quarter 2012, p. 22-27.
- CHAUMEIL Grégoire, LLOUQUET Anne-Lise et MOUSSU Nelly, « Cyberespace le 5ème champ de bataille », *Armées d'aujourd'hui*, novembre-décembre 2011, n° 365, p. 32-52.
- COUSTILLIÈRE Arnaud (Contre-amiral), Officier Général Cyberdéfense, État-major des armées, « La cyberdéfense : une priorité pour les armées », *Transmetteurs*, 1er semestre 2013, n° 6, p. 18-19.
- COUSTILLIÈRE Arnaud (Contre-amiral), Officier Général Cyberdéfense, État-major des armées « La cyberdéfense est l'une des priorités de la Défense », *Armées d'aujourd'hui*, décembre 2012 - janvier 2013, n° 376, p. 38-39.
- DARBY Roger, "Cyber Defense in Focus: Enemies Near and Far – or Just Behind the Firewall: The Case for Knowledge Management", Defense Studies, *Journal of Military and Strategic Studies*, vol. 12, n° 4, December 2012, p. 523-538.
- DELON Francis, « Infrastructures critiques : le château de cartes numérique », *Défense, Enjeux de défense et de sécurité civils et militaires*, n° 160, janvier - février 2013, p. 4-5.
- DUPUY Emmanuel, « Quels enjeux politiques en matière de cyberdéfense ? », *Revue militaire suisse*, janvier-février 2013, n° 1, p. 19-21.
- DE GEYER D'ORTH, Paul (Capitaine de frégate), « Les enjeux des systèmes militaires de navigation par satellite », *Les Carnets du Temps*, n° 94, février 2013, p. 10-11.

- HECKER Marc, « Armées contre insurgés : à qui profite le web ? », entretien réalisé par Joseph HENROTIN, *DSI*, septembre 2009, n° 51 p.28-31.
- HENROTIN Joseph, « Conséquences tactiques du hacking radar », *DSI*, février 2013, n° 89, p. 98-103.
- HERNANDEZ Rhett A. (LTG), "U.S. Army Cyber Command: Cyberspace for America's Force Of Decisive Action", *The Magazine of the Association of the United States Army*, October 2012, p. 205-208.
- HOLLIS David, "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command", National Defense University, *Joint Force Quaterly*, issue 58, 3rd Quarter 2010.
- HUYGHE François-Bernard (dir.), « Faux, rumeurs et désinformation dans le cyberespace », Observatoire géostratégique de l'information, IRIS, 16 janvier 2013.
- KALLABERG Jan, THURAISINGHAM Bhavani, "Cyber Operations: Bridging from Concept to Cyber Superiority", *Joint Force Quarterly*, Issue 68, 1st Quarter 2013, p. 53-58.
- KEYMER Eleanor, "The cyber-war", *Jane's Defense Weekly*, 29 septembre 2010, vol. 47, issue 39, p. 24.
- LANGLOIT Philippe, « Au cœur de la spatio dépendance : la navigation par satellite », *DSI Hors Série*, février-mars 2013, n° 28, p. 28-31.
- LANHAM Michael J. (LCL), "When the network dies", *Armed Forces Journal*, décembre 2012, p. 11-13, http://www.andrew.cmu.edu/user/mlanham/pubs/Lanham2012_WhenTheNetworkDies.pdf
- LARATTE Jacky (LCL R), « Dossier spécial : le projet EIC NEB SIMU de l'infanterie (Espaces d'instruction collectifs à la numérisation Espace de Bataille par la Simulation) », *Magazine Fantassins*, Printemps - Été 2012, n° 28, p. 60-62.
- LAWRENCE Susan S. (LTG), "Land War Net: Powering America's Army In a Joint, Interagency, Intergovernmental And Multinational Environment", *The Magazine of the Association of the United States Army*, October 2012, p. 185-190.
- MIELCAREK Romain, « Guerre et communication 2.0 », *DSI*, juin 2013, n° 93, p. 54-58.
- MIELCAREK Romain, « Transmissions : "Do you speak SIC?!" », *DSI*, décembre 2012, n° 87, p. 46-50.
- MILLER Robert A., KUEHL Daniel T., LACHOW Irving, "Cyber War; Issues in Attack and Defense", *Joint Force Quarterly*, Issue 61, 2nd quarter 2011, p. 18-23.
- OLSON Soren, "Shadow boxing: cyber warfare and strategic economic attack", *Joint Force Quarterly*, Issue 66, 3rd Quarter 2012, p. 15-21.
- RID Thomas, Mc BURNEY Peter, "Cyber-weapons", *The RUSI Journal*, février-mars 2012, vol. 157, n° 1, p. 6-13.
- SALVADOR Luc-François, « Vers une approche systémique de la cybersécurité », *Revue de la Gendarmerie Nationale*, 4e trimestre 2012, p. 37-42.
- STAVRIDIS James G., PARKER III Elton C., "Sailing the cyber sea", *Joint Force Quarterly*, Issue 65, 2nd Quarter 2012, p. 61-67.
- STEPHENSON Scott (LCL), "The Revolution in Military Affairs: Observations on an Out-of-Fashion Idea", *Military Review*, mai - juin 2010, p. 38-46.
- WASSERBLY Daniel, "CYBERCOM formulating "offensive teams"", *HIS Jane's Defense Weekly*, 20 mars 2013, Vol. 50, issue 12.
- WASSERBLY Daniel, "DoD could opt for 'cyber service', says Carter", I*HS Jane's Defense Weekly*, vol. 50, Issue 25, 19 juin 2013, p. 10.

Articles de presse écrite et numérique

- BALDACCHINO Julien, « Comment les djihadistes se servent du web 2.0 », *France Info*, 28 février 2013, http://www.franceinfo.fr/monde/comment-les-djihadistes-se-servent-du-web-2-0-906347-2013-02-28
- BORGER Julian, "Pentagonkept the lid on cyberwar in Kosovo", *theguardian.com*, 9 novembre 1999, http://www.theguardian.com/world/1999/nov/09/balkans
- BOURASSI Nabil, « cyberguerre : comment la France se protège », *LaTribune.fr*, 28 janvier 2013, http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/20130111trib000742055/cyberguerre-comment-la-france-se-protege.html
- CABIROL Michel, « Cyberdéfense : les espions vont disposer de capacités informatiques offensives », *LaTribune.fr*, 13 mars 2013, disponible à l'adresse suivante : http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/20130313trib000753767/cyberdefense-les-espions-vont-disposer-de-capacites-informatiques-offensives-24.html
- CABIROL Michel, « Les deux Corée sont-elles au bord d'une cyberguerre ? », site Internet de *La Tribune*, 20 mars 2013, disponible à l'adresse suivante : http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/20130320trib000755026/les-deux-coree-sont-elles-au-bord-d-une-cyberguerre-.html
- CAPRONI Nicolas, « Stuxnet : le retour de Flame », *www.cyber-securite.fr*, 4 juin 2012, http://www.cyber-securite.fr/2012/06/04/stuxnet-le-retour-de-flame/).
- CHAPLEAU Philippe, « La campagne de publicité de l'armée de terre fait un carton », *Lignes de défense*, 28 juin 2013 (http://lignesdedefense.blogs.ouest-france.fr/archive/2013/06/28/cocorico-terrien-la-campagne-de-publicite-fait-un-tabac.html).
- CYPEL Sylvain, « Le piratage du compte Twitter d'AP fait plonger Wall Street », *LeMonde.fr*, 24 avril 2013, http://www.lemonde.fr/economie/article/2013/04/24/demain-une-cyberguerre-sur-les-marches_3165087_3234.html
- CYPEL Sylvain, « Les plans des fleurons de la défense américaine aux mains de cyberespions chinois », *LeMonde.fr*, 29 mai 2013, http://www.lemonde.fr/international/article/2013/05/29/les-plans-des-fleurons-de-la-defense-americaine-aux-mains-de-cyberespions-chinois_3420002_3210.html
- DIXON Robyn, "Russia to Pour Money Into Chechen Fight", *Los Angeles Times*, 7 octobre 1999 (http://articles.latimes.com/1999/oct/07/news/mn-19719).
- GOLLION Anne-Laurence, « L'armée française désavoue un militaire ayant menacé un journaliste togolais », *L'express.fr*, 11 août 2010, http://www.lexpress.fr/actualite/monde/l-armee-francaise-desavoue-un-militaire-ayant-menace-un-journaliste-togolais_911811.html
- GREENWALD Glenn, Mac ASKILL Ewen, "Obama orders US to draw up overseas target list for cyber-attacks", *theguardian.com*, 7 juin 2013, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas
- GUISNEL Jean, « Cyberguerre. La France à l'offensive », *Le Télégramme*, 1er décembre 2012.
- GUISNEL Jean, « Exclusif. Somalie : le raid pour libérer Denis Allex a été conduit depuis le Mistral », *LePoint.fr*, 13 janvier 2013, http://www.lepoint.fr/editos-du-point/jean-guisnel/exclusif-somalie-le-raid-pour-liberer-denis-allex-a-ete-conduit-depuis-le-mistral-13-01-2013-1613080_53.php
- HARBULOT Christian, « De la guerre de l'information aux cyberconflits », *Horizons stratégiques*, supplément au n° 21152 *Les Echos*, 26 mars 2012, p. 61-63.

- KALLENBORN Gilbert, « La Suisse attaquée par les Anonymous, dans un exercice de cyberdéfense », *01net*, 24 mai 2013, http://www.01net.com/editorial/595985/la-suisse-attaquee-par-lesanonymous-dans-un-exercice-de-cyber-defense/
- KARIMI Nasser, "Report: Iran's paramilitary launchers cyber attack", *TheWashingtonPost.com*, 14 mars 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/03/14/AR2011031401029.html
- LAGNEAU Laurent, « Le Pentagone demande un budget de 526,6 milliards de dollars pour 2014 », *opex360.com*, 11 avril 2013, http://www.opex360.com/2013/04/11/le-pentagone-demande-un-budget-de-5266-milliards-de-dollars-pour-2014/
- LAGNEAU Laurent, « Vers la création d'une force de réaction rapide de l'Otan en cas de cyber-attaque », *opex360.com*, 6 juin 2013, http://www.opex360.com/2013/06/06/vers-la-creation-dune-force-de-reaction-rapide-de-lotan-en-cas-de-cyber-attaque/
- LERT Frédéric, interview de Gilles ROUSSET, directeur Stratégie & Marketing Services, Thales, 29 mai 2013, *Forcesoperations.com*, http://forcesoperations.com/2013/05/29/fob-interview-gilles-rousset-directeur-strategie-marketing-services-thales/
- LONDONO Ernesto, "Pentagon: Chinese government, military behind cyberspying", *The Washington Post*, 7 mai 2013, http://www.washingtonpost.com/world/national-security/pentagon-chinese-government-military-behind-cyberspying/2013/05/06/f4851618-b694-11e2-b94c-b684dda07add_story.html
- MARDIROSSIAN Florence, « Géorgie-Russie, les enjeux de la crise », *Le Monde Diplomatique*, 15 août 2008, http://www.monde-diplomatique.fr/carnet/2008-08-15-Georgie
- MESSMER Ellen, "Kosovo cyber-war intensifies", *Network World Fusion*, 5 décembre 1999, http://www.networkworld.com/news/1999/0512kosovo.html
- MERCHET Jean-Dominique, « Les armées attaquées par un virus informatique », *Secret Défense*, billet publié le 5 février 2009, http://secretdefense.blogs.liberation.fr/defense/2009/02/les-armes-attaq.html
- NAKASHIMA Ellen, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies", *TheWashigtonPost.com*, 28 mai 2013, http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html
- NAKASHIMA Ellen, "List of Cyber-Weapons Developed by Pentagon to Streamline Computeur Warfare", *TheWashigtonPost.com*, 31 mai 2011, disponible à l'adresse suivante : http://articles.washington-post.com/2011-05-31/national/35264250_1_cyber-computer-warfare-stuxnet
- NAKASHIMA Ellen, "Pentagon to boost cybersecurity force", *TheWashigtonPost.com*, 27 janvier 2013, http://articles.washingtonpost.com/2013-01-27/world/36583575_1_cyber-protection-forces-cyber-command-cybersecurity
- O'HARROW Robert Jr., GELLMAN Barton, "Secret cyber directive calls for ability to attack without warning", *TheWashingtonPost.com*, 8 juin 2013, http://articles.washingtonpost.com/2013-06-07/world/39817439_1_cyber-tools-president-obama-directive
- REED John, "How many cyber troops does the U.S Have?", *ForeignPolicy.com*, 7 mars 2013, http://killerapps.foreignpolicy.com/posts/2013/03/07/how_many_cyber_troops_does_the_military_have
- SUPLY Laurent, « Définition : réseau social », *Suivez le Geek*, 1er janvier 2008, http://blog.lefigaro.fr/high-tech/2008/01/definition-reseau-social.html
- TROUILLARD Stéphanie, « Aqmi a conçu un jeu video pour désintégrer l'armée française au Mali », *France24*, 27 mars 2013, http://www.france24.com/fr/20130313-djihad-jeu-video-mali-armee-francaise-avion-al-qaida-forum-islamiste

- Anonyme, « Bercy, l'Élysée et le Quai d'Orsay visés par une cyberattaque », *LePoint.fr*, 7 mars 2011, http://www.lepoint.fr/societe/bercy-l-elysee-et-le-quai-d-orsay-vises-par-une-cyberattaque-07-03-2011-1303652_23.php
- Anonyme, "China War Games: Army To Conduct Its First Digital Technology Military Exercise", *Reuters*, 28 mai 2013, http://www.huffingtonpost.com/2013/05/28/china-war-games-digital-technology-exercise-planned_n_3349794.html
- Anonyme, « Engagements terrestres à l'horizon 2020, quelles guerres, quelles capacités ? », *Revue Doctrine tactique*, 2012, Numéro spécial.
- Anonyme, "Hype and fear", *The Economist*, 8 décembre 2012, disponible à l'adresse suivante : http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may
- Anonyme, « La cyberdéfense, un marché en plein boom ? », 24 mai 2012, *cyber-défense.fr*, http://cyber-defense.fr/blog/index.php?post/2012/05/24/La-cyberdefense%2C-un-marché-en-plein-boom
- Anonyme, « L'Élysée confirme avoir été la cible d'une cyberattaque au cours des derniers mois », *LeMonde.fr*, 12 juillet 2012, http://www.lemonde.fr/technologies/article/2012/07/12/l-elysee-confirme-avoir-ete-la-cible-d-une-cyberattaque-au-cours-des-derniers-mois_1732517_651865.html
- Anonyme, « Un contrat entre Microsoft et le ministère de la Défense fait jaser », 21 avril 2013, accessible en suivant le lien http://www.opex360.com/2013/04/21/un-contrat-entre-microsoft-et-le-ministere-de-la-defense-fait-jaser/
- Anonyme, "South Korea on alert for cyber-attacks after major network goes down", *The Guardian*, 20 mars 2013, http://www.theguardian.com/world/2013/mar/20/south-korea-under-cyber-attack
- Anonyme, « Tsahal ouvre sa cellule de guerre contre les cyber-attaques », *Tsahal.fr*, 4 mars 2013, http://tsahal.fr/2013/03/04/tsahal-ouvre-sa-cellule-de-guerre-contre-les-cyber-attaques/
- Anonyme, « Togo : l'officier français rappelé « immédiatement » à Paris », *L'Express.fr*, 13 août 2010, http://www.lexpress.fr/actualite/monde/afrique/togo-l-officier-francais-rappele-immediatement-a-paris_912319.html
- Auteurs multiples, Dossier « La Cyberguerre est déclarée », *Courrier international*, N° 1165, 28 février - 6 mars 2013, p. 30-37.

Documents officiels

- ANSSI, « Défense et sécurité des systèmes d'information : Stratégie de la France », SGDSN, Février 2011.
- ANSSI, « Maîtriser la SSI pour les systèmes industriels – La cybersécurité des systèmes industriels », version 1.0, Juin 2012.
- Assemblée de l'Union de l'Europe Occidentale, Recommandation 831 (décembre 2008).
- Assemblée européenne de sécurité et de défense, « La guerre informatique », document C/2022, 5 novembre 2008.
- BOECKEL Jean-Marie, « Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense », n° 681, enregistré à la Présidence du Sénat le 18 juillet 2012.

- CICDE, « Glossaire interarmées de terminologie opérationnelle », PIA-7.2.6-3_GIAT-O(2012), N° 001/DEF/CICDE/NP du 3 janvier 2012 amendée le 1er février 2012.
- CICDE, « Réseaux sociaux. Nature et conséquences pour les forces armées », Réflexion doctrinale interarmées RDIA-2013/001_RS(2013), n° 067/DEF/CICDE/NP, du 19 avril 2013.
- Commission européenne, Haut Représentant de l'Union aux Affaires étrangères et à la Politique de sécurité, "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions", 7 février 2013.
- DANINO Olivier, « L'utilisation stratégique du cyber au Moyen-Orient », Délégation aux Affaires Stratégiques, Ministère de la Défense, EPS 2013.
- DAS - CEIS, « Observatoire du Monde Cybernétique, Lettre n° 6 », juin 2012.
- DAS - CEIS, « Observatoire du Monde Cybernétique, Lettre n° 7 », juillet 2012.
- DAS - CEIS, « Observatoire du Monde Cybernétique, Lettre n° 17 », mai 2013.
- DAS - CEIS, « Observatoire du Monde Cybernétique, Lettre n° 18 », juin 2013.
- DAS - CEIS, « Observatoire du Monde Cybernétique, Trimestriel septembre 2012 », septembre 2012.
- Disarmament Forum, "Confronting Cyberconflict", UNIDIR, 2011, http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=143274
- État-Major des Armées, « Utilisation d'Internet à des fins privées dans le cadre de la condition du personnel en opération », Publication interarmées PIA-4.0.1.1_UIFP-CPO(2011), N° D-11-009052/DEF/EMA/SC-SOUT/SLI/SDO/NP, du 18 novembre 2011.
- HEALEY Jason et VAN BOCHOVEN Leendert, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", Atlantic Council Issue brief, 2011.
- Joint Chiefs of Staff, "Capstone Concept for Joint Operations: Joint Force 2020", United States Department of Defense, 10 septembre 2012.
- Joint Chiefs of Staff, "Joint Terminology for Cyberspace Operations", United States Department of Defense, 2010.
- KLIMBURG Alexander (Ed.), "National Cyber Security Framework Manual", NATO CCD COE Publication, Tallinn, 2012.
- LYNN William, "Department of Defense strategy for operating in cyberspace", United States Department of Defense, July 2011.
- OTAN, « Briefing : l'OTAN face aux nouveaux défis de sécurité » (Référence BRIEF11TNSFRE - 0527-11 NATO Graphics & Printing), 2011.
- OTAN, « Concept stratégique pour la défense et la sécurité des membres de l'Organisation du Traité de l'Atlantique Nord », 19 novembre 2010.
- PIGNON Dominique, « La prospective du caractère stratégique du cyberespace », Délégation aux Affaires Stratégiques, Ministère de la Défense, 2012.
- ROMANI Roger, « Rapport d'information fait au nom de la commission des Affaires étrangères, de la défense et des forces armées sur la cyberdéfense », n° 449, Annexe au procès-verbal de la séance du 8 juillet 2008.
- SGDSN, « Défense et sécurité des systèmes d'information : la stratégie de la France », février 2011.

- SGDSN, « La France face aux évolutions du contexte international et stratégique, document préparatoire à l'actualisation du livre blanc sur la défense et la sécurité nationale », février 2012.
- SGDSN, Livre Blanc Défense et Sécurité Nationale 2013.
- TRADOC, "Cyberspace Operations. Concept Capability Plan 2016-2028", The United States' Army, TRADOC pamphlet 525-7-8, 22 february 2010.
- United States Department of Defense, "Capstone concept for joint operations: joint force 2020", 2012.
- The White House, "International Strategy for Cyberspace, Prosperity, Security and Openness in a Networked World", Mai 2011.

Discours

- M. Jean-Yves Le Drian, Ministre de la Défense, discours prononcé en ouverture du colloque « Cybersécurité : un enjeu mondial, une priorité nationale, des réponses régionales », Rennes, 3 juin 2013.

Sites Internet

- Centre des Hautes Études du Ministère de l'Intérieur, web émission CyberTalk n° 3, « Le ministère de la défense dans le cyberespace », mars 2013, http://www.defense-et-strategie.fr/index.php?option=com_content&view=category&id=116:le-cybertalk&Itemid=374
- LATU Philippe, « Un article sur les concepts élémentaires de sécurité informatique » *(traduction libre d'une page publiée sur le blog de Daniel Miessler)*, disponible à l'adresse suivante : http://www.inetdoc.net/pdf/infosecconcepts.pdf, consulté le 21 mars 2013.
- MOUSSU Nelly, « Cyberdéfense, enjeu du 21e siècle », dossier en ligne sur le site du Ministère de la Défense à l'adresse suivante : http://www.defense.gouv.fr/actualites/dossiers/sept-2011-cyberdefense-enjeu-du-21e-siecle, consulté le 17 janvier 2013.
- Chaire de cyberdéfense et cybersécurité Saint-Cyr Sogeti Thalès, rattachée au Centre de Recherche des Écoles de Saint-Cyr Coëtquidan, http://www.st-cyr.terre.defense.gouv.fr/index.php/crec/Centre-de-recherche-des-ecoles-de-Saint-Cyr-Coetquidan/Menu-Principal/Les-chaires/Chaire-de-Cyberdefense

Entretiens réalisés :

- Colonel Jérôme Pellistrandi, Centre Interarmées de Concepts, de Doctrines et d'Expérimentations.
- Colonel Aymeric Bonnemaison, État-major de l'armée de Terre.
- Colonel Stephan Uro, Centre de Doctrine d'Emploi des Forces.
- Chef de bataillon Michel Baud, Institut français des relations internationales.
- Chef de bataillon Yann Couderc, Section Technique de l'Armée de Terre.
- Capitaine Pierre-Luc Hennet, 8e Régiment des Transmissions.

Colloques/séminaires :

- HESLAULT Laurent (Symantec), « Stuxnet, Duqu, Flame et autres malicieux : nouvelles armes informatiques ? », conférence organisée par l'ANAJ-IHEDN, Paris, 21 mars 2013.
- TISSIER Guillaume (Compagnie Européenne d'Intelligence Stratégique), « Les opérations dans le cyberespace : quels risques juridiques ? », colloque *La Robe et l'Épée*, Centre de Recherche des Écoles de Saint-Cyr Coëtquidan, Paris, 6-7 décembre 2012.
- Les 5 à 7 du CICR, « Cyberguerre : défi du futur pour l'humanitaire ? », débat organisé le 18 décembre 2012 à Paris.

Directeur de la publication : Général Jean-François PARLANTI
CDEF - 1 place Joffre – Case 53 - 75700 PARIS SP 07
Téléphone du secrétariat : 01 44 42 51 02. **Fax du secrétariat :** 01 44 42 81 29

Rédacteur en chef : Colonel Pierre ESNAULT, officier pilote du dossier. **Téléphone :** 01 44 42 41 61
Auteur : Mlle Élodie SIMON, sous la direction du Colonel Michel GOYA. **Téléphone :** 01 44 42 81 65

Crédits photos (Couverture) : Adjudant Marc KLEIN © 54e RT
Maquettage : Sonia RIVIÈRE/CDEF/DAD/PUB
Infographie (Couverture) : Nanci FAUQUET/CDEF/COM

Impression - Routage : EDIACA - 76 rue de la Talaudière - BP 80508 - 42007 SAINT-ÉTIENNE CEDEX 1
Téléphone : 04 77 95 33 21 ou 04 77 95 33 25
Tirage : 1 800 exemplaires
Diffusion : CDEF/DAD/PUB. **Téléphone :** 01 44 42 43 18

Dépôt légal :
ISBN 978-2-11-138908 - Juin 2014
ISSN de la collection Cahier du RETEX
La version électronique de ce document est en ligne sur les sites Intradef et Internet du CDEF
à l'adresse **htpp://www.cdef.defense.gouv.fr**

CENTRE DE DOCTRINE D'EMPLOI DES FORCES
DIVISION RECHERCHE ET RETOUR D'EXPERIENCE
1, place Joffre - Case 53 - 75700 PARIS SP 07
www.cdef.terre.defense.gouv.fr