

# Origine, éléments de doctrine et évolution de la Guerre de l'Information

par Etienne de SEREVILLE,  
ingénieur, chef de peloton au 11<sup>ème</sup> Chasseurs à Berlin (1990), fondateur du *Cercle Fortitude*, directeur du département Stratégie & Architecture IT de IBM Global Technology Services.

L'année en cours va voir une avancée significative en matière de Guerre de l'Information militaire: le démarrage opérationnel de l'US Air Force Cyber Command (AFCYBER) prévu le 1er octobre 2008. Sa mise en œuvre complète devrait prendre un an. Ce « commandement majeur » au sein de l'US Air Force est le résultat de 15 années de réflexions théoriques, de modélisations, de « révolution des affaires militaires » (*Revolution Military Affairs*), d'expérimentations du concept de Guerre de l'Information lors des guerres du Golfe. L'AFCYBER est un élément principal de la stratégie américaine de Domination Informationnelle (*Information Dominance*) dont les missions sont de maintenir et protéger les infrastructures informationnelles pour un accès permanent et fiable, de protéger les données, de défendre les infrastructures contre le brouillage et autre piratage, et d'attaquer les infrastructures ennemies. Il sera sous l'autorité du *Joint Information Operations Warfare Command*, du *JFCC Network Warfare*<sup>1</sup> et du *JTF Global Network Operations*<sup>2</sup> de l'US Strategic Command, soit au plus haut niveau de la structure de commandement. Cette mise en œuvre n'est pas sans poser des problèmes légaux car les cibles pourraient être civiles (voir le Rapport du Congrès « *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues* » de mars 2007). Pour ne pas être en reste, l'OTAN a annoncé en avril la création de la *Cyber Defense Management Authority* dont le but sera de protéger les infrastructures informationnelles, les réseaux informatiques et de communication de ses membres. Ces évolutions doivent être comprises à l'éclairage de leur origine et des différents éléments qui ont conduit leur aboutissement. Ainsi, les lignes qui suivent présenteront des éléments fondateurs de la Guerre de l'information<sup>3</sup> (GI), des éléments de doctrine américaine et française, et quelques points de développement prospectif.

Que ce soient les espions de Sun Tzu, le chiffrement de César, le décryptage de Georges Painvin qui sauve Paris en 1917 ou bien l'opération d'intoxication Fortitude en juin 1944, la maîtrise de l'environnement informationnel (*Military Information Environment*) est un but recherché depuis longtemps pour vaincre. Bien que ne donnant pas la victoire mais y contribuant, les armées se sont dotées de moyens pour s'assurer cette supériorité tant organisationnelle que technique. Les moyens modernes de communication et de traitement automatique de données, support de l'information, offrent des possibilités nouvelles et extraordinaires jamais connues dans l'histoire, et les progrès à venir sont prometteurs. Afin

---

<sup>1</sup> Joint Functional Component Command Network Warfare

<sup>2</sup> Joint Task Force-Global Network Operations

<sup>3</sup> Ou Infoguerre, *Information Warfare*

de profiter pleinement des TIC<sup>4</sup>, pour qu'elles offrent de nouvelles opportunités opérationnelles ou qu'elles permettent d'identifier de nouveaux risques tactiques, les armées développent des doctrines, mettent en œuvre des organisations et s'appuient sur des moyens techniques pour assurer la cohérence, l'efficacité et l'interopérabilité sur le champ de bataille. Acquérir de nouvelles informations, protéger ses propres informations, perturber les informations adverses, influencer les acteurs de la situation, partager et communiquer, toutes ces actions sont constitutives de ce qui est regroupé aujourd'hui sous le concept de « guerre de l'information » (*Inforwar* ou *Information Warfare*). Celle-ci vise la suprématie informationnelle (*Information Dominance*), c'est-à-dire à obtenir une supériorité à acquérir et utiliser l'information stratégique, opérationnelle et tactique sur l'adversaire ainsi que la maîtrise les risques informationnels lors d'une situation conflictuelle.

Le concept de GI n'est pas nouveau. L'un des premiers théoriciens ayant eu une approche globale est Martin Libicki, professeur américain du National Defense University Institut for National Strategic Studies. Il a publié en 1995 l'ouvrage « *What is Information Warfare ?* » qui propose de définir le périmètre de la GI autour de sept domaines: guerre de commandement et de contrôle, guerre du renseignement, guerre électronique, guerre psychologique, guerre de piratage informatique, guerre économique par l'information et la cyberguerre. A sa suite, de nombreux ouvrages détailleront les thèmes et iront plus loin dans la théorisation, comme *l'Information Age Anthology* Vol I-II-III de Alberts et Papp ou *Power to the edge* de Alberts et Hayes. Cette taxinomie n'a que peu été remise en cause depuis son écriture et elle fait encore école. Elle a la vertu d'être aisément compréhensible car s'appuyant sur des domaines connus, complétés des nouveautés hackers, économie et cyberguerre. C'est un prolongement du concept de domination informationnelle dans des champs plus larges que le seul domaine militaire. Cette révolution technologique ou « révolution de l'information », liée aux TIC et à leurs nouvelles capacités démontrées lors de la 1<sup>ère</sup> guerre du Golfe, a conduit à repenser le rôle de l'information. Elle a conduit à une réforme stratégique majeure, la Révolution dans les Affaires Militaires pour formater le Monde (*Shaping the World*), s'appuyant sur la maîtrise de l'information avec les SIC et les satellites (*space power*). Cependant, le concept de GI apparaissant comme plutôt flou, il a évolué vers le terme d'opérations informationnelles (*Information Operations*) plus appréhendable et concret. Au pays de Descartes, la conceptualisation de la GI n'a pas pris la forme d'un catalogue de domaines et de concepts parfois nouveaux, mais celles d'intentions : la guerre par l'information, pour l'information et contre l'information<sup>5</sup>. Cependant, il est apparu à la réflexion que l'information n'est que la matière première de la connaissance. Ainsi, les théoriciens français C.Harbulot, D.Lucas ou F-B.Huyghe ont ils développés le concept de guerre de la connaissance ou cognitive<sup>6</sup>. Ces évolutions encore récentes doivent maintenant diffuser dans les doctrines militaires.

En 1998 aux Etats-Unis, le document *Presidential Decision Directives* 63 est publié. Il pose les bases de la stratégie américaine pour protéger les infrastructures contre des actes délibérés, visant à priver les autorités fédérales de leurs moyens de remplir des missions de sécurité nationale, qui va conduire à la déclinaison de la doctrine américaine. Le *Joint Doctrine for Command and Control Warfare*<sup>7</sup> comporte cinq domaines : opérations de sécurité, opérations psychologiques, déception militaire, guerre électronique et destruction

---

<sup>4</sup> Technologies de l'Information et de la Communication

<sup>5</sup> Général Pichot-Duclos, Les guerres secrètes de la mondialisation

<sup>6</sup> La guerre cognitive, 2002

<sup>7</sup> Joint Pub 3-13, 1998

physique. L'objectif est d'influencer ou de détruire les capacités C2<sup>8</sup> adverses en protégeant les propres capacités. La *Joint Doctrine for Information Operations* présente les Opérations d'information (OI)<sup>9</sup> qui comprennent toutes les actions pour endommager les systèmes adverses. Les opérations offensives incluent l'utilisation des capacités et des activités qui ont pour objectif de toucher et détruire les systèmes d'information adverses comme par exemple une attaque du réseau informatique. Les opérations d'information défensives intègrent et coordonnent les procédures, les opérations, le personnel et la technologie, destinés à protéger et à défendre les systèmes d'information. De plus, il existe un document interarmées intéressant sur la mise en œuvre des Opérations Psychologiques<sup>10</sup>. Les opérations psychologiques opérationnelles sont utilisées dans le cadre d'une manœuvre tactique par les forces conventionnelles ou spéciales opérant en territoire adverse afin de circonvenir l'adversaire.

La doctrine française en matière de GI repose sur le corpus documentaire dont le premier à citer est la Doctrine Interarmées d'emploi des forces en opération<sup>11</sup>. Elle présente le concept de « Maîtrise de l'information », qui « vise principalement à disposer de la bonne information au bon moment et au bon endroit mais également à entretenir la tenue de situation pertinente pour, in fine, obtenir la supériorité décisionnelle ». Les domaines traités sont : le renseignement, la guerre du commandement, les actions dans les champs physiques, les actions dans les champs psychologiques, la guerre électronique et l'informatique. Le document d'expertise de théâtre et d'expertise pré-décisionnelle<sup>12</sup> contient un chapitre dédié au renseignement Cette expertise a pour but de connaître le théâtre d'opération et de comprendre, par ailleurs, la structure, les objectifs, les stratégies et les aptitudes de tous les acteurs qui s'y trouvent. L'expertise de renseignement destinée à la planification pré-décisionnelle doit fournir les renseignements nécessaires à l'élaboration des différentes options stratégiques et permettre le choix le plus pertinent. Le mémento de connaissances militaires interarmées<sup>13</sup> présente la fonction Commandement avec les SIC<sup>14</sup> et la fonction Renseignement. Il présente les moyens français de renseignements : la chaîne, la brigade et les moyens des unités opérationnelles. Cette organisation est structurée sur le modèle de l'armée de terre. La doctrine d'emploi des formations de guerre électronique (GE) de l'armée de terre<sup>15</sup> donne le cadre général et la place et le rôle de la GE, ainsi que le commandement, la coordination et les mesures de GE. Le document sur « les actions dans les champs psychologiques »<sup>16</sup> n'est pas un document de doctrine officielle mais présente des éléments intéressants pour comprendre le champ de la GI par ses buts, ses principes et ses modes d'actions. La doctrine interarmées sur la communication opérationnelle<sup>17</sup> traite les aspects C2 en précisant les principes (unicité du commandement, coordination des actions, subsidiarité), les règles d'emploi (la volonté d'informer, l'exactitude, l'anticipation, la réactivité), les limites (suivant le contexte opérationnel, les raisons de l'opération, le respect des personnes), l'organisation (niveaux politique, opératif et tactique) et la communication opérationnelle (média, locale, interne, relation publique). Le document d'étude du Centre de recherche et d'étude de doctrine de l'armée de terre sur la supériorité dans le domaine du

---

<sup>8</sup> Commandement et Contrôle

<sup>9</sup> Opérations d'Informations ou Informationnelles, *Information Operations*

<sup>10</sup> *Doctrine for Joint Psychological Operations* (Joint Pub 3-53, 2003)

<sup>11</sup> Instruction 1000, 2001

<sup>12</sup> N°529 DEF/EMEA/EMP.1/NP, 2002

<sup>13</sup> à l'usage des stagiaires de l'École d'Etat Major, édition 2000

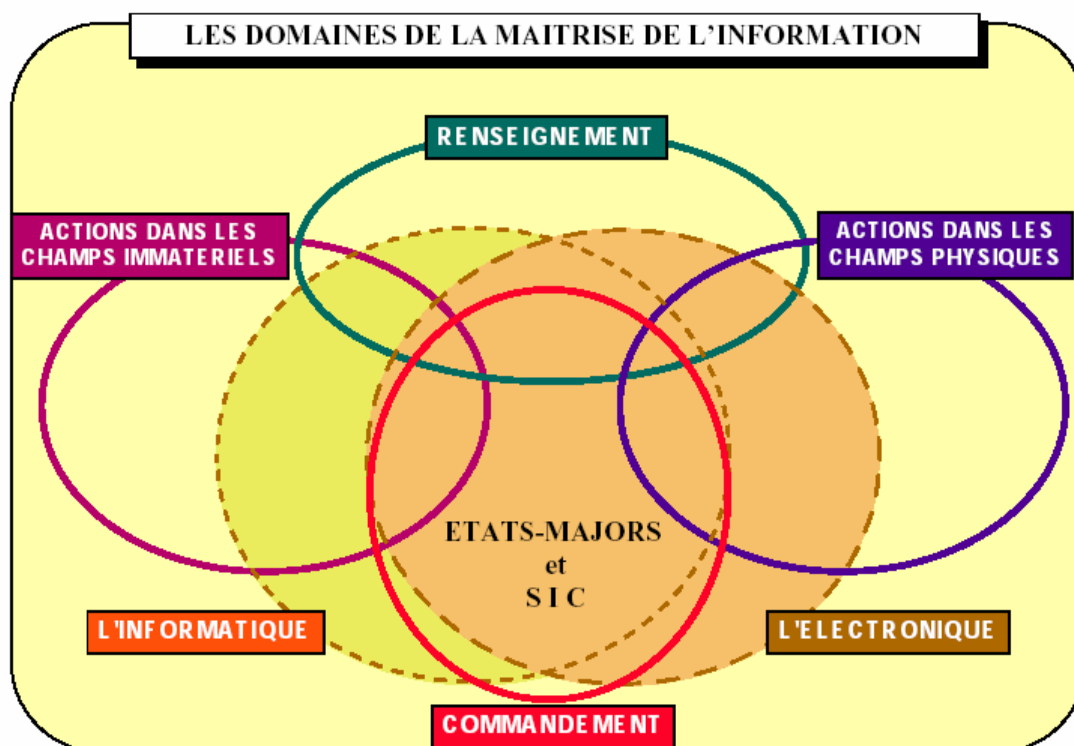
<sup>14</sup> Systèmes d'information et de commandement

<sup>15</sup> N°957/CDES/CREDAT/B6, 1999

<sup>16</sup> Etude du CDE/CR, 1999

<sup>17</sup> N°000658/DEF/EMA/EMP.1/NP, 2001

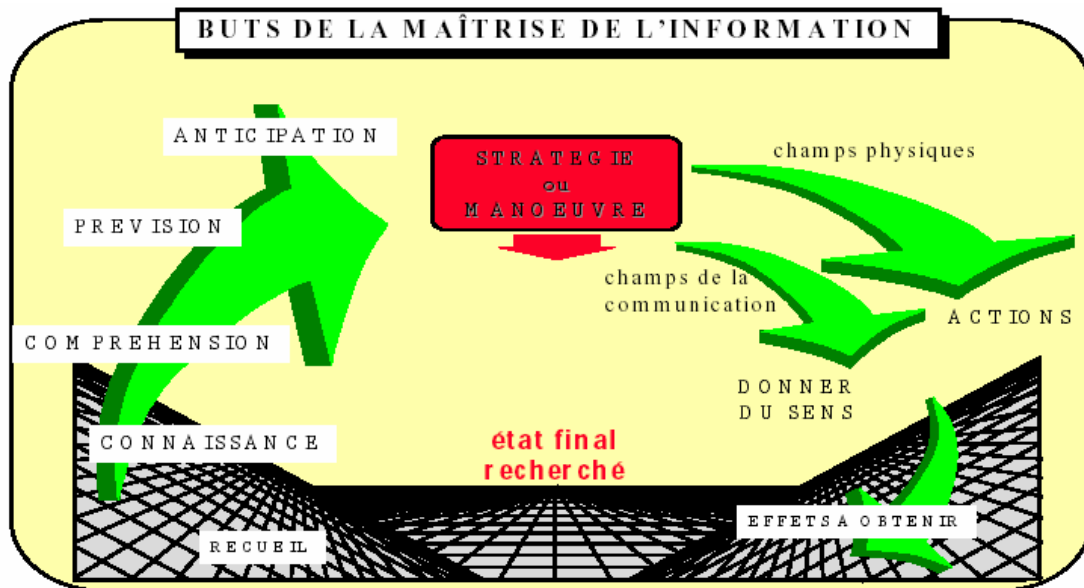
commandement présente une trame de doctrine GI sur la télématique, le renseignement, la GE, la guerre informatique, la simulation et l'analyse opérationnelle et les destructions physiques. Il faut aussi noter le document Gestion de l'environnement psychologique en opération<sup>18</sup>, qui apporte des compléments opérationnels utiles.



La Loi de programmation militaire 2003–2008 prévoit pour la maîtrise de l'information de « ...renforcer l'interopérabilité de nos forces armées avec celles de nos partenaires et alliés, et progresser dans la maîtrise de l'information devenue essentielle pour garantir la supériorité et le contrôle en temps réel de la situation sur les théâtres d'opérations ». La notion de maîtrise de l'information ne s'oppose pas à celle de « guerre de l'Information » mais doit s'entendre plutôt comme l'équivalent du terme « information dominance » des Américains<sup>19</sup>. Maîtriser l'information, c'est : acquérir et gérer les informations sur les espaces physiques, humains et structurels afin d'avoir la connaissance la plus précise possible de la situation ; l'acquisition est indissociable de la gestion d'une quantité très importante de données, comprendre au mieux la situation et en prévoir l'évolution afin de permettre l'anticipation stratégique, arrêter une stratégie ou une manœuvre grâce aux moyens d'aide à la décision, conduire les actions dans les champs physiques grâce à l'information numérisée, indiquer le sens de l'action au travers de la gestion de l'environnement psychologique qui recouvre la communication opérationnelle et l'appui psychologique.

<sup>18</sup> N°00358/DEF/EMA/EMP.1/NP, 2000

<sup>19</sup> Général Loup Francart, magazine Diplomatie, 2003



Voir n'est pas savoir. L'évolution de la GI est la guerre de la connaissance. La perception précoce de signaux faibles, la maîtrise des flux, la structuration des données et leur exploitation doivent conduire à un usage efficace et efficient pour maîtriser l'information et créer des éléments de connaissance pour décider. A partir d'informations de plus en plus nombreuses, hétérogènes et multiformes qui doivent être collectées, regroupées, synthétisées et présentées, la connaissance produite doit aussi être compréhensible, accessible et adaptée aux destinataires. Pour ce faire, de nouvelles formes d'organisation doivent être créés et nécessiteront un « socle de défense globale », composé d'organisations industrielles et d'armement, de recherche et d'expertises. Elles devront s'appuyer sur de nouveaux outils, capteurs, satellites entre autres, reliés à des bibliothèques, en vue d'analyser et d'identifier des risques et des opportunités pour réagir instantanément en tout lieu et en tout temps. Dans cette vision « centrée réseaux » (*networkcentric*), la maîtrise de la connaissance permettra de décider et d'agir avant les autres. Vaincre sans combattre, serait l'*ultima ratio* de la guerre, et la victoire serait ainsi double comme le disait l'Empereur Napoléon 1er.