La défense et les technologies de l'information et de la communication

Les technologies de l'information et de la communication se sont diffusées largement dans les systèmes et équipements des armées. Mais elles ont surtout provoqué une transformation profonde des organisations et de la conduite des forces par une mise en réseau de toutes les informations opérationnelles, rendant leur transmission possible au niveau de chaque combattant.

par François Levieux,
Directeur des processus techniques,
Groupe Thales

Si vous demandez à dix spécialistes des affaires militaires leur opinion sur les technologies de l'information, nul doute que vous obtiendrez au moins dix réponses différentes et contradictoires. En cela, la communauté militaire ne se distingue pas vraiment du reste de la population-! Mais elle entretient vis-à-vis de ce domaine technique une relation complexe, liée à l'évolution des trente dernières années. La défense a été, en effet, le principal marché de l'informatique jusqu'en 1960, et un donneur d'ordre significatif, jusqu'aux années 70. Aujourd'hui, le numérique et le logiciel ont pénétré tous les systèmes opérationnels du commandement, des équipements et de la logistique, et cependant la défense n'est plus un marché significatif pour les fournisseurs du domaine de l'information et de la communication, alors même qu'entre un quart et la moitié de la valeur ajoutée d'un équipement militaire moderne relève aujourd'hui de ces disciplines.

Les technologies de l'information et de la communication (pour simplifier nous dirons désormais-: les TIC) sont depuis plus de vingt ans des technologies duales, c'est-à-dire communes à l'économie et à la défense. On pourrait donc croire que les armées se contentent d'acheter les produits disponibles, un peu partout, pour les faire intégrer, tels quels, dans les architectures de leurs outils. La situation réelle est beaucoup plus complexe. Les possibilités offertes par la révolution permanente du monde informatique transforment les organisations militaires, de la même façon qu'elles modifient le reste de l'organisation sociale. Tout d'abord, nous allons examiner la réorganisation radicale imposée aux militaires par l'informatique et les télécommunications et ensuite nous exposerons quels produits et technologies du domaine des TIC jouent un rôle significatif dans les armées et quelles sont les contraintes propres à leur utilisation.

Les TIC et la «-transformation-» des armées

«-Murat, vas-tu nous laisser dévorer par ces gens-là?-» [1]

Pour lancer en quelques minutes la plus grande charge de cavalerie de l'histoire moderne, Napoléon n'a eu besoin que d'une longue vue et de sa voix. Le besoin était clair-: réorganiser immédiatement les forces disponibles, pour faire face à un événement imprévu. Ce besoin est toujours d'actualité – deux siècles plus tard – et l'urgence toujours présente, mais ni la voix ni une longue vue ne peuvent suffire. Un réseau complexe de transmissions est nécessaire, associant grande fiabilité, distances considérables et haute performance, car le combat est toujours le monde du temps instantané.

Ce que faisait Napoléon à Eylau s'appelle aujourd'hui «-boucle OODA-» (observer, orienter, décider, agir)-; mais le champ de bataille est à la taille d'un état, la chaîne logistique traverse océans et continents et le combat se planifie sur des semaines, voire des mois. De plus l'information est fournie par une grande variété de capteurs portés par des plates-formes diverses (avions, chars, drones, navires, robots… ou observateurs humains).

Le délai de re-planification des opérations est un paramètre critique. Pour donner des ordres de grandeur, il était de l'ordre de la semaine en 1945, de l'ordre de la journée lors de la première guerre du Golfe, de l'ordre de l'heure en Afghanistan, inférieur à l'heure en Irak [2]. Ceci suppose une actualisation de la situation de toutes les unités en quelques minutes. Collecter toutes ces données sur le terrain, les transmettre au quartier général, parfois au niveau politique, pour décision, réaffecter les ressources et agir-: voilà qui serait impossible sans un réseau de transmission cohérent et homogène, depuis l'observateur, humain ou automate, jusqu'à l'arme sollicitée, elle-même plateforme pilotée ou module automatique.

Un exemple-: pendant l'opération *Enduring Freedom* en Afghanistan, un sergent des forces spéciales, sur son

cheval, identifia une cible. Il téléchargea à partir d'un drone une photographie aérienne de son environnement, envoya par satellite une demande d'engagement aux USA. Le quartier général affecta un avion d'armes à la mission, qui reçut du sergent les coordonnées de la cible. Le pilote vérifia la situation opérationnelle pour s'assurer de l'absence de troupes amies et neutralisa la cible, par l'intermédiaire d'un engin muni d'un GPS.

Pas une seule de ces actions qui n'ait largement recouru aux TIC (sauf le cheval, bien sûr…).

Deux questions priment-: comment accélérer la transmission de la bonne information au bon utilisateur, et quelle est l'information pertinente pour chaque niveau de commandement-? La réponse à la seconde question, de nature opérationnelle, doit être apportée par les militaires, et sort par conséquent du sujet de cet article. En revanche, la première réponse est technique et elle fait largement appel aux TIC. Selon les pays, elle porte un nom différent-: *Network Centric Warfare* aux USA [3], *Network Enabling Capability* en Grande-Bretagne, Réseaux Info-Centrés en France. La conséquence en fut une profonde réorganisation des armées dans tous les pays de l'Otan, baptisée aux USA «-transformation des forces-».

Les organisations info-centrées

«-The network is the computer-»

Ce slogan marketing du début des années 90 est dû à la société SUN Microsystems. Il montre dès cette date qu'un système informatique, ne pouvant plus se limiter à une collection d'ordinateurs reliés entre eux, devient un tout cohérent, dont la colonne vertébrale est le réseau, élément central de l'organisation. Dix ans plus tard, ce même concept se généralise, dans les armées.

Un premier niveau de mise en réseau concerne plusieurs plates-formes militaires-: flotte d'avions ou escadre navale, par exemple. On parle dans ce cas d'engagement coopératif, et les informations sont souvent homogènes (radars, sonars, senseurs de guerre électronique, contre-mesures, etc.). La difficulté principale réside dans la maîtrise de la latence. Non pas la latence technique, liée à la transmission, qui est de l'ordre de la microseconde, ni la latence liée aux traitements, nettement plus élevée du niveau de la milliseconde, mais la latence induite par l'intervention de l'homme dans la boucle de décision, d'une durée variable, mais considérable, par rapport aux deux premières (quelques dizaines de secondes, voire plusieurs minutes). Ceci pousse à une organisation sans intervention humaine (*man out of the loop)* qui suppose des algorithmes de robotique, d'intelligence artificielle et une puissance de calcul considérable, même compte tenu de l'état de l'art actuel. L'usage du drone en aéronautique, ou encore du robot marin ou terrestre, va donc se généraliser dans les armées, avec les transmissions, les senseurs et les logiciels de mission correspondants.

Aujourd'hui, le numérique et le logiciel ont pénétré tous les systèmes opérationnels du commandement

Un deuxième niveau est le concept de «-bulle-». La mise en réseau des moyens militaires des trois armes, appuyés et relayés par des observations et des transmissions spatiales, crée des zones de sûreté appelées «-bulles opérationnelles-» qui protègent les unités ou les équipements critiques de tout risque de destruction. Ce principe peut d'ailleurs être aisément étendu à la sécurité civile lorsque c'est réaliste économiquement (protection des aéroports ou des côtes, par exemple). Il faut bien sûr disposer de moyens variés, faisant ici aussi une large place aux engins automatiques et aux capteurs sophistiqués.

Le troisième niveau est dédié à la conduite des opérations militaires elles-mêmes. La mise en réseau structure le mode de conduite des forces engagées. Les observations de toute nature sont regroupées, fusionnées et transmises à chaque unité combattante qui en a l'usage. Ceci suppose la capacité de gérer, traiter et transmettre en faible temps différé des quantités d'informations très importantes à toutes les positions de combat, dont il faudra bien sûr actualiser les mouvements. Ces principes ont été mis en œuvre par l'armée américaine pendant l'offensive en Irak, en 2003. Les résultats, variables, sont encore en cours d'analyse aujourd'hui [4].

L'interopérabilité des armées coalisées

«-J'admire beaucoup moins Napoléon, depuis que je sais ce qu'est une coalition-»

Le maréchal Foch se posait déjà la question en 1918-: avec des organisations collectives aussi sophistiquées, comment mener une coalition-? Ces organisations étant construites en fonction des capacités des TIC à fournir des réponses instantanées, et deux systèmes informatiques conçus séparément n'étant jamais parfaitement compatibles, deux armées alliées de pays distincts sont confrontées au problème de la cohérence de leurs informations et de leurs actions. Ce n'est pas très difficile à résoudre avec des messageries classiques. Mais comment, en revanche, faire tirer une frégate française ou britannique sur une cible identifiée et codée par un bateau américain (ou l'inverse)-? La réponse est malaisée et, illustrant le cas extrême, il y eut encore de nombreux morts par tir fratricide en 2003, un des drames les plus spectaculaires de ce type ayant été la destruction d'un avion britannique par les défenses US [5].

Pour éviter de telles situations, une coopération étroite entre armées alliées est indispensable, au point de poser le problème – difficile – du commandement et des procédures partagés. Des méthodes et cultures variées coexistant par nécessité historique, une telle harmonisation est irréaliste sur l'ensemble de l'OTAN, par exemple. L'impact des TIC accroît clairement la difficulté. Un premier objectif serait sans doute d'arriver à une grande compatibilité entre les armées des nations majeures européennes. C'est en cours, mais même dans ce cadre restreint, le travail à accomplir est considérable. Les accords franco-britan-

niques et franco-allemands, la création de l'agence européenne de défense, participent à cet effort préalable à toute concrétisation d'une force militaire européenne intégrée. Tous ceux qui ont essayé de rationaliser l'informatique interne d'un grand groupe industriel comprendront sans doute quelle est la nature des difficultés rencontrées…
Passons maintenant à l'examen de quelques problèmes techniques liés à l'utilisation des TIC dans les armées

Les télécommunications militaires

Depuis toujours, les télécommunications jouent un rôle décisif dans la conduite des armées et des flottes. Le téléphone portable, produit emblématique du marché des télécommunications civiles depuis dix ans, existe au moins depuis la première guerre mondiale dans sa version militaire et, sous sa forme moderne, au moins depuis les systèmes de la classe RITA ou MSE de la fin des années 80. Mais la version civile banalisée ne résout pas deux besoins critiques – le chiffrement et l'antibrouillage – lesquels justifient la conception de solutions spécifiques. De plus, se pose le problème de la compatibilité avec les formes d'ondes des matériels militaires préexistants.

La mise en réseau structure le mode de conduite des forces engagées

La solution en préparation est la radio logicielle dont les caractéristiques du signal émis résultent de l'exécution d'un des programmes de l'ordinateur intégré au poste [3]. Ainsi, malgré son succès éclatant sur le marché civil, l'impact du portable sur les armées induit surtout une certaine baisse des coûts.
La version civile d'Internet et son complément – le Web – ont en revanche modifié le mode d'organisation et de conception des réseaux et, comme nous l'avons vu, des armées. Le protocole Internet (IP), bien connu des internautes, est en passe de se substituer à tous ses prédécesseurs. On peut observer que cela termine une évolution originale qui aura vu l'Arpanet de la guerre froide devenir le Web de la recherche physique fondamentale, puis envahir les messageries privées et les méthodes documentaires de toute l'économie, avant de revenir offrir aux armées une solution exceptionnellement robuste et économique pour la réalisation des réseaux de transmission critiques.

L'informatique militarisée

Internet fournit la transition entre les télécommunications, domaine d'une certaine continuité, et l'informatique, lieu de tous les bouleversements. L'informatique est, après le nucléaire, la technologie qui a eu le plus d'impact sur la défense depuis les années 1950. A l'origine de l'évolution du matériel, une seule cause-: l'intégration des composants sur silicium et la célèbre loi empirique de «-Moore-»-(1). A l'opposé, la pesanteur et l'inertie considérable des standards de logiciel de base-(2) (Dos, Unix, Windows, MacOS, Linux…) et des logiciels d'application qui en dépendent représentent un investissement coûteux qui pèse sur des décennies. Une des conséquences de ces évolutions contradictoires (le silicium qui pousse, le logiciel qui retient) est l'apparition de cycles de sept à huit ans générant des ruptures brutales sur le marché informatique, que les utilisateurs ont été obligés de prendre en compte, du fait notamment de la disparition de fournisseurs précédemment dominants et de leurs lignes de produits. Ceci est aggravé par la banalisation des produits militarisés.
En effet, le même matériel pouvant être utilisé au nord du Canada en hiver ou en Arabie Saoudite en été, on a connu une prolifération de circuits et logiciels «-militarisés-» jusqu'au milieu des années 90. Mais l'automobile, devenue un marché dominant pour les composants, a imposé à tous les fabricants de produits électroniques des contraintes autrefois réservées aux seules applications militaires. Le marché du «-militarisé-» a disparu, en-dehors du cas particulier du spatial.
Aujourd'hui, les systèmes militaires utilisent les mêmes composants numériques élémentaires que les civils (mémoires, microprocesseurs, interfaces…). Le problème d'accès à un matériel robuste et bon marché ne se pose plus. Mais, comme toujours, la situation est plus complexe pour le logiciel.

Un dilemme technique : le choix des standards logiciels

Dans un célèbre tableau de W.-Turner, un navire de ligne du milieu du 18e siècle, le «-Téméraire-», héros de la bataille de Trafalgar, est remorqué par un vapeur à roue à aubes… Ceci montre que le système d'armes représenté par ce bâtiment a été utilisé pendant plus d'un demi-siècle. Ce constat perdure pour les systèmes militaires d'aujourd'hui, où l'informatique a remplacé la hausse manuelle des canons et la manœuvre au sifflet. Les armées font campagne avec des outils imaginés, au mieux 20 ans plus tôt, et souvent, bien avant. Pensons au bombardier B-52, conçu comme outil stratégique de la guerre froide, mis en service dans les années 50 et prévu pour servir, avec une informatique qu'on suppose rénovée, jusqu'en…2030 au moins-!
Changer en cours de développement le logiciel de base (2) des ordinateurs utilisés est pratiquement impossible, sans une remise à zéro des applications déjà réalisées, et donc un coût prohibitif. Or, les standards les plus répandus – Windows, UNIX, MAC-OS – sont, tous, la propriété de sociétés privées qui n'ont aucun intérêt à s'intéresser à la défense et à ses exigences originales, surtout en-dehors du marché dominant des USA. Un fournisseur célèbre a déjà déclaré-: «-Je n'ai pas un seul de mes rares ingénieurs à affecter à ce marché stupide !-».
Que faire, quand votre poste de travail et son logiciel sont abandonnés par tous en trois ans et que votre développement s'étale sur dix, voire quinze ans, sans

(1)-Dès 1966, G.-Moore, le fondateur d'Intel, a prédit que les circuits numériques doubleraient leur capacité tous les dix-huit mois sur… les dix années suivantes. En 2005, c'est toujours vérifié…

(2)-Un logiciel de base (système d'exploitation, gestion de la mémoire et des interfaces) est nécessaire au fonctionnement d'un ordinateur. Un logiciel d'application est dédié à une utilisation précise. Le code source (ou, simplement-: la source) d'un logiciel utilise un langage «-proche-» du langage humain, ce qui en permet la modification. La version de tout logiciel, fournie contractuellement à l'utilisateur, est le code binaire, qu'on ne peut interpréter sans connaître le code source.

parler de la logistique, sur…vingt-cinq ans-! Le fournisseur de systèmes militaires doit donc soit négocier – difficilement – un accord technologique avec l'un d'entre eux, soit acheter tel quel leur produit, avec, comme seul support, celui dédié aux applications civiles [3]. La première option est satisfaisante sur le plan technique, mais coûteuse et risquée si le partenaire périclite et la seconde, très dangereuse car ne garantissant en aucun cas le bon fonctionnement du système. Ces deux solutions génèrent de plus un risque opérationnel.

Un enjeu de souveraineté

Comme dans tous les pays de l'OCDE, le matériel de guerre américain est soumis à des restrictions aux pratiques d'exportation. Et ce n'est pas une clause de style-: Boeing a par exemple été mis en cause pour avoir fourni à la Chine des avions civils comportant un circuit critique coûtant seulement 1 000-$! Tout produit « concourant à la supériorité des forces américaines-» peut être concerné-: on le constate, il s'agit d'une définition pour le moins large de la notion de matériel militaire stratégique.

Pas de risque, en revanche, pour le matériel et logiciel informatique classique, par exemple les microprocesseurs, car une application à ce type de produit de restrictions commerciales aurait des conséquences économiques insupportables pour les industriels américains. Pour des produits plus spécifiques ou la source (2) des logiciels, la situation est tout autre, comme l'illustra l'exemple des supercalculateurs, à l'origine de quelques frictions transatlantiques demeurées célèbres. Des refus de commercialisation, même au sein des pays membres de l'Otan, surviennent régulièrement. Or, sans support technique permanent, aucune application informatique militaire ne peut être mise au point. Enfin, subsiste le risque que le logiciel fourni contienne des « failles-», connues du seul fournisseur, ce qui accroît l'effet de dépendance souligné plus haut.

Comment contourner cette difficulté dans le contexte européen-? Le véritable enjeu porte sur l'usage – ou non – de Windows et de l'énorme quantité de logiciels d'applications associés au monde Microsoft. Ceci est particulièrement vrai en ce qui concerne les applications jugées non-critiques. Pour un architecte de systèmes militaires, éliminer une partie des aléas de l'informatique, en choisissant ce standard propriétaire, est très tentant. (Il y a trois décennies, la même logique jouait en faveur d'IBM). Mais, dans ce cas, la mise au point et la logistique, voire le fonctionnement, dépendent du bon vouloir de la firme de Redmond…

L'impact des logiciels libres

La solution à ce dilemme provient de façon inattendue de la communauté universitaire, car la mission d'éducation pose ce même problème d'accès aux sources (2) des logiciels de base. Les informaticiens universitaires ont donc décidé, au niveau mondial, dès 1991, de créer leurs propres standards gratuits et universels, dont l'élément le plus célèbre est le système d'exploitation Linux. Cette solution des «-logiciels libres-» («-Open Source-» en anglais) n'a été rendue possible que grâce à la généralisation d'Internet, qui rend la diffusion gratuite aisée et assure une mise au point d'une qualité exceptionnelle. Linux représente aujourd'hui une excellente option technique pour les systèmes de commandement et tous les systèmes militaires hors «-temps réel-».

Le rôle des logiciels libres est décisif. Ces technologies sont extraterritoriales et l'accès aux sources via Internet est totalement garanti (et accessoirement presque gratuit). Plusieurs sociétés (dont au moins une en France) assurent la diffusion et le support de ces logiciels pour ceux des utilisateurs qui souhaitent se décharger de cette tâche. C'est à terme la solution la plus sûre pour toutes les applications de défense. La panoplie des logiciels d'application accessibles autour de Linux est désormais très complète. Aux USA, le lancement de plusieurs procès contre les fournisseurs de logiciels libres montre d'ailleurs que cette solution est considérée par les fournisseurs traditionnels comme une concurrence très sérieuse. Le frein le plus gênant à leur plus large adoption tient aux habitudes des utilisateurs, qui bénéficient aux produits Microsoft. On a vu des systèmes de commandement utiliser Windows pour la seule raison qu'il était plus pratique de transférer en fichiers Excel les rapports à l'état-major, grâce à ce logiciel-! Cependant les considérations de sécurité et de souveraineté imposeront le choix de l'indépendance, et donc l'usage généralisé des logiciels libres.

Depuis toujours, les télécommunications jouent un rôle décisif dans la conduite des armées et des flottes

Un dernier problème technique-: le temps réel…

De nombreux équipements militaires ne peuvent réagir qu'après un temps de latence incompressible. Ceci est dû à des servitudes essentiellement mécaniques (tour d'antenne sur les radars, identification et validation des objets observés, vitesse de défilement des avions d'observation, etc.). Pour des raisons de mémorisation (que nous n'exposerons pas ici), un ordinateur muni d'un logiciel classique est tributaire de la vitesse de rotation de son disque dur. Celle-ci, prenant du retard sur le développement des performances de l'électronique, devient un goulet d'étranglement que tout utilisateur peut constater sur son PC lorsqu'il doit attendre, durant d'interminables secondes, que sa demande apparemment anodine daigne être prise en compte…

Ce type de contrainte doit être contourné par un logiciel de base spécifique à ce type d'application-: le système d'exploitation en temps réel (2). Les militaires sont les plus gros consommateurs de ces produits, qui ont pour seul inconvénient d'exiger l'adaptation de tous les logiciels qui en dépendent. Il existe une spécificité des applications temps réel, protégée par les loi d'inertie de la mécanique et le théorème empirique (encore un-!) – ironiquement intitulé-«-théorème des gaz parfaits informatiques-» – qui rend compte de la boulimie d'occupation des mémoires,

trop largement répandue chez la plupart des concepteurs de logiciels.

Quelques perspectives

La «-loi-» de Moore (1) restera sans doute valable encore au moins dix ans. Nous verrons donc apparaître au moins quatre générations d'ordinateurs avant tout éventuel ralentissement de l'évolution technologique. La capacité des transmissions sous protocole IP ira croissant, avec l'-«-encapsulation-», puis l'absorption, sous IP, des réseaux préexistants. Tout ceci améliorera l'efficacité des armées, notamment par la réduction des destructions dites «-collatérales-». Où les futures opportunités vont-elles donc se créer et quels goulots d'étranglement sont-ils susceptibles de freiner la diffusion des TIC dans le domaine militaire ?

Rappelons les quatre étapes de toute action militaire-: Observer, Orienter, Décider, Agir (OODA).

- Observer-: les TIC induisent une numérisation généralisée et une banalisation des traitements numériques de tous les capteurs physiques. Le traitement radar ressemble à celui du sonar, de la guerre électronique, des contre-mesures, etc. En parallèle, le traitement de l'information dépend de la fusion des données issues de ces capteurs et de renseignements extrêmement diversifiés-: voix, textes, cartes, images vidéo… On peut imaginer que des technologies du grand public, telles celles illustrées par Google, ou des concepts de diffusion grand public comme le *triple play* soient bientôt nécessaires aux armées, ce qui représente un champ presque vierge pour les concepteurs des systèmes futurs.

- Orienter-: première phase du commandement, la préparation et la planification des actions devront recourir à des simulations mélangeant les niveaux opérationnels et physiques, et ceci, en temps quasi réel. Les moyens informatiques nécessaires n'existent pas encore, de nos jours, mais avec un peu de patience, cela ne devrait pas tarder.

- Décider-: le rôle de l'aide à la décision et des nombreuses techniques d'intelligence artificielle sera ici primordial. Une partie de la chaîne de décision échappera nécessairement au contrôle humain. Comment en vérifier le bon fonctionnement-? En prévenir les éventuelles dérives ? La bonne architecture des futurs systèmes de commandement reste encore à préciser, tant les champs du possible ouverts par les TIC s'élargissent sans fin.

- Agir-: Les armes sont déjà largement pénétrées par des solutions numérisées-: commandes de vol des avions, contrôle des commandes de l'armement des navires, réglage automatique des tirs, pilotage des missiles, etc. Cette évolution va continuer sans heurts. En revanche, la rupture proviendra vraisemblablement de l'amélioration des drones et autres robots. Le sans pilote ou le piloté à distance vont inévitablement devenir la règle, l'amélioration de la sécurité des combattants se conjuguant à la baisse du coût des pertes éventuelles pour justifier un recours systématique à ce type de moyens.

L'informatique est, après le nucléaire, la technologie qui a eu le plus d'impact sur la défense depuis les années 1950

En conclusion-: Les TIC sont-elles stratégiques-pour la défense ?

Nous avons vu que la réponse à cette question est loin d'être simple. Stratégiques, les supercalculateurs l'ont été, or ils ne le sont plus aujourd'hui, où n'importe quelle université peut en concevoir un, au moyen de microprocesseurs et de logiciels libres. Les systèmes d'exploitation le sont, alors même qu'ils sont apparemment très répandus et facilement accessibles. Demain, les moteurs de recherche ou de messagerie peuvent le devenir, en fonction de l'évolution de l'organisation industrielle des fournisseurs.

Mais il y a, dans tous les cas, une certitude-: la maîtrise des technologies informatiques et de télécommunications par une large communauté d'ingénieurs et de chercheurs est une condition nécessaire de la création et de l'entretien de forces armées efficaces. Si la puissance des nations dépend de leur capacité reconnue à exercer éventuellement leur *ultima ratio* militaire, alors, n'en doutons pas, cette communauté des technologies de l'information et de la communication jouera un rôle majeur dans la crédibilité de l'ensemble du dispositif de défense d'un Etat moderne.

Ceci dit, restons modestes-: quelle TIC permettra-t-elle de se protéger contre le tir à très courte distance d'un missile rudimentaire lancé…depuis une charrette tirée par un âne-? La métallurgie et le blindage ont peut-être encore un certain avenir militaire devant eux… ●

BIBLIOGRAPHIE

[1] Napoléon Bonaparte à la bataille d'Eylau. Citation rapportée notamment par G. Plon dans son ouvrage «-La Grande Armée-», éd. R. Laffont, 1979, p. 130.

[2] Annales du colloque «-Nouvelles Technologies et Art de la Guerre-» – CID 28 avril 2004 – http://www.college.interarmees.defense.gouv.fr.

[3] IT Special Report «-Connecting the Dots-», J. C. Anselmo, AW & ST, February 28th, 2005, pp. 19-25.

[4] US Army Transformation; An Update, M. Leibstone, in Military Technology, Vol. XXVIII, issue 10, 2004, pp. 19-25.

[5] «-Unfriendly Fire-», D. Barrie, AW & ST, April 7th, 2003.