

Source : <https://press.armywarcollege.edu/parameters/vol28/iss1/12/>

The US Army War College Quarterly: Parameters

Volume 28
Number 1 *Parameters Spring 1998*

Article 12

2-17-1998

L'esprit n'a pas de pare-feu

Timothy L. Thomas

Suivez ce travail et d'autres travaux à l'adresse suivante :
<https://press.armywarcollege.edu/parameters>

Citation recommandée

Timothy L. Thomas, "The Mind Has No Firewall", *Parameters* 28, no 1 (1998), doi:10.55540/0031-1723.1871.

Cet article vous est proposé en accès libre et gratuit par USAWC Press. Il a été accepté pour inclusion dans *The US Army War College Quarterly : Parameters* par un éditeur autorisé de USAWC Press.

L'esprit n'a pas de pare-feu

TIMOTHY L. THOMAS

From Parameters, printemps 1998, pp. 84-92.

"Il est tout à fait clair que l'État qui sera le premier à créer de telles armes obtiendra une supériorité incomparable. -- Major I. Chernishev, armée russe[1]

Le corps humain, à l'instar d'un ordinateur, contient une myriade de processeurs de données. Il s'agit notamment de l'activité chimique et électrique du cerveau, du cœur et du système nerveux périphérique, des signaux envoyés de la région du cortex du cerveau vers d'autres parties du corps, des minuscules cellules ciliées de l'oreille interne qui traitent les signaux auditifs, et de la rétine et de la cornée sensibles à la lumière qui traitent l'activité visuelle[2]. Nous sommes à l'aube d'une ère où ces processeurs de données du corps humain peuvent être manipulés ou affaiblis. Les exemples d'attaques non planifiées contre les capacités de traitement des données du corps sont bien documentés. Les lumières stroboscopiques sont connues pour provoquer des crises d'épilepsie. Il n'y a pas si longtemps, au Japon, des enfants qui regardaient des dessins animés à la télévision ont été soumis à des lumières pulsées qui ont provoqué des crises chez certains d'entre eux et en ont rendu d'autres très malades.

La défense des capacités de traitement des données du corps des amis et des adversaires semble être un point faible dans l'approche américaine de la théorie de la guerre de l'information, une théorie fortement orientée vers le traitement des données des systèmes et conçue pour atteindre la domination de l'information sur le champ de bataille. C'est du moins ce qui ressort des informations publiées dans la presse ouverte et non classifiée. Cette lacune des États-Unis pourrait être grave, puisque les capacités de modifier les systèmes de traitement des données du corps existent déjà. Une récente édition du U.S. News and World Report a mis en lumière plusieurs de ces "armes miracles" (acoustique, micro-ondes, lasers) et a noté que les scientifiques "recherchent dans les spectres électromagnétique et sonique des longueurs d'onde susceptibles d'affecter le comportement humain"[3]. Un récent article militaire russe a présenté le problème sous un angle légèrement différent, déclarant que "l'humanité se trouve au bord d'une guerre psychotronique" avec l'esprit et le corps comme point de mire. Cet article traite des tentatives russes et internationales visant à contrôler l'état psychophysique de l'homme et ses processus décisionnels par l'utilisation de générateurs VHF, de "cassettes silencieuses" et d'autres technologies.

Un arsenal d'armes entièrement nouveau, basé sur des dispositifs conçus pour introduire des messages subliminaux ou pour altérer les capacités psychologiques et informatiques du corps, pourrait être utilisé pour neutraliser les individus. Ces armes visent à contrôler ou à altérer le psychisme, ou à attaquer les différents systèmes sensoriels et informatiques de l'organisme humain. Dans les deux cas, l'objectif est de brouiller ou de détruire les signaux qui assurent normalement l'équilibre du corps.

Cet article examine les armes basées sur l'énergie, les armes psychotroniques et d'autres développements conçus pour modifier la capacité du corps humain à traiter les stimuli. L'une des

conséquences de cette évaluation est que l'utilisation courante du terme "guerre de l'information" ne suffit pas lorsque le soldat individuel, et non son équipement, devient la cible de l'attaque.

La théorie de la guerre de l'information et l'élément informatique de l'être humain

Aux États-Unis, la conception commune de la guerre de l'information se concentre principalement sur les capacités des systèmes matériels tels que les ordinateurs, les satellites et les équipements militaires qui traitent les données sous leurs diverses formes. Selon la directive S-3600.1 du 9 décembre 1996 du ministère de la défense, la guerre de l'information est définie comme "une opération d'information menée en temps de crise ou de conflit pour atteindre ou promouvoir des objectifs spécifiques face à un ou plusieurs adversaires spécifiques". Une opération d'information est définie dans la même directive comme "des actions entreprises pour affecter les informations et les systèmes d'information de l'adversaire tout en défendant ses propres informations et systèmes d'information". Ces "systèmes d'information" sont au cœur de l'effort de modernisation des forces armées américaines et d'autres pays, et se manifestent sous la forme de matériel, de logiciels, de capacités de communication et de personnes hautement qualifiées. Récemment, l'armée américaine a mené une bataille simulée qui a permis de tester ces systèmes dans des conditions de combat simulées.

Le manuel de l'armée américaine 101-5-1, *Operational Terms and Graphics* (publié le 30 septembre 1997), définit la guerre de l'information comme "les actions entreprises pour atteindre la supériorité en matière d'information en affectant l'information, les processus basés sur l'information et les systèmes d'information d'un ennemi, tout en défendant sa propre information, ses processus d'information et ses systèmes d'information". Le même manuel définit les opérations d'information comme une "opération militaire continue dans l'environnement d'information militaire qui permet, améliore et protège la capacité des forces amies à collecter, traiter et agir sur l'information pour obtenir un avantage dans toute la gamme des opérations militaires. [Les opérations d'information comprennent l'interaction avec l'environnement d'information global . et l'exploitation ou le déni des capacités d'information et de décision de l'adversaire]"[4].

Cette approche "systémique" de l'étude de la guerre de l'information met l'accent sur l'utilisation de données, appelées informations, pour pénétrer les défenses physiques de l'adversaire qui protègent les données (informations) afin d'obtenir un avantage opérationnel ou stratégique. Elle tend à ignorer le rôle du corps humain en tant que processeur d'informations ou de données dans cette quête de domination, sauf dans les cas où la logique ou la pensée rationnelle d'un individu peut être perturbée par la désinformation ou la tromperie. Par conséquent, la protection de l'esprit et du corps à l'aide d'un pare-feu, comme nous l'avons fait pour les systèmes matériels, ne fait pas l'objet d'une grande attention. Aucune technique n'a non plus été prescrite à cet effet. Pourtant, le corps est capable non seulement d'être trompé, manipulé ou désinformé, mais aussi d'être arrêté ou détruit, comme n'importe quel autre système de traitement des données. Les "données" que le corps reçoit de sources externes - telles que les ondes électromagnétiques, vortex ou acoustiques - ou qu'il crée par ses propres stimuli électriques ou chimiques peuvent être manipulées ou modifiées, tout comme les données (informations) de n'importe quel système matériel peuvent être altérées.

Le seul élément de guerre de l'information lié au corps considéré par les États-Unis est les opérations psychologiques (PSYOP). Dans la publication conjointe 3-13.1, par exemple, les opérations psychologiques figurent parmi les éléments de la guerre de commandement et de contrôle. La publication note que "la cible ultime de la [guerre de l'information] est le processus

dépendant de l'information, qu'il soit humain ou automatisé...". La guerre de commandement et de contrôle (C2W) est une application de la guerre de l'information dans les opérations militaires. . . . La guerre de commandement et de contrôle est l'utilisation intégrée de la PSYOP, de la déception militaire, de la sécurité des opérations, de la guerre électronique et de la destruction physique"[5].

Une source définit l'information comme un "signal non accidentel utilisé comme entrée dans un ordinateur ou un système de communication"[6] Le corps humain est un système de communication complexe qui reçoit en permanence des signaux non accidentels et accidentels, tant externes qu'internes. Si la cible ultime de la guerre de l'information est le processus dépendant de l'information, "qu'il soit humain ou automatisé", la définition de la publication conjointe implique que le traitement humain des signaux internes et externes peut clairement être considéré comme un aspect de la guerre de l'information. Des chercheurs étrangers ont noté le lien entre le traitement des données par l'homme et la conduite de la guerre de l'information. Si certains n'étudient que le lien PSYOP, d'autres vont au-delà. Dans le premier cas, un article russe récent décrit la guerre de l'information offensive comme visant à "utiliser les canaux Internet pour organiser la PSYOP ainsi que pour "l'alerte politique précoce" sur les menaces pesant sur les intérêts américains"[7]. [et] aujourd'hui, cela doit inclure l'Internet". L'auteur affirme que le Pentagone veut utiliser Internet pour "renforcer les influences psychologiques" lors d'opérations spéciales menées en dehors des frontières américaines afin de recruter des sympathisants qui accompliront une grande partie des tâches précédemment confiées aux unités spéciales des forces armées américaines.

D'autres, cependant, vont au-delà des simples liens PSYOP et considèrent d'autres aspects de la capacité de traitement des données de l'organisme. L'un des principaux chercheurs en sources ouvertes sur la relation entre la guerre de l'information et la capacité de traitement des données de l'organisme est le Russe Victor Solntsev, de l'Institut technique Baumann de Moscou. Solntsev est un jeune chercheur bien intentionné qui s'efforce d'attirer l'attention du monde sur les dangers potentiels de l'interface ordinateur-opérateur. Soutenu par un réseau d'instituts et d'académies, Solntsev a produit quelques concepts intéressants[8] : il insiste sur le fait que l'homme doit être considéré comme un système ouvert plutôt que comme un simple organisme ou un système fermé. En tant que système ouvert, l'homme communique avec son environnement par le biais de flux d'informations et de moyens de communication. Selon Solntsev, l'environnement physique, qu'il s'agisse d'effets électromagnétiques, gravitationnels, acoustiques ou autres, peut provoquer un changement dans l'état psychophysiologique d'un organisme. Un tel changement pourrait affecter directement l'état mental et la conscience d'un opérateur informatique. Il ne s'agirait pas d'une guerre électronique ou d'une guerre de l'information au sens traditionnel du terme, mais plutôt au sens non traditionnel et non américain du terme. Il pourrait s'agir, par exemple, d'un ordinateur modifié pour devenir une arme en utilisant sa production d'énergie pour émettre des sons qui affaiblissent l'opérateur. Il peut également s'agir, comme indiqué ci-dessous, d'armes futuristes visant le "système ouvert" de l'homme.

Solntsev s'est également penché sur le problème du "bruit de l'information", qui crée un écran dense entre une personne et la réalité extérieure. Ce bruit peut se manifester sous la forme de signaux, de messages, d'images ou d'autres éléments d'information. La cible principale de ce bruit serait la conscience d'une personne ou d'un groupe de personnes. La modification du comportement pourrait être l'un des objectifs du bruit d'information ; un autre pourrait être de perturber les capacités mentales d'un individu au point de l'empêcher de réagir à tout stimulus. Solntsev conclut que tous les niveaux du psychisme d'une personne (subconscient, conscient et "superconscient") sont des cibles potentielles de déstabilisation.

Selon Solntsev, le virus russe 666 est un virus informatique capable d'affecter le psychisme d'une personne. Il se manifeste à chaque 25ème image d'un écran visuel, où il produit une combinaison de couleurs qui mettrait les opérateurs informatiques en transe. La perception subconsciente du nouveau motif finit par provoquer une arythmie cardiaque. D'autres informaticiens russes, et pas seulement Solntsev, parlent ouvertement de cet "effet 25ème image" et de sa capacité à gérer subtilement les perceptions d'un utilisateur d'ordinateur. Le but de cette technique est d'injecter une pensée dans le subconscient du spectateur. Elle peut rappeler à certains la controverse sur la publicité subliminale aux États-Unis à la fin des années 1950.

Le point de vue des États-Unis sur les "armes merveilleuses" : Modifier la capacité de traitement des données du corps humain

Quelles sont les technologies examinées par les États-Unis qui ont le potentiel de perturber les capacités informatiques de l'organisme humain ? Le numéro du 7 juillet 1997 du U.S. News and World Report en décrivait plusieurs, destinées, entre autres, à faire vibrer l'intérieur de l'homme, à l'étourdir, à lui donner la nausée, à l'endormir, à le réchauffer ou à l'assommer par une onde de choc[9]. Ces technologies comprennent des lasers éblouissants qui peuvent forcer les pupilles à se fermer, des fréquences acoustiques ou sonores qui font vibrer les cellules ciliées de l'oreille interne et provoquent le mal des transports, le vertige et la nausée, ou des fréquences qui font résonner les organes internes et provoquent des douleurs et des spasmes, et des ondes de choc qui peuvent faire tomber des êtres humains ou des avions et qui peuvent être mélangées à du gaz poivré ou à des produits chimiques[10].

Si elles sont modifiées, ces applications technologiques peuvent avoir de nombreuses utilisations. Les armes acoustiques, par exemple, pourraient être adaptées pour être utilisées comme fusils acoustiques ou comme champs acoustiques qui, une fois établis, pourraient protéger des installations, aider à la libération d'otages, contrôler des émeutes ou dégager des voies pour les convois. Ces ondes, qui peuvent pénétrer dans les bâtiments, offrent de nombreuses possibilités aux militaires et aux forces de l'ordre. Les armes à micro-ondes, en stimulant le système nerveux périphérique, peuvent réchauffer le corps, provoquer des crises épileptiques ou un arrêt cardiaque. Les rayonnements à basse fréquence affectent l'activité électrique du cerveau et peuvent provoquer des symptômes grippaux et des nausées. D'autres projets visaient à induire ou à empêcher le sommeil, ou à affecter le signal du cortex moteur du cerveau, afin de neutraliser les mouvements musculaires volontaires. Ces dernières sont appelées armes à ondes pulsées, et le gouvernement russe aurait acheté plus de 100 000 exemplaires de la version "Black Widow" de ces armes[11].

Toutefois, cette vision des "armes miracles" a été contestée par quelqu'un qui devrait les comprendre. Le brigadier général Larry Dodgen, assistant adjoint du secrétaire à la défense pour la politique et les missions, a écrit une lettre au rédacteur en chef au sujet des "nombreuses inexactitudes" contenues dans l'article du U.S. News and World Report qui "déforment le point de vue du ministère de la défense"[12].

Le principal reproche de M. Dodgen semble être que le magazine présente de manière erronée l'utilisation de ces technologies et leur valeur pour les forces armées. Il a également souligné l'intention des États-Unis de travailler dans le cadre de tout traité international concernant leur application, ainsi que leur intention d'abandonner (ou au moins de revoir la conception) toute arme pour laquelle des contre-mesures sont connues. On a toutefois le sentiment que la recherche dans ce domaine est intense. Une préoccupation non mentionnée par Dodgen est que d'autres pays ou

acteurs non étatiques pourraient ne pas être soumis aux mêmes contraintes. Il est difficile d'imaginer quelqu'un de plus désireux que les terroristes de mettre la main sur ces technologies. Le "psychoterrorisme" pourrait être le prochain mot à la mode.

Le point de vue russe sur la "guerre psychotronique" Le terme "psycho-terrorisme" a été inventé par l'écrivain russe N. Anisimov, du Centre antipsychotronique de Moscou. Selon Anisimov, les armes psychotroniques sont celles qui agissent pour "retirer une partie de l'information stockée dans le cerveau d'un homme. Elle est envoyée à un ordinateur, qui la retravaille au niveau requis par ceux qui doivent contrôler l'homme, et l'information modifiée est ensuite réinsérée dans le cerveau".

Ces armes sont utilisées contre l'esprit pour provoquer des hallucinations, des maladies, des mutations dans les cellules humaines, la "zombification" ou même la mort. L'arsenal comprend des générateurs VHF, des rayons X, des ultrasons et des ondes radio. Le major de l'armée russe I. Chernishev, écrivant

dans la revue militaire *Orienteer* en février 1997, a affirmé que des armes "psy" étaient en cours de développement dans le monde entier. Les types d'armes spécifiques mentionnés par Chernishev (qui n'ont pas tous des prototypes) sont les suivants :

- Un générateur psychotronique qui produit une puissante émanation électromagnétique capable d'être envoyée à travers les lignes téléphoniques, les réseaux de télévision et de radio, les tuyaux d'alimentation et les lampes à incandescence.
- Un générateur autonome, un appareil qui fonctionne dans la bande 10-150 Hertz et qui, dans la bande 10-20 Hertz, forme une oscillation infrasonique destructrice pour toutes les créatures vivantes.
- Un générateur de système nerveux, conçu pour paralyser le système nerveux central des insectes, qui pourrait s'appliquer de la même manière à l'homme.
- Les émanations d'ultrasons, qu'un institut prétend avoir développées. Les appareils utilisant les émanations d'ultrasons sont censés pouvoir effectuer des opérations internes sans effusion de sang et sans laisser de trace sur la peau. Ils peuvent aussi, selon Tchernishev, être utilisés pour tuer.
- Cassettes silencieuses. Chernishev affirme que les Japonais ont développé la capacité de placer des motifs vocaux à basse fréquence sur la musique, motifs qui sont détectés par le subconscient. Les Russes prétendent utiliser des "bombardements" similaires avec une programmation informatique pour traiter l'alcoolisme ou le tabagisme.
- L'effet 25ème image, auquel il a été fait allusion plus haut, est une technique selon laquelle chaque 25ème image d'une bobine de film ou d'une séquence de film contient un message qui est capté par le subconscient. Cette technique, si elle fonctionne, pourrait éventuellement être utilisée pour lutter contre le tabagisme et l'alcoolisme, mais elle a des applications plus vastes et plus sinistres si elle est utilisée sur un téléspectateur ou un opérateur informatique.
- Les psychotropes, définis comme des préparations médicales utilisées pour induire une transe, une euphorie ou une dépression. Qualifiés de "mines à action lente", ils peuvent être glissés dans la nourriture d'un homme politique ou dans l'approvisionnement en eau d'une ville entière. Les symptômes comprennent des maux de tête, des bruits, des voix ou des ordres dans le cerveau, des vertiges, des douleurs dans les cavités abdominales, des arythmies cardiaques, voire la destruction du système cardiovasculaire.

Des chercheurs américains confirment que ce type d'étude est en cours. Le Dr Janet Morris, coauteur de *The Warrior's Edge*, se serait rendue à l'Institut de psychocorrélation de Moscou en 1991. On lui a montré une technique mise au point par le département russe de psychocorrection de l'Académie de médecine de Moscou, dans laquelle les chercheurs analysent électroniquement l'esprit humain afin de l'influencer. Ils introduisent des messages de commande subliminaux, en utilisant des mots clés transmis dans un "bruit blanc" ou de la musique. Le message acoustique de psychocorrection est transmis par conduction osseuse à l'aide d'une transmission infrasonore à très basse fréquence[13].

- En résumé, Chernishev a noté que certains des aspects militairement significatifs de l'armement "psy" méritent d'être étudiés de plus près, notamment les méthodes non traditionnelles suivantes pour perturber le psychisme d'un individu :
- Recherche ESP : déterminer les propriétés et l'état d'objets sans jamais entrer en contact avec eux et "lire" dans les pensées des gens.
- Recherche sur la clairvoyance : observation d'objets situés juste au-delà du monde visible, utilisée à des fins de renseignement.
- Recherche sur la télépathie : transmission de pensées à distance - utilisée pour des opérations secrètes.
- Recherche sur la télékinésie : actions impliquant la manipulation d'objets physiques par la force de la pensée, les faisant bouger ou se briser - utilisées contre les systèmes de commande et de contrôle, ou pour perturber le fonctionnement des armes de destruction massive.
- Recherche sur la psychokinèse : interférer avec les pensées des individus, que ce soit au niveau stratégique ou tactique.

Alors que de nombreux scientifiques américains remettent sans aucun doute en question ces recherches, elles bénéficient d'un soutien important à Moscou. Ce qu'il faut souligner, c'est que des personnes en Russie (et dans d'autres pays également) pensent que ces moyens peuvent être utilisés pour attaquer ou voler l'unité de traitement des données du corps humain.

Les recherches de Solntsev, mentionnées ci-dessus, diffèrent légèrement de celles de Chernishev. Par exemple, Solntsev s'intéresse davantage aux capacités matérielles, et plus particulièrement à l'étude de la source d'énergie de l'information associée à l'interface ordinateur-opérateur. Il souligne que si ces sources d'énergie peuvent être captées et intégrées dans l'ordinateur moderne, il en résultera un réseau valant plus que "la simple somme de ses composants". D'autres chercheurs étudient les générateurs à haute fréquence (conçus pour assommer le psychisme avec des ondes à haute fréquence telles que les ondes électromagnétiques, acoustiques et gravitationnelles), la manipulation ou la reconstruction de la pensée d'une personne par des mesures planifiées telles que les processus de contrôle réflexif, l'utilisation de la psychotronique, de la parapsychologie, de la bioénergie, des biochamps et de la psychoénergie[14], ainsi que des "opérations spéciales" non spécifiées ou des formations anti-ESP.

Le dernier point est particulièrement intéressant. Selon une émission de la télévision russe, les forces de fusées stratégiques ont commencé à s'entraîner à la lutte contre l'ESP afin de s'assurer qu'aucune force extérieure ne puisse s'emparer des fonctions de commandement et de contrôle de la force. En d'autres termes, elles tentent de construire un pare-feu autour de la tête des opérateurs.

Conclusions

Fin juillet 1997, les planificateurs de la démonstration d'interopérabilité Joint Warrior '97 "se sont concentrés sur les technologies qui améliorent la planification collaborative en temps réel au sein d'une force opérationnelle multinationale du type de celles utilisées en Bosnie et dans le cadre de l'opération Tempête du désert". Le réseau JWID '97, appelé Coalition Wide-Area Network (CWAN), est le premier réseau militaire qui permet aux nations alliées de participer en tant que partenaires égaux et à part entière"[15]. La démonstration était en fait une foire commerciale permettant aux entreprises privées de présenter leurs produits ; les ministères de la défense ont pu décider où et comment dépenser leur argent de manière plus avisée, dans de nombreux cas sans avoir à supporter le coût des prototypes. C'est un bon exemple de la façon de faire des affaires avec moins de moyens. Les technologies présentées comprenaient :[16]

- Les soldats utilisant des ordinateurs portables pour faire glisser des croix sur des cartes afin de déclencher des frappes aériennes.
- Des soldats portant des bipeurs et des téléphones portables plutôt que des armes à feu
- Les généraux suivant les mouvements de chaque unité, comptant le nombre précis d'obus tirés autour du globe et inspectant en temps réel les dégâts infligés à l'ennemi, le tout avec des graphiques multicolores[17].

Tous les comptes rendus de cet exercice ont mis l'accent sur la capacité des systèmes à traiter des données et à fournir des informations en retour grâce à la puissance investie dans leurs microprocesseurs. La capacité d'affecter ou de défendre la capacité de traitement des données des opérateurs humains de ces systèmes n'a jamais été mentionnée au cours de l'exercice ; elle n'a fait l'objet que d'une attention limitée au cours d'innombrables exercices au cours des dernières années. Le moment est venu de se demander pourquoi nous semblons ignorer les opérateurs de nos systèmes. Il est clair que l'opérateur d'information, exposé à une vaste gamme d'armes potentiellement immobilisantes, est le point faible des ressources militaires de toute nation. Il existe peu d'accords internationaux protégeant le soldat individuel, et ceux-ci reposent sur la bonne volonté des combattants. Certaines nations, et les terroristes de tout poil, n'ont que faire de ces accords.

Cet article a utilisé le terme "traitement des données" pour démontrer son importance dans la détermination de ce que sont la guerre de l'information et les opérations d'information. Le traitement des données est l'action que notre pays et d'autres doivent protéger. L'information n'est rien d'autre que le résultat de cette activité. Par conséquent, l'accent mis sur la terminologie de la guerre de l'information ("domination de l'information", "carrousel de l'information") qui a proliféré pendant une décennie ne semble pas correspondre à la situation à laquelle nous sommes confrontés. Dans certains cas, la bataille pour affecter ou protéger les éléments de traitement des données oppose un système mécanique à un autre. Dans d'autres cas, les systèmes mécaniques peuvent être confrontés à l'organisme humain, ou vice versa, puisque les humains peuvent généralement arrêter n'importe quel système mécanique en appuyant sur un interrupteur. En réalité, le jeu consiste à protéger ou à affecter les signaux, les ondes et les impulsions qui peuvent influencer les éléments de traitement des données des systèmes, des ordinateurs ou des personnes. Nous sommes potentiellement les plus grandes victimes de la guerre de l'information, parce que nous avons négligé de nous protéger.

Notre obsession pour un "système de systèmes", la "domination de l'information" et d'autres termes de ce genre est très probablement l'une des principales causes de notre négligence du facteur humain dans nos théories sur la guerre de l'information. Il est temps de changer notre terminologie et notre paradigme conceptuel. Notre terminologie nous embrouille et nous oriente dans des directions qui traitent principalement des composantes matérielles, logicielles et de communication du spectre de traitement des données. Nous devons consacrer plus de temps à la recherche de moyens de protéger les êtres humains dans nos structures de gestion des données. Rien dans ces structures ne peut être maintenu si nos opérateurs ont été affaiblis par des adversaires potentiels ou des terroristes qui - en ce moment même - sont peut-être en train de concevoir les moyens de perturber la composante humaine de notre notion soigneusement construite d'un système de systèmes.

NOTES

1. I. Chernishev, "Les dirigeants peuvent-ils fabriquer des 'zombies' et contrôler le monde ? Orienteer, février 1997, pp. 58-62.
2. Douglas Pasternak, "Wonder Weapons", U.S. News and World Report, 7 juillet 1997, pp. 38-46.
3. Ibid, p. 38.
4. FM 101-5-1, Operational Terms and Graphics, 30 septembre 1997, p. 1-82.
5. Joint Pub 3-13.1, Joint Doctrine for Command and Control Warfare (C2W), 7 février 1996, p. v.
6. The American Heritage Dictionary (2d College Ed. ; Boston : Houghton Mifflin, 1982), p. 660, définition 4.
7. Denis Snezhnyy, "Cybernetic Battlefield & National Security", Nezavisimoye Voennoye Obozreniye, n° 10, 15-21 mars 1997, p. 2.
8. Victor I. Solntsev, "Information War and Some Aspects of a Computer Operator's Defense", exposé présenté lors d'une conférence Infowar à Washington, D.C., septembre 1996, parrainée par la National Computer Security Association. Les informations contenues dans cette section sont basées sur les notes de l'exposé de M. Solntsev.
9. Pasternak, p. 40.
10. Ibid, pp. 40-46.
11. Ibid.
12. Larry Dodgen, "Nonlethal Weapons", U.S. News and World Report, 4 août 1997, p. 5.

13. "Background on the Aviary", Nexus Magazine, téléchargé sur Internet le 13 juillet 1997 à partir de www.execpc.com/vjentpr/nexusavi.html, p.7.

14. Aleksandr Cherkasov, "The Front Where Shots Aren't Fired", Orienteer, mai 1995, p. 45. Selon l'auteur, cet article est basé sur des informations parues dans la presse étrangère et russe, ce qui ne permet pas de déterminer avec précision la source de cette référence.

15. Bob Brewin, "DOD looks for IT `golden nuggets", Federal Computer Week, 28 juillet 1997, p. 31, extrait du Earlybird Supplement, 4 août 1997, p. B 17.

16. Oliver August, "Zap ! Hard day at the office for NATO's laptop warriors", The Times, 28 juillet 1997, tiré du Earlybird Supplement, 4 août 1997, p. B 16.

17. Ibid.

Le lieutenant-colonel Timothy L. Thomas (USA Ret.) est analyste au Foreign Military Studies Office, Fort Leavenworth, Kansas. Il a récemment écrit de nombreux articles sur la vision russe des opérations d'information et sur les questions militaro-politiques russes actuelles. Au cours de sa carrière militaire, il a servi dans la 82e division aéroportée et a été chef du département des affaires politico-militaires soviétiques à l'Institut russe de l'armée américaine à Garmisch, en Allemagne.

Révisé le 25 février 1998. Veuillez envoyer vos commentaires ou corrections à carl_Parameters@conus.army.mil