L'Europe et la Suisse face aux nouvelles menaces. 2e partie

Autor(en): **Weck, Hervé de**

Objekttyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **144 (1999)**

Heft 6-7

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-348706

L'Europe et la Suisse face aux nouvelles menaces (2)

«Lorsque les tensions externes diminuent, nécessairement aussi les tensions internes s'accroissent. Les anciens antagonismes se réveillent, tels d'anciens volcans redevenus actifs.»

Eric Werner,
L'avant-guerre civile

Les médias, dans le monde occidental, qui prennent grand soin d'épargner les nerfs et les humeurs du peuple souverain, recourent à des «esprits fort», des docteurs «Tant-mieux» incurablement optimistes. Les prestations de cette élite «consensuelle» prennent invariablement une forme binaire. D'abord, sous le signe de l'autruche, on nie le problème: la mafia n'existe pas, il n'y a pas d'islamistes en Algérie ou si peu. Il se trouve toujours des prêtres, des pasteurs, des bonnes sœurs, des inconscients pour prendre la défense des associations les plus indéfendables. Banlieues chaudes, insécurité, montée de la délinquance? N'exagérons pas, Paris, Zurich ou Lausanne, ce n'est pas le Bronx...

Col Hervé de Weck

2. Des «cancers» dans les démocraties

Nous avons tendance à localiser les guerres dans des régions lointaines, sous-développées et à croire qu'elles remontent au sous-développement, au décalage historique. En réalité, il y a longtemps que la «guerre civile» a refait son apparition chez nous. Ses «métastases» font partie de la vie quotidienne des grandes villes. A la périphérie des mégapoles d'Occident se trouvent des poches d'instabilité génératrices de bouffées soudaines de violences, sauvages et désorganisées.

Nous vivons une crise de société, voire une crise de civilisation. La délitescence dans les grandes villes, le vandalisme, l'état de non-droit, la faillite de l'école publique qui ne sait plus à quoi elle doit servir, qui n'arrive plus à atteindre des objectifs simples et quantifiables (que les jeunes qui en sortent sachant lire, écrire et compter). Des bandes de jeunes, qui sèment la terreur, comptent une forte proportion d'Européens. Ce n'est donc pas l'entité ethnique qui les réunit, mais un habitat dans un quartier, la misère et le désœuvrement. Le même constat vaut pour les chômeurs en révolte.

Tout cela fait comprendre que la menace est là, que l'influence de groupuscules extrémistes suffirait pour que cette «épidémie d'incivisme» prenne une dimension politique. Toutes les manipulations sont en effet possibles. Parmi les chômeurs occupant illégalement des locaux s'infiltrent des éléments révolutionnaires, encore très minoritaires, mais qui s'efforcent de dépasser le stades des revendications sectorielles par des visées insurrectionnelles.

Un renouveau de mouvements terroristes du type «Action directe» ou des «Brigades rouges» est possible. Ils trouveraient dans ces zones de non-droit des abris, des bases et des troupes à encadrer.

La guérilla urbaine, latente dans les banlieues défavorisées, peut se répandre hors de celles-ci et se transformer en guerre civile. La nécessité de recourir aux forces armées n'est donc pas à exclure. Les moyens de juguler une émeute, presque une insurrection doivent exister. Il faut prendre en

Les menaces criminelles contemporaines

Criminalité mafieuse (groupes transnationaux à finalité criminelle),

Trafics de stupéfiants (production, flux, réseaux, incidences financières),

Trafics d'armes, d'œuvres d'art, de médicaments, d'organes, d'êtres humains (flux d'émigration clandestine, prostitution entre autres enfantine),

Blanchiment d'argent (capitaux «innocentés» servant à pénétrer et à déstabiliser l'économie légale),

Fanatismes religieux et sectes,

Formes multiples de terrorismes, dont l'éco-terrorisme (forme de violence fondée sur la défense d'une vision de l'environnement) et le bio-terrorisme (utilisation d'agents biologiques à des fins hégémoniques ou simplement criminelles),

Guérillas dénaturées,

Violences urbaines et «jungles de béton» (périmètres «interdits» aux forces de l'ordre, économies parallèles, micro-cultures violentes fondées sur toutes sortes de trafics),

«Infocrime» (formes de criminalité fondées sur la vulnérabilité des systèmes informatiques et des transports de l'information).

compte des scénarios où les forces de l'ordre classiques se trouveraient dans l'incapacité de faire face à la situation[1]. Il est difficile de «reconquérir» une zone urbaine sans destructions et atteintes à des personnes innocentes. Se poserait alors le problème de la couverture médiatique des opérations.

Crime organisé, cartels et mafias

Une étude du Fonds monétaire international, portant sur la période 1975-1991 montre que l'économie criminelle pakistanaise dépasse en valeur absolue l'économie légale du pays et croît plus vite qu'elle!

Répression de la violence urbaine made in USA

Dans l'Amérique des années 1980, mise au point de lois répressives, augmentation des effectifs de la police et construction de multiples prisons ont été menées avec détermination. New-York symbolise ce choix de société. En 1994, le vote d'une loi anti-criminalité par le Congrès a considérablement développé la répression à l'endroit des petits méfaits, amené une baisse de 60% des homicides en 1997 par rapport à 1993. En mars 1998, pour la première fois, aucun crime n'a été commis à Brooklyn pendant une semaine!

En 1996, il s'est vendu aux Etats-Unis, au prix du deal de rue, pour 45 milliards de francs suisses de cocaïne et environ 22 milliards d'héroïne, ceci pour donner une idée de ce que pèsent financièrement les activités illicites à l'échelle planétaire!

Les bénéfices du narco-trafic s'élèveraient à plus de 700 milliards de dollars, plus que la vente de voitures dans le monde. Avec de tels moyens, mafias et cartels de tous genres peuvent se payer de véritables armées privées. Selon des sources de l'ONU en 1995, les organisations criminelles transnationales brasseraient, seulement dans le narco-trafic, entre 45 et 75 milliards de francs suisses par année, dont la moitié serait recyclée dans l'économie mondiale. Une fusion serait actuellement en train de

> «Dans le désordre mondial d'aujourd'hui, il vaut toujours mieux savoir qui vraiment pose les bombes et massacre; pour le narco-trafic savoir qui, vraiment, vend l'héroïne et la cocaïne par tonnes.»
>
> *Dictionnaire des nouvelles menaces*

s'opérer entre le trafic illicite des stupéfiants, des armes et des immigrants clandestins...

Il ne faut pas confondre les mafias quasiment indestructibles[2] et les cartels, plus fra-

[1] *Paris, Henri: «La menace terroriste et insurrectionnelle»,* Défense nationale, *avril 1998, pp. 51-53.*

[2] *Contrairement à ce qu'on prétend souvent, aucune mafia n'a jamais été détruite à ce jour, malgré les moyens engagés.*

Sur le lieu d'un attentat...

giles, que l'on trouve en Colombie ou au Mexique, qui manquent de longévité et de «traditions». Plus que dans une entreprise classique, le passage à une seconde génération de dirigeants s'avère critique dans le monde des cartels. En une vingtaine d'années, certains sont pourtant devenus de véritables multinationales qui contrôlent chaque stade du narco-trafic. Ces formidables machines à générer du profit constituent de véritables empires qui disposent de moyens financiers, de systèmes de transport, de renseignements et de télécommunications bien plus importants et sophistiqués que ceux de nombreux Etats-nations.

Le crime organisé manifeste une foudroyante capacité d'adaptation. Les organigrammes, très hiérarchisés, à la fin des années 1970, le rendait très visible. Les organisations mafieuses se sont transformées en petites et moyennes entreprises criminelles noyées dans le paysage, fonctionnant en réseaux, donc beaucoup plus difficiles à détecter et à détruire. Place à la toile d'araignée! La chute du Mur de Berlin aidant, les grandes sociétés criminelles entreprennent de conquérir de nouveaux marchés.

Des secteurs entiers de la Birmanie, de la Chine, de la Colombie, du Mexique, du Pérou, du Surinam, de la Turquie et de l'Ukraine se trouvent de facto sous le contrôle du crime organisé. Les «mauvais prêts» des banques japonaises s'élèveraient à 1500 milliards de francs suisses, une part significative de ceux-ci relevant de l'extorsion criminelle des Yakuzas (la mafia japonaise). Depuis sa création en 1992 sur les ruines de l'armée soviétique, l'armée russe connaît une importante corruption et on y constate la multiplication de joint-ventures avec le crime organisé, la constitution de véritables agences de tueurs à gage réalisant sur commande des «contrats» pour le milieu, l'implication dans le narco-trafic. Des véhicules ou des avions militaires assurent des transports d'héroïne du Croissant d'or vers l'Europe, Prague, Budapest et Bucarest jouant le rôle de plaques tournantes du crime organisé.

Quand le crime organisé international dispose des moyens de déstabiliser des régions, voire de menacer l'existence de certains Etats, l'affaire ne relève plus du maintien de l'ordre,

Corruption et narco-trafic
(quelques chiffres en francs suisses)

Salaire annuel du chef de la police des stupéfiants (GB)	255000
Salaire annuel d'un fonctionnaire de la Drug Enforcement Administration (USA)	38000 -145000
Salaire annuel d'un douanier (GB)	30000 - 55000
Gain annuel du propriétaire d'un petit laboratoire d'extasy à Amsterdam	400000
Gain de policiers britanniques ayant fermé les yeux sur une livraison de Cannabis de 5 millions de francs (selon le grade)	410000 - 620000
Salaire pour la livraison de 1 tonne de cannabis de Rotterdam à Londres	150000

mais de la sécurité nationale et internationale. Dans la répression du narco-trafic, une voie n'a jamais été suivie sérieusement: la constitution d'une coalition d'Etats de droit, fermement décidés à démanteler les huit ou dix grandes organisations criminelles transnationales qui sont les indispensables pivots du narco-trafic mondial, qui relient les laboratoires perdus dans les zones grises de la planète aux dealers des banlieues chaudes des métropoles occidentales.

L'immigration clandestine

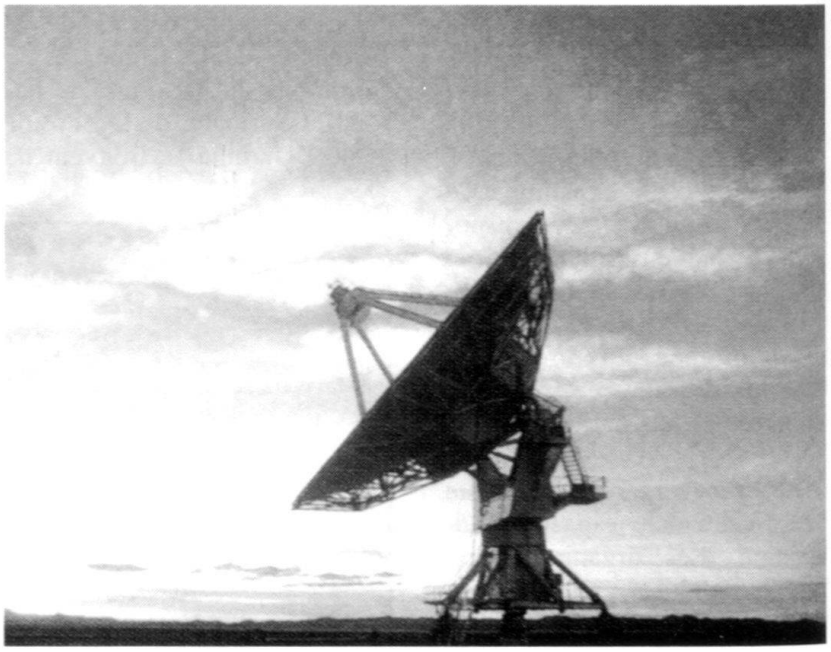
Les immigrants clandestins qui arrivent en Suisse passent surtout par la frontière «verte» au Tessin et à Genève. Beaucoup trouvent immédiatement refuge et hébergement chez des parents déjà établis dans le pays, ce qui confirme la thèse selon laquelle l'immigration engendre l'immigration. D'autre part, il faut admettre, quoi qu'en disent les «gentils», que l'attractivité de notre pays est trop élevée.

L'immigration clandestine, associée à la prostitution et au narco-trafic, prend une dimension mafieuse sous l'impulsion de poids lourds du crime organisé, qui y trouvent d'immenses sources de profit, grâce à des réseaux très structurés. Les associations, qui s'opposent aux extraditions ou aux renvois et qui mènent des actions «charitables» et «humanitaires», ne cherchent pas toujours à séparer le bon grain des cas méritoires de l'ivraie des éléments criminels. Pour les mafieux, la situation est idéale: ils peuvent faire pénétrer aisément les clandestins, trouver des relais sur place pour les accueillir et se ménager des soutiens pour s'opposer à l'expulsion de leurs «clients». Il faut également convenir qu'une partie des immigrants officiellement recensés éprouvent des difficultés à s'adapter au cadre de vie du pays-hôte. Selon un sondage de janvier 1998, 34% des musulmans de France se sentent «musulmans» plus que Français[3].

Comme l'affaire des fonds en déshérence et les actions du Congrès juif mondial, qui ont fait monter l'antisémitisme en Suisse, l'immigration non gérée risque de générer dans la population de notre pays des sentiments de xénophobie et de racisme qui pourraient devenir incontrôlables. «Pour donner le change, les gouvernements européens évoquent les bienfaits de la société multiculturelle, mais sans prendre en compte le fait que la guerre civile est malheureusement le lot de la plupart des Etats pluri-ethniques et/ou multiconfessionnels (...)[4].»

3. Le «Cyberspace Warfare»

Le *cyberterrorisme*, le *cyberspace warfare*, c'est la possibilité d'attaquer et de neutraliser à distance le potentiel stratégique civil et militaire d'un Etat, à partir de l'enchevêtrement des multiples réseaux et sous-réseaux d'Internet: le *cyberespace* se superpose en effet aux espaces marins et sous-marins, terrestres, aé-



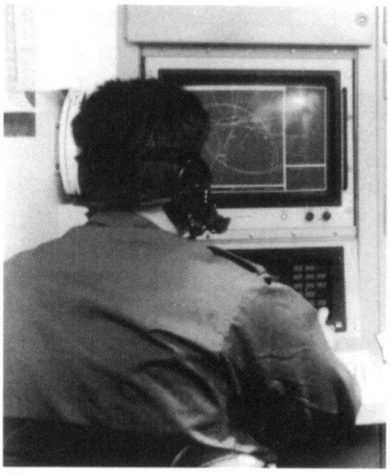
Cette antenne, arme ou cible du «Cyberspace Warfare»?

[3] *Eric Werner, op. cit., p. 51.*
[4] *Ibidem, p. 50.*

riens et extra-atmosphériques. En clair, il s'agit de l'attaque préméditée des ordinateurs cruciaux d'un Etat, en vue de les saboter, de les piller, d'en prendre le contrôle ou de les détruire. La crainte d'un cataclysme informatique ne s'avère pas toujours innocente. Parmi ceux qui clament le plus fort leur angoisse, les marchands de sécurité informatique…

Internet, le «réseau des réseaux», qui devait à l'origine satisfaire des besoins militaires en matière de recherche scientifique, se trouve au centre d'un débat stratégique aux Etats-Unis, connu sous le nom de *Revolution in Military Affairs*. On voit maintenant dans cet espace à géométrie variable une nouvelle source de menace, puisque des lacunes importantes existent en matière de sécurité des réseaux informatiques, tant civils que militaires. Les réseaux informatiques, utilisés pour les communications militaires, peuvent être «mis à genou» par un simple «ver», c'est-à-dire un programme destiné à l'endommager, le paralyser ou le rendre inutilisable.

Moyennant de très faibles coûts d'acquisition, des Etats, peu ou faiblement industrialisés, qui ne disposent pas de capacité nucléaire ou balistique, des cartels de narco-trafiquants, des groupes de fanatiques religieux ou politiques, de simples pirates informatiques (les fameux *hackers*) ont



Et la sécurité des réseaux informatiques?

la possibilité de passer à l'offensive[5].

En 1995, le nombre d'utilisateurs d'Internet se situait aux environs de 75 millions! Déjà des dizaines de milliers de serveurs informatiques, partout, dans le monde, ont été les victimes de pirates informatiques. Aux Etats-Unis, la plupart de ces tentatives visaient les administrations fédérales. Il s'avère que la probabilité de réussite est de 50%, la probabilité de capture après intrusion s'élevant à 80%.

Un *hacker*, membre du *Chaos Computer Club*, a piraté des sites américains pour le compte du KGB; il lui fournissait des programmes, des listes de mots de passe, agissant, non par idéologie mais pour gagner de quoi s'offrir de la drogue! Deux sociétés françaises, SGS-Thomson et Philips-France, qui travaillaient sur des programmes de cerveaux électroniques pour l'OTAN, ont subi des attaques informatiques du KGB. Outre le pillage des plans de fabrication, un grand nombre d'informations contenues dans les serveurs des deux entreprises ont été corrompues, générant un préjudice financier estimé à plus de 500 millions de francs suisses. Depuis 1997, les Tigres de l'Eelam Tamil effectuent une opération de *cyberterrorisme* appelée «Suicide Email Bombing».

Trois types d'attaques dans le «cyberspace»

Attaque physique qui consiste à endommager les équipement de manière classique (bombe, incendie).

Attaque syntaxique qui consiste à modifier la logique du système afin d'y introduire des délais ou d'en rendre le comportement imprévisible; une attaque au moyen de virus ou de «chevaux de Troie» entre dans cette catégorie.

Attaque sémantique, la plus perfide, qui exploite la confiance qu'ont les utilisateurs dans leur système; il s'agit de modifier les informations entrant dans le système ou en sortant, à l'insu des utilisateurs afin de les induire en erreur.

[5] *Ce chapitre reprend en les vulgarisant les idées essentielles du mémoire d'Alexis Bautzmann,* Le concept de «Cyberspace Warfare». *D.E.A. Histoire militaire, défense sécurité. Mémoire préparé sous la direction d'André Martel. Manuscrit. Année scolaire 1996-1997. 171 pp. Voir également Wautelet, Michel:* Les Cyberconflits. Internet, autoroute de l'information et Cyberespace: quelles menaces? *Editions Complexes/GRIP, 1998.*

Divers laboratoires de défense ont créé des «canons à fréquence radio de haute intensité», capables de «tuer» à distance les puces au sein même des ordinateurs. On imagine une telle arme entre les mains d'une secte apocalyptique ou d'un groupe terroriste.

Un scénario étudié par les Américains

Sous l'égide de la Defence Advanced Research Projets Agency, un exercice de simulation «The Day after in Cyberspace II» se joue en mars 1996 aux Etats-Unis. Au printemps 2000, les responsables américains s'inquiètent de la situation dans «l'arc de crise islamiste» (le golfe Persique, le Pakistan, les Etats musulmans issus de l'Union soviétique, l'Afrique du Nord) où des prédateurs ont développé la capacité de mener des opérations stratégiques contre «l'infrastructure globale d'information». Pour la grande majorité des télécommunications, on utilise aux Etats-Unis un réseau PSN, créé par les opérateurs privés du câble, des téléphones portables et des satellites. Pour prévenir les attaques de virus informatiques, une infrastructure minimale a été mise en place. L'interdépendance n'en reste pas moins croissante entre le PSN, le réseau électrique, les bases de données qui régissent le trafic aérien, le GPS et de nombreuses infrastructures-clés.

Dans le golfe Persique, un mouvement transnational, appelé «Campagne pour un renouveau islamiste et démocratique», exploite toute une gamme de technologies sophistiquées d'information et de communication; il dispose d'importants relais au sein de la communauté musulmane aux Etats-Unis.

L'Iran, devenu la principale puissance du Moyen-Orient, pratique une stratégie visant à regrouper les fondamentalistes de la région. Son intérêt pour la guerre électronique est devenu évident. L'Iran, avec la Syrie, est suspecté d'avoir participé au «vol électronique» d'environ un milliard de dollars à la Banque d'Arabie saoudite... Un virus polymorphe mortel a été introduit dans les logiciels de contrôle de la dernière variante de l'*Airbus A-330*. Des virus sont détectés dans le système de transfert de fonds de la Banque d'Angleterre. Les systèmes électroniques de commandement et de contrôle de l'armée israélienne sont la cible d'une série d'attaques d'une nouvelle génération de «renifleurs» et de «bombes logiques» d'origine inconnue.

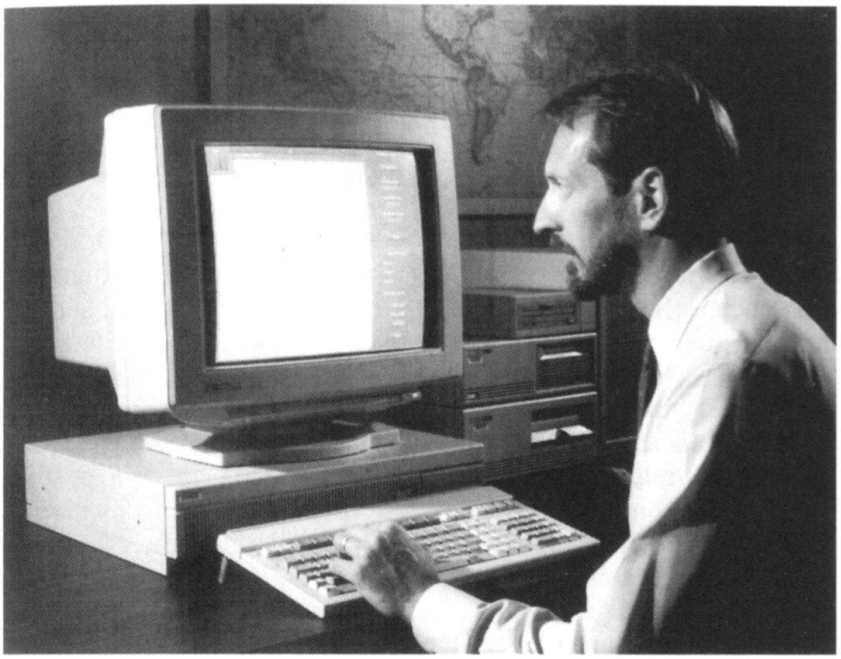
Aux Etats-Unis, les réseaux PSN de l'Oregon et de la Californie du Nord, le système téléphonique de Fort Lewis à Washington sont soumis à d'intenses attaques via Internet. Les guichets automatiques des deux plus grandes banques d'Atlanta tombent en panne. Il en va de même des émetteurs de CNN. Le nouveau métro à grande vitesse du Maryland percute à 300 km/h un autre train apparemment détourné

> Les technologies sophistiquées d'information et de communication (Internet et des codes «incassables») donnent à n'importe qui, dans un sanctuaire intouchable, l'équivalent gratuit et mondial d'un Centre de commandement et de contrôle, qui était jusqu'à la guerre du Golfe, l'apanage des armées «hi-tech».

Exploration et guerre dans le «cyberspace»

Tout écran d'ordinateur émet des radiations Van Eck. Malgré les normes civiles les plus strictes, il est possible, avec un équipement adéquat, de reconstituer à distance le contenu de l'écran. Cette technique a été employée par le FBI pour la surveillance de Alrich Ames, un agent du KGB infiltré à la CIA. Le Pentagone utilise plusieurs satellites de surveillance militaire afin de détecter, via l'espace extra-atmosphérique et de manière absolument indétectable, le rayonnement Van Eck émis par les moniteurs informatiques. A condition de connaître précisément l'endroit où se trouve un groupe de *hackers*, il est possible d'intercepter toute action contre l'infrastructure d'information des Etats-Unis.

Une bombe *EMP-T* (*Electro-Magnetic Pulse Transformer*), de faible coût, est capable de neutraliser durablement tout système informatique à une distance allant de 200 mètres pour les plus faibles à plus d'un kilomètre pour les plus puissantes.



« L'ennemi » peut-il lire le contenu de cet écran ?

sur une mauvaise voie, à la suite d'un intrusion dans le système de contrôle du réseau ferroviaire de la côte Est. Bilan : 60 morts et 120 blessés.

Les services secrets occidentaux en arrivent à la conclusion que l'Iran, employant des experts étrangers, est à même de menacer les communications, l'économie et les transports des Etats-Unis et de l'Europe de l'Ouest. Entre-temps, Téhéran a mobilisé d'importantes forces terrestres et aériennes. Le gouvernement américain décide de mesures de précaution et de mobilisation qui prennent du retard à la suite d'attaques locales contre les réseaux téléphoniques de plusieurs bases-clés.

Alors que le réseau téléphonique de Washington/Baltimore tombe en panne, que la bourse vit des fluctuations sauvages dues, semble-t-il, à une manipulation électronique, on s'achemine vers une deuxième édition de la guerre du Golfe contre l'Iran…

Le président Clinton et la « *Cyberwarfare* »

Lors de sa présentation du budget 2000, le président Clinton annonce que les menaces non conventionnelles vont faire l'objet d'une attention particulière. Il est prévu de répartir 2,8 milliards de dollars au profit de la lutte contre les menaces NBC sur le territoire américain et contre le terrorisme « cybertechnique ».

TTU Europe, 11 février 1999.

Ce scénario qui, à bien des égards, reste simpliste, illustre pourtant de manière didactique les dangers qui menacent les réseaux informatiques mondiaux. Seuls les Etats-Unis semblent pour l'heure y prêter attention. Est-ce bien raisonnable de la part d'Etats, même petits comme la Suisse, de négliger de telles hypothèses ?

H. W.