Centre de Recherche sur les Menaces Criminelles Contemporaines
(Université Panthéon-Assas (Paris II)

Conférence des Mardis du MCC

Mardi 18 janvier 2000

# Crimes, violence et terreur dans la société de l'information

*Le visible et le réel, médias et communication,*

*réalité et manipulation*

*François-Bernard* HUYGHE

Résumé :

*De l'affrontement militaire ou géopolitique à l'économie dite d'infoguerre, de la délinquance à la vie privée, on se bat avec ou contre des bits informatiques, avec des électrons comme avec des mots et des images. Sous toutes ses dimensions de bien immatériel, mémorisable, inscriptible et reproductible, l'information inflige un dommage ou procure un avantage contre le gré de l'autre. Les hommes ont toujours lutté en s'espionnant, en se mentant, en propageant des croyances, en dissimulant ou falsifiant des réalités. Désormais, la conjonction entre les possibilités technologiques, les stratégies inédites de l'information et des pratiques culturelles émergentes donne une autre dimension à ces phénomènes la sphère politique, économique et celle de la vie privée.*

*" Crime, violence et terreur dans la société de l'information "*

Demander quelles formes de violence caractérisent les sociétés dites de l'information, c'est traiter des rapports entre des réalités techniques (telle l'informatique et les réseaux), des réalités stratégiques (l'action organisée de groupes en lutte) et des réalités symboliques (des idées, croyances et affects, l'environnement mental dans lequel se déroulent ces conflits). Il faut cartographier un nouveau champ de conflit : il est déterminé par les possibilités offensives que portent les technologies, par les méthodes d'agression ou de domination auxquelles recourent les acteurs et, enfin, par des représentations mentales au nom desquelles ils sont prêts à s'affronter. Notre perspective ne sera ni celle de l'angélisme technologique (exalter le monde merveilleux que produira la révolution de la communication), ni celle de la déploration (dénoncer l'aliénation de l'homme victime du système technique). Il s'agit d'étudier froidement quelques indices : ils indiquent qu'une expérience immémoriale du conflit comme mouvement, exploitation et destruction de forces doit être révisée. Il faut comprendre le rôle inédit qu'y jouent maintenant des images, des mots, des ondes et des électrons.

Des formes spécifiques de violence apparaissent donc dans l'environnement géopolitique, culturel, économique d'une supposée " révolution de l'information ". Les pratiques hostiles par lesquelles des groupes infligent un préjudice ou gagnent une suprématie mobilisent de nouveaux outils et supposent de nouveaux discours. L'agression se pratique par contrôle, modification ou destruction des savoirs, croyances, et moyens d'information d'un adversaire qui ne sait parfois même pas qu'il est une victime. L'usage de termes aussi forts que " violence " ou " terreur " rappelle que de tels conflits, où l'information intervient comme arme, comme enjeu et comme mesure, supposent une rivalité exaspérée (et non une simple concurrence), une intentionnalité agressive, et des enjeux graves. Celui-ci se mesure souvent à l'illégalité, parfois au caractère quasi guerrier de ces opérations, toujours aux dommages qui en résultent, en termes de perte de richesses, de sécurité ou d'autonomie.

Faute de pouvoir traiter exhaustivement de ce phénomène, on se contentera d'en proposer une définition générale, puis d'en traiter deux aspects : la désinformation et le secret.

**I Information et violence du conflit**

La formule " société de l'information ", assez largement acceptée, en dépit ou grâce à son flou, apparaît au tout début des années 80. Elle exprime l'espérance d'une société postindustrielle globale, pacifiée, vouée à la transparence démocratique, aux technologies de l'intelligence et au partage des savoirs. Même débarrassée de ses connotations utopiques (idéologiques et trompeuses, disent ses adversaires qui y voient la justification des réalités impitoyables de la mondialisation), cette terminologie définit implicitement l'information comme **facteur dominant**, voire pour les plus déterministes comme un **facteur explicatif** unique.

Le génitif de société "de" l'information permet plusieurs interprétations :

- Société dans laquelle une part croissante de la **valeur** économique résulte de la production, de la distribution et de la demande de données, images ou symboles, une part non moins importante du travail consistant à manier des **signes** et non des **choses**. L'invention d'informations, innovations techniques plus efficaces, images et spectacles plus séduisants, discours plus convaincants est jugée hautement désirable. C'est ce qu'impliquent des notions comme nouvelle économie, ou économie de l'immatériel.

- Société où les **machines et dispositifs informationnels** se multiplient, et où chacun est confronté sans cesse à un **nombre de messages** (signaux et instructions nouvelles, connaissances à assimiler, loisirs, communications interpersonnelles, etc.) sans commune mesure avec ce qu'ont connu les générations précédentes et où par conséquent la masse totale des **connaissances** factuelles, théoriques, ludiques disponibles est immense. On pense alors à la société des réseaux, à la " cyberculture ", à l'intelligence collective...

- Société dont le destin serait lié au développement téléologique d'une sorte de **principe historique** du nom d'information, par contraste avec les sociétés agraires ou industrielles dominées, par le principe de la possession, de l'exploitation et de la transformation de richesses et d'énergies matérielles. La communication représenterait à la fois une **force motrice** et une **valeur** à réaliser, tendant vers une véritable communion

entre les hommes. Cet arrière-plan se retrouve dans le discours optimiste sur les sociétés " de troisième vague " ou l'âge de l'information.

Que l'on mette l'accent sur l'aspect technico-économique, sur les pratiques sociales ou sur quelque douteux sens de l'histoire, on accepte implicitement deux idées :

1) Que les fameuses nouvelles technologies de l'information, nées de la convergence de l'informatique, des télécommunications, de l'audiovisuel et du multimédia, engendrent de nouveaux rapports de savoir, d'avoir et de pouvoir

2) Que l'essence de ces technologies est de traiter l'information, de la numériser, de la transporter, de la stocker, de la diffuser, d'une manière jusque-là inédite.

Soit que le mot " information " a plusieurs acceptions. Le mot a trois sens usuels principaux que rendent assez bien les mots anglais *data, knowledge* et *news* :

Des **données**, traces matérielles telles des écritures ou archives qui sont quelque part, comme dans " vous trouverez l'information sous telle référence... ",

Des **connaissances** ou **croyances** intégrées par des individus ou des groupes, comme dans " être informé que... ",

Et enfin des **messages** circulant, décrivant généralement des événements. L'exemple le plus évident est constitué par les informations ou nouvelles dont traitent les médias, comme dans " les informations de la T.V. disent que... ".

Il s'agit de trois formes de la même réalité, de trois dimensions de l'information : les données sont des messages potentiels, les messages ne sont jamais que des données transportées par des vecteurs, les informations-connaissances s'acquièrent par messages,...

À ces trois catégories s'ajoutent maintenant des informations-programmes, celles des algorithmes informatiques, celles qui dirigent des machines. Elles se présentent comme des actions virtuelles, même si " techniquement ", ce ne sont que des données d'un genre particulier dans listes d'instructions.

On insiste généralement sur les caractères positifs de l'information - le fait qu'elle est immatérielle, innovante. C'est négliger que la communication est aussi un moyen de modifier les choses et les gens, et l'information la source d'un pouvoir, donc que sa détention est la cause de conflits. L'information n'est pas seulement ce qui se partage mais aussi ce qui se propage.

La technologie - ou plutôt les Nouvelles Technologies de l'Information et de la Communication - autorisent d'autres formes de lutte et d'agression. Dans cette perspective, les informations sont soit désirables (des bases de données, des images satellite, des codes d'accès, de la monnaie électronique, des messages cryptés...), soit vulnérables (des logiciels, des mémoires, des sites, des réseaux...) soit redoutables (des virus informatiques, mais aussi des " rumeurs électroniques "). Parallèlement, la disponibilité instantanée des mémoires interconnectées ou la facilité d'accès à Internet font du secret et de son viol des enjeux cruciaux. La bataille, puisque bataille il y a, se déroule selon d'autres rapports de temps (toute information est à la fois pérenne, conservée dans d'inépuisables mémoires et instantanée immédiate dans sa production et sa circulation) et d'autres rapports d'espace (le territoire physique, la frontière ou la distance sont des notions obsolètes dans le cyberspace). Des stratégies adaptées à ces moyens se développent.

Pendant que circulent ces armes invisibles que sont les électrons, les médias plus anciens, à commencer par la télévision, ont plus que jamais un pouvoir moral qui sanctifie et censure des causes, fait et défait des images. Là, le conflit porte sur ce qui est visible et ce qui ne l'est pas, ce qui nous touche et ce que nous ignorons, il dépend de qui contrôle le flux des informations, plus que leur nature particulière. Bref, on ne peut pas penser le monde des nouvelles technologies séparé de celui des " vieux " mass media.

Pour prendre deux exemples récents, on a vu avec quels moyens dérisoires une poignée de " hackers " a pu s'attaquer aux pionniers de la nouvelle économie et à paralyser, fut-ce très provisoirement, des mastodontes comme Yahoo. Avec le rapport du Parlement Européen sur Echelon, on a constaté que le politique est désarmé face aux moyens de surveillance planétaires par satellite. Mais on ne comprend la portée de ces événements que par rapport à leur traitement médiatique et aux mythologies (le cyberterrorisme, Big Brother qu'ils évoquent et réactivent)Ce ne sont que les symptômes d'un phénomène plus vaste dont tente de rendre compte une phraséologie récente.

Le vocabulaire **judiciaire** reflète l'émergence de ces formes d'atteinte à la sécurité, inconnues hier : criminalité informatique, vol de données, cyberterrorisme. Il s'agit de faire rentrer dans les catégories existantes ces atteintes à la propriété intellectuelle, à l'intimité, aux bases de données, et autres usages dommageables ou appropriations indues de l'information.

Ainsi, par Internet on peut, non seulement, voler ou altérer des données et des systèmes de traitement mais aussi emprunter une identité ou une autorisation et procéder à des opérations illicites, à distance et anonymement. Voler, altérer, pénétrer. Une terminologie technique énumère les panoplies de ces nouvelles batailles : *chips*, chevaux de Troie, virus, attaques logiques, etc.

Parallèlement, le monde **militaire** crée ses néologismes, Ram (Révolution des Affaires Militaires), cyberguerre, guerre électronique, etc. pour sa part, le vocabulaire anglo-saxon remplirait des volumes. Il parle de *global information warfare*, de *third wawe war*, d'*infodominance,* etc. Ces mots nouveaux renvoient à trois ordres de phénomènes et à leur traduction doctrinale dans la pensée stratégique :

1) Le rôle croissant des technologies d'observation, de calcul, de direction des armes intelligentes dans la guerre, bref tout ce que ces moyens peuvent ajouter aux forces destructrices. Sous sa forme ultime et peut-être purement fantasmique, le conflit serait géré à distance depuis une *chambre de guerre* à Washington ; les missiles frapperaient chirurgicalement un ennemi aveugle et impuissant, dépourvu de moyens de communication ou de riposte. Il subirait plutôt un châtiment tombé du ciel qu'il ne livrerait bataille. L'information est ici au service des armes.

2) Les actions qui visent à détruire ou prendre le contrôle de la structure de communication adverse : le priver de moyens d'expression, créer le chaos en altérant son infrastructure de communication et de transport, l'amputer de sa mémoire et de son intelligence par le sabotage informatique, etc. L'information est l'arme.

3) Les rapports géostratégiques de contrôle des flux d'information et de leurs vecteurs. Ces rapports de force naissent dès le temps de paix des différents niveaux technologiques ou moyens d'influence sur l'opinion. L'information est le pouvoir.

Le monde de l'**économie** est affecté par l'infoguerre, la désinformation, la " concurrence hypercompétitive ". L'économie dite de l'immatériel augmente la valeur de l'information, celle de son monopole ou de son antériorité, mais accroît aussi l'âpreté de la rivalité. On passe de la **concurrence** comme recherche de l'avantage au **conflit** comme poursuite agressive de l'hégémonie. La globalisation offre un champ d'action à des acteurs menant une stratégie planétaire. Les moyens qu'ils emploient sont nommés guerre de l'information économique, mais on pourrait dire plus crûment : vol de secrets, sabotage et dénigrement des rivaux auprès de

l'opinion publique, des médias et des autorités. Symétriquement, un fantasme se répand : le **chaos**, l'énorme machine paralysée par une attaque indécelable en son point de fragilité, par des virus, par l'action d'une poignée d'informaticiens terroristes. Là encore le concept très flou de " guerre de l'information " recouvre différents domaines et il faut distinguer :

1) L'**acquisition** d'information " ouverte " ou non, par des procédés qui vont de la " veille " à des procédés clandestins dignes de romans d'espionnage. Il s'agit alors d'acquérir une meilleure connaissance que le concurrent, de s'approprier des innovations techniques ou des données, voire de connaître sa stratégie et ses intentions, bref d'acquérir une supériorité en termes de savoir permettant une action plus efficace.

2) Les actions visant à causer un **dommage** direct ou indirect, sur ou par de l'information. Ceci inclut diverses formes d'altérations des connaissances adverses, dans tous les sens du terme, de l'intoxication à l'attaque contre des bases de données. S'y ajoutent le dénigrement de la victime, par faux bruits, campagnes de presse, rumeurs, atteintes à l'image, etc. ces pratiques semblent se multiplier. Leur but est d'affaiblir le concurrent plus que de le surpasser.

3) **L'hégémonie**, l'avantage structurel par le contrôle d'une norme technique ou culturelle, tel un standard en situation monopolistique, ou l'influence d'une langue et de modèles de consommation.

Enfin, cette conflictualité intervient dans la sphère de la **vie privée** sur un triple front :

Celui des délits astucieux perpétrés par vol, falsification de données, emprunt d'identité, etc. dont les particuliers sont autant menacés que les entreprises

Celui des divers procédés d'identification et **profilage** du consommateur et citoyen, souvent à son insu. La confrontation de multiples informations, dans un dessein de surveillance, ou dans un but dit commercial (connaître goûts et besoin) confère un pouvoir inédit à qui gère les flux d'information.

Celui des " cybermilitants ", protestataires ou activistes, alors qu'apparaissent des regroupements nouveaux, des " tribus virtuelles " qui **militent** pour le droit au code secret, **contre les institutions** suspectes de nous surveiller ou de nous manipuler. Des enjeux comme la protection de l'anonymat ou la liberté de la cryptologie deviennent des thèmes militants.

Corollairement, l'action ludique ou délictueuse ou idéologique de *hackers* reflète à la fois la fascination de la technologie et des tendances libertaires toujours hostiles aux institutions, aux moyens de diffusion dits officiels. Ils sont réceptifs aux mythologies du complot ou de Big Brother... Faits techniques et faits culturels se conjuguent pour susciter de nouvelles formes d'affrontement entre groupes et individus, mais aussi entre ces groupes et les institutions politiques voire entre citoyens et entreprises.

Il serait simpliste d'imaginer que le conflit informationnel se déroule à trois niveaux séparés : géostratégique, économique et privé. Les trois se mêlent (par exemple lorsque Bill Clinton met ostensiblement au service des entreprises américaines les moyens d'espionnage hérités de la guerre froide, ou lorsque des groupes de citoyens militants montent sur Internet des actions de pression, agression ou dénonciation contre des entreprises transnationales). On pourrait tout aussi bien soutenir que le conflit informationnel **remet en cause les anciennes définitions des sphères politiques, économiques, privées**. Les notions traditionnelles d'État comme instance exerçant une autorité sur un territoire ou détentrice du monopole de la violence légitime est passablement malmenée. La guerre change : les militaires se soucient de satellites d'observation, d'ordinateurs à saboter ou de systèmes à protéger mais aussi d'images télévisées et de gestion de l'opinion. Le monde économique recourt à des procédés assimilables à l'espionnage, à la désinformation, au sabotage, etc. tous les coups sont bons, intoxication, manipulation, falsification au service des géostratégies mondiales : bref la concurrence se militarise. Quant à la sphère privée, elle ne se résume plus au seul domaine des libertés publiques (par exemple au degré d'intimité et d'indépendance que l'État garantit à chacun). Le privé dépend des rapports des citoyens avec des instruments techniques, alors que, suivant les mots de Deleuze, les sociétés disciplinaires deviennent des **sociétés de contrôle**.

Ceci se traduit dans la controverse récurrente qui oppose technophiles et technophobes, partisans et dénonciateurs des nouvelles technologies. Les réseaux informatiques opèrent une véritable **déterritorialisation**, abolissent des frontières et mettent chacun en contact avec chacun. Cela veut dire, répondent les accusateurs, que pirates, espions, saboteurs, voleurs de données, désinformateurs, propagateurs des pires ignominies, peuvent agir de tout point de la planète, attaquer des banques de données, répandre de fausses nouvelles. Les réseaux se jouent des **délais**, permettent l'accès en temps direct, et l'archivage quasi illimité d'une masse d'informations. Aux dépens du temps de sélection et de réflexion : une rumeur va plus vite qu'une information vérifiée, l'événement occulte l'histoire, la réaction

primaire court-circuite les médiations. Le **pouvoir** est dématérialisé, transformé en flux et stocks. Le véritable pouvoir en deviendra occulte, les manipulations informatiques clandestines, répliquent les autres.

Autre sujet de controverse : la **connaissance**. Elle sera numérisée, transformée en série de bits plus faciles à stocker, traiter, ou transmettre et qui rendront toutes les connaissances et créations aisément disponibles. À cela d'autres répliquent : les trucages en seront facilités, la disponibilité d'une masse énorme de données empêchera la constitution d'un véritable savoir, le contrôle du citoyen sur la réalité qui lui est imposée diminuera, concluent les accusateurs. Infos riches et info pauvres s'affronteront. Dans les quatre dimensions de l'espace, du temps, du pouvoir et du savoir, la technologie a donc bouleversé des expériences séculaires.

De ce fait, collecte, archivage, ordonnancement, traitement, diffusion, commutation de l'information ont subi un changement dont les effets sont plus importants que ceux que l'on remarque généralement, c'est-à-dire augmentation quantitative, disponibilité, accélération, mondialisation.

L'information étant numérisée son stockage, ses flux, son origine, son intégrité (c'est-à-dire le fait de persister sous sa forme première et non truquée ou modifiée), sa force opératoire sont soumis à de nouveaux aléas et nouveaux usages. Les nouvelles technologies ont bouleversé les conditions

Du **faire savoir** (avec la constitution de méga-archives numériques et des réseaux informatiques),

Du **faire percevoir** (avec à la fois des instruments de surveillance omniprésents, le cyberspace et les réalités virtuelles),

Du **faire faire** (les machines informationnelles qui "commandent" l'action d'hommes ou de machines, d'une station spatiale au portillon du métro),

Et du **faire-croire** (à l'époque des télévangélistes ou de la politique-spectacle, on ne croit plus de la même façon qu'à l'époque de la chaire ou du préau d'école).

Nous découvrons maintenant que l'information est susceptible de trois usages offensifs :

- - Une **appropriation** non désirée, rançon de sa **durabilité**.

Qu'elles soient relatives à des choses (techniques autorisant certaines performances, connaissances déterminant des stratégies) ou qu'elles concernent des individus (localisation, repérage, surveillance et fichage), les informations sont génératrices de pouvoir. Avec la perte de la confidentialité protectrice, allant du vol de brevet au viol de la vie privée, il y a toujours danger et perte pour quelqu'un**. L'information menace la confidentialité.**

• - Une **pénétration** dommageable, rançon de sa **transmissibilité** L'information est aussi une force agissante. Elle crée des choses ou des relations et en détruit. Elle produit de l'ordre et du désordre. En particulier l'information fausse, déstructurante occulte la vérité, enlève la capacité de réagir de façon appropriée, détruit la mémoire ou annihile la capacité de traitement. De la désinformation politique au virus informatique, du bobard au sabotage, **l'information menace l'information.**

• - Une **propagation** inacceptable rançon de sa **reproductibilité**. Le monopole de sa diffusion ou le contrôle sur sa réception, par la manipulation ou la propagande, menacent la pensée critique, la possibilité de réponse, et partant toute relation humaine libre**. L'information menace la communication.**

Notre tradition intellectuelle nous incite à nous méfier du pouvoir de la persuasion et de l'illusion, avec autant de force qu'elle prône contradictoirement les bienfaits de la communication. Dénonciateurs ou apologistes des Nouvelles Technologies reproduisent une querelle ancienne avec des mots nouveaux. Peut-être est-il temps de penser l'information comme champ de conflit.

**II La désinformation**

Pouvons-nous appliquer les principes que nous venons de dégager à une notion comme celle de désinformation, qui semble pourtant typiquement héritée de la guerre froide ? La récente redécouverte du mot appliqué notamment à la guerre économique nous incite à poser la question.

La désinformation est une réalité agonistique, une attaque délibérée par l'arme de l'information. Comme telle elle répond aux conditions que nous énoncions. Elle traduit des rapports entre des organisations matérialisées (partis, clans, entreprises, États, armées) mais aussi une réalité technique, les modes matériels de propagation et de transmission propres à une époque. En même temps, elle implique des croyances, des jugements de

valeurs, des affects, bref des représentations mentales plus ou moins répandues qui fassent que telle ou telle forme de désinformation sera ou non recevable à tel moment. Il n'est pas non plus indifférent pour la comprendre que nous soyons placés entre deux systèmes de transmission : grossièrement celui des **mass media** et celui des **Nouvelles Technologies** de l'Information et de la Communication. Si la désinformation n'est facile ni à établir, ni à prouver dans un cas particulier, son emploi général doit présenter certaines régularités, suggérer certaines corrélations et périodisations. Nous en suggérons cette définition opérationnelle :

*" La désinformation consiste à propager délibérément des informations fausses pour influencer une opinion et affaiblir un adversaire. "*

- "*Propager*" sous-entend un caractère public. Plus que le simple bouche-à-oreille ou l'usage de messages privés, il faut avoir recours à des médias et à des vecteurs.

- "*Délibérément*" demande au moins chez l'acteur la connaissance de sa finalité, même si les "repreneurs" et propagateurs de l'information peuvent être inconscients du processus. Qui se ment à soi-même par erreur ou aveuglement idéologique ne peut désinformer, au plus relayer la désinformation.

- "*Des informations*" ce qui requiert ici qu'il s'agisse de relations de faits, de descriptions de la réalité, non de simples jugements moraux ou opinions. La désinformation a pour base la description d'événements fictifs.

- "*Fausses*" implique qu'elle comporte des affirmations contraires à la réalité ou recadrées de façon à en altérer l'interprétation. Il ne saurait s'agir de simple rhétorique, d'exagération, etc. qui ne constituent pas un processus de falsification, ni même de constructions ou explications de la réalité à l'aide de stéréotypes ou catégories idéologiques. Le mensonge dans la désinformation porte sur la réalité qu'il décrit, sur la personne ou l'appartenance de qui la rapporte et sur le but de son énonciation qui est de provoquer un dommage. Cela en fait une sorte de mensonge au cube. Et un **jeu à trois : initiateur, public, victime.** La désinformation fait souvent appel de véritables mises en scène ou la construction d'apparences de réalité. Cela marque la frontière entre la falsification et la simple illusion.

- "*Pour influencer une opinion*" veut dire que l'on cherche à imposer une **croyance** ou des attitudes à un public plutôt qu'une **décision** à un responsable, même si les deux peuvent se combiner. Ce public peut être l'opinion adverse, des alliés, des neutres ou l'opinion internationale en général ; on peut viser le grand public ou des cercles plus restreints. La désinformation se distingue de l'intoxication qui est la fourniture délibérée

d'éléments de décision erronée à l'adversaire. La désinformation n'est possible que là où existe **un espace public**, un lieu de débat et une **pluralité** d'opinion et de connaissances. Elle n'a de sens que là où sont en concurrence diverses sources de savoir et diverses interprétations. Big Brother ne désinforme pas, il contrôle le présent, le passé et le futur, il contrôle jusqu'à la langue même. Dans un système totalitaire, il y a la vérité officielle et la rumeur clandestine. Le dictateur dicte ce qui doit être su et cru, et pour y résister on ne peut recourir qu'à une propagation clandestine de contre-information. La désinformation n'est donc possible que là où il y a connaissance imparfaite de la réalité, non-fiction absolue,, là où règne au moins un pluralisme apparent

- "*Et affaiblir un adversaire*" : la désinformation est un instrument utilisé dans un conflit. Elle sert à diminuer les capacités offensives de l'autre, en **divisant** l'autre camp ou en **l'inhibant**, moralement, par désorganisation, etc. En cela, la désinformation, toujours négative ou agressive, diffère de la publicité commerciale, de l'endoctrinement, etc. dont la finalité est d'obtenir l'adhésion. C'est pourquoi elle recourt à l'imputation d'actes ou d'intentions inavouables à l'adversaire, à la perversion de son image. Ou plus simplement encore la désinformation accroît la confusion et le désordre. Elle devient alors le contraire de l'information au sens étymologique : mise en forme de connaissances. Ceci se réalise à travers deux dimensions de la croyance qu'elle suscite : d'une part comme **incitation** propageant des passions et sentiments de manière quasi épidémique, telle de la haine, et, d'autre part, comme **représentation** erronée, confuse, biaisée de la réalité. Le délire idéologique, la faculté d'auto-illusion, la clôture informationnelle, l'hallucination interprétative, et tant d'autres formes de déni de la réalité ne constituent pas de la désinformation, pour autant qu'elles ne sont pas dirigées **contre** un adversaire.

La désinformation se distingue ainsi du mensonge, de la ruse, de l'intoxication, de la légende, de la rumeur, de la publicité, du bobard journalistique, du faux bruit, du trucage, de la rhétorique, et de la propagande, même si elle fait peu ou prou appel aux mêmes éléments.

La désinformation ne peut se réduire à une lutte de discours ou à une compétition entre nouvelles vraies et fausses. Elle n'a pas qu'un **objet**, elle a un t**rajet**, c'est un **contenu** qui suppose un contenant : il lui faut des vecteurs de propagation, des multiplicateurs, bref des médias. La reprise dans les têtes suit la reproduction par des mots, des images, et maintenant des bits électroniques. On ne croit pas de la même manière à l'époque de Gutenberg ou de CNN. De même, on ne désinforme pas de la même manière selon que l'on fait imprimer des Protocoles des Sages de Sion, que

l'on truque un reportage vidéo à Timisoara, ou que l'on attaque les forums de discussion.

L'instrument technique détermine :

- Ce qui est **énonçable** : le complot sioniste, le Prolétariat ou le sens de l'histoire passent mal à la télévision, le regard d'un réfugié dans un camp se décrit difficilement dans un courriel, mais un dossier technique sur les défauts d'un avion est accessible à des millions de gens qui fréquentent les forums

- Le **mode de preuve** : à l'heure de la télévision, ce qui n'est pas vu n'existe pas, une guerre sans image n'est pas une guerre, mais un mort en direct condamne une cause, sur Internet des milliers de gens peuvent répéter un bruit issu d'une source officieuse unique

- Le **temps** de circulation : une information touche toute la planète en quelques heures, un démenti trois jours après n'intéresse plus personne ; sur la Toile une annonce que personne n'a eu le temps de vérifier pénètre sur le réseau instantanément.

Tout média impose sa hiérarchie de ce qui est important, crédible, séduisant, probant, etc., son style de rhétorique, sa mémoire, sa temporalité, sa portée géographique, sa relation avec le récepteur. Aucun n'est par nature plus véridique qu'un autre, mais chacun a son mode d'usage et de mésusage. Chaque type de désinformation a son indice de performance propre sur chaque média. Selon les époques, un éditorialiste sous influence, un témoin télégénique ou une bonne pratique des moteurs de référencement garantit le succès.

La critique de la télévision comme instrument à " fictionner " et à simplifier la réalité a été menée cent fois. De fait, elle accentue le rôle du visuel, de l'immédiat, de l'émotionnel, du simple, de l'exemplaire par rapport au général, au conceptuel. Elle privilégie la construction événementielle, l'urgence, la relation coupable-victime, les stéréotypes...

Que pour autant elle rende plus puissante la désinformation resterait à prouver, tant sont aléatoires les pouvoirs d'une image. Ce que la rhétorique a gagné en simplicité est perdu en imprévisibilité. Il se pourrait que l'intention de convaincre par l'image ne soit que peu de choses au regard du pouvoir général de la télévision : discriminer entre ce qui est visible et ce qui est ignoré, déterminer plus que le contenu les objets et les catégories du débat, imposer moins ce que l'on pense que ce qui est pensable.

Or, les Nouvelles Technologies de l'Information et de la Communication changent les règles du jeu. Deux phénomènes non exclusifs au moins

semblent redonner une nouvelle jeunesse à la notion de désinformation : la **rumeur électronique** et la " **guerre de l'information** ".

La rumeur, le plus vieux média du monde, a trouvé des conditions idéales pour fleurir sur Internet :

- Possibilité pour chacun de devenir éditeur sans moyens matériels et quasiment sans responsabilité éditoriale, ce qu'on appelle la " désintermédiation " dans le jargon de " l'infocom " Internet supprime ce qu'il est convenu d'appeler l'intermédiation (des institutions, tels des rédacteurs en chefs qui sélectionnent les nouvelles ou d'autres "garde-barrière", les gate-keepers des sociologues américains) et donne à chacun la possibilité de publier impunément de n'importe quel point du réseau. Du coup, s'il n'existe plus guère de censure efficace (exemple : le livre du docteur Gûbler qui s'appelle justement "Le grand secret" ou de Matt Drudge court-circuitant les grands médias sur Internet dans l'affaire Lewinsky).

Il n'existe plus non plus de procédure de **vérification** ou d'**accréditation** : tout le monde peut tout dire. En cela, le plus moderne des médias devient un support de la calomnie, des "légendes urbaines", des bruits fous, etc... Avec pour résultat que n'importe qui peut se faire le propagateur de désinformation volontairement ou involontairement. Pierre Salinger répandant la nouvelle que le Boeing de la Panam a été abattu par un missile ou Matt Drudge rapportant des informations fausses sur le passé judiciaire d'un Sénateur parce qu'ils l'ont appris sur la toile en sont des exemples.

- Fin des modes traditionnels de **consultation** des médias. L'internaute parvient à l'information par recherche thématique, navigation hypertextuelle ou via des forums thématiques. L'internaute se dirige vers l'information en suivant un lien sémantique plutôt que vers une source précise (comme un journal réputé). L'autorité de la source devient une notion dépassée.

- Mode de **circulation** de l'information par commutation (A va vers B) et non plus par diffusion (X émet, tout le monde reçoit). Cela favorise une propagation erratique des rumeurs. Elles conservent le caractère du bouche-à-oreille traditionnel mais à l'échelle de la planète. Une diffusion par relation interpersonnelle alterne avec des phases de mise en forme par des sites spécialisés voire de reformulations par les médias traditionnels qui se nourrissent de l'actualité d'Internet.

Ces conditions techniques jouent en synergie avec des tendances culturelles :

• C'est d'abord la prolifération des **communautés** virtuelles. Les internautes rassemblés à distance par une passion commune forment par excellence un milieu favorable à la diffusion de ces vérités officieuses que sont les rumeurs. Les tendances idéologiques " techno-libertaires " notées plus haut rendent méfiants à l'égard de l'information commune que favorables à toute version alternative.

• De surcroît, la diffusion de la rumeur sur Internet est à rapprocher de phénomènes comme le **piratage** informatique. Face à une rumeur sur Internet, il devient de plus en plus difficile de savoir si l'on est en présence d'un jeu consistant uniquement à faire croire une énormité au maximum de gens (un " hoax " en jargon d'Internet), d'une légende spontanée ou d'une véritable opération politique de désinformation.

Second élément : la guerre économique dite de l'information. Ces diverses formes d'agression par l'information qu'elle suppose comportent notamment des campagnes de dénigrement sous le couvert de groupes d'experts ou organisations écologistes révélant les prétendus dangers d'un appareil ou d'un produit, affirmant sa nocivité pour l'environnement, découvrant les liens supposés d'une compagnie avec une dictature. Un autre procédé consiste en la multiplication de dénonciations " spontanées " de citoyens ou consommateurs. La calomnie en question peut maintenant être déléguée, en ce sens que la propagation de ces messages sur les forums de discussion peut être confiée à des logiciels. Ils interviennent en fonction de thèmes-clefs et remplacent des messagers humains.

Sur fond de **thèmes porteurs**, sécurité du consommateur, droits de l'homme, protection de la Nature, dénonciation du système de surveillance des citoyens, Internet peut devenir une arme au service de desseins privés. Cette désinformation-là est encore moins facile encore à prouver que la forme classique : instiller du faux dans le système des mass media. Ici, ni le caractère délibéré du processus, ni les finalités politiques, économiques ou autres de ses auteurs ne sont manifestes.

**III Le secret**

L'enjeu du "qui sait quoi ?" est devenu vital pour chacun de nous. De nouveaux vocables comme "**traçabilité**" reflètent bien la situation. Nous sommes tous devenus "traçables". Par des moyens informatiques de surveillance et par la connexion de bases de données, il est possible non seulement de dire ce que nous sommes, d'avoir une multitude de renseignements sur nous, sur les facettes de notre identité, mais aussi de noter ce que nous avons fait, où nous sommes passés soit physiquement

soit par moyens de communication interposés. Il est très facile de savoir quels sites Internet nous fréquentons, où nous allons, ce que nous payons...

Ainsi "profilés", révélés dans toutes les composantes de notre identité nous éprouvons la peur du contrôle absolu. Si nos actes nous poursuivent, notre comportement est prévisible. Sil est prévisible, il peut être dirigé. L'homme ordinaire, et non seulement le criminel, le stratège ou l'espion, découvre l'importance de ces notions : protection d'informations contre la divulgation ou l'altération, recherche de l'anonymat, vérification de l'identité de ses interlocuteurs, peur d'être espionné ou piraté. Nous vivons bardés de codes, obsédés de confidentialité, menacés par toutes sortes de délits d'information ou d'outils de fichage. Ce n'est pas encore la guerre, mais c'est une manifestation de la gravité du conflit informationnel.

La lutte pour et autour du secret est déterminée par :

- La désirabilité et la **valeur** commerciale ou pratique de connaissances, recettes, inventions, que certains possèdent et d'autres non s'accroissent considérablement

- Le taux de **renouvellement** des secrets augmente parallèlement. Il y a urgence à savoir vite et à exploiter avant les autres.

- Dans la **masse des messages** qui circulent, il devient de plus en plus difficile de distinguer ce qui doit rester secret, ce qui est bénin, ce qui est disponible, ce qui est dangereux, etc.

- Dans la mesure où nous confions le traitement de ces opérations à des **machines** sophistiquées, notre maîtrise diminue en même temps que les possibilités de fraude, trucage, etc. menées par des moyens technologiques invisibles.

- La question du secret n'est pas séparée des grands enjeux de nos sociétés : La puissance politique repose en grande partie sur la capacité de tout voir et tout savoir. La puissance économique ne repose plus sur quelques plans ou brevets qu'il suffirait d'enfermer dans un coffre, mais sur l'exclusivité de millier d'informations et de données.

- La démocratie suppose une forme particulière de publicité et de transparence. Mais de manière quelque peu contradictoire, elle suppose aussi la distinction entre les affaires privées qui ne concernent que l'individu et les affaires publiques. Cette contradiction risque de devenir dramatique dans la société du secret qui est la nôtre.

La lutte pour et autour du secret implique trois nouvelles dimensions : la publicité, la disponibilité et la lisibilité de l'information.

**La publicité**

La publicité est une notion relative. Il y a toujours des "initiés" : ce peuvent être des conspirateurs qui ont juré silence sur leur vie, mais aussi le Tout-Paris médiatique qui se répète dans les dîners en ville quelques confidences qui n'aboutiront pas dans les journaux.

Inversement, il y a des informations parfaitement disponibles mais si discrètement diffusées par rapport à leur gravité que cela équivaut presque à un secret. L'**étouffement** de l'information significative ou dérangeante sous le **flux** de ce que les médias répètent et désignent comme débat, événement, fait de société, question " qui nous interpelle ", etc. est infiniment plus efficace que toute forme de censure.

**La disponibilité**

L'Internet offre des possibilités de pénétrer dans des mémoires en bénéficiant d'un accès en tout point. L'espace n'est plus un obstacle, ni le temps : on peut agir en temps réel mais aussi à retardement comme le font les " chevaux de Troie " introduits dans les systèmes informatiques pour en prendre le contrôle ultérieurement. L'identité de l'attaquant est assez bien protégée. Du coup, se développent de nouvelles catégories de violeurs, agissant à faible risque, soit par goût de l'exploit gratuit (*hackers*), soit par ressentiment et goût du vandalisme (*crackers*).

L'effraction est invisible et indolore et la pénétration immatérielle : parfois on ne réalisera jamais que le secret a été violé. Ou, dans le cas de marquage, de "*chips*" etc. on ne saura jamais qu'il existe un moyen de reconstituer vos activités : il subsiste toujours une trace de tout ce que l'on a reçu et émis, un indice de tous ses mouvements physiques ou virtuels (connexions).

Ceci fonctionne dans les deux sens : "**prélèvement**" d'informations, mais aussi **pénétration**. *Cookies*, chevaux de Troie, virus, bombes à retardement, etc. introduisent frauduleusement soit des machines de guerre (qui opèrent destruction, désorganisation, falsification, etc.) soit des machines de contrôle (qui permettront de prélever de l'information ou d'exécuter des instructions).

Corollairement, les techniques de défenses changent, elles deviennent physiques ou sémantiques. Dans le premier cas, il ne faut pas laisser de points de passages aux signaux hostiles. Dans ce second cas, il faut les discriminer, l'information protége contre l'information. Distinguer l'ami de l'ennemi devient un problème technique voire informatique, et plus seulement pour les militaires.

D'où le caractère crucial de l'**identification** (authentification et signature). L'impératif du "prouve qui tu es" forme l'exact pendant de la revendication d'anonymat du citoyen. La 7/03/00valeur probante du document numérique et de la signature électronique soulève des questions de liberté publique autant que d'économie. En l'absence physique de l'individu accrédité, il faut faire appel à l'emploi de symboles. Il faut prouver que l'on sait A, pour prouver que l'on est X et avoir le droit de savoir B ou de rentrer en Y. De surcroît, il faut pouvoir laisser une signature, une empreinte, une preuve de son passage.

**La lisibilité**

Des pharaons aux cyberpunks, de la substitution de hiéroglyphes à la lutte pour le contrôle d'Internet, le code suppose un processus perpétuel : il se reconstitue à mesure que progresse l'art du déchiffrement. Le codage est désormais délégué à des puces : les éléments du texte clair deviennent des sériées de 0 et de 1 qui, elles-mêmes, sont comme "brassées" suivant un ordre. Un des systèmes les plus populaires le D.E.S., *Data Encryption Standard* d'IBM transpose le texte en séries de 64 bits, puis, au cours de 16 étapes successives, échange et transpose ces blocs suivant un rythme déterminé par sa clé secrète à 56 bits. Le destinataire procède à l'inverse, dans ce système dit à clé symétrique. Il existe aussi des systèmes à clef publique où chacun communique un algorithme à son éventuel correspondant, ce qui permet d'en recevoir des messages cryptés, mais se réserve la clef privée qui seule permet le déchiffrement : chiffrement et déchiffrement sont devenues non réversibles, asymétriques. On parle également de cryptologie quantique par envoie d'électrons qui ne peuvent être interceptés, d'identification des interlocuteurs par envoie d'images de leur rétine, etc. Bref, la **capacité de coder** ou de décoder n'est plus une affaire d'ingéniosité mais de **puissance industrielle** et de **technologie de pointe.**

On proclame souvent que tel algorithme résisterait à tant d'ordinateurs, de telle puissance travaillant pendant tant de siècles. Ce peut être présomptueux, comme l'a démontré le récent "craquage" de D.E.S. : la montée en puissance des ordinateurs, qui de surcroît travaillent en chaîne à briser le code, rend de tels calculs très éphémères. Reste pourtant la notion de nombre d'essais et erreurs qui se mesure en puissance mathématico-informatique. Un service secret (telle la National Security Agency américaine, dont a dit cent fois que c'est le premier employeur de mathématiciens au monde) ou un groupe de pirates informatiques peut ou ne peut pas casser une clef de tant de bits, dans un délai de tant d'heures ou

de jours. La décision du gouvernement français de relever de 40 à 128 bits la longueur des clés librement disponibles, et donc de ne plus les classer comme matériel stratégique, offre au citoyen les armes cryptiques qui étaient autrefois celles du stratège et de l'espion. Cela satisfait une curieuse revendication : le droit de dissimuler pour tous, la **démocratisation du secret.**

Qu'on l'examine sous ses trois aspects, publicité, disponibilité, lisibilité, le secret a changé de statut : pour le garder, il ne suffit plus de se taire, pour le vaincre, il faut bien davantage que des indicateurs ou des espions. Qui garde ou qui viole le secret, voilà qui reflète maintenant un **rapport de force** militaire, politique, économique, technique et idéologique.

**Conclusion**

Quel que soit le domaine du conflit informationnel, nous sommes mal préparés pour mesurer comment techniques, pratiques, idéologies, stratégies parcourent les champs politique, économique mais aussi la vie quotidienne et en bouleversent les frontières.

Mal préparés d'abord pour apprécier les faits : difficile de distinguer ce qui est significatif ou exceptionnel dans toutes les histoires d'intelligence économique ou de fraude informatique. L'efficacité ou l'ampleur réelles des techniques de guerre de l'information sont mal documentées. Sans compter que tout ce qui touche au secret est, par définition, discret.

Nous sommes surtout mal préparés théoriquement. Un discours technique énumère des possibilités : dangers, recettes et panoplies. Il oscille souvent entre science-fiction paranoïaque (le grand chaos informatique) et anecdotes excitantes (espions et pirates sur Internet). Les sciences de l'information et de la communication négligent souvent le conflit et le secret au profit d'une réflexion sur le pouvoir ou la crédibilité des messages médiatiques, sur le rapport vertical médias-public. Entre les deux, complexité et dualité du conflit nous échappent souvent. Le besoin sinon d'une discipline, du moins, d'une méthode s'impose. De notre capacité à comprendre ces phénomènes de manière transdisciplinaire, de la rigueur intellectuelle avec laquelle nous saurons appréhender et anticiper les tendances nouvelles, dépendra la façon dont nous serons armés pour les affronter.

**François-Bernard Huyghe**, docteur d'État en sciences politiques et habilité à diriger des recherches en sciences de l'information et de la communication, enseigne la sociologie des médias au Celsa (Paris IV). Consultant pour des études sur les Nouvelles Technologies de l'Information et de la Communication, il mène des recherches en médiologie. Derniers ouvrages parus : *Images du monde* (J.C. Lattès, 1999) *Histoire des secrets* (Hazan, 2000). Courrier électronique de l'auteur : huyghe@club-internet.fr