Des vigiles invisibles: Les administrateurs-réseaux et la sécurité informatique

Francis Chateauraynaud, Patrick Trabal

Des vigiles invisibles

Les administrateurs-réseaux et la sécurité informatique

Francis Chateauraynaud et Patrick Trabal

Groupe de Sociologie Pragmatique et Réflexive

EHESS, Paris

Papier soumis pour publication dans les Annales des Télécommunications

Version de septembre 2006

Mots-clefs : sociologie, administrateurs-réseaux, informatique, internet, risques, alertes, responsabilité, usages, apprentissage, régulation

Une activité professionnelle, comme celle des administrateurs-réseaux, sur laquelle reposent l'ancrage et la pérennité de la « société de l'information », peut-elle rester ignorée des sociologues ? Pour combler quelque peu le « vide sociologique » qui entoure ces professionnels, on s'est intéressé aux modes de traitement des situations critiques et des alertes qui émaillent le fonctionnement ordinaire des réseaux informatiques. L'enquête a porté à la fois sur un corpus d'alertes, saisies sur différents supports (courriels, listes de diffusion et sites Web) et sur un ensemble de responsables de réseaux informatiques ou de sites internet. On parlera d' « administrateur-réseau » bien que de multiples appellations aient cours dont les frontières sont, en pratique, assez poreuses : « administrateur système », « ingénieur-réseaux », « ingénieur système-réseau », « architecte réseau »… Ces dénominations renvoient à des compétences et des missions différentes mais on observe une superposition des fonctions au sein des mêmes services informatiques. Il s'agit de personnages-clés, placés au nœud de la conception et du fonctionnement des réseaux et dont la mission est de faire en sorte que l'énorme empilement d'objets techniques, de machines, de câbles, de connecteurs et de logiciels, résumé sous le terme de « réseau », devienne invisible ou transparent pour ses utilisateurs. De fait, on va moins privilégier ici la question du statut que celle de l'activité (Bidet, 2006 ; Hubault, 2006).

L'étude des critiques de l'internet a montré comment le développement du « monde virtuel » redouble le monde réel, par la production continue de points de recoupement (Chateauraynaud et. Trabal, 2003). D'où l'importance des agents chargés du fonctionnement des réseaux. Pour ces acteurs-là, anti-baudrillardiens par vocation, le virtuel n'a pas tué le réel mais lui a, au contraire, donné une prégnance encore plus forte. La coordination des interventions techniques et des interactions avec les utilisateurs d'un réseau donne lieu à différents processus d'apprentissage, dont la teneur est variable selon les milieux et les organisations. S'il s'agit le plus souvent pour les administrateurs d'intervenir sur les repères communs dont disposent les utilisateurs d'un réseau, y compris dans la partie souvent jugée « triviale » qu'est la messagerie, ils parviennent, à l'occasion d'alertes jugées sérieuses, à transmettre de nouvelles connaissances et à susciter une dynamique d'apprentissage collectif. Quels sont les ressorts de la confiance nécessaires au fonctionnement des réseaux ? Sur quelles scènes se joue le type de délégation socio-technique qui sous-tend ce que l'on appelle la gouvernance de l'internet (Berleur, 2004).

I. Une sociologie des alertes informatiques

De multiples acteurs lancent des alertes en matière de sécurité informatique. Par exemple, dans un rapport de janvier 2006, le Club de la sécurité des systèmes informatiques français (Clusif), estime que « la cybercriminalité est en hausse », les réseaux ayant connu un nombre croissant d'attaques en 2005[1]. Mais la sécurité informatique suscite des réactions défensives ou des charges critiques de la part d'autres acteurs. Si la question du « cyber-terrorisme » est à l'ordre du jour, l'organisation de la sécurité informatique se heurte à la défense des libertés

[1] La plupart des attaques visent avant tout le détournement ou l'extorsion de fonds (avec une montée spectaculaire du « phishing »), mais les affaires d'espionnage de données sont aussi légion.

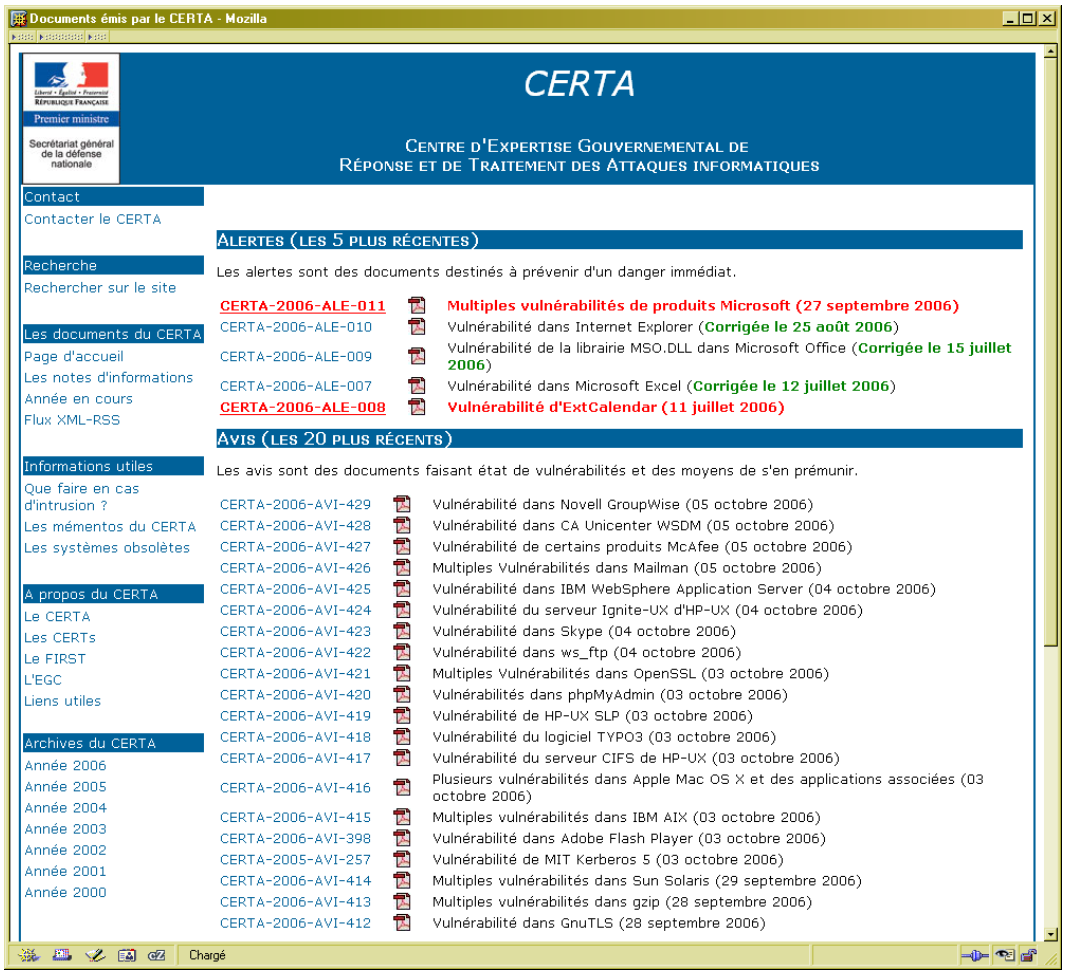
individuelles et au développement d'un Web prometteur d'espaces de libres expressions[2]. On a montré comment les formes de mobilisation suscitées par les risques émergents engageaient les expertises de différents acteurs aux prises avec les processus en cause (Chateauraynaud et Torny, 1999). Avec l'internet, les dossiers techniques et les dossiers politiques semblent encore fortement dissociés, ou, plus exactement, le fossé est encore profond entre les activités ordinaires et les représentations déployées dans les arènes publiques – bien que le conflit du téléchargement « illégal » de fichiers ait contribué à rapprocher les deux plans.

La « sécurité informatique » engage des dispositifs intentionnels, puisqu'il s'agit, dans la plupart des cas, d'actes d'intrusion ou de destruction, qu'ils soient le fait d'individus isolés ou de groupes organisés. Lancer une alerte dans ces domaines prend essentiellement deux formes : alerter, c'est d'abord imputer une intention de commettre un délit, ou pour le moins une mauvaise action, ce qui se décrit, dans le langage ordinaire, sous le terme de délation (le lanceur d'alerte est alors un délateur) ; mais c'est aussi mettre en évidence des débordements affectant la liberté des personnes ou des groupes, ce qui revient à dénoncer des abus de pouvoir ou la violation de libertés fondamentales. Le contrôle des réseaux par des puissances d'action (Etats, firmes, organismes internationaux) devient le foyer de visions dystopiques. Mais ce tableau oublie un autre mode d'existence du danger : le travail continu, presque invisible, opéré quotidiennement par les acteurs engagés dans les réseaux techniques pour identifier, qualifier et rendre tangibles des vulnérabilités ou des sources de défaillance.

Des instances officielles ont été créées pour traiter des questions de sécurité informatique et de cybersurveillance. Sans refaire ici l'histoire des CERT (Computer Emergency Response Team), liée en France au réseau Renater, rappelons que c'est à l'issue du Comité Interministériel pour la Société de l'Information (CISI), de janvier 1999, qu'a été institué le CERTA (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques). Rattachée à la Défense Nationale, cette structure travaille en réseau avec les services chargés de la sécurité de l'information dans l'ensemble des administrations. Les deux principaux objectifs sont ainsi d'assurer la détection des vulnérabilités et la résolution d'incidents concernant la sécurité des systèmes d'information. Des documents totalisent les opérations dites de « sécurisation » des accès aux réseaux, et un site, abondamment fréquenté par les administrateurs-réseaux, tient à jour la liste des événements et des alertes affectant ou susceptibles d'affecter la sécurité des réseaux[3].

[2] On a ainsi étudié un forum français autour du projet INES (Identité nationale électronique sécurisée). La carte d'identité électronique est supposée relier tous les citoyens par des « technologies sécurisées » et des « procédures garanties » sous contrôle de l'administration. Il ne s'agit pas seulement d'identifier les personnes mais de leur permettre de signer des transactions en ligne ou de porter sur une puce électronique un « portfolio personnel ». Face à la révélation continue de cas de fraudes et d'actes d'intrusion ou de détournement, la sécurité informatique de ce nouvel artefact techno-politique est fortement controversée. On touche ici aux enjeux de la convergence de différentes technologies et de la redéfinition du mode de production des formes légales, convergence qui fait écho à celle qui est engagée par les nanotechnologies. Voir Dupuy (2004) et Chateauraynaud (2005).

[3] The CERT® Guide to System and Network Security Practices : http://www.cert.org/security-improvement/



La cybersurveillance mêle deux logiques d'enquête : la première repose sur une traçabilité fondée sur l'enregistrement de tous les messages et les évènements survenus pendant un temps donné sur de multiples supports ; la seconde passe par la participation des agents de surveillance aux activités des réseaux (ce qui suppose, dans certains cas une « infiltration » de certains milieux, comme on le voit dans le cas des réseaux pédophiles mais aussi des groupes de hackers lors des compétitions et autres rencontres[4]). Du même coup, la tentation est grande pour de multiples acteurs de tenter de subvertir les dispositifs de surveillance en retournant contre eux leurs propres techniques et en rendant public des failles de sécurité (Auray, 2000).

[4] Voir par exemple : http://www.defcon.org . La « presse Hacker » (Zataz, Hackademy, Pirates Mag'), diffusée en kiosques, donne à lire les cibles (déjà atteintes ou potentielles) des réseaux des hackers.

II. Une collection de précédents

Une des tensions éprouvées par les organisations face à une intrusion est celle de la révélation publique de l'événement. Evoquons rapidement le cas, très typique, de l'Université de Berkeley.

Le système informatique de Berkeley piraté en août 2004
Un pirate informatique a pu accéder aux noms et coordonnées de 1,4 million de personnes enregistrées sur les systèmes de l'université de Californie à Berkeley. Les noms auxquels il a pu accéder étaient utilisés par un chercheur dans le cadre d'un travail sur l'impact des soins à domicile sur les loyers. Les données comprenaient ls adresses postales, numéros de téléphone, dates de naissance et numéros de sécurité sociale, collectés avec l'autorisation des autorités mais sans l'accord des individus concernés. Un porte-parole de l'université de Berkeley a estimé que ce piratage constituait l'attaque informatique la plus grave de l'histoire de l'établissement. Le FBI a été chargé de l'enquête.

Ce genre d'attaque engage les acteurs dans un processus d'enquête qui mêle les traits de l'enquête policière et les techniques de la « cyber-investigation », à travers laquelle sont rendues descriptibles des compétences et des activités opaques, comme celles qui font le quotidien des administrateurs-réseaux. D'un point de vue cognitif, la logique de l'enquête n'est pas déductive ni inductive mais *abductive* : quelles conditions faut-il imaginer pour que l'on puisse tirer Y de X ?[5] Mais il ne s'agit pas seulement d'un exercice logique. La détection de l'anormalité d'une situation se prolonge par des tractations en interne, les principaux protagonistes étant confrontés à des dilemmes organisationnels (Vaughan, 1998). L'épreuve atteint un maximum d'intensité lorsque des acteurs extérieurs se trouvent mobilisés (comme l'administration californienne et le FBI dans l'exemple ci-dessus). Enfin, si l'affaire donne lieu à une déclaration publique, via le Web, celle-ci peut être reprise sur de multiples supports[6]. L'événement rejoint alors la liste des précédents utilisés pour élaborer des guides pratiques de sécurité informatique.

Quelle est la part de cas de figure qui ne surgissent pas dans l'espace public ? Il est difficile de répondre, d'autant que la notion d'espace public est elle-même à géométrie variable. De nombreux incidents ne donnent pas lieu à une publicité extérieure, ce qui ne signifie pas qu'ils n'ont pas d'impact sur les dispositifs et les formes de vigilance mis en œuvre par les acteurs concernés. Car de multiples événements sont couramment invoqués, analysés ou discutés sur des forums de discussion et dans des communautés restreintes d'acteurs rassemblés autour d'un type de système, de protocole ou de logiciel, comme dans les communautés du logiciel libre (Proulx, Massit-Folléa et Conein, 2005). On sait que ce sont parfois des hackers ou des « defacers »[7] qui rendent eux-mêmes publique leur « œuvre de piratage ». L'affaire Humpich a été de ce point de vue exemplaire.

L'affaire Serge Humpich
Cette affaire a opposé, en 2000, Serge Humpich au Groupement d'intérêt économique (GIE) Cartes bancaires. Cet ingénieur informaticien a cherché à établir les failles de la carte à puce bancaire. Fort de sa découverte, il a tenté de négocier son « savoir-faire » auprès du GIE, mais ce dernier, alors qu'il tentait de vérifier la crédibilité

[5] Sur la théorie de l'enquête, voir Dewey (1985) et sur l'abduction chez Peirce, Chauviré (2004).

[6] Le Web a changé les modalités de diffusion publique des événements, contraignant à revoir les anciens modèles d' « amplification ». (Kasperson & Kasperson, 1996).

[7] Défacer un site Web (du terme anglais « defacer », qui signifie « défigurer ») consiste à remplacer la page principale du site par une autre, évidemment sans l'autorisation de son propriétaire.

de l'information, avait porté plainte en secret contre Humpich pour « intrusion frauduleuse dans un système automatisé de données » et « contrefaçon de cartes bancaires ». Bien qu'il ait défendu sa cause en présentant sa démarche comme désintéressée, l'ingénieur a été déclaré coupable de contrefaçon et de falsification, d'accès frauduleux dans un système de traitement automatisé de données et d'usage de cartes de paiement contrefaites, (jugement du 25 février 2000 du tribunal correctionnel). Une large partie de la communauté juridique en matière de nouvelles technologies s'est indignée de cette décision « assimilant les scientifiques à des hackers et condamnant la recherche dans le domaine de la sécurité des cartes à puce» ». L'affaire Humpich a surtout jeté un doute sur la fiabilité des cartes de crédit, engendrant des efforts pour « sécuriser » le système de cryptographie.

La recherche des points de vulnérabilité engage trois formes de preuve (Chateauraynaud, 2004) : le travail perceptuel au contact des choses qui fournit des prises nouvelles (c'est le travail de veille associé aux activités de routine, qui conduit à faire attention à des détails qui importent peu pour les gens à distance) ; le surgissement d'un événement marquant qui rend caduque une représentation antérieure (c'est précisément la production de cet événement qu'assume un acteur comme Humpich : mettre devant le fait accompli, situation toujours vécue comme « désagréable » par les responsables d'un dispositif sensible) ; enfin, la formation d'un accord collectif sur des rapprochements entre des signes (ce qui renvoie à l'émergence des standards de l'expertise). Lorsque les trois formes convergent, les acteurs n'ont plus de raison de poursuivre l'enquête. Ils disposent de nouveaux standards d'appréciation et d'action pour réorganiser leur système de veille. D'un point de vue pragmatique, ce qui importe, c'est de pouvoir vérifier en cas d'urgence, de doute ou de désaccord. La « vérificabilité », qui se confond avec le sentiment de confiance, est plus importante que la vérification elle-même, car elle pointe sur une vérification potentielle ou virtuelle.

Tous les événements ne sont pas traités comme exemplaires, et nombreux sont ceux qui tombent dans l'oubli – à l'image des virus qui ne cessent de changer d'aspect et de procédé. Mais la forte pression sécuritaire pèse lourdement sur la gestion ordinaire des systèmes informatiques, contraignant à organiser une mémoire longue des événements.

Tout hacker qui cherche à faire ses preuves est tenté d'usurper l'identité d'administrateur ou de le défier en contournant ou « crackant » les sécurités mises en place. On assiste ainsi à de véritables luttes d'emprise sur des territoires virtuels.

Des pirates attaquent le site internet de Cisco Systems (4 août 2005)
Des pirates informatiques ont attaqué le site internet de Cisco Systems en exploitant une vulnérabilité. La faille a été révélée à Cisco par une société d'études spécialisée dans la sécurité. Cisco déclare « avoir apporté un correctif informatique et immédiatement solutionné le problème », mais ajoute ne pas savoir précisément combien de temps la vulnérabilité a duré avant que le groupe ne la découvre. Le mode de communication adopté a déclenché la colère de nombreux « pirates » après que Cisco ait tenté de bloquer une présentation révélant une faille dans ses routeurs informatiques, lesquels dirigent environ 60% du trafic internet.

Mais les hackers ne sont pas les seules sources d'incertitude. Ils peuvent être eux-mêmes subsumés par les virus, créatures étranges, dont le nom évoque la biomédecine et l'épidémiologie.

Zotob.
Ce virus informatique s'est attaqué à de nombreux utilisateurs de Windows 2000, avec une nette prédilection pour les médias. Les chaînes de télévision CNN et ABC News ainsi que le New York Times ont constaté des pannes. Symantec, l'éditeur de logiciels antivirus, a indiqué que Zotob - qui fait redémarrer à répétition les ordinateurs – était classé à un niveau de risque «moyen». Microsoft a néanmoins conseillé aux utilisateurs

touchés de contacter au plus vite le FBI. Le virus s'est attaqué aux PC en utilisant une faille mise à jour par Windows. Dès qu'elle a été dévoilée, les pirates ont exploité cette brèche dans la sécurité des plates-formes Windows. Selon l'Internet Security Systems d'Atlanta, six attaques ont été enregistrées en quelques jours, la dernière ayant touché un ordinateur par seconde. F-Secure, groupe finlandais de sécurité informatique, a déclaré à propos de cette offensive apparemment planétaire : « […] trois différents gangs écrivent des virus et produisent des nouveaux vers informatiques à une vitesse alarmante, comme s'ils étaient en concurrence pour construire le plus grand réseau de machines infectées».

L'administrateur-réseau jour un rôle-clé dans ces affaires. Il exerce en effet plusieurs fonctions au sein de l'organisation : outre la gestion du système, il assure sa configuration, en fait évoluer l'architecture, participe à la maintenance des équipements et intervient dans la définition des usages – notamment des systèmes de courriers et de transferts de données. L'administrateur pouvant accéder à toutes les fonctionnalités (de l'accès aux fichiers jusqu'à la modification du profil des utilisateurs), son rôle doit être protégé et fait l'objet d'une vigilance particulière. L'administrateur-réseau peut, dans le cadre d'une cybersurveillance, accéder à toutes les correspondances des utilisateurs, ce qui lui confère un large pouvoir de contrôle. Il en résulte une difficile cohabitation entre impératif de sécurité du réseau et protection de la vie privée lors de l'interception de courriers[8]. D'un point de vue juridique, tenu par le secret professionnel, l'administrateur ne peut pas divulguer les données auxquelles il a accès. La jurisprudence lui permet cependant de prendre des mesures justifiées par la sécurité. Ainsi, la divulgation d'informations et de messages à des membres de la direction peut être considérée comme une mesure impérative « en cas d'atteinte grave aux intérêts de l'entreprise ».

Dans un rapport de la CNIL sur la « cybersurveillance au travail » (février 2002), on trouve des précisions quant au rôle des administrateurs réseau. Ils ne sont pas tenus au secret professionnel dans deux cas : la mise en cause du bon fonctionnement des systèmes informatiques et de l'intérêt de l'organisation qui les emploie ; des dispositions législatives particulières contraignant à dévoiler des informations.

III. De la responsabilité du fait des liens

La sécurité informatique produit une suite indénombrable d'entités, qui peuplent désormais notre activité quotidienne dans le monde dit « connexionniste »[9], tels que les outils de connexion, les systèmes de login et de cryptage, les logiciels espions, les antivirus, les firewalls, les bornes Wi-Fi… Tous ces artefacts engendrent des dispositifs professionnels et juridiques complexes qui suscitent un « sentiment de vulnérabilité ». Les réseaux portent ainsi à étendre, dans des proportions inconnues jusqu'alors, le principe classique de la responsabilité du fait des choses. Le cas de l'hébergeur est au cœur des batailles juridiques. Actuellement, il ne voit sa responsabilité engagée qu'à trois conditions : qu'il ait la faculté technique d'intervenir ; qu'il ait eu connaissance du site critiquable ; qu'il ait choisi de ne rien faire. Concernant la responsabilité professionnelle, une juriste comme Murielle Cahen conclut

[8] L'arrêt Nikon de la Cour de Cassation en date du 2 octobre 2001 est considéré comme un arrêt de principe par la doctrine. Il a érigé au rang de correspondance privée le courrier électronique, lequel doit bénéficier à ce titre de la protection de la loi du 10 juillet 1991 sur les télécommunications. Voir le texte de l'arrêt sur le site de la CNIL : http://www.declaration-cnil.com/Jurisprudence/J20011002-arret-nikon.php

[9] Selon la métaphore utilisée par L. Boltanski et E. Chiapello (1999).

à la nécessité de responsabiliser les internautes « ordinaires », ce qui rejoint les argumentaires des administrateurs que l'on a interrogés. Le principe de liberté, fondateur de l'économie des réseaux, crée un mouvement pendulaire entre irresponsabilité et responsabilité des acteurs (les intermédiaires notamment). Et le droit n'en finit pas de courir derrière les reconfigurations permanentes des réseaux d'objets et des pratiques qu'ils engendrent : « *L'Internet n'échappe pas à la tendance à la multiplication des responsables afin que la victime puisse obtenir réparation. On en vient à imposer, comme dans le cadre de la législation de la consommation, un devoir de vigilance du professionnel pour décharger l'internaute (profane !). C'est à penser que l'Internet devient un outil de grande consommation, mais il faut garder à l'esprit que la notion de diffusion d'informations implique une responsabilité civique et que moralement, le " cyber-citoyen " doit prendre et assumer les décisions qui l'engagent.*» (Cahen, 2005)

Les tensions qui naissent des usages routinisés des technologies et de l'introduction continue d'innovations engagent les acteurs dans des redéfinitions permanentes des droits d'accès et des outils de surveillance. En France, au début de l'année 2004, dès lors que l'on était équipé d'une carte Wi-Fi on pouvait quasiment se connecter sur toutes les bornes existantes. En l'espace d'un an, la grande majorité des sources Wi-Fi ont été « sécurisés » selon l'expression en vigueur. Le cadre réglementaire, qui relève ici de l'Autorité de Régulation des Télécommunications (ART), institue un partage entre usage interne aux bâtiments et usages externes. Bien que des outils de sécurisation aient été élaborés, comme par exemple le remplacement du protocole à clé fixe WEP par un nouveau système de chiffrement, de nouveaux types de piratage informatique ne cessent d'apparaître. Autrement dit, la sécurité informatique suppose un travail continu de vigilance et d'adaptation des dispositifs, qui rend encore plus décisive la visibilité publique des cas de violation des droits. Et l'occurrence régulière de défaillances et d'attaques est l'occasion pour que les professionnels de la sécurité informatique d'éprouver leurs dispositifs.

IV. Des professions de l'ombre

En décrivant le travail quotidien de veille et d'intervention sur les réseaux, on découvre que la « société de l'information » engendre des « professions de l'ombre ». Combien d'opérations humaines, socialement invisibles, sont nécessaires pour que les routeurs et les serveurs, les cartes et les câbles par lesquels transitent les flux d'informations désormais « à portée de clic », puissent accomplir leur office ? La sociologie de l'alerte a montré que le traitement des risques engage les ressorts de l'action et du jugement au cours des épreuves ordinaires dans le monde sensible. Or, loin de rompre avec le monde sensible, l'univers des TIC produit de nouvelles formes d'attestation, de nouveaux opérateurs de factualité, donnant au monde sensible une forme accrue de tangibilité. Le monde réel ne s'évanouit pas. Il pousse au contraire derrière les ramifications infinies qui se tissent chaque seconde sur la Toile. Prenons un exemple tout à fait ordinaire d'alerte :

« Bonjour à tous !
Le CERTA (Organisme OFFICIEL) nous envoie la note suivante. Il y est question de messages SEMBLANT PROVENIR du Conseil de l'union européenne ou de la direction de communication et de l'information du ministère des affaires étrangères. ATTENTION CE SONT DES FAUX MESSAGES PORTEURS DE VIRUS.
Pour les identifier lisez attentivement la note qui suit qui vous aidera à les détecter. [...]
Un rappel des bonnes pratiques à l'attention des utilisateurs a été mentionné http://www.certa.ssi.gouv.fr/site/CERTA-2005-MEM-001.pdf), les administrateurs peuvent filtrer le trafic POP3 (port 110/tcp) à destination du serveur de messagerie "mail.tut.by" et détecter les éventuelles machines à l'origine de ce trafic ».

Ce message d'alerte engage les ressorts constitutifs des « principes de réalité » associés par les acteurs au fonctionnement du réseau. Il y a d'abord le caractère éminemment collectif ou public des informations en jeu ; on relève également le découplage du réel et de son « double », le mensonge, représenté ici par une tentative d'usurpation, qui contraint à rétablir une structure hiérarchique en se référant à une autorité incontestable. Le message fournit des éléments de tangibilité, ou si l'on préfère de recoupement : l'attention à des signes, permettant une authentification, et une série de dispositifs techniques ou de codes informatiques qui mettent à l'épreuve à la fois les compétences et la fiabilité du système. Enfin, l'alerte est rapportée à une série d'événements de même type, l'effet de collection étant primordial pour la clôture de l'enquête collective et la restauration de la confiance. Comme pour le cas des canulars et des rumeurs (hoaxes) traités par le site Hoaxbuster, les acteurs se sont dotés d'instances de référence, dans le but de réduire les asymétries de prises occasionnées par la « naïveté » supposée des internautes.

Si l'on regarde les définitions, les missions et les règles formalisées dans des ouvrages ou autres manuels précisant le travail d'administration de réseaux informatiques, on n'entrevoit que l'ombre des acteurs humains. Les « guides de l'administrateur » portent surtout sur les systèmes informatiques (par exemple : Stanfield et Smith, 2003 ; Aulds, 2003 ; E., Brooksbank 2000). Les textes ne décrivent pas le métier mais les fonctions accessibles à celui qui dispose, selon la formule consacrée, des « droits administrateur ». On trouve néanmoins un ouvrage centré sur « le webmaster, ses activités, le positionnement et les métiers rattachés » (Lacroix, 2003, pp. 3-23). Cet ouvrage débute par une forme de paradoxe puisqu'il invite tout d'abord le lecteur à « fuir à toutes jambes face aux tâches et responsabilités » qui incombent au webmestre (Ibid., p. 3). L'auteur entend ainsi valoriser les compétences qui sous-tendent cette activité professionnelle. Dans l'ensemble des définitions d'activité fournies par la littérature, il s'agit d'abord de soigner les machines et autres objets techniques tout en restant au service des utilisateurs. La question des alertes est endogénéisée sous la forme d'une norme ISO[10]. En préambule, on note la présence de l'humain surgissant au milieu d'une description d'objets techniques proliférant :

« Diverses études montrent qu'une large majorité des problèmes de sécurité de l'information viennent de l'intérieur de l'entreprise et que les actes commis ne sont pas toujours délibérés, la négligence et la méconnaissance des risques étant des facteurs importants. Les pirates, chevaux de Troie et autres virus agissant de l'extérieur de l'organisme ne sont pas la cause de tous les sinistres. Les aspects organisationnels (à travers la rédaction de procédures et de guides), pédagogiques (par une sensibilisation des utilisateurs et une formation adaptée aux outils utilisés) et juridiques (par la mise en œuvre de contrats et de chartes décrivant les responsabilités de chacun) constituent, à côté des dispositifs techniques, le cœur du système de gestion de la sécurité de l'information. » (Linlaud, 2003, pp. 1-2)

Les défaillances trouveraient leur origine dans une forme d'insouciance ou d'innocence des agents humains portés à faire confiance aux dispositifs, faute de prises suffisantes sur le fonctionnement des chaînes d'artefacts et d'automatismes. Il s'agit de mettre en œuvre une série de dispositifs coopératifs intégrant les objets techniques et les agents humains, regroupés sous la forme de normes et de procédures dûment décrites. Pour faire tenir les chaînes de solidarité technique (Dodier, 1995), il faut mettre les personnes en condition de prendre soin des dispositifs :

[10] Il s'agit de la norme ISO 17799

« - en assurer un suivi quotidien et les exploiter dans un environnement optimal, au moyen de procédures adaptée ;
- se ternir informé des évolutions techniques et technologiques ainsi que des nouvelles vulnérabilités, au moyen d'une veille technologique régulière ;
- élaborer des procédures d'alerte permettant de réagir rapidement et avec efficacité en cas de problème, en assurant la traçabilité des actions entreprises et la conservation des preuves » (Linlaud, 2003, pp. 5-6)

Ce texte rend manifeste l'importance des objets physiques. De quoi nous éloigner encore un peu plus d'un monde « dématérialisé » qui fait passer au second rang les questions d' « intendance » et de « maintenance »[11]. L'expérience du temps est ici marquée par une double contrainte, celle de la régularité et celle de l'urgence.

La sociologie du travail a mis en lumière les limites des seules prescriptions et, à la manière des ergonomes, on peut s'interroger sur les écarts entre les « tâches prescrites » et les « tâches réelles » effectuées par les personnes, en prenant pour objet les conditions d'accomplissement pratique des règles et des normes. Mais l'opposition du « prescrit » et du « réel » est insatisfaisante (Zarifian, 1997), car il s'agit d'affronter deux niveaux de réalité, celui des prescriptions et celui des pratiques. Et l'essentiel de la tâche des acteurs est de veiller aux points de recoupement qui font converger les deux plans. Si le couple machines / utilisateurs est très structurant, les entretiens décrivent une activité distribuée, où entrent en lice des opérateurs multiples, des utilisateurs internes ou externes, des clients et des fournisseurs, des instances de contrôle officielles ou des administrations (Pavard et Karsenty, 1997). Dans les entretiens, la figure de « la direction » ou de la « hiérarchie » émerge rarement positivement. La direction surgit sous la forme de deux contraintes. La première est d'ordre économique : les choix réalisés pour gérer les réseaux et le parc de machines ne doivent pas être « coûteux » ; la seconde renvoie surtout à l'éternel problème de la « reconnaissance au travail » (Jobert, 1998). Comme toute activité qui vise à assurer des routines organisationnelles, la question de la lisibilité du travail est problématique. On ne retient généralement que l'incident ou la défaillance, et on entre en rapport avec le « technicien » que lors de l'émergence d'un problème :

« Tout ça prend du temps. C'est du travail que personne ne voit, et quand je dis 'personne', c'est vraiment personne ! On considère que tout fonctionne, c'est très bien, mais comme je le disais à mon directeur : ' ça je vous l'ai déjà dit - si ça fonctionne bien, ce n'est pas par hasard, c'est parce qu'il y a tout un travail qui se fait, qui est un travail qui se fait dans l'ombre et qui doit se faire'. Et c'est impalpable, on ne peut pas faire sentir cela à un non-spécialiste. » (Admin4)

On ne trouve pas de trace, dans le corpus des entretiens, de moments de crise conduisant à une perte de confiance envers les administrateurs, mais le thème de la méfiance est présent. Un membre de l'équipe de direction (appelons-le Paul) surgit lors d'une discussion avec des informaticiens :

« Paul : dans les boîtes informatiques, quand un responsable système est licencié, il n'entre pas dans la boîte, on l'attend à l'entrée ; le directeur du personnel, un psychologue et le garde de sécurité. Il y a moyen de restreindre des accès mais dans le cas où quelqu'un quitterait une société en mauvais terme avec son patron, je ne sais pas jusqu'où cela pourrait aller. Ça pourrait aller assez loin. On l'accompagne pour aller chercher ses petites affaires dans son bureau mais il n'allume pas un PC. [...]
Admin3 : Monsieur Paul, vous pouvez me foutre à la porte demain. Vous n'allez pas me lobotomiser.
Admin4 : celui qui est vraiment méchant peut prévoir son coup à l'avance aussi.

[11] Sur l' « économie numérique », voir Curien (2000), Brouseau (2000), Brousseau & Curien (2001).

Admin5 : je suis sûr que demain je n'aurai pas oublié le mot de passe administrateur. Et si vous devez passer sur toutes les bécanes, là, vous êtes mal.
Admin3 : On n'est pas en train de flipper toute la journée. On a apporté une solution, pas meilleure qu'une autre. Mais de toute façon, ça ne vous protège pas de la malveillance des co-contractants. De toute façon, et ça, c'est bien connu au niveau de la sécurité, on considère que trois quarts des attaques sur les réseaux sont des attaques venant de l'intérieur. Des gens qui se connectent chez vous via VPN ou via l'intérieur. C'est un danger qui existe. »

Le contexte de cette prise de parole ne permet pas de remonter aux tensions qui se jouaient dans l'institution au moment de l'enquête, mais les acteurs font preuve d'une certaine dureté de ton, même si elle n'est pas dépourvue d'ironie. Ce dialogue fait poindre l'intensité vécue des risques générés par les réseaux, et de l'importance pour les acteurs de ce qu'ils apprennent les uns des autres lors des situations d'alerte ou de crise. La direction peut toujours soupçonner le « responsable système » d'avoir anticipé un conflit et de la tenir potentiellement en otage. A l'anticipation de la direction d'un risque de malveillance, Admin4 rappelle qu'il s'agit d'un pur rapport de force. Le vainqueur sera celui qui saura anticiper les actions de ses (supposés) adversaires. Admin5, à ce jeu, rappelle qu'il détient les clés. Le risque, prévient-il, serait d'occasionner un travail énorme à l'institution, puisqu'il peut facilement nuire à l'ensemble du parc de machines. Dans cet exercice de sociologie du pouvoir au sein de l'entreprise, Admin4 joue un double jeu : d'une part, il dédramatise l'interaction en rappelant que ce genre d'anticipations n'est pas au cœur des priorités quotidiennes et invite la direction à se munir d'outils permettant de pallier ces risques ; mais, d'autre part, il reconnaît ces dangers en rappelant que la malveillance vient très souvent de l'intérieur. Cette dernière intervention souligne les limites du dispositif rappelé par Paul. L'intérieur ne peut être localisé géographiquement puisque les connections via VPN (Virtual Private NetWork), permettent d'agir à distance. L'administrateur informe ainsi la direction de la capacité de nuisance de son personnel et lui suggère de veiller à ne pas se séparer de ses salariés dans de mauvaises conditions. Se trouve aussi épinglée la méconnaissance du travail et des ressources de l'équipe, car le directeur fait montre d'une conception naïve de l'activité des « techniciens ».

V. Des hommes et des ordinateurs

Discuter avec des administrateurs et autres responsables informatiques conduit à plonger dans un univers peuplé de machines et surtout de protocoles. Dans les entretiens, la notion de protocole est centrale : elle sert de pivot entre la description du réseau proprement dit, la référence aux outils logiciels, et l'entrée dans les configurations installées sur les machines. Mais le protocole, comme en droit, s'adresse aussi aux opérateurs humains, il a en quelque sorte force de loi, bien qu'il soit généralement le produit de négociations multiples. Tout comme le nom d'« administrateur » renvoie à la fois à l'agent humain qui administre et au type de droits que lui laisse la machine lorsqu'il est identifié comme « root »[12], le protocole désigne, par extension, la connexion aux périphériques voire les périphériques eux-mêmes. La solidarité des entités du réseau est constamment rappelée par les administrateurs, qui en sont les garants et les porte-parole : l'essentiel consiste dans la répartition de charge. Cette fonction de distribution, qui s'exprime par métonymie, a pour conséquence de faire de la redondance une vertu :

[12] Issu du monde Linux, c'est le nom donné au « super-utilisateur » ayant tous les droits de lecture, d'écriture et d'exécution sur une ou plusieurs machines.

« L'idéal, c'est que le matériel soit redondant, donc qu'il y ait au moins deux fois chaque pièce de l'ensemble. Dans un serveur, par exemple, il n'y a jamais un seul disque ; c'est toujours ce qu'on appelle du RAID [...], c'est au moins trois disques et ces trois disques-là sont montés de telle façon que toutes les données sont en double [...] L'idéal, c'est que ça redirige sur plusieurs machines. C'est ce qu'on appelle la répartition de charge. Donc, on va avoir 10 machines qui font exactement la même chose, qui sont en parallèle, et le répartiteur de charge, lui attribue [...] en tout cas, il va répartir uniformément les demandes sur les 10 machines. » (Admin8)

Doubler, répartir, redistribuer. La « sécurisation » d'un réseau dépend de la manière dont les acteurs organisent la solidarité technique au cœur même de la société des machines. Mais si les ordinateurs jouent le rôle principal, il faut compter aussi avec les utilisateurs. L'association la plus forte qui émerge des entretiens est celle qui relie la référence aux utilisateurs à la mention de « problèmes ». Les administrateurs passent beaucoup de temps à « gérer » les relations humaines médiatisées par les objets. Alors que l'informaticien suspecte un usage peu orthodoxe des machines, dont il se fait le défenseur, l'utilisateur se demande de son côté comment un agent humain peut prendre fait et cause pour des machines sans entendre d'abord sa version des faits. Pour réduire les tensions et assurer la coordination entre les acteurs humains et non-humains (Latour, 1992), l'administrateur a besoin de deux compétences décisives. Savoir trouver l'origine du problème, ce qui renvoie à la logique d'enquête décrite plus haut. La seconde compétence majeure engage une sociologie des types d'utilisateur qui le sollicitent – même si cette sociologie emprunte souvent les traits d'une « psychologie spontanée ».

« Mais en fait tous les problèmes dont on a parlé jusque-là sont des problèmes humains. Après, certains sont débrouillards et d'autres nous appellent à chaque fois sans essayer à résoudre leur problème seul. Dans ces cas là, on sait que c'est facile à résoudre. Quand les personnes débrouillardes nous appellent, on sait que c'est un peu plus compliqué. [...] Les extrêmes d'un côté ou de l'autre ne sont pas bons : la personne qui va trop loin toute seul nous pose des soucis après parce qu'elle aura fait un peu n'importe quoi. La personne qui ne va pas assez loin et qui ne cherche pas à aller plus loin va nous appeler toutes les dix minutes. [...] L'utilisateur idéal est juste au milieu : il se débrouille pour faire ce qu'on lui a déjà montré, il apprend vite et cherche un peu quand même s'il a un nouveau problème, qui ne va pas aller tout casser. Le plus dangereux, c'est celui qui va essayer, qui ne va pas lire les messages d'erreur et tout faire un peu au hasard. » (Admin16)

L'activité de l'administrateur doit ainsi faire converger un travail d'authentification des problèmes informatiques et un travail de représentation des utilisateurs, fondé sur une longue expérience des relations entre machines et usagers.

« Pour remplacer une cartouche de toner, il faut pas être ingénieur. Ici, il y a un service informatique, mais on pourrait imaginer qu'il n'y en ait pas. On ferait appel à un sous-traitant, avec un coût évident. Je ne sais pas si on tolérerait qu'une facture débarque chaque fois qu'il faut remplacer une cartouche d'encre. C'est d'une banalité affligeante !»(Admin11)

En recueillant peu à peu des séries d'anecdotes avec les différents utilisateurs, puis en repérant des régularités qui rendent manifestes compétences et incompétences, degré d'autonomie et propension à la « panique » (comme l'incapacité de changer la cartouche de toner de son imprimante, qui sert souvent de paradigme), les administrateurs parviennent à insérer les relations humaines dans le réseau et à les rendre solidaires des objets techniques. Mais, des changements continus venant affecter les entités du réseau, il leur faut également pouvoir modifier ces relations. Cela passe à la fois par des actes, mineurs mais cependant marquants, de « répression », ou plutôt de « menace de répression » vis-à-vis des manoeuvres « trop téméraires » responsables de désordre dans le système et par des incitations tournées vers ceux qui sont trop distants des machines pour effectuer de manière autonome des opérations élémentaires. Il y a ainsi une dimension pédagogique visant à initier les usagers à une relation juste avec la machine. Essayons d'expliciter ce travail.

VI. Les administrateurs écrivent aux usagers

Une façon de saisir l'évolution des relations entre les administrateurs et les utilisateurs est d'analyser leurs communications. La sémiologie des courriers est fort instructive puisqu'ils engagent à la fois des signes d'intercompréhension des éléments du réseau et des signes d'asymétrie ou de tension entre les entités en présence. Une partie de ces mails collectifs résulte de sollicitations des usagers et peuvent se lire comme une réponse à des demandes exprimées sur des tons variables :

« Une grande partie de nos utilisateurs reçoit de plus en plus de messages venant d'adresses du type "postmaster@quelquechose". Avec la recrudescence de spams et virus, beaucoup de sites ont mis en place des filtres. Or, une catégorie de virus s'attaque de façon détournée à ces filtres. La machine infectée envoie des mails avec des virus en se faisant passer pour quelqu'un d'autre. Ces mails sont rejetés par le filtre du site et renvoyés au "soi disant" expéditeur, en l'occurrence vous, qui n'êtes pour rien. Nous ne pouvons pas rejeter les messages venant d'un postmaster. Le compte postmaster est le compte utilisé par les serveurs de messagerie pour s'envoyer des alertes et signaler les erreurs. C'est un mécanisme indispensable au fonctionnement de la messagerie. Malheureusement on a trouvé le moyen de détourner ce système pour le saboter. La seule solution est la même que nous avions indiqué pour tous les spams. Il faut filtrer à l'arrivée dans machine locale de l'utilisateur (rappel: création d'une boîte à lettres nommée par exemple: postmaster, et puis application d'un filtre aux mails entrants). Nous vous rappelons que nous ne rejetons aucun message (pour ne pas perdre de message). Donc si des messages n'arrivent pas, ce n'est pas notre serveur qui est en cause mais probablement le filtre du serveur destinataire. »

Pour faire face à une série de plaintes d'utilisateurs, qui vont de la colère jusqu'à des propositions de correctifs, notamment dans les filtres, l'administrateur est conduit à expliciter le fonctionnement d'un « postmaster ». Cette explicitation des contraintes d'administration du réseau face aux risques de déstabilisation a pour but de fournir une réponse juste à des demandes techniques (et ainsi d'assurer les utilisateurs les plus critiques que le service informatique connaît bien le processus et le maîtrise), mais aussi de faire découvrir à ceux qui ignorent tout du dispositif, la nature des entités et des processus en cause[13]. Quoi qu'il en soit, il s'agit de rendre visible un travail que bon nombre d'utilisateurs ne soupçonnent pas dans les opérations aussi banales que l'envoi ou la réception d'un mail. L'invitation à agir (créer une boîte aux lettres pour rediriger ce type de spam) responsabilise l'utilisateur en l'associant à la chaîne socio-technique.

Les demandes adressées aux utilisateurs vont de l'invitation, peu contraignante, à prendre conscience du travail accompli, jusqu'à des opérations plus lourdes à réaliser sur la machine. Mais elles posent comme exigence de ne pas contribuer, en les aggravant, aux nuisances engendrées par les pièges que tendent les hackers. La première d'entre elle est la diffusion de hoaxes. Les mises en garde sont toujours pédagogiques mais le ton peut être variable :

« Bonjour à tous !
SURTOUT NE TENEZ AUCUN COMPTE DU MESSAGE ENVOYE PAR XXX il y a qq instants : C'EST UN FAUX APPEL (en fait un appel qui circule depuis plus de 2 ans et qui a peut-être été vrai il y a deux ans mais qui ne l'est plus). Ce genre de message est dans la quasi-totalité des cas un "HOAX". Pour le vérifier il y a un site très bien informé : http://www.hoaxbuster.com.
Cordialement. »

[13] Un mail du même administrateur se terminait ainsi : « J'espère que ces explications satisferont les inquiets et, pourquoi pas, les moins inquiets mais néanmoins curieux. ».

L'autre danger est l'encombrement du serveur par les fichiers des utilisateurs. La « faute » ici est plus difficilement imputable à la méconnaissance de l'utilisateur puisqu'il s'est engagé via un contrat (l'échange des identifiants de son compte et d'une signature de la charte informatique). Tout en rappelant la nature du danger, on parle de sanction. La forme de ces messages est souvent identique. On mobilise un problème ou plusieurs précédents (ce qui justifie le message), on montre le danger en annonçant une saturation du serveur, on énonce une solution (utiliser le serveur de liste), voire une sanction possible.

« Bonjour à tous !
NOUS RAPPELONS QU'IL EST FORMELLEMENT DECONSEILLE (sans litote DISONS INTERDIT) D'ENVOYER DES DOCUMENTS ATTACHES dans les listes de distribution en particulier [NOM de la liste].
Un gros document vient d'être envoyé qui pourrait entraîner, pendant le week-end, la saturation de l'espace disque du serveur provoquant son arrêt pur et simple.
Nous rappelons qu'il existe un espace Documents sur le serveur de liste destiné à cet usage et qui évite les envois inutiles et encombrant.
Toute entorse à cette règle exposerait son responsable à l'interdiction d'accès à [NOM de la liste].
Cordialement. »

Le cauchemar des administrateurs reste néanmoins le cas du virus qui contamine l'ensemble du parc de machines. Le message est alors organisé comme un signal d'alarme de façon à attirer l'attention des utilisateurs, et les conduire à sonder l'état des milieux et des dispositifs qui sous-tendent les routines. Pour cela il faut non seulement nommer le danger et en montrer sa portée, mais aussi solliciter l'utilisateur. Car, si les administrateurs gardent l'initiative de l'enquête et de l'intervention, ils ont besoin des usagers. On peut alors recourir à une forme d'hyperbole (« un virus d'une extrême dangerosité ») ou convoquer un organisme faisant autorité :

« Bonjour à tous !
Une nouvelle offensive MASSIVE et encore plus rapide que les mises à jour d'antivirus est partie hier. Il y a donc des mails infectés qui sont arrivés jusqu'à certain d'entre vous. Normalement ils devraient être bloqués maintenant, mais, étant donné la fréquence avec laquelle les virus se renouvèlent en se moment, il y a lieu d'être quasiment paranoïaque. »

« Re bonjour à tous !
L'organisme spécialisé CERTA (http://www.certa.ssi.gouv.fr/) nous signale une attaque importante de "chevaux de Troie" sur des réseaux gouvernementaux britanniques. »

Il s'agit ensuite de donner des « prises » (Bessy et Chateauraynaud, 1995) pour authentifier l'agresseur : cela revient à fournir des indices et des signes suffisamment perceptibles pour que tous les utilisateurs puissent reconnaître les marques du danger.

« Un nouveau virus vient de voir le jour, mais il est un peu particulier. Il se propage par mail, mais au lieu d'envoyer une pièce attachée (que vous prenez soin de ne pas ouvrir habituellement), le message contient un lien vers un site web qui vous parait utile. [...] Nous rappelons que sur PC Windows nous déconseillons d'utiliser Internet Explorer, utilisez plutôt Firefox ou Mozilla moins sujet à ce type de vulnérabilités ce qui se justifie encore plus aujourd'hui. »

A plusieurs reprises, on trouve, en conclusion des messages, l'injonction : « Vigilance ! » (Roux, 2006). La demande de vigilance fait pleinement partie de l'enrôlement des utilisateurs. Ceux-ci sont appelés à prendre soin de leurs machines, à utiliser les logiciels préférés des administrateurs (FireFox et Mozilla plutôt qu'Internet Explorer) et à exercer un sens critique sur tout événement qui pourrait surgir. Lorsque les règles de conduite préexistent, la vigilance repose sur un système de signes et de codes dans lequel chaque événement ou chaque micro-variation doit trouver sa place : rien de ce qui est retenu comme pertinent par les concepteurs

du système ne doit se dérober à la surveillance. On sait que cette conception fonctionnaliste de la vigilance est facilement mise en échec, a fortiori dans un monde en réseau soumis à des reconfigurations et des déplacements continus. Tout dispositif présente des failles, des points aveugles, pointe sur des milieux plus ou moins étendus, mouvants, silencieux, se laisse travailler par des micro-transformations ou des altérations encore imperceptibles. On en appelle alors à un surplus d'attention et de vigilance de la part des agents ou des opérateurs humains, on invite à relever les « signaux faibles ». C'est parce que l'on ne sait pas ce qui peut réellement se passer que l'on entre en vigilance. On passe ainsi de la vigilance comme simple mot d'ordre à la veille, comme forme de présence et de participation active aux processus (Varela, 1993). En tant qu'activité collective, la vigilance est une médiation décisive entre les expériences et les représentations – le réseau étant vécu comme un étrange mélange de proximité et de distance, de contact et de représentation. Tout appel à la vigilance engage ainsi la question de ce qui compose le monde et des différentes manières de s'y engager.

VII. Conclusion

D'un côté on a des agents dont le degré de compétence se mesure pratiquement à leur degré d'invisibilité : moins on les voit, moins on entend parler d'eux et plus on est enclin à penser que les réseaux fonctionnent tout seul. De l'autre, on voit se multiplier les annonces, les dispositions, les alertes et les rumeurs qui développent le thème de l'ultra-vulnérabilité de la société de l'information. Le rapport entre les deux plans s'éclaire dès lors que l'on décrit les arènes et les moments d'épreuve dans lesquels les acteurs sont amenés à discuter des problèmes de sécurité informatique, à en faire des objets collectifs. Entre l'invisibilité sociale d'un groupe professionnel dont les acteurs n'émergent le plus souvent qu'en cas de conflit et via des porte-parole, et les montées en généralité sur la sécurité, la cybersurveillance et les enjeux de la société de l'information à l'échelle planétaire (Beck, 2005), on peut rendre lisibles les processus qui font tenir les artefacts collectifs.

Un des diagnostics souvent porté par les administrateurs eux-mêmes sur leur milieu est le haut niveau d'individualisme : si les échanges sont continus au plan technique sur les multiples plateformes collectives, les carrières et les jeux organisationnels sont traités comme des aspects personnels et secrets. Une grève générale des administrateurs-réseaux serait-elle envisageable ? Dans les analyses du travail, la grève a joué un triple rôle : rendre tangible le caractère névralgique de métiers ou d'activités que l'on tend à oublier dans le fonctionnement ordinaire ; faire émerger des entités collectives et des mots d'ordre qui produisent des effets dans d'autres secteurs, en vertu de leur exemplarité ; contraindre les autres acteurs à s'intéresser à des activités qui restaient inaperçues. A l'exception de quelques cas de reprises ou de fusions d'entreprises de la nouvelle économie – comme le conflit ibazar/ebay – qui ont produit des grèves de l'ensemble des salariés, on n'a pas vu de cas de figure explicitement centré sur les administrateurs[14]. On lit dans de multiples interventions liées à des conflits dans les SSII des formules qui témoignent, parfois de manière critique, du haut degré d'individualisme de ces professions De fait, les associations professionnelles n'ont pas donné lieu à une structuration forte comme dans d'autres secteurs d'activité.

Les administrateurs interrogés s'efforcent d'associer les utilisateurs à la chaîne socio-technique. Cet enrôlement présente deux types d'avantage : d'une part, en incluant les usagers dans le réseau technique, l'activité de l'administrateur a plus de chance d'être lisible et reconnue. D'autre part, l'administrateur sollicite, a minima, un sens de la responsabilité vis-à-vis du dispositif. En rendant manifeste sa métastabilité, il éloigne les protagonistes d'une approche féérique dotant la forme « réseau » d'une puissance immanente. La communication continue et coopérative, rend plus difficile un rapport magique au « réseau » lequel évoluerait indépendamment des actions des personnes. Rappelant les menaces permanentes qui pèsent sur lui, l'administrateur fait partager les préoccupations des techniciens voire leur attachement aux machines. Au fond, ce travail continu montre la dimension politique du travail technique : déléguer les tâches, étendre le réseau, associer les utilisateurs pour qu'ils soient engagés dans son bon fonctionnement. Si les objets soutiennent les acteurs humains (Latour, 1992), c'est parce que des acteurs humains les soutiennent de manière continue : la maintenance et la vigilance en matière technique est la première boucle à prendre en compte pour saisir le fonctionnement des étages supérieurs, et surtout des derniers étages formés par la splendide « société de l'information », sur laquelle repose elle-même la non moins fameuse « économie de la connaissance ».

[14] Début 2005, plus de trois cents informaticiens ont fait grève pendant trois semaines chez Schneider Electric à Grenoble pour protester contre les conditions de leur transfert chez Capgemini... Voir *01 Réseaux*, le 01/02/2005

Note méthodologique

Cet article est issu d'une étude réalisée dans le cadre du programme Société de l'information (Chateauraynaud et Trabal, 2006). Les exemples sont issus d'un corpus de documents provenant de rapports, de listes électroniques, de revues ou d'articles de presse, et d'entretiens auprès de 19 administrateurs. Afin de disposer d'un espace de variation suffisant, on a choisi des personnes engagées dans des organisations différentes : associations, entreprises et institutions. On s'est efforcé de garantir un anonymat absolu aux personnes et aux organisations étudiées. Une des opérations importantes de cette enquête a consisté à rassembler et analyser un corpus de courriers et d'échanges électroniques, de façon à bien saisir la production écrite des administrateurs et leurs modes d'entrée en relation avec les utilisateurs[15].

[15] Il s'agit à proprement parler d'étudier des « écrits de travail » (Borzeix et Fraenkel, 2001).

Bibliographie

AULDS (C.), *Apache 2.0 : guide de l'administrateur*, Paris, Eyrolles 2003

AURAY (N.), *Politique de l'informatique et de l'information. Les pionniers de la nouvelle frontière électronique*, Thèse de sociologie (Dir. Laurent Thévenot), EHESS, Paris, 589 p., 2000

BECK U., *Qu'est-ce que le cosmopolitisme ?*, Paris, Aubier, 2006.

BERLEUR (J.), Éthique et régulations dans la société de l'information, in *Ethique publique ; Revue internationale d'éthique sociétale et gouvernementale*, Numéro spécial « Les enjeux éthiques de la gestion de l'information », Montréal (Canada), Editions Liber, **6**, n° 2, pp. 69-79, Automne 2004.

BIDET (A.) , et alii (dir), *Sociologie du travail et activité*, Toulouse, Octares, 2006.

BOLTANSKI (L.) et CHIAPELLO (E.), Le Nouvel Esprit du Capitalisme, Paris, Gallimard, 1999.

BORZEIX (A.) et FRAENKEL (B.), dir., *Langage et travail. Communication, cognition, action*, Paris, CNRS-Editions, 2001.

BROOKSBANK (E.), *Samba, le guide de l'administrateur*, Paris, OEM, 2000

BROUSSEAU (E.) et CURIEN (N.), Economie d'Internet, Economie numérique, in Economie d'Internet, *Revue Economique*, Numéro Spécial, octobre 2001.

BROUSSEAU E., What Institutions to Organize Electronic Commerce: Private Institutions and the Organization of Markets, *Economics of Innovation and New Technology*, **9**, n°3, pp. 245-273, July-September, 2000,

CHATEAURAYNAUD (F.) et TRABAL (P.) (dir), *Internet à l'épreuve de la critique. Rumeurs, alertes et controverses au cœur des nouvelles technologies,* GSPR, Programme "Société de l'information", CNRS, novembre 2003.

CHATEAURAYNAUD (F.) et TRABAL (P.), *Internet à l'épreuve de la critique. L'expression des situations critiques dans l'administration ordinaire des réseaux*, Rapport pour le programme Société de l'information du CNRS, GSPR-EHESS, 140p février 2006.

CHATEAURAYNAUD (F.), et TORNY (D.), *Les sombres précurseurs : une sociologie pragmatique de l'alerte et du risque*, Paris, Editions de l'EHESS, 1999.

CHATEAURAYNAUD (F.), *Les asymétries de prise. Des formes de pouvoir dans un monde en réseau*, document du GSPR, EHESS, 2006.

CHATEAURAYNAUD (F.), *Nanosciences et technoprophéties. Le nanomonde dans la matrice des futurs,* document de travail, Paris, EHESS, 2005

CHAUVIRE (C.), Aux sources de la théorie de l'enquête. La logique de l'abduction chez Peirce, *La croyance et l'enquête, Raisons pratiques*, Paris, Ed de l'EHESS, **15**, p. 55-84, 2004

CURIEN (N.), *L'économie des réseaux*, La Découverte, Coll. Repères, Paris, 2000 ;

DEWEY (J.), *Logique. La théorie de l'enquête*, Paris, PUF, 1985.

DODIER (N.), *Les Hommes et les machines*, Paris, Métailié, 1995.

DUPUY (J.-P.), Pour une évaluation normative du programme nanotechnologique, *Annales des Mines*, février 2004.

HUBAUD (F.) (dir), *Le stable, l'instable et le changement dans le travail*, Toulouse, Octares, 2006.

JOBERT (G.), *La compétence à vivre. Contribution à une anthropologie de la reconnaissance au travail*, Tours, Université François Ralelais, Mémoire pour l'habilitation à diriger des recherches, 1998.

KASPERSON (R. E.) et KASPERSON (J. X.), The Social Amplification and Attenuation of Risk, *Annals of the American Academy of Political and Social Science*, **545**, p. 95-105, May 1996.
KEFI H. et KALIKA (M.), *Evaluation des systèmes d'information : une perspective organisationnelle*, Paris, Economica, 2004.
LACROIX (P.), *Webmaster*, Paris, Dunod, 2003.
LATOUR (B.), *Aramis ou l'amour des techniques*, Paris, la Découverte, 1992.
LINLAUD (D.), *Sécurité de l'information : élaboration et gestion de la politique de l'entreprise suivant l'ISO 17799*, Paris, Afnor, 2003
MERCIER (D.), 2001 Heurts et malheurs de la certification dans des centres de tri de La poste, in MAUGERI, (S.), dir., *Délit de gestion*, Paris : La Dispute, pp. 31-50.
Murielle-Isabelle CAHEN (M. I.), Responsabilité civile des fournisseurs d'accès, http://www.devparadise.com/technoweb/droit/a138.php, 2005 :
PAVARD (B.) et KARSENTY (L.), Différents niveaux d'analyse du contexte dans l'étude ergonomique du travail collectif, *Réseaux*, **85**, pp. 73-100, 1997.
PROULX (S.), MASSIT-FOLLEA (F.) et CONEIN (B.), *Internet : une utopie limitée. Nouvelles régulations, nouvelles solidarités*, Presses de l'Université de Laval, 2005.
ROUX (J.), *Etre vigilant. L'opérativité discrète de la société du risque*, Publications de l'Université de Saint-Etienne, 2006.
STANFIELD (V.) et SMITH (R.W.), *Linux guide de l'administrateur*, Paris, Eyrolles ; 2003
VARELA (F.), ROSCH (E.) et THOMPSON (E.), *L'Inscription corporelle de l'esprit*. Paris, Seuil, 1993.
VAUGHAN (D.), Rational Choice, Situated Action and the Social Control of Organization, *Law & Society Review*, **32**, p. 23-61, 1998.
ZARIFIAN P., Travail, langage et civilité, *Multitudes*, septembre 1997.