CONTAGION, DÉBORDEMENT ET SAIGNÉE DANS LE CYBERSPACE

LE 10 MAI 2010 ***YANN LEROUX***

Trois figures communes sont à l'œuvre dans différentes régions de l'Internet ou dans différents dispositifs. Elles forment un système cohérent, autour de la référence au corps.

Dans l'espace Internet, quatre caractéristiques – le temps subverti, l'espace aboli, la pluralité et la trace – organisent les représentations que l'on se fait du réseau, selon que l'on mette l'accent sur l'une ou l'autre d'entre elles ou encore sur certaines combinaisons. Ainsi, la représentation du réseau en termes de rapidité et d'efficacité s'appuie sur les caractéristiques spatio-temporelles telles que nous venons de les décrire tandis que celle qui présente Internet comme un lieu d'échange et de rencontre renvoie plutôt à la pluralité.

Cette grille de lecture permet de dégager quelques processus qui se déploient sur Internet et dont certains prennent forme de figures du réseau. On a tout intérêt à prendre ici le terme dans toute sa gamme polysémique, c'est-à-dire, comme le propose Elias Sanbar qu'il s'agit « *tout à la fois d'une physionomie, d'un visage aux traits changeants et pourtant reconnaissables, d'un timbre de voix, du portrait et de la silhouette, d'une configuration du monde telle celle des cartes géographiques dites « figures de la terre », d'une structure géométrique, d'une chorégraphie, figures de dans, à un moment précis sur la scène d'un pays, d'une typologie (figure du révolté, figure du réfugié) de symboles enfin, figures de style ou de rhétorique* »[1] Ces figures sont pour le réseau tout à la fois des visages (des représentants), des ébauches (comme simplification et comme juste -presque ?- né), et des mouvements. Cela permet de saisir des parentés et des similitudes qui apparaissent difficilement par ailleurs et de voir ainsi des processus commun à l'œuvre dans différentes régions de l'Internet ou dans différents dispositifs. Trois figures peuvent être isolées : la contagion, le débordement, la saignée.

1. La contagion

Le processus infectieux donne lieu aux grandes figures de l'Internet qui comprend **les différents virus qui englobent toute une famille de « malfaisants »** qui va des programmes informatiques causant des dommages plus ou moins grand aux trolls (eGroupes) et autres campeurs (jeux vidéos) qui hantent l'Internet.

1982 voit une grande innovation en informatique : Elk cloner, premier virus se disséminant de façon incontrôlée. Jusque là, quelques virus avaient été programmés à des fin d'observation et d'étude. Elk cloner se propage en infectant le système d'exploitation d'Apple II enregistré sur disquette. À chaque démarrage avec une disquette infectée, une copie du virus est activée et se loge en mémoire vive. Il contamine alors toute disquette saine introduite dans le lecteur de disquette, et se propage ainsi de machine à machine. Telle est en effet la grande nouveauté d'Elk cloner : sortir d'un pré carré de machines et aller comme à l'aventure. Tous les cinquante démarrages, il signale sa présence par un petit texte[2]

Ce premier virus est une sorte d'épure d'un fait dont l'auteur du programme, Nick Skrenta, 15 ans à l'époque, était coutumier. Il donnait à ses amis des jeux piratés, qu'il avait pris soin de modifier afin qu'au bout d'un certain temps ils ne puissent être utilisés. Les bénéficiaires du cadeau avaient ainsi la joie de recevoir un jeu, et, lorsqu'ils avaient joué suffisamment pour être attaché a ce jeu, le désappointement de ne plus le voir fonctionner, non sans que le généreux donateur ne se soit rappelé à leur souvenir par un dernier message « humoristique ». Les amis de Skrenka auraient appris à ne jamais le laisser approcher de leurs ordinateurs, et Elk cloner aurait été pour lui une façon de contourner ce dispositif défensif.

On a là tous les ingrédients de ce que l'on va ensuite appeler les malwares *(***mal**icious soft**ware**) : **l'appât, et puis dans un second temps, la désillusion qui peut prendre des allures de sévère punition, l'objet caché, le désir de nuire**[3].**[3]** Voir aussi le mythe du

cadeau empoisonné avec Pandore.

On désigne sous le nom de *malware* tout programme ayant pour but de nuire à un système informatique en en prenant le contrôle sans le consentement de son opérateur ou sans même qu'il ne s'en aperçoive ; la gêne occasionnée est variable, et le spectre d'action des *malwares* va de la gêne bénigne aux dommages irrécupérables. Les *malwares* peuvent prendre la forme de virus, de ver, d'un cheval de Troie ou d'une porte dérobée.

Un **virus** est un programme qui est activé lorsque l'utilisateur ouvre un programme contaminé. Le virus se répand alors dans le système informatique en attachant des copies de lui-même à des fichiers ou à des unités de stockage. Le virus ne peut contaminer que les fichiers contenant des instructions programmables. Avec le développement de l'Internet, les virus ont trouvé dans le mail un hôte de choix. Ils se présentent alors sous la forme d'un mail tentant de persuader le destinataire d'ouvrir le fichier joint qu'il contient, lequel est bien entendu infecté.

Comme le virus, l**e ver** à la capacité de s'auto-répliquer mais contrairement à ce dernier, il n'a pas besoin d'être contenu dans un fichier. Plus exactement, c'est le système informatique infecté dans son entier qui devient son hôte. Le ver est également capable d'effacer des fichiers, d'envoyer des e-mails, d'installer des portes dérobées (Sobig, Mydoom) transformant alors la machine infectée en zombie qui pourra être utilisée par les spammers pour envoyer leur pourriel ou pour masquer leur adresse I.P. Le premier ver a été programmé par le Xerox PARC en 1978. Le nom viendrait du fait que le ver est, comme son équivalent dans le monde animal, composé de « segments » qui s'exécutent sur des machines différentes. Mais comme toujours sur Internet, on trouve des liens avec le monde de la science-fiction ou de l'heroïc fantasy. Le terme avait déjà été utilisé par John Brunner en 1975 dans son roman *The shockwave rider* et décrivait alors un programme informatique qui se répand seul à travers un réseau informatique. Le programme est activé alors que le héros est prisonnier et ne peut donc physiquement plus rien faire. Il sert à la manifestation de la vérité en rendant public sur le réseau les malversations du gouvernement (expérimentations génétiques illégales donnant naissance à des enfants monstrueux, corruption etc.) : toute personne concernée par un crime gouvernemental se voit recevoir un e-mail l'informant sur les crimes dont elle est l'objet. Ainsi, **le ver se donne comme envers de l'endoctrinement : l'endoctrinement se fait aux yeux de tous ; le ver a une action souterraine.** L'endoctrinement cache quelque chose ; le ver révèle. L'endoctrinement est massif ; le ver diffuse des messages hautement individualisés. L'endoctrinement est un trompe l'œil ; le vers est plein de sens.

Le roman de John Brunner reprend des éléments de la thèse développés par le sociologue Alvin Toffler en 1970 dans *Future Shock* : il tentait d'y montrer que la société industrielle était en train d'évoluer à une vitesse telle que les individus étaient submergés par les changements technologiques et sociaux. Trop de changements en trop peu de temps confronterait à une sorte de stress temporel (« future shock ») dont les effets seraient visibles dans la majorité des problèmes sociaux.

Sur Internet, le premier ver a attirer l'attention fut Morris, le 2 novembre 1998, écrit par Robert Tappan Morris alors qu'il était encore étudiant, ce qui lui valut une condamnation à trois

années de probation, quatre cent heures de travaux communautaires et une amende de plus de dix mille dollars. Morris eut un effet dévastateur sur Internet, à la fois du fait des pannes réelles qu'il a provoqué en surchargeant le fonctionnement des machines, et du fait de l'effet de panique, sans doute excessif, qu'il a provoqué. Morris est aussi connu sous le nom de Great Worm [Grand Dragon] de Tolkien : Glaurun et Scatha.

Un **Cheval de Troie** est un programme se présentant sous une apparence légitime mais exécutant lors de son installation des tâches à l'insu de l'utilisateur. Le plus souvent, le cheval de Troie installe d'autres programmes ayant pour fonction d'espionner l'utilisateur (*spywares*, *keyloogers*) de lui imposer des publicités (adwares). Le cheval de Troie peut également ouvrir des portes dérobées (*backdoors*) permettant à l'émetteur de prendre le contrôle de tout ou d'une partie du système informatique. La motivation est financière, voir frauduleuse, lorsqu'il s'agit de programme permettant de récolter les numéros de carte bancaire (*keyloggers*) ou encore de transformer la machine cible en en un zombie-PC pour un envoi massif de *spams*. Contrairement aux virus et aux vers, le cheval de Troie ne peut se dupliquer lui-même.

La référence à la guerre de Troie est explicite : celui qui laisse entrer en son sein un objet sans s'être préalablement assuré de son innocuité se met en péril ; **tout n'est pas incorporable impunément. On quitte là les métaphores biologiques pour la cité comme lieu à défendre contre un extérieur potentiellement menaçant.** Il est amusant de noter que Laocoon, qui averti les troyens par son fameux « *timeo Danos, et dona ferentes* »[4], sera dévoré, ainsi que sa progéniture, par deux énormes serpents.

Virus, vers, trojans, mettent en jeu **une image du corps qui est agie dans les différentes mesures de protection ou de désinfections que prend l'utilisateur** : l'endiguement, le tri de ce que l'on peut accepter ou pas, la limite mise entre un « dedans sain » et un « dehors contaminé », brûlant, même si l'on en croit l'existence de « pare-feux ». Il s'agit dans tous les cas de maintenir son unité face à une multitude dont le contact peut être dangereux. Cette image du corps peut renvoyer. Maintenance, contenance, pare-excitation : on retrouve là les grandes fonctions du Moi-peau. **Non pas que les systèmes informatiques aient un psychisme. Mais simplement du fait que ceux qui les conçoivent et les utilisent les investissent comme des prolongements de leur propre corps.** Et cette tendance est d'autant plus forte que les mondes numériques manquent cruellement de chair.

Au-delà du simple aspect sadique dont sont chargés ces différents *malwares,* ils ont pour effet de marquer différents territoires dans un espace qui se donne pourtant comme sans limites. Du côté de l'utilisateur, les dispositifs mis en place délimitent, comme nous l'avons vu, une zone différente de tout le cyberspace et dans laquelle il peut travailler et interagir normalement avec les autres. Du coté de l'auteur du virus, à partir du moment où celui-ci est lâché dans le cyberspace, l'espace contaminé porte sa marque ; chaque poste contaminé contient une partie de lui et plus la pandémie est grande, plus grand est le territoire qui porte sa signature. On peut faire, je pense, le parallèle avec les *tags* qui couvent avec plus ou moins de bonheur les façades de nos bâtiments et, plus loin, avec les différents types de marquage du corps qui sont réapparus dans notre culture ces vingt dernières années. **Les *malwares* réintroduisent le corps via la problématique du toucher : il y a des objets dont le contact peut être dangereux** ; chaque machine contaminée avoue ne pas avoir fait de la plus élémentaire prudence dans ses contacts avec d'autres machines[5]. Une des motivations des programmeurs de virus s'ancre, me semble-t-il dans ce fantasme de pouvoir suivre les contacts des uns avec les autres et *in fine* d'être de toutes les scènes primitives.

Il nous faut encore remarquer que **le ver était dans le fruit pour ainsi dire dès le départ** : sur l'Internet, les communications entre les machines se font d' « hôte » à « invité ». Cela laisse clairement entendre que d'autres peuvent être malvenus, et d'autre part que l' « invité » est toujours susceptible de se dégrader en commensal puis en parasite.

2. Le débordement

Il s'agit là d'une figure que l'on retrouve dans différents dispositifs sur Internet. Pour une part, elle est une conséquence de la contagion : **elle dit à la fois le pullulement des virus qui se multiplient dans le cyberspace** – c'est la peste qu'il faut contenir hors les murs -, ou dans un site donné – c'est alors le débordement des capacités de calcul de la machine. Mais **c'est aussi le débordement de la capacité de liaison de tout un eGroupe lorsqu'il est attaqué par un troll**. Une des technique du troll est de faire exploser chaque message en une multitude de questions sans jamais prendre en considération aucune des réponses qui lui est faite, si ce n'est pour à nouveau les faire exploser en une nouvelle multitude de questions. C'est aussi la saturation d'une session de chat lorsque quelqu'un poste de façon répétitive le même message. C'est enfin une tactique de combat qui est utilisée dans les jeux multijoueurs : un camp submerge un autre en utilisant des unités dont la faible valeur est

contrebalancé par leur grand nombre. Cette tactique a pris le nom de *zerg* (ou *zerging*) du nom d'une race d'insectoïdes sur le jeu Starcraft, les Zergs, qui étaient très utilisés pour cette tactique.

3. La saignée

Stricto sensu, la saignée désigne le fait qu'un site puisse héberger en son sein les pages d'un autre site, sans que celui-ci en soit averti. Ce qui est en jeu, c'est moins le motif de l'inclusion, que l'exploitation d'un site par un autre qui voit alors son trafic s'appauvrir. Cette représentation d'un contenu qui s'échappe, se vide, parfois au profit d'un autre, se retrouve aussi dans le peer-to-peer et désigne le téléchargement sans réciprocité, ce qui au final met à mal le réseau concerné et peut même conduire à sa disparition. On la retrouve dans les jeux vidéos ou le *leeching* désigne alors le fait pour un joueur de bénéficier des efforts d'un groupe sans contribuer. Dans les jeux vidéo, le *leeching* désigne les joueurs qui bénéficient personnellement des efforts d'un groupe mais qui ne participe pas à l'effort commun. Dans tous les cas, **il s'agit de situations ou l'on reçoit sans donner, c'est-à-dire de situations où la réciprocité si chère à Internet est mise à mal.**

À chacune des déclinaisons de ces figures, des dispositifs défensifs ont été inventés : pour le chat, une *temporisation* peut être mise en place pour éviter la répétition stérilisante du même. Pour le troll, l'exclusion ou la censure peuvent parfois être mises en place ou encore le groupe peut être organisé de façon à ce que le troll ait moins de prise.

Il y a une remarquable cohérence de **ces différentes figures, qui se répondent l'une l'autre et qui se recouvrent partiellement**. L'unité en est donnée par la référence à l'image du corps. C'est ainsi que la contagion campe l'attaque d'un par une multitude et que les fantasmes qui accompagnent cette représentation sont ceux de pénétration violente, d'usurpation d'identité, de perte hémorragique de son contenu, de perte de la capacité à recevoir. Les virus mettent en scène un toucher corrompu/corrompant, les *backdoors* l'entrée interdite, non sue, les *trojans* un corps ville forte mais toujours soumis au risque de la séduction et les vers le mauvais en soi que l'on est susceptible d'héberger à son corps défendant. À cela, la réponse défensive est la création d'une barrière radicale entre le système informatique de l'utilisateur et le cyberspace ou encore l'utilisation curative d'agents de désinfection. La *saignée* fait intervenir les fantasmes de vol des contenus, d'anémie et finalement de vampirisation tandis que le *débordement* renvoie à la saturation d'un espace rendant problématique voire impossible toute inscription ou encore au débordement de ses propres capacités.

//

Elias SANBAR, Figures du Palestinien. NRF essais. Gallimard. p 15 [↩]
Elk Cloner: The program with a personality.It will get on all your disks / It will infiltrate your chips / Yes it's Cloner! / It will stick to you like glue / It will modify ram too / Send in the Cloner! [↩]
Précisons, pour la petite histoire, que Richard Skrenta saura rester pionner sans utiliser sa créativité de façon moins agressive. Il participera à *VMS monster*, un des premiers Multi User Dongeon. *VMS monster* inspirera le célèbre TinyMud [↩]
« Je crains les grecs, même lorsqu'ils offrent des présents » [↩]
Une des motivations des programmeurs de virus s'ancre, me semble-t-il dans ce fantasme de pouvoir suivre les contacts des uns avec les autres et *in fine* d'être de toutes les scènes primitives. [↩]
—

Billet initialement publié sur **Psy et geek ;-)** sous le titre "Trois processus du cyberespace: la contagion, le débordement et la saignée"

Image CC Flickr **Sterin**et **Quiplash!**

1 ping

Les tweets qui mentionnent Contagion, débordement et saignée dans le cyberspace » Article » owni.fr, digital journalism -- Topsy.com le 10 mai 2010 - 10:51

[...] Ce billet était mentionné sur Twitter par Aurélien Fache, Owni, Samuel Dixneuf, Frédéric DEBAILLEUL, Flash Presse et des autres. Flash Presse a dit: Contagion, débordement et saignée dans le cyberspace http://goo.gl/fb/Dbfqt [...]