PRODUCTION DU COMMUN, RESEAUX ET BIO-HYPERMEDIA : MENACES ET OPPORTUNITES

Andrée Steidel et Giorgio Griziotti

Intervention au séminaire « Du public au commun », Paris le 11 mai 2011

Les mouvements qui secouent une vaste partie du monde, de la Méditerranée au Moyen Orient, et jusqu'au Royaume Uni, et agitent périodiquement l'Europe sous la poussée d'une jeune génération qui refuse les coupes budgétaires, mettent en lumière des phénomènes nouveaux.
Ces mouvements, et les luttes qu'ils expriment, sont ici considérés comme une forme de production du commun. Celle-ci s'appuie et exploite les ressources d'un outil global centré sur les NTIC (Nouvelles Technologies de l'Information et Communication) constitué par l'univers des réseaux et des dispositifs de production immatérielle.
Dans ces lieux et par ces outils se joue aujourd'hui la bataille en cours entre gouvernances financiarisées et multitudes connectées.
Une bataille dont l'issue est en équilibre fragile entre d'une part ***les menaces*** de captation et de contrôle qui peuvent s'exercer à travers cet univers de réseaux, et d'autre part ***les opportunités*** innombrables d'en utiliser la puissance pour construire un nouveau commun.

L'évolution quasi exponentielle de ces outils tant par leurs fonctions que par leur pénétration dans des populations de plus en plus vaste en fait un vecteur d'une croissance considérable et difficilement mesurable à la fois d'usages et de décloisonnement.

Nous souhaitons, par la présentation d'aujourd'hui apporter notre contribution à la compréhension de ces phénomènes, en montrant à la fois les opportunités et les menaces dont sont porteurs les réseaux et les contenus qu'ils permettent de diffuser. Nous nous efforcerons d'éviter un inventaire fonctionnel ou technique en nous concentrant sur les usages et leurs effets.

LA « GENERATION HACKTIVISTES »

Avec la fin de la restriction de la maîtrise technologique aux technocrates, il apparaît qu'une génération de « digital natives » s'empare du potentiel du net pour créer des nouvelles formes de démocratie.
Cette maîtrise technologique se concentre auprès des Hackers et c'est partant d'eux que se diffuse la pratique des Hacktivistes (les hackers activistes ou médiactivistes d'Internet).
Ce qui est nouveau et qui semble extraordinaire c'est la quasi simultanéité de ce mouvement tant dans les pays émergeants que dans le monde industrialisé, mais nous verrons plus loin que cela est moins surprenant dans notre analyse de l'internet mobile.

L'exemple Tunisien : les media et même les témoignages de participants aux événements Tunisiens, qui ont eu lieu récemment en un *séminaire parallèle*, nous ont fait prendre conscience que la révolution populaire née d'un mouvement sans leaders et sans avant-gardes organisés n'aurait pas pu voir le jour sans l'existence d'une génération de « hacktivistes » et de jeunes qui disposent d'une façon diffuse et répandue de compétences leur permettant d'impulser un contre-pouvoir réel sur la toile.

Les années de restriction de la liberté en Tunisie, comme dans d'autres dictatures, ont constitué le ferment au contournement par les populations des moyens de la censure et à l'appropriation, voire au détournement des outils. Par ailleurs, les pays du sud ont vu une pénétration très forte des réseaux mobiles et internet, lesquels sont de mieux en mieux maîtrisés par une population jeune, formée et diplômée : les éléments étaient donc réunis pour que des actions ponctuelles qui apparaissaient comme des défis vis-à-vis du pouvoir se cristallisent le moment venu en un véritable levier de contre-pouvoir.

Et ce moment est venu, lors de la mort d'un jeune chômeur à Sidi-Bouzid, où l'usage tant des téléphones mobiles que des réseaux sociaux, a été le vecteur de la diffusion et de la circulation de l'information incitant aux actions de protestation contre le pouvoir. Celui-ci n'a pas tardé à s'infiltrer dans les réseaux sociaux pour y espionner les comptes des utilisateurs FACEBOOK notamment. Action rapidement identifiée par les hacktivistes, aussitôt sont apparues immédiatement en riposte des instructions pour se protéger de ces attaques policières.

Dans les pays industrialisés, les hacktivistes en se battant contre le Copyright et du feu DRM (Digital Right Management) ont contraint les Multinationale de l'*Entertainement* et les gouvernances locales à reculer dans le contrôle et l'extraction de profit via les droits d'auteur. Il n'a pas servi à grand-chose qu'en France et dans d'autres pays on tente de mettre en place des dispositifs de contrôle complexes, inefficaces, et souvent obsolètes au moment même de leur mise en fonction. Il en est ainsi d'HADOPI !
Comme dans les deux situations évoquées partout les hacktivistes contribuent à la production commune du Net et du freeware, et ainsi à celle des nouvelles formes de démocratie.

Lieu d'expression du contre-pouvoir, perpétuellement surveillé par les pouvoirs et les opérateurs qui l'exploitent, le « net » devient le primo terrain où se jouent les batailles qui se déplacent ensuite sur le terrain réel de la cité.
Protection et intrusion, captation, ou destruction : maîtriser et perfectionner les outils qui permettent ces opérations constitue un enjeu où la compétition se déroule entre les multitudes et les instances de la gouvernance financiarisée : Corporates, Institutions financières internationales, gouvernements nationaux et à leurs incontournables produits dérivés les corporations mafieuses, intégrismes extrémistes religieux, xénophobes et parfois terroristes.

En premier lieu on évoquera la protection des singularités, celles de leurs données personnelles et de leurs biens, la plupart du temps légitime qui est continument victime de tentatives d'attaque et de violation tant par les entreprises (officielles ou non) que par les institutions étatiques (policières).
C'est ainsi que dans les usages des réseaux et les traces laissées par chacun que les opérateurs se constituent de gigantesques bases de données qu'ils s'envient mutuellement.
Les opérateurs de réseau, Google, Facebook, Microsoft, disposent d'infiniment plus d'information sur les individus connectés que les institutions publiques. (Voir les données de localisations capturées par Google et Apple à l'insu des usagers)
Ce n'est pas un hasard si l'on constate aujourd'hui une explosion aussi bien au niveau de la R&D publique et privée, que des applications déjà disponibles, des outils d'analyse de graphes de réseaux sociaux[1] et de fouilles d'opinion en temps réel[2].

[1] Il suffit de faire une recherche Google « Algorithmes fouille de graphes »
[2] Voir SEMIOCAST

Un enjeu majeur dans les luttes en cours et pour celles du futur devient donc la maximisation de l'anonymat qui se confronte en permanence à la dissémination des traces laissées sur les réseaux.

Deux aspects sont particulièrement importants pour cela, notamment:

- savoir se rendre complètement anonyme sur le Net symbolisé par l'image du masque de Guy Fawkes symbole d'Anonymous et popularisée par la BD et le film V comme Vendetta
- pouvoir protéger et authentifier les messages afin de les diriger avec précision et sûreté vers des destinataires reconnus.

ANOMYMOUS

Dans cette mouvance de jeunes Hacktivistes et « Digital natives » (Geeks) naît le concept d'Anonymous.
Il désigne les actions coordonnées de plusieurs communautés constituées d'internautes intervenant de manière anonyme pour agir collectivement dans un objectif défini en commun. C'est aussi une dénomination adoptée par une communauté informelle, non structurée et dynamique qui se lance dans des protestations et des actions sur Internet.
Les singularités qui composent Anonymous tissent une toile dynamique et fluctuante à travers diverses instances Internet : les forums, les *imageboards* (des forums anonymes et utilisant du matériel graphique) et de nombreux sites web. Avant de passer à l'action elles se coordonnent sur des cibles en utilisant les réseaux sociaux.

Son arme principale est l'attaque en Déni de Service, ou DDOS (**distributed denial-of-service attack**) (cf. Annexe) utilisée dans l'opération Payback Avenge Assange et plus récemment dans l'attaque contre le site Playstation.com et autres sites de Sony. Cela en réponse à la persécution en justice de hacker George Hotz (aka "GeoHot") et autres « coupables », selon la firme nippone, d'avoir « cracké » la console de jeux PS3 pour la rendre accessible aux logiciels libres.
Sans constituer une organisation au sens traditionnel du terme, Anonymous est de fait une avant-garde capable de coaliser et de catalyser des forces croissantes dans des moments déterminants de la bataille du Net, créant par ce mode d'action une production de communauté globale.

LA PROVOCATION DE WIKILEAKS

En 2010, les révélations et l'action de WikiLeaks ont montré la maturité à l'émergence du nouveau paradigme de la possession et de la diffusion de l'information. Précédent de peu les mouvements de revendication d'Afrique du Nord, la « Cyberguerre » en modèle réduit qui a été déclenchée par la publication d'informations « secrètes » et les ripostes, puis contre-ripostes qui s'en suivirent a révélé en avant première la capacité des réseaux à devenir le lieu de déroulement des conflits du XXIème siècle.

Dans les milieux des Hacktivistes on a pu observer, à l'occasion des révélations de WikiLeaks, que les réactions peu "démocratiques" des gouvernements mondiaux, USA en tête, furent des ripostes totalement disproportionnées et même illicites, par rapport au scandale des contenus diffusés, au demeurant passablement banals, sur lesquels nous reviendrons ultérieurement.
En cela, on peut estimer que le rôle le plus significatif de WikiLeaks a été celui de révélateur et de catalyseur.

Dérangé par l'attaque non prévue et la nouvelle tactique de WikiLeaks, le pouvoir étatique et capitaliste (de Biden à Sarkozy en passant par Paypal et Amazon) réagit par des actions dépassant largement le concept de « légitime défense [3]» parce qu'elles-mêmes illégales :

- le site WikiLeaks est attaqué sur le net grâce aux réseaux d'ordinateurs Zombies
- des corporations comme Amazon, Paypal, BankAmerica, PostFinance en Suisse, Master Card et Visa bloquent la collaboration et gèlent sur Internet les dons faits à WikiLeaks, sa source de financement.

Les contre-ripostes ne se font pas attendre : environ 600 sites s'offrent comme "miroirs" et, donnant le change aux serveurs WikiLeaks, lui permettent de continuer le service
A son tour, Anonymous lance l'opération Payback Avenge Assange avec la technique du Déni de service et répond à l'attaque en bloquant Visa, Mastercard, Paypal et PostFinance.
Demain, ce type d'attaque pourra s'effectuer grâce à des terminaux mobiles, ce qui décuplera tant la dissémination des sources que la diversité des cibles.

[3] Le concept de légitime défense numérique n'est pas encore présent dans la loi française, ni européenne, c'est un sujet en débat actuellement, un séminaire a eu lieu sur ce thème fin avril à Paris. Le principe qui semble se dégager est que, pour qu'elle soit légitime, une contre attaque doit être proportionnée et immédiate.

FREEWARE ET CROWDSOURCING

La sophistication perpétuelle des outils d'anonymisation est également indispensable des communautés de développeurs travaillant en mode collaboratif, la plupart du temps « gratuitement ».

Cette production commune du freeware rassemblant des individus qui ne se connaissent la plupart du temps que par leurs compétences techniques et leurs réalisations, d'où le concept de « crowdsourcing[4] », est probablement la forme la plus annonciatrice de possibilités de modes nouveaux de développement du commun.
Chacun contribue en fonction de sa propre évaluation de ses compétences et par l'acceptation des ses pairs (ceux qui travaillent au même produit). Il n'est pas jugé par un supérieur : seul compte le résultat dans sa collaboration.

De leur coté les acteurs du capitalisme numérique orientent leur action vers la captation de ces comportements de la vie telle qu'elle se développe dans ces nouveaux environnements.
C'est l'axe principal de la reconstitution du profit après la perte de poids du capital fixe.
Ils font du « crowdsourcing» l'axe de l'externalisation du travail vers la multitude et un instrument très puissant pour extraire du travail gratuit ou en tout cas pour en extraire du profit.
Ainsi, le crowdsourcing est utilisé de la même façon que la finance quand elle capte d'autres aspects de la vie : le droit au logement, le droit à la retraite, etc., .
Un exemple typique est l'intégration des applications de la plateforme Web avec le reste de l'économie qui est exploitée pour ses possibilités de captation. En sont des démonstrations :

- la publicité et le marketing sont les plus évidents, voir le cas Google ;

- le soi disant *« self-care »* : un must, dont les meilleures figurations sont IKEA dans le domaine matériel et MICROSOFT dans le domaine immatériel. A l'époque du prototype permanent (perpetual beta) l'usager est appelé à se débrouiller par lui-même, chercher les causes de sa panne, ou de la complexité du fonctionnement ; il devra faire les tests , signaler les « bugs » ou les virus et les innombrables essais, des appels sans résultats satisfaisants sur des numéros payants ; les éditeurs et opérateurs en mettant en service des produits non finis, faiblement testés reportent sur les utilisateurs une charge qui étaient auparavant incluse dans leurs tests ;

- le phénomène des *low-cost* : démarré avec les vols d'avions et étendu désormais à une bonne portion du transport implique le transfert vers le client des tâches qui étaient précédemment effectuées par les compagnies, s'y ajoute le paiement anticipé.
- le *e-commerce* en général qui permet au fournisseur d'écouler les marchandises en fonction de la demande, et demande au client d'effectuer toutes les procédures d'achat surtout celles

[4] Wikipedia : le **crowdsourcing** est un des domaines émergents du management de la connaissance : c'est le fait d'utiliser la créativité, l'intelligence et le savoir-faire d'un grand nombre de personnes (des internautes en général), en sous-traitance, pour réaliser certaines tâches traditionnellement effectuées par un employé ou un entrepreneur. Ceci se fait par un appel ciblé (quand un niveau minimal d'expertise est nécessaire) ou par un appel ouvert à d'autres acteurs. Le travail est éventuellement rémunéré. Il peut s'agir de simplement externaliser des tâches ne relevant pas du métier fondamental de l'entreprise, ou de démarches plus innovantes.

de produits ou services plus complexes (ex. choix et configuration d'abonnements téléphoniques mobiles etc.) ;

- la *déclaration des impôts en* ligne : ce n'est pas un hasard si l'administration française rétribue les contribuables qui font leur déclaration sur Internet ;

- le constat de la récupération des logiciels à l'origine « freeware » ou des « open source » ;

En outre ces technologies sont le système nerveux de la société de contrôle via l'introduction de la biométrie en mobilité et, en général, des services de géolocalisation, de la biosurveillance et du biotraçage.

Cependant le crowdsourcing peut aussi mobiliser l'intelligence collective autour de grands projets de production commune comme l'exemple classique et exceptionnel de Wikipedia

Parfois la ligne de démarcation entre les deux camps est difficile à percevoir, confuse, les imbrications étant si denses. Comment nier que Skype, Corporate privée, en cours de rachat par Microsoft, en permettant de téléphoner gratuitement entre deux ordinateurs via Internet a permis de réduire drastiquement le prix de la téléphonie fixe dans le monde, sans que personne ne se préoccupe de comprendre ce qui se passait dans sa boîte noire ou Ebay cas encore plus complexe par ses cotés claires et obscurs Il en est ainsi des réseaux sociaux : l'attrait de la gratuité des outils occulte les risques qu'ils font prendre à la protection des internautes.

Une autre analyse, que nous ne développerons pas ici, mériterait d'éclairer la complexité de l'activité de créations des logiciels appelés malware : virus, ver (Worm), chevaux de Troie (Trojan), logiciels espions (Spyware) etc., qui se diffusent sur les réseaux et dont on attend une explosion avec la croissance des smartphones. Limitons nous à observer que leur production est devenue une activité florissante dans certain pays, notamment dans l'est Européen.

Collaboration spontanée et gratuite, de la multitude capable de capturer et transmettre de l'information (expérimentation de la « Montre verte »[5] , « Spipoll » [6]), elle devient une arme aux mains du biopouvoir via les NTIC (localisation et transmission de données personnelles à Apple ou Google)
On assiste donc à un élan indiscutable et porteur d'espoir démontré par les tentatives, dont nombre sont réussies, de contributions à des projets commun et l'aptitude d'une multitude à se mobiliser sur des collaborations informelles et non hiérarchisées. Mais cet élan risque souvent d'être détourné, perverti ou censuré.
C'est ainsi que dans le cadre de l'actuelle crise systémique, se joue une confrontation permanente entre, d'une part une *opportunité* historique extraordinaire de construire le nouveau commun de

[5] http://www.lamontreverte.org/

[6] Suivi photographique des insectes Pollinisateurs : Projet de sciences participatives, le SPIPOLL a pour but d'obtenir des données quantitatives sur les insectes pollinisateurs et/ou floricoles en mesurant les variations de leur diversité et celles de la structure des réseaux de pollinisation, sur l'ensemble de la France métropolitaine**.**

l'ère cognitive et d'autre part la *menace* perpétuelle de la récupération par le Moloch (ou plutôt Cyborg ?) Ecomomicus blessé.

LE BIO-HYPERMEDIA LA RENCONTRE D'INTERNET AVEC LE CORPS DANS LA PHASE BIOPOLITIQUE QUI S'OUVRE

Déjà à Téhéran en 2009 les téléphones et réseaux mobiles ont permis la coordination sur le terrain et l'information sur les scènes de violence de la police immédiatement répercutée sur le Web.
A fin 2010 environ 5,3 milliards de personnes représentant 77% de la population mondiale disposent d'un téléphone mobile connecté et 1,8 milliards de nouveau terminaux seront vendus en 2011. Ces chiffres plus impressionnants encore que ceux des autres NTIC : 1,4 milliards de PC connectés à Internet ou les 1,2 milliards de lignes téléphoniques fixes[7], font de la téléphonie cellulaire la révolution technologique la plus largement et rapidement diffusée.
En outre, à la différence de l'automobile ou de la télévision, il s'agit d'une expansion quasi uniforme et simultanée tant dans les pays industrialisés que dans ceux émergents ou pauvres où elle permet un saut de génération technologique et un accès plus démocratique aux communications.
Dans nombre de pays faiblement développés, la téléphonie fixe restait un luxe réservé à une élite urbaine, alors que le téléphone mobile est pratiquement accessible à tous, où qu'ils soient.

Comme pour les savoir faire des « hacktivistes » et des « geeks », dans ces pays se développent des usages et technologies qui parfois devancent celles des pays industrialisés.
Si le Kenya, l'Inde ou les Philippines, on vu se développer des solutions, de paiements et transactions mobiles (m.payment) c'est parce qu'en l'absence d'un vrai réseau bancaire, les services de m.payment y suppléent par des moyens simples et économiques rendus possibles par la présence massive des téléphones mobiles.
A partir de ce socle de diffusion et d'usages en expansion nous assistons à la naissance du nouveau paradigme de l'Internet Mobile dont l'utilisation va dépasser dans les toutes prochaines années celui de l'internet classique au niveau mondial.

Cet usage de l'internet mobile se fait dans un contexte et par des dispositifs technologiques et fonctionnels qui ont des caractéristiques bien différentes du vieux PC sous Windows, lent, lourd, peu fiable et surtout doté d'une IHM (Interface homme machine) limitée et vieillissante.
Les nouveaux smartphones, tablettes et autres terminaux mobiles intelligents sont les héritiers tant des ordinateurs que des téléphones mobiles.
Des premiers, les ordinateurs, ils ont reçu le meilleur et le plus complexe: des Systèmes d'exploitation (Operating Systems – O.S.) toujours plus puissants sophistiqués en terme de capacité de traitement, les deux premiers O.S. mobiles (iOS d'Apple pour Iphone, Ipod Touch et Ipad) et Android de Google ne sont que des dérivés de LINUX un des piliers de la production commune du Freeware ou Logiciel libre.[8]
Des seconds, les téléphones mobiles, ils présentent d'abord cette caractéristique essentielle d'être toujours à coté de notre corps et surtout, ils ont étendu la capacité à être toujours connectés aux

[8]source : The International Telecommunication Union
[8] http://www.gnu.org/

multiples réseaux locaux ou globaux dont les débits sont en constante augmentation (du WIFI, au GPS en passant par la 3G ou la 4G).

Comme il advient souvent dans l'histoire scientifique, la fusion de deux technologies donne vie à un nouveau paradigme qui dépasse la simple addition des fonctionnalités préalablement existantes.
Capacité d'interagir de plus en plus avec nos portails sensoriels et notre corps, miniaturisation des équipements périphériques, fonctionnalités tactiles, reproduction de son, visualisation en 3D, géolocalisation,… ouvrent les portes à une variété infinie d'applications capables d'interagir et/ou de contrôler notre vie.
Le concept de «store »[9] où nombre d'applications sont gratuites, bien qu'exploité par des firmes privées (Apple, Google, Microsoft, etc.[10]), est quant à lui, une nouvelle figure du « crowdsourcing » et de la production commune de la multitude. Il devient aussi un important terrain de diffusion des malware en version mobile et donc de moyens de pénétrer les terminaux, d'en extraire des données ou d'y installer des virus.

Ces applications, intégrant les « périphériques sensoriels » peuvent interagir avec l'usager à chaque instant de son quotidien contribuant à imbriquer indissolublement vie et travail.
Par exemple : non seulement ils le situent physiquement et socialement par rapport à un contexte métropolitain (la ville ubiquitaire) mais ils deviennent un « œil » où s'incrustent les informations non visibles par notre œil sur le terrain (réalité augmentée) ou des instruments de monitorage de son état de santé.

L'instanciation sur le terrain de ces potentiels conjugués avec les réseaux sociaux permet d'imaginer et de créer de nouveaux usages et de nouvelles dynamiques, comme de photographier, filmer, enregistrer, prendre des mesures, et les mettre en commun, un peu sur la lancée de Twitter qui s'est préfiguré à l'occasion des manifestations altermondialistes.

Pour cet ensemble d'innombrables usages nous assistons aujourd'hui, à mon sens, à la naissance d'un **bio-hypermedia**.
J'utilise ce terme pour mettre évidence le fait que via ces terminaux sophistiqués il y a un saut de qualité dans l'interaction avec l'Internet Mobile : le corps, les sens, le « soi » ou simplement la vie - le Bios- entrent dans un contact plus intime avec les réseaux. (Curieusement, bios — Basic Input Output System — est aussi le terme qui définit le cœur initial de chaque PC depuis trente ans).
Les derniers mois ont vu des nouvelles formes de lutte de la multitude s'appuyer sur les simples téléphones cellulaires associés aux réseaux sociaux.
Demain, avec la diffusion du « bio-hypermedia », la distribution dans le terminal de tout un chacun de possibilités d'acquérir et de transmettre de l'information multimédiale, puis de constituer des bases de connaissances alternatives offrira des opportunités considérables de compléter ou de contester celles produites par les professionnels ou les organes officiels (photographes, journalistes, policiers…).

[9] App Store (Apple), Android Market (Google), Ovi Market (Nokia) Windows Marketplace (Microsoft) etc. sont des plateformes de téléchargement d'application et boutiques en ligne permettant de télécharger des applications mobiles développés par des sociétés ou des développeurs indépendants sur les Smartphones et Tablettes dont le O.S. (et parfois les terminaux) sont développés par les firmes respectives.
[10] Qui peuvent se réserver le droit de publier ou non une application à leur catalogue, selon des critères non nécessairement publics.

La multitude, par la multiplicité de ses sources et sa capacité à se reconfigurer de manière dynamique en réseaux multiformes, saura engendrer des avatars mobiles à Anonymous, en fonction de ses objectifs et de ses luttes.

Il s'agit aussi d'un outil typique de notre ère biopolitique où les usages d'une technologie de plus en plus intégrée à notre ***bios*** deviennent un élément fondamental de l'exercice du biopouvoir. Ces usages qui sont pistés en continu par les opérateurs et les entreprises privées visent à susciter toujours plus de consommation. Les logiciels du marketing, qui se nourrissent de tous les contenus de navigation et de connexion savent définir des scores de préférence et «d'appétence » de manière quasi instantanée[11]et ainsi adresser de la publicité orientée vers chaque utilisateur, l'incitant à consommer, toujours davantage, des produits de marques qui auront acheté les données comportementales. Enrichis par les données de localisation, ils vous orientent vers les lieux de consommation les plus profitables[12].
Mais outre les entreprises officielles, ces immenses gisements de traces de toutes sortes intéressent aussi les entreprises mafieuses. Nul doute que les réseaux, les graphes des liens et le contenu des échanges intéressent également le banditisme à tous niveaux[13].
Ainsi, le bio-hypermédia, devenu un instrument incontournable et irrésistible aux mains de la multitude dans la métropole, est tout autant puissant et crucial pour tous les pouvoirs en place.

Pour terminer, il importe de souligner comment des multitudes, en Tunisie, en Egypte et dans un nombre croissant de pays de cette zone du monde ont pu gagner ou sont en train de gagner, au prix de souffrances et de sang versé, certes, mais sans devoir déléguer le commandement à quiconque (organisations islamistes, syndicats ou partis politique de la vieille gauche) en construisant une force réticulaire irrésistible, capable de s'informer et de se doter d'une détermination sans faille.
Cela préfigure les capacités des nouvelles générations à créer des nouvelles formes de démocratie par une production cognitive commune qui intègre et fait évoluer les technologies diffuses et le bio-hypermedia. Concurremment, les menaces de contrôle biopolitique s'alourdissent.

Il faut attendre que les luttes s'intensifient sur le terrain des technologies et des réseaux.
Nous sommes bien à l'orée d'une nouvelle ère.

---

[11] Par exemple : vous recherchez des prix de cafetières sur Internet, pendant des semaines ont vous affichera des modèles de cafetières en bandeau sur votre navigateur, sans que vous le demandiez

[12] Les entreprises choisies par les consommateurs reversent des royalties aux opérateurs, ceux-ci présentent les listes en fonction de la rémunération qu'ils perçoivent des entreprises

[13] C'est ainsi qu'en interceptant sur un réseau social les données de localisation, par exemple le restaurant où l'on dîne et la durée moyenne du service, le bandit aura tout loisir de cambrioler le logement du l'usager.

ANNEXE

DENI DE SERVICE

Le principe de fonctionnement de l'attaque par Déni de service est simple : un réseau qui va de quelques centaines à plusieurs centaines de milliers d'ordinateurs zombies ou volontaires, appelé aussi Botnet (de Robot et network) lance automatiquement et en même temps une rafale de requêtes de service vers le site ciblé jusqu'à le saturer et le paralyser.
Cette technique est utilisée universellement, qu'il s'agisse de la mafia ou d'agences gouvernementales, des deux conjointement, ou de groupes informels de contrepouvoir comme Anonymous.
Pensons ne serait-ce qu'à la célèbre attaque de 2007 contre les sites du gouvernement et de l'administration d'Estonie dont le premier ministre accusa ouvertement le gouvernement russe d'être l'instigateur ou aux plus récentes attaques chinoises contre Google.
Ici il semble important souligner une différence, au départ, fondamentale : si la technique est la même, la mafia et certains services d'état bâtissent leurs Botnets en infectant les PC par des virus que les usagers ignorent et subissent, alors qu'Anonymous a construit son Botnet sur la base du volontariat.
En proposant un outil facile à utiliser et appelé ironiquement LOIC, *low orbit ion cannon (*d'après les Guerres stellaires) les usagers pourront participer à l'attaque coordonnée en indiquant l'adresse du site ciblé. Cependant, ne maîtrisant pas le contenu de ce qu'ils installent, ils ne sont pas à l'abri d'un autre « cheval de Troie » caché qui pourrait être à l'origine d'espionnage ou d'actions malveillantes incontrôlées. Dès lors, ce qu'ils croyaient inoffensif pour eux-mêmes pourrait devenir une arme qui leur échappe.
Les attaques en Déni de Services ne constituent qu'une infime partie de l'arsenal de la cybercriminalité. Des techniques comme « l' injection SQL » permettent d'altérer, de voler ou de détruire des données comme cela s'est produit récemment sur le site de VISA selon le milieu averti. En cas de vol des données, seul le cryptage pourrait constituer un dernier verrou de sécurité…là encore les techniques de cryptanalyse se répandent y compris dans les milieux délinquants.