LES RÉSISTANCES ~~DU NET~~ IV :
LA MENTALITÉ HACKER

Cette série sur les résistances sur le Net aurait pu continuer encore longtemps : on aurait pu parler de la tradition des tutos qui détruit le pouvoir factice de ceux qui font de la rétention d'informations ; on aurait pu parler de la collaboration et de l'horizontalité, mode d'organisation très présent sur le Net et qui amène des gens de la planète à œuvrer ensemble pour une cause commune ; on aurait pu parler du monde des logiciels libres, sous l'aspect de cette collaboration, mais aussi dans cette conception de non-propriété, d'information accessible qui s'oppose totalement au monde verrouillé ; on aurait pu parler des défenseurs de la vie privée contre la terreur imposée des sécuritaires ; on aurait pu parler de ceux qui ont à cœur de connecter les populations ; on aurait pu parler de l'importance de la neutralité du Net.

Peut-être qu'on reviendra un jour sur ces sujets formidables, mais il nous a semblé qu'il était temps d'en venir directement au cœur du sujet, au noyau lumineux qui illumine toutes ces questions : le hacking.

Ce noyau puissant a plus de cinquante ans, et si le legs matériel est bien visible (les ordinateurs et Internet, entre autres) il y a un moins moins palpable, mais qui s'est néanmoins bien transmis : la mentalité hacker, acquise par mème culturel à nos générations via les objets et la façon dont ils les ont conçus. Elle s'est transmise aux générations pour qui l'ordinateur est l'outil le plus utilisé, au-delà de ses simples fonctions d'assistance formelle du quotidien ; à ces générations qui utilisent cet outil comme moyen pour s'autodéterminer et aider autrui à s'autodéterminer. Cette mentalité s'est transmise à ceux qu'on nomme geeks (selon la définition originelle) transmise à cette génération « Y » qu'on dit indomptable, transmise sans même qu'on en ait véritablement conscience, nous voici à avancer et à agir avec la mentalité des hackers en héritage.

Mais avant de rentrer dans ces questionnements épiques, il nous faut préciser quelques points.

Précisions

Pour titrer cet article, nous avons – après moult hésitations – choisi le terme de « mentalité », qui signifie :

> « Ensemble des habitudes intellectuelles, des croyances et des dispositions psychiques caractéristiques d'un groupe ». Source : Larousse

Nous voulions parler des hackers de manière psychologique, parce que nos recherches, nos rencontres, ont clairement mis en lumière des points psychologiques qui rassemblent avec beaucoup de puissance à la nébuleuse des hackers, qui pourtant sont sociologiquement des groupes assez distincts et dont les réalisations, les finalités, peuvent être extrêmement diverses.

Cette mentalité est un noyau commun, qu'on pourrait d'ailleurs attribuer à d'autres groupes de personnes que les hackers, c'est un noyau extrêmement ouvert qui intrinsèquement, empêche les verrous donc le formatage. Là est sa grande force.

Nous parlerons d'**éthique des hackers** (= valeurs qui peuvent être appliquées personnellement ou professionnellement) : cette éthique découle directement de la mentalité des hackers, elle « coule de source » avec ce que vivent intellectuellement et psychiquement les personnes qui hackent. Nous avons été fascinés de découvrir dans nos recherches cette prolongation naturelle entre un vécu psychologique intense, rayonnant de plaisir, de ludisme, d'enthousiasme et, par logique avec ce vécu, la fondation d'une éthique qui se transmet sans avoir nécessairement besoin de mots, parce qu'elle fait directement écho au vécu, à ce qui est fait.

Nous n'emploierons pas le mot « **hackerisme** » qui lui, s'attarde sur le champ politique. De la pratique du hack né une mentalité du hacker qui, en tout logique, crée une forme d'éthique, et tout ceci découle des nécessités d'hacker la politique ou de considérer le hacking comme une nouvelle vision politique. Là n'est pas l'objet de l'article, même si c'est une question passionnante.

Mais qu'est-ce que c'est qu'un hacker ?

On va tout de suite oublier la traduction française « officielle » de hacker qui est « fouineur » : elle est trompeuse, réductrice, non représentative en plus d'être péjorative. On oublie également l'amalgame avec « pirate / piratage » qui au fil du temps a pris le sens de télécharger illégalement des fichiers (on en a parlé ici).

La définition la plus simple, la plus représentative et à la fois la plus exhaustive que j'ai trouvée est celle d'Amaëlle Guitton.

Le hacking, c'est : « **Comprendre. Bidouiller. Détourner. Et s'amuser au passage.** »

Nous aimerions rajouter à cette définition la notion de système, le hacking consisterait donc à comprendre un ou plusieurs systèmes, à les bidouiller, à les détourner tout en s'amusant.
Pour comprendre cette notion de système je vous renvoie à un des articles sur Quest to learn qui enseigne la pensée systémique à ses élèves. Tout est système, que ce soit une lampe, une cellule, un programme, un groupe social, une mesure politique… Et, précision qui me tient à coeur, il n'y a pas « un » système, mais des millions de systèmes qui cohabitent, collaborent ou s'affrontent, leurs liens formant à eux d'autres systèmes.

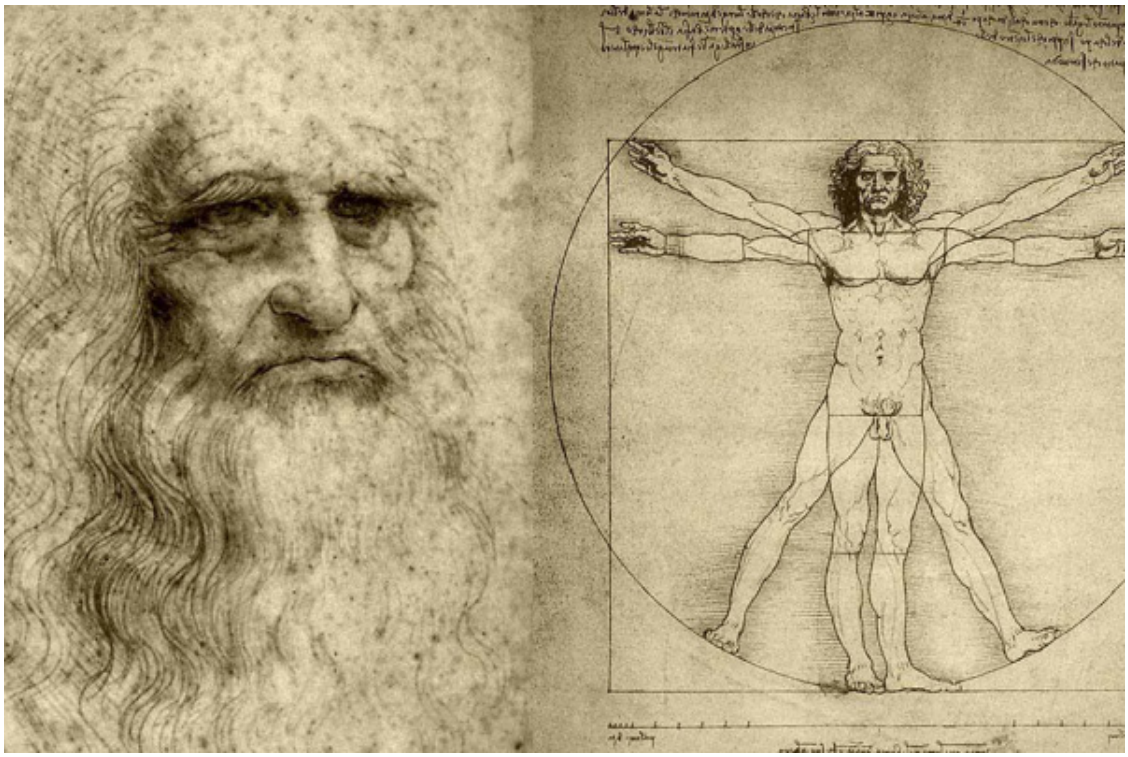
Le hacking n'est donc pas une discipline, il est une manière de faire et de considérer les problèmes, il est un mouvement particulier de l'intelligence, mouvement qui s'exprime de façon très concrète dans une action, une production, une construction. Ce concret, c'est le hack. On pourrait oser dire qu'il est une forme de travail très particulier. En philosophie on parlerait d'une intentionnalité : le hacking est une certaine forme d'intentionnalité instituant un rapport particulier entre le sujet et le monde, entre le sujet et autrui, entre le sujet et l'objet, entre le sujet qui conçoit aussi le rapport comme fait à étudier. La mentalité du hacking institue un certain rapport dont l'intuition de ce rapport est lui-même pensé

Un « life hack » un hack du quotidien, pour s'éviter de frotter.

Le hacker est donc quelqu'un qui fait du hacking. Ce statut de hacker n'est pas (et ne le sera sans doute jamais) institutionnalisé, on ne l'obtient pas par diplôme/formation. On peut être hacker sans le savoir, et un hacker peut avoir n'importe quel objet ou discipline de prédilection : le bricolage, l'informatique, les sciences, le social, le politique, l'éducation, l'agriculture…

On reconnaît le hacker à l'ingéniosité de son hack, ce sont donc les pairs qui le déclarent hacker. L'appellation est souvent un honneur parce qu'il s'agit d'une reconnaissance de l'intelligence du hack, une reconnaissance des compétences et de leur créativité. C'est un peu comme le statut de philosophe, certes on peut apprendre de façon institutionnelle la philosophie, cependant le master de philosophie ne délivre pas le statut de philosophe et les individus ne sont pas déclarés en tant que philosophe. Des penseurs venant de n'importe quelle discipline peuvent être dits philosophes, il s'agit d'une forme de reconnaissance quant à leur pensée et à la manière dont ils vivent leurs pensées.

Si le terme de hacker est récent, faire du hacking peut s'apparenter à des activités qui existaient bien avant que l'on emploie le mot hacker : le hack a quelque chose de l'enthousiasme des scientifiques lorsqu'ils découvrent quelque chose auquel personne n'avait pensé auparavant, le hacking a quelque chose de parenté avec la démarche artistique dans sa façon de briser les codes, les hackers dans leur visée de partage de l'info et dans leur façon de travailler ont beaucoup de points communs avec les milieux universitaires. Au-delà de ses sphères, le hacking a un lien avec tous ces débrouillards invisibles qui composent leur quotidien avec un élan créatif détonnant.



Léonard de Vinci est souvent considéré comme hacker

Ce terme hacker a cette nouveauté de tisser des liens communs avec des univers séparés (je pense aux artistes et aux scientifiques), à révéler ce qui les lie, au-delà de la simple créativité.

Il se peut que nous soyons amenés à parler du terme **hacktiviste** : il s'agit là de militer pour défendre des causes avec une mentalité et des méthodes de hacker. On peut citer en exemple Anonymous, Télécomix, mais on pourrait également parler des Yes Men en terme d'hacktivistes, étant donné que chaque étape de leur action est un hack, de la création des faux sites web aux hacks des conférences ou du territoire médiatique.

Il nous faut aussi **distinguer les hackers des crackers**. Les crackers sont des personnes ou des groupes de personnes qui exécutent des hack dans un but de destruction, de profit personnel ou d'intérêts du groupe. Ce sont les « black hats » dont on a parlé dans l'article sur le trolling.

Toute personne qui cracke un programme/un fichier n'est pas black hat : celui qui casse les verrous que sont les DRM d'un ebook libère l'information pour le plus grand nombre et il le fait sans profit personnel, si ce n'est la satisfaction du hack et la satisfaction de ceux qui en profitent.
Attention donc, **ce n'est pas parce qu'un hack paraît destructif ou illégal qu'on peut taguer son créateur de « black hat »**, il faut regarder les conséquences de ce hack, le replacer dans un contexte plus large.

White hat

Un white hat (en français : "chapeau blanc") est un hacker éthique ou un expert en sécurité informatique qui réalise des tests d'intrusion et d'autres méthodes de test afin d'assurer la sécurité des systèmes d'information d'une organisation. Par définition, les "white hats" avertissent les auteurs lors de la découverte de vulnérabilités. Ils s'opposent aux black hats, qui sont les hackers mal intentionnés.

Grey hat

« Un grey hat (en français, "chapeau gris"), est un hacker ou un groupe de hackers, qui agit parfois avec éthique, et parfois non. Un exemple courant est une personne qui accède illégalement à un système informatique sans rien détruire ou endommager (du moins, pas volontairement), et qui ensuite informe les responsables de ce système informatique de l'existence de la faille de sécurité et possiblement émet certaines suggestions pour régler ce problème. Malgré ces bonnes intentions, ceci est tout de même considéré comme un crime dans la plupart des pays. Un type de hacker grey hat est le hacker agissant au nom d'une idéologie qu'il considère juste, commettant des délits non pas pour son propre profit mais dans le but de lutter pour une cause [sic], telles que la liberté d'expression et la protection de la vie privée pour les hackers grey hat des groupes LulzSec et Anonymous.

HS Source : wikipédia

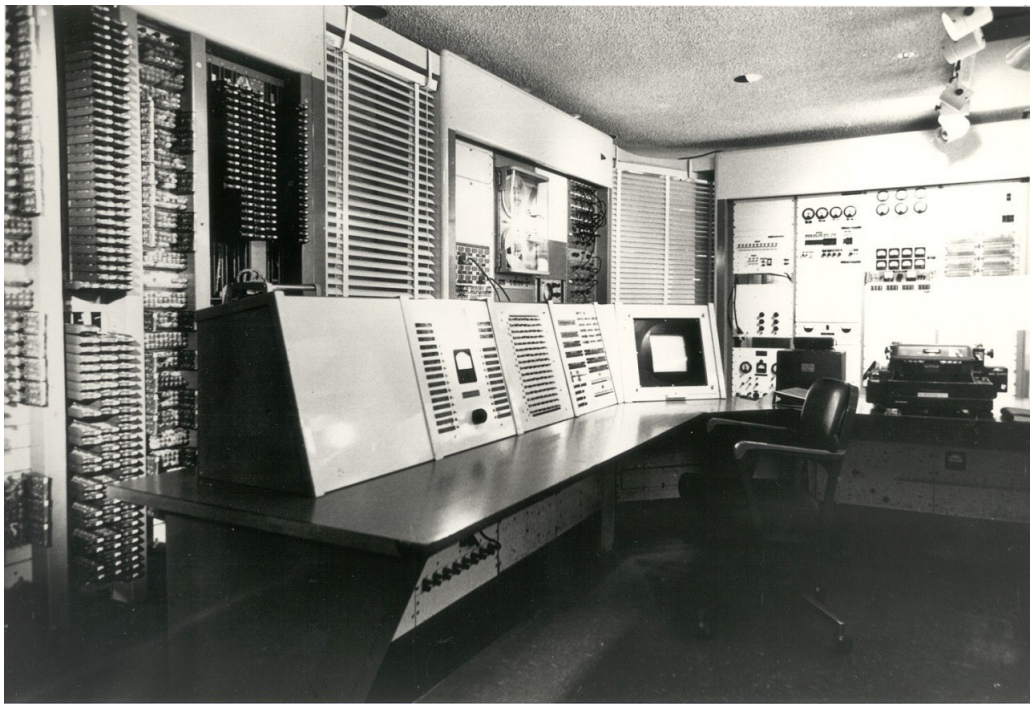
Black hat

Un black hat (en français : "chapeau noir") est, en argot informatique, un hacker mal intentionné.
Les black hats ont une nette préférence pour les actions illégales. Cela va de la création de virus aux chevaux de Troie en passant par les vers et les logiciels espions.
Ces personnes utilisent leurs compétences informatiques de façon à en tirer un bénéfice financier ou bien dans le but de nuire à des individus ou à des organisations.

Toutes ces subtilités, la société a fort du mal à les comprendre ou certains dominants font clairement exprès de faire des amalgames péjoratifs pour conserver leur acquis, leurs pouvoirs et leur domination sur autrui.
Or c'est loin d'être une « mode » récente, le hacking, c'est une mentalité, une éthique et une philosophie extrêmement concrète qui a plus de 50 ans. Nous en avons appris les codes culturels inconsciemment (ou sciemment), nous les jeunes et moins jeunes, en utilisant les machines, les programmes et cet Internet si particulier qu'ils nous ont légués.
Même si cela n'est qu'une hypothèse, nous pensons qu'il est là ce mystère qu'on attribue à cette génération Y indomptable au travail et soi-disant incompréhensible. Nous avons absorbé, sans nous rendre compte, une culture de hacker. Parce qu'elle nous ouvre au monde, parce qu'elle est enthousiasmante, concrète, parce qu'elle rime avec un plaisir et une jubilation folle pour toutes les choses, parce qu'elle offre clairement des outils pour penser et tester le futur, sans nous formater ou nous brider par des idéologies cloisonnantes et aliénantes.

Les premiers hackers

Tout démarre au prestigieux MIT (Massachusetts Institute of Technology), au tout début des années 60. L'institution a un objet très rare, très coûteux, très lourd et demandant beaucoup de moyens humains, il s'appelle ordinateur :



[*Ici le TX-0, une des machines sur laquelle ont travaillé les premiers hackers*]

Ces monstres de technologie exercent une fascination absolument incroyable sur les membres d'un club du campus, le TMRC (Tech Model Railroad Club of MIT), notamment les personnes qui ont les mains sous les circuits, dans les systèmes. Parfois ce sont aussi les fascinés par l'ordinateur qui rejoignent le club, les activités technologiques ayant alors de nombreux points communs.
L'ordinateur est perçu comme une lampe d'Aladin, ils en présentent de formidables capacités, cela les fascine à un point inimaginable.

Le TMRC a repris le terme hack, qui est à l'époque sur le campus un synonyme de blague potache (par exemple recouvrir le dôme surplombant le campus avec un matériau réfléchissant) et lui a donné un autre sens : un hack est pour eux une connexion entre des relais techniques de leurs circuits, une connexion ingénieuse, inattendue et élégante :

« Un projet entrepris au nom d'un plaisir personnel, sans aspiration collective, s'appelait un « *hack » [...].* Lorsque quelqu'un qualifiait une connexion ingénieuse entre relais de « hack sérieux », cela signifiait que l'opération se distinguait par sa nouveauté, son style et sa virtuosité technique »

L'éthique des hackers, Steven Levy

[le TMRC en 1960 et leur travail avec les modèles réduits.]

Le premier point qui unit ces hackers, c'est la fascination pour les systèmes, leurs possibilités, qu'ils soient sous les rails ou liés aux ordinateurs et à leurs programmes qu'ils écrivent. Ils se fichent de leurs études, allant parfois jusqu'à oublier les dates d'examen, se fichent de leur carrière universitaire, se fichent d'être en couple ou de sortir comme leurs camarades, en viennent à oublier leur corps et ses besoins en sommeil.

La seule chose qui vient à compter est de gagner du « temps-machine » : l'accès à l'ordinateur est sous planning, très contrôlé. Les hackers en viennent à mettre en place des tours de garde pour saisir les moments ou tel étudiant inscrit ne serait pas venu prendre son tour. Ils en viennent à vivre de nuit, parce que ce sont les moments où les ordinateurs sont les plus disponibles et choisissent des machines moins « tyrannisées » par la bureaucratie. En cela, ils s'opposent aux règlements et normes qui leur font perdre du temps-machine.

Parfois, ces monstres de technique ont besoin de réparations, mais l'institution a clairement interdit les réparations en autonomie, les outils et composants de remplacement (les diodes par exemple) sont sous verrous. Les hackers apprennent donc à crocheter les serrures, à s'infiltrer littéralement dans les lieux où ils pourront emprunter du matériel nécessaire pour optimiser leur temps-machine. Ils se mettent à fabriquer des passe-partout, envisagent même de les distribuer aux nouveaux.

> « La clef maîtresse [la clef passe-partout qu'ils fabriquent] était l'épée magique qui chassait le mal. Le mal, naturellement, c'était une porte close. Même s'il n'y avait pas le moindre outil derrière cette porte, les serrures symbolisaient le pouvoir de la bureaucratie, un pouvoir qui ne servait qu'à entraver l'Éthique des Hackers. Ceux qui veulent savoir comment les choses fonctionnent ont toujours constitué une menace pour les bureaucraties. Les bureaucrates savent qu'ils ne doivent leur survie qu'à l'ignorance dans laquelle ils tiennent les gens, par des moyens artificiels,

> comme les serrures. Aussi, quand un administrateur fit monter d'un cran la pression en installant une nouvelle serrure ou en faisant l'acquisition d'un coffre-fort de deuxième catégorie (garanti par l'État pour la protection de documents secrets), les hackers se mirent immédiatement au travail pour craquer la serrure et ouvrir le coffre. »
>
> *L'éthique des hackers*, Steven Levy

Cet acharnement à laisser toute porte ouverte, lutter contre les verrous quitte à prendre des cours par correspondance pour devenir serrurier, quitte à prendre des risques considérables, n'est pas qu'une lubie bizarre d'étudiant. « *La clef maîtresse symbolisait la passion des hackers pour le libre accès.* » Cet épisode de lutte contre les verrous, encore aujourd'hui, est vivant, sous bien d'autres formes, il se transmet comme une valeur fondamentale.

[Alan Kotok, Steve Russell, and J. M. Graetz sur l'ordinateur PDP-1 jouant sur le tout premier jeu video qu'ils ont créé, SpaceWar]

Au même titre, les hackers ne cachent pas les informations qu'ils produisent : tous les programmes qu'ils créent sont à disposition dans une armoire, chacun peut se servir, corriger les programmes, les modifier, les améliorer. Les hackers peuvent même s'énerver que les autres ne prennent pas cette initiative et viennent les embêter avec des fautes qu'ils auraient faites : les autres doivent être autonomes comme eux. La notion de propriété, ils s'en balancent, et la réprouvent lorsqu'elle s'exprime par ses « serrures ». Lorsqu'un industriel vient leur demander s'il peut inclure le programme qu'ils ont créé dans les machines qu'ils délivrent, ils ne demandent pas d'argent. Ils en sont au contraire fiers :

> « Comparée aux royalties, la conception d'un logiciel était une récompense plus grande, un cadeau fait au monde, une satisfaction en soi. L'idée majeure était de mettre l'ordinateur à la portée de tous, d'en faire un objet

> si désirable que tout le monde aurait envie de jouer avec, d'en explorer les possibilités, voire de devenir hacker à son tour. En écrivant un beau programme, on s'inscrivait dans une communauté; on ne se contentait pas de produire à la chaîne un produit manufacturé.
> Et, surtout, personne ne devait avoir à payer pour un logiciel: l'information devait être gratuite! »
>
> *L'éthique des hackers*, Steven Levy

De manière plus générale, ils leur étaient insupportables d'être face à un système défaillant et de ne pas avoir les permissions de le bidouiller pour le réparer ou l'optimiser. Cette mentalité dépasse de loin le cadre de l'ordinateur, et une anecdote rapportée par Steven Levy semble porter en elle tout ce qu'hacking peut vouloir dire.

Le groupe du MIT prend l'habitude de fréquenter un restaurant asiatique. Progressivement, les hackers se rendent compte que les plats servis aux Occidentaux et aux Asiatiques ne sont pas les mêmes, ceux des Asiatiques semblant bien meilleurs, plus complexes. Quelqu'un ne pensant pas de façon systémique, un non-hacker, se serait peut être plaint (confrontation), aurait cherché un autre restaurant (fuite) ou encore aurait tenté de négocier (collaboration).
Mais ces hackers pensant en système, ils ont d'abord convaincu un autre hacker passionné d'idéogrammes chinois de venir avec eux :

> « Ils y revinrent [au restaurant chinois] munis de dictionnaires bilingues et demandèrent à consulter le menu en chinois. Le chef, Mr. Wong, s'exécuta à contrecœur; Gosper, Samson et les autres se penchèrent sur la carte comme s'il s'agissait d'un livre de code. Samson assurait la traduction, qui révéla plein de surprises. Ainsi, le bœuf à la tomate du menu anglais se traduisait littéralement par « bœuf-porc aux aubergines barbares ». *Wonton* voulait dire « gorgée de nuage ». Il y avait bien des choses passionnantes dans ce système! Aussi, après avoir décidé de commander les trucs les plus intrigants (« une aile d'hibiscus? Voyons à quoi ça ressemble »), ils appelèrent Mr. Wong qui, dans sa langue rocailleuse, rouspéta avec vigueur. En vérité, il rechignait à servir de la vraie cuisine chinoise à des Américains, persuadé qu'ils ne sauraient pas l'apprécier. Mr. Wong les avait pris pour des Américains lambda, alors qu'ils étaient des aventuriers! Ils avaient exploré les tréfonds de la machine, ils pouvaient en raconter tous les sortilèges – en langage assembleur, de préférence. Mr. Wong rendit les armes. Sur la table, arriva le meilleur dîner chinois qu'on n'eût jamais mangé de mémoire de hacker. »
>
> *L'éthique des hackers*, Steven Levy

Lors de ces dîners, ils parlent code. La « vraie vie » a peu d'importance : « *Un événement n'était intéressant que s'il pouvait nourrir leur curiosité pour le mode d'emploi du monde.* »

De même les différences entre individus, notamment ceux qui sont admis dans ce cercle de hacker, n'ont pas d'importance. Il ne s'agit pas de tolérance, de volonté

de ne pas avoir de préjugé, c'est une posture liée à la compétence :

> « On pouvait être un garçon dyslexique de 14 ans et être un winner [= *un hacker considéré comme génial dans sa pratique]*. On pouvait être brillant [*dans les études*], sensible et assoiffé de connaissances et être un loser. »
>
> *L'éthique des hackers*, Steven Levy

Les hackers font rentrer au MIT des enfants de 14 ans pour leur génie, mais rejettent tous ceux qui ne le sont pas, quelles que soient leurs autres qualités. Le milieu des hackers du MIT est élitiste, mais un élitisme très particulier, basé sur la capacité à avoir une intelligence atypique, créative. Ce n'en était pas moins violent pour autant.

La passion pour l'ordinateur au MIT, si extraordinaire soit l'éthique qu'elle fit naître, n'était pas pour autant lavée de tous défauts : certains hackers y avaient un égo bien trop développé pour ne pas dériver (dont le rejet des « losers), d'autres étaient complètement coupés du monde extérieur et ne s'interrogeaient pas sur la contradiction qu'il y avait à œuvrer certes, avec démocratie, liberté et volonté d'ouverture, mais dans un laboratoire financé par la défense, qui n'avait d'intérêts qu'à développer l'ordinateur pour la guerre.

Fort heureusement, une nouvelle génération de hacker arriva, une génération consciente du monde social, consciente qu'il était catastrophique que les ordinateurs ne soient dédiés qu'à la guerre et que les industries de l'époque, telle qu'IBM, refusent catégoriquement de faire accéder à la population cet outil pourtant incroyable. Des années 70 à 80, toute une génération de hacker de matériel, bidouillant avec des composants trouvés dans des poubelles, vendus sous le manteau comme de la drogue, va s'atteler à fabriquer des ordinateurs personnels et inonder le monde d'informatique. Cette génération, qui avait pour objectif de transmettre à tous cette passion n'en avait pas pour autant oublié l'éthique des hackers du MIT (à moins que cette éthique ne découle naturellement de la logique de l'outil informatique?) et la perpétua.

[Le premier ordinateur n'a pas été conçu par les grands groupes de l'époque (IBM) qui ne voyaient pas l'intérêt de distribuer les ordinateurs au peuple. L'Altair (ici le 8800), premier ordinateur personnel, était distribué en kit par MITS une petite compagnie dans les années 70]

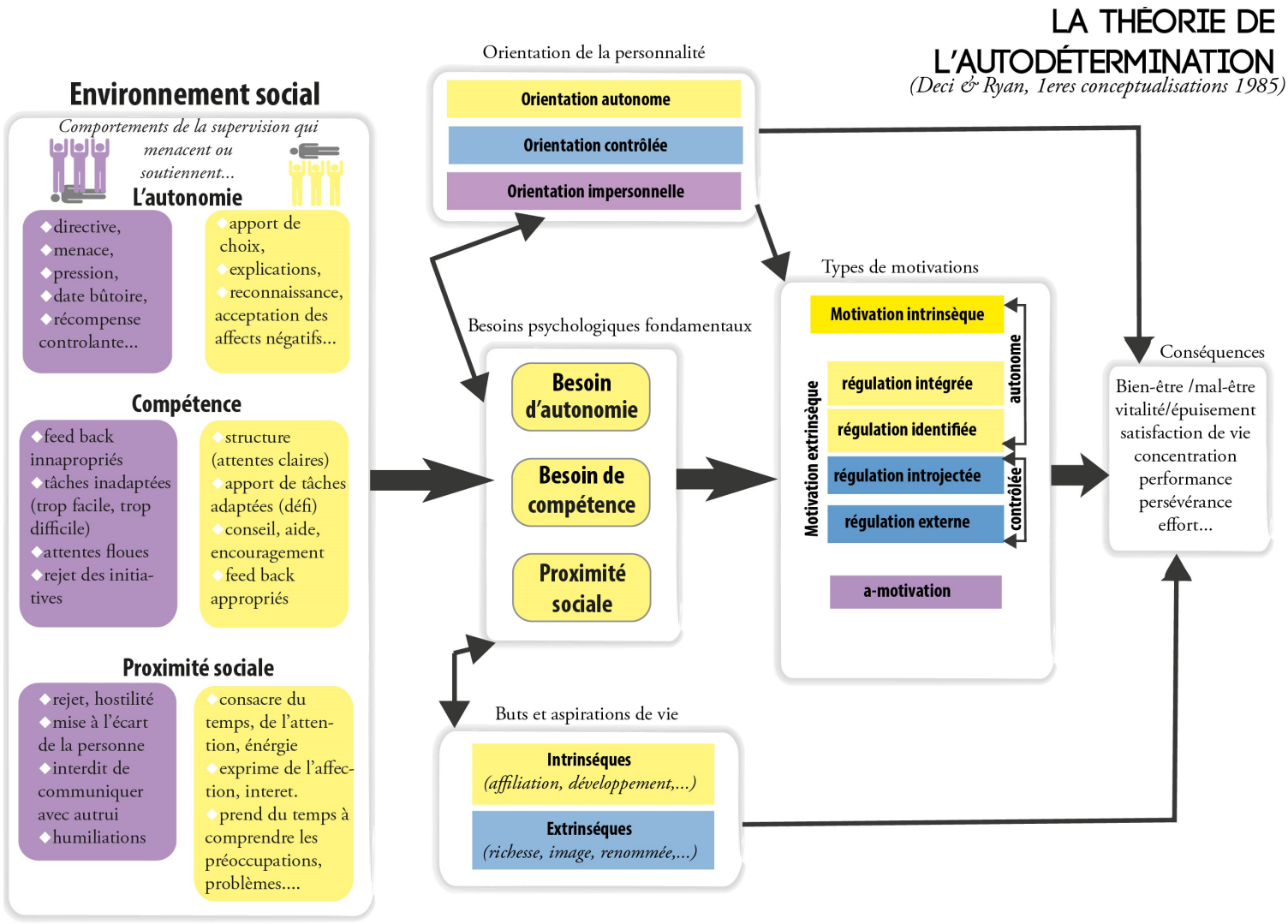
La suite, on la connaît. Bill Gates a été le premier à réclamer de l'argent pour ses logiciels, et si Wozniak, petit génie a fait les premiers Apple dans son garage avec un amour intrinsèque pour chaque composant, Steve Jobs en a fait un business fort lucratif et a petit à petit imposé des verrous totalement à l'opposé de l'Éthique hacker. Cette volonté de démocratisation s'est plus ou moins alliée au business, et certaines corporations ont exploité les hackers qui se fichaient de l'argent.

Cependant, l'Éthique hacker perdure et elle a conquis des milieux qui ne sont pas liés à l'informatique. Parce que cette éthique, elle est synonyme de bonheur, de puissance, d'autodétermination, d'appétence sans limites pour toutes les choses du monde. Parce que cette éthique, c'est un contre-pouvoir à ce qui crée de l'injustice, de la souffrance, des dérives des autorités et qu'en cela, beaucoup l'ont saisi par nécessité pour faire face à ce monde qui est à recoder avec un nouveau langage de programmation.

À l'origine, il y a la passion

Cette passion, dans toutes nos recherches et expériences liées au hacking, on la voit vivace, patiente, téméraire, tranquille, frénétique, acharnée, concentrée, du tiède au frémissant, mais elle est toujours présente chez le hacker, sous une forme ou une autre. On sent ce feu ardent chez les premiers hackers des années 60, on le retrouve chez les hackers de matériel des années 70, il rayonne chez les libristes, il se teinte d'engagement chez les hacktivistes de notre génération.
Un hacker sans ce feu ardent n'est pas un hacker, parce que pas de hack sans cet appétit sans limites pour la connaissance, la compétence et les illuminations intellectuelles de son intellect ou celles d'autrui.

Pas de doute, le hacker carbure à la motivation intrinsèque (donc, par extension, au flow), donc pour aller plus loin nous allons devoir nous replonger dans la théorie de l'autodétermination (TAD) :



Procédons par élimination pour appliquer la TAD au hacker : **il ne peut pas avoir une orientation impersonnelle**, sinon il ne ferait rien, pas même apprendre des connaissances ou chercher à comprendre le moindre mécanisme, quel qu'il soit. Il subirait la vie en subordonné résigné, incapable d'envisager qu'il puisse avoir le moindre impact sur celle-ci.

L'orientation contrôlée n'est pas celle des hackers : ils détestent les injonctions bridant leurs activités inutilement, ils ne marchent pas au bâton et à la carotte, ils ne font pas leurs activités parce qu'autrui veut qu'il les fasse. Attention, cela ne veut pas dire qu'ils ignorent autrui ni qu'ils ne sont jamais dans une situation subordonnée. Cela veut dire que sa motivation, son élan, sa créativité naissent en lui, non commandés ou sous l'influence forcée de l'extérieur. Un hacker ne hacke pas uniquement pour un salaire ou parce qu'untel va le gronder s'il ne le fait pas.
Cependant, certains hackers peuvent avoir comme indicateur non leur activité elle-même, mais la reconnaissance d'autrui avant tout, ce qui est une motivation extrinsèque dont le moteur est le narcissisme.

Généralement **les hackers ont une orientation autonome**, et pour certains cela se voit dès l'enfance où ils s'attellent à des projets pharaoniques, sans penser à épater qui que ce soit, juste pour les projets eux-mêmes. Un autre indicateur de cette orientation autonome est qu'ils poursuivent les buts qu'ils se sont donnés même si l'environnement y est opposé, qu'ils encourent des risques à leur hack. Nous pensons à Aaron Swartz qu'on peut qualifier d'hacktiviste, qui pour la cause du partage d'info, a libéré plus de 4 millions d'articles scientifiques ce qui lui a valu des condamnations judiciaires très oppressantes, certainement pas étrangères à son suicide.

https://www.youtube.com/watch?v=7ZBe1VFy0gc

Si on continue l'élimination dans la TAD, il semble évident que **le hacker n'est pas a-motivé**, **n'a pas de motivation externe ou introjectée**. Dans certains cas, il y a des moteurs de motivations extrinsèques tels que la motivation à régulation identifiée ou intégrée : c'est la forme d'élitisme qu'on a pu voir chez les hackers du MIT qui rejetaient tous ceux qui n'étaient pas géniaux comme eux ; on le voit dans nos temps modernes également, lorsqu'il y a dédain du noob ou de la personne qui n'a pas les mêmes compétences que le hacker, qu'il y a rejet du monde extérieur, ou agressivité quand ils considèrent comme « inférieurs » des personnes qui n'ont pas les mêmes valeurs qu'eux (parce que ces personnes ne chiffrent pas les messages, ont un Facebook ou ne comprennent pas Linux, par exemple). On a là une forme de Netocratie, une aristocratie du monde du Net, plus motivée par son pouvoir, son élévation au-dessus de la masse des gens considérés comme incompétents, que par son activité.
Là aussi cela peut être une question de narcissisme, d'égo, d'expression de complexe d'infériorité… Il n'en reste pas moins que cette Netocratie peut avoir

néanmoins une capacité de hack, avoir du talent, mais qu'elle ne sortira pas de sa sphère, puisque tout élément extérieur à elle n'étant pas identique à elle, est rejeté, moqué ou humilié.

La motivation intrinsèque reste l'apanage du hacker le plus puissant en terme de créativité. Wozniak, hacker de génie montrait des signes très forts de motivation intrinsèque :

> « Les échanges d'informations, l'énergie créatrice tourbillonnante, plus la possibilité d'épater tout le monde avec un bidouillage élégant… Voilà les stimulants qui motivaient Woz: construire le genre d'ordinateur qu'il voulait pour jouer avec. L'informatique représentait le comble de ses désirs; il ne courait ni après la richesse ni après la célébrité, et la convoitise des clients d'ordinateurs le laissait de marbre. »
>
> *L'éthique des hackers*, Steven Levy

Cette motivation intrinsèque est une énergie puissante, mais également démesurément généreuse, car le hacker se contrefout sincèrement des rétributions pour le travail, symboliques ou matériels, de la flatterie au gros chèque. Même l'absence de reconnaissance (dans une certaine mesure) n'empêche pas celui qui est motivé intrinsèquement de continuer à développer ses compétences ou faire preuve de créativité.
C'est une chose merveilleuse, mais le danger de cette motivation où la personne semble être sous flow quasi-permanent, c'est que n'étant pas arrêtée par les affronts de son égo ou de sa personne, elle peut se faire exploiter. Le génie de Wozniak a clairement été exploité par Steve Jobs, par exemple :

> « Steve Jobs n'a jamais écrit une seule ligne de programme, affirme Wozniak. Il n'a pas davantage réalisé de design original. En revanche, il en connaissait assez sur la technique pour modifier ou améliorer le design des autres. »
> [Steve Jobs est employé chez Atari dans les années 70, il n'exerce que la nuit, car les autres employés le trouvent insupportable et arrogant.]
> « Vers la fin de l'année 1974, Nolan Bushnell [le fondateur d'Atari, boss de Jobs à l'époque] a l'idée d'un nouveau jeu, Breakout, dans lequel un joueur devrait briser un mur de briques pour se libérer. Lorsqu'il évoque ce jeu à ses ingénieurs, ils estiment le délai de réalisation à plusieurs mois. Le hasard veut qu'il en parle à Jobs. Surprise, l'employé de nuit se vante de pouvoir réaliser Breakout en quatre jours ! Bushnell lance un défi à Jobs : s'il peut réellement programmer le jeu dans un tel délai, il touchera une belle prime.
> Jobs ne possède aucunement les compétences nécessaires, mais il sait pertinemment que Wozniak peut réaliser Breakout dans le temps imparti. Il n'est pas déçu ; le zélé barbu conçoit le circuit nécessaire et programme le jeu en Basic. Il crée bel et bien Breakout en quatre nuits de travail chez Atari. Pour Woz, c'est une vraie révélation :
> « Jusqu'alors, je n'avais pas réalisé à quel point le logiciel pouvait aider à créer des jeux. J'ai dit à Steve Jobs que les jeux ne seraient plus les mêmes

> désormais. Rien qu'en y pensant, je me mettais à trembler ! » [considération admirablement intrinsèque, passionnée]
>
> Signe patent du génie de Wozniak, *Breakout* repose sur un nombre extrêmement faible de composants : trente-six, au total. Seul problème : Jobs se révèle incapable d'expliquer aux ingénieurs d'Atari comment il a pu créer Breakout ! Pas dupe, l'ingénieur Al Alcorn d'Atari, devra reprendre lui-même une grande partie du design.
> Pour Breakout, Jobs reçoit la coquette somme de 5 000 dollars. Il en rétrocède 350 à Wozniak qui, sur le moment, considère cette somme comme un joli bonus sur son salaire de Hewlett-Packard. Bien plus tard, lorsqu'il apprendra que le partage a été inéquitable, il se sentira outragé ! »
>
> *les 4 vies de Steve Jobs*, Daniel Ichbiah

Steve jobs récoltait l'argent, mais aussi la reconnaissance symbolique. On le voit avec le recul, les gens pensent que Jobs était un génie et le créateur matériel d'Apple, or c'était surtout un homme d'affaires. Le génie était Wozniak, et par la suite, toutes les petites mains d'Apple dont personne ne connaît le nom. Jobs lui se contentait d'être complètement obsédé par le design, pas par les composants de ces objets.

Plus généralement, toute l'histoire de l'informatique est parsemée de personnes totalement passionnées, qui avancent à la motivation intrinsèque – ce qui en fait de grand créateurs –, mais qui sont exploités par d'autres. Pendant des années, les programmeurs de jeu n'avaient même pas leurs noms dans les crédits des jeux, alors qu'ils l'avaient conçu tout seul et que le jeu connaissait un succès monstre. Encore aujourd'hui, les personnes dans le jeu-vidéo sont très mal payées.

L'environnement social

Dans la TAD pour alimenter l'autodétermination d'autrui, l'environnement doit nourrir trois besoins de la personne, à savoir l'autonomie, la compétence et la proximité sociale. Ainsi la personne peut développer sa motivation intrinsèque.

Pas mal de hackers sont issus de milieux où la bidouille est encouragée, où il y a des parents eux-mêmes très curieux, ouverts d'esprit ; il y a « permission » à être créatif, que ce soit dans le cercle familial ou dans d'autres groupes sociaux (amis, association, école…).

Cependant ce n'est pas une constante, et on constate aussi très souvent le contraire : Lee Felsenstein par exemple, était un hacker de matériel qui souhaitait démocratiser l'usage des ordinateurs et qui participa à installer les premiers terminaux dans des lieux publics, où les gens pouvaient par exemple poser des annonces, consulter des informations (un moteur de recherche avant l'heure, que les gens avaient détourné en se laissant des mots mystérieux, en jouant le rôle de personnages fictifs :))

> « Grosse tension familiale; il y avait des conflits entre Lee, son frère Joe (de trois ans son aîné) et une cousine adoptive de l'âge de Lee, comme une sœur pour les garçons. Les aventures politiques du père, Jake, membre du Parti communiste, s'étaient terminées au milieu des années 1950, quand il avait perdu son poste de responsable de cellule à la suite de conflits internes, mais la politique restait la grande affaire de la famille.
> Mais quand les problèmes devenaient trop sérieux à la maison, il se retirait dans l'atelier du sous-sol encombré de matériel électronique provenant de télévisions et de radios abandonnées.
> C'était un lieu où l'indéniable supériorité de son frère, tant physique qu'intellectuelle, n'avait pas cours. Lee Felsenstein avait un don pour l'électronique qui lui permettait de surpasser son aîné pour la première fois. Il avait presque peur de développer ses capacités – il construisait des choses, mais n'osait jamais les mettre en application, craignant un échec qui aurait conforté son frère dans son jugement, à savoir que « ces choses-là ne marcheront jamais».

L'environnement social des hackers est souvent assez hostile. Pour ceux du MIT, IBM faisait tout pour empêcher les personnes d'avoir de l'autonomie sur les ordinateurs, les obligeant à remplir quantité de paperasses et autre engeances de la bureaucratie. La passion folle des hackers étaient moquée des autres, que ce soit les autres étudiants, certains profs ; la population les prenait littéralement pour des extra-terrestres, des gens anormaux aux mauvaises intentions (parce que l'informatique n'était lié qu'au militaire dans leurs esprits).
Même après la démocratisation de l'informatique, les écrits des hackers ne cessent de conter ce rejet de l'environnement social de leur compétence, de ce qu'ils sont :

> « Je suis un hacker, entrez dans mon monde...
> Le mien est un monde qui commence avec l'école... Je suis plus astucieux que la plupart des autres enfants, les conneries qu'ils m'apprennent me lassent... Je suis au collège ou au lycée. J'ai écouté les professeurs expliquer pour la quinzième fois comment réduire une fraction.
> Je l'ai compris. «Non Mme Dubois, je ne peux pas montrer mon travail. Je l'ai fait dans ma tête»
> Satané gosses. Il l'a certainement copié. Tous les mêmes.
> J'ai fait une découverte aujourd'hui. J'ai trouvé un ordinateur.
> Attends une minute, c'est cool. Ca fait ce que je veux. Si ça fait une erreur, c'est parce que je me suis planté.
> Pas parce qu'il ne m'aime pas...
> Ni parce qu'il se sent menacé par moi...
> Ni parce qu'il pense que je suis petit filou...
> Ni parce qu'il n'aime pas enseigner et qu'il ne devrait pas être là...
> Satané gosse. Tout ce qu'il fait c'est jouer. Tous les mêmes.
> (...)
> Nous explorons... et vous nous appelez criminels.
> Nous recherchons la connaissance... et vous nous appelez criminels.

> Nous existons sans couleur de peau, sans nationalité, sans dogme religieux… et vous nous appelez criminels.
> Vous construisez des bombes atomiques, vous financez les guerres,
> Vous ne punissez pas les patrons de la mafia aux riches avocats,
> Vous assassinez et trichez, vous manipulez et nous mentez en essayant de nous faire croire que c'est pour notre propre bien-être, et nous sommes encore des criminels.
> Oui, je suis un criminel. Mon crime est celui de la curiosité.
> Mon crime est celui de juger les gens par ce qu'ils pensent et disent, pas selon leur apparence.
> Mon crime est de vous surpasser, quelque chose que vous ne me pardonnerez jamais.
> Je suis un hacker, et ceci est mon manifeste.
> Vous pouvez arrêter cet individu, mais vous ne pouvez pas tous nous arrêter…
> Après tout, nous sommes tous les mêmes. »
> *The Hacker Manifesto*, 8 janvier 1986, Loyd Blankenship après son arrestation, sous le pseudonyme de « The Mentor »

Pour résumer, la vie des hackers donne presque tort à la TAD : on peut continuer à œuvrer, être motivé, alors que l'autonomie est bridée (par exemple par la bureaucratie d'IBM), que la proximité sociale s'approche du néant (rejet des proches, rejet des environnements sociaux extérieurs, rejet via les représentations de la société).

Leur flow était-il si intense que cela évinçait tous problèmes extérieurs ?

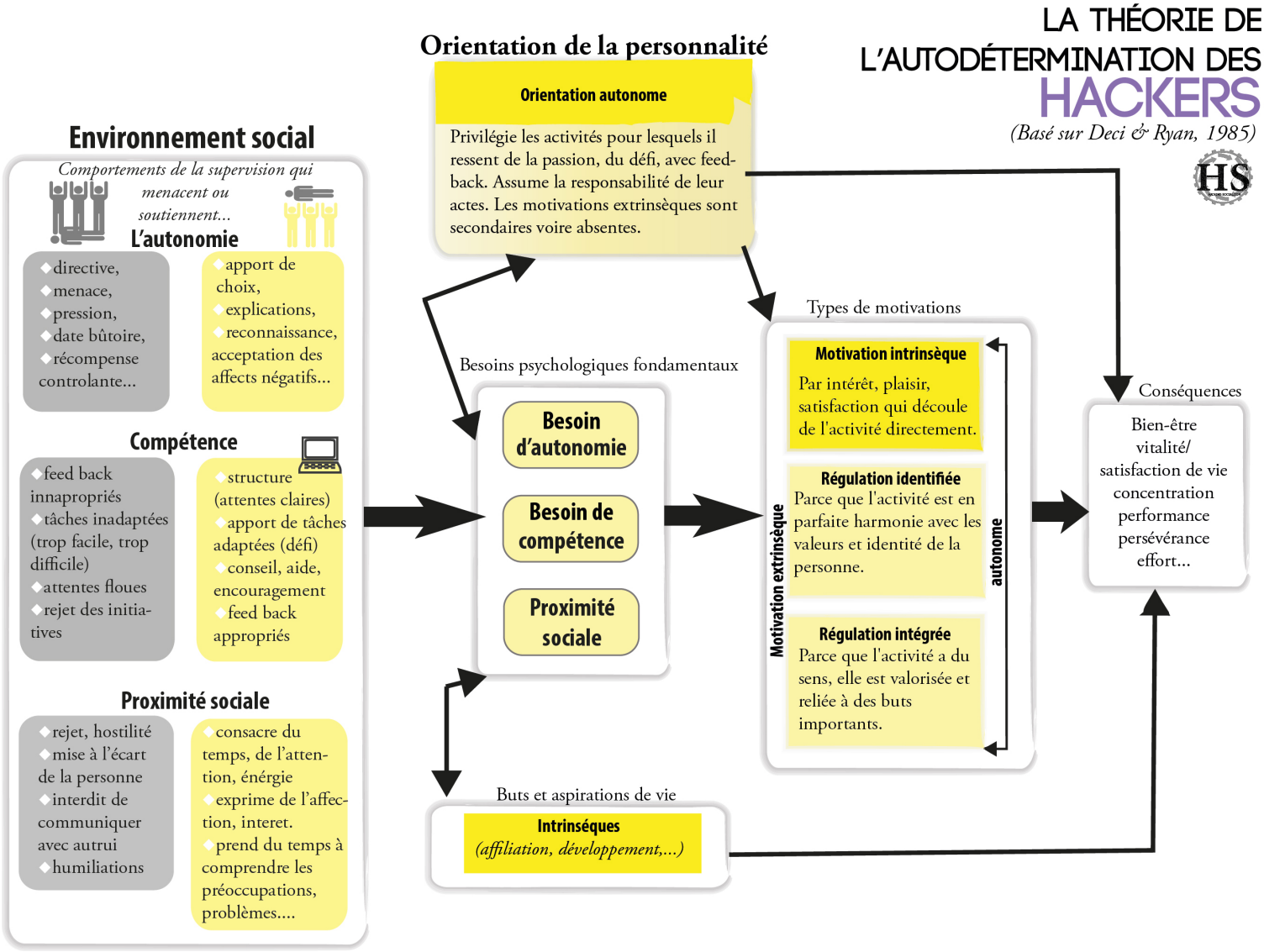
Les hackers du MIT étaient clairement sous flow, quand volontairement, de leur propre décision, ils programmaient 72 heures d'affilée, qu'ils en oubliaient leurs examens de fin d'année, que l'un d'entre eux, plutôt que de se servir de la calculatrice mécanique de l'époque pour un simple exercice requis par un prof, préfère consacrer tout son temps à programmer un logiciel qui transforme le TX-0 en calculette (alors que celui-ci, vu son prix est réservé à des « causes » beaucoup plus importantes).

Les signes d'expérience du flow sont nombreux, et si on les couple à l'inédit, la terre inconnue que représentait l'ordinateur à l'époque, il y a là quelque chose qui explique pourquoi les hackers n'avaient pas besoin réellement d'être nourris/choyés par l'environnement social pour être motivés.

On pourrait aussi expliquer cet acharnement à poursuivre leurs passions par le fait que malgré leurs difficultés d'intégration, ils ont su créer leurs communautés où là, il y avait proximité sociale, soutien, aide à l'autonomie. Le TMRC par exemple, mais aussi plus tard les associations de hackers de matériel, les communautés libristes, les hackerspaces, etc. L'ARPANET, puis internet ont permis la communication avec des personnes, qui même si la société ne les acceptait pas, même s'ils étaient rares, leur a permis de nourrir leurs compétences et besoins sociaux.

Il y a néanmoins une autre explication à cette appétence pour le hacking malgré l'environnement social en ennemi : l'environnement, c'est aussi l'ordinateur lui-même, et celui-ci est en soi, un objet qui répond à des besoins psychologiques, notamment ce besoin de compétence. Attention, ce n'est pas une dérive animiste de notre part : on crée des objets pour nous assister, pour aller plus loin dans nos possibilités, donc on transmet à ces objets des facultés qui peuvent répondre à des besoins. Autrement dit, l'ordinateur n'a pas une âme bienveillante qui est sympa avec nous, mais sa conception, ses possibilités et ses interactions avec nos propres compétences répondent à certains de nos besoins.

The Mentor l'explique simplement, alors qu'il semble être rejeté par l'école qui ne comprend pas ses compétences ; l'ordinateur, lui, donne un feed-back très clair, sans ambiguïté « *Si ça fait une erreur, c'est parce que je me suis planté. Pas parce qu'il ne m'aime pas… Ni parce qu'il se sent menacé par moi… Ni parce qu'il pense que je suis petit filou… Ni parce qu'il n'aime pas enseigner et qu'il ne devrait pas être là…* » Autrement dit, l'ordinateur nourrit les besoins de compétences pour celui qui a compris son langage et sa logique, et cela peut être suffisamment pour alimenter son flow, sa motivation intrinsèque.



Comportements que tout superviseur* susceptible de soutenir VS menacer les besoins psychologiques du supervisé (éléve, patient, employé, joueur...)

**enseignant, cadre, thérapeute, entraineur...*

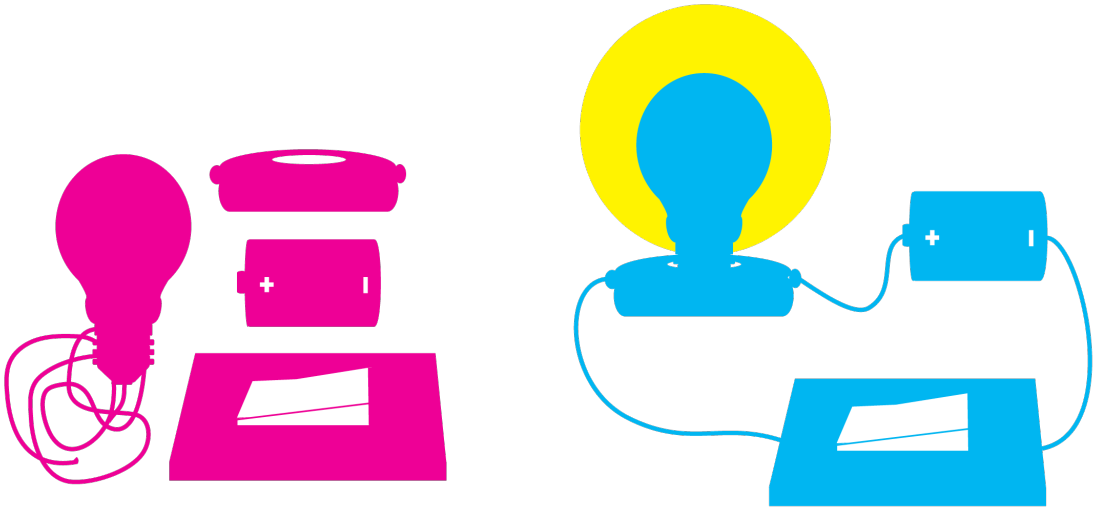
Si on reprend les conseils de la TAD pour nourrir la compétence d'autrui, on voit que l'ordinateur, pour celui qui l'a dompté, a un « comportement » qui soutient l'individu :

- il utilise une communication qui aide à diagnostiquer et à résoudre les problèmes
- il donne une liberté totale d'action, pour qui sait avoir des idées
- il communique des procédures claires
- il délivre des feed-back positifs (ça marche)
- il ne condamne pas l'initiative, s'il y a échec, c'est qu'il y a une erreur
- il laisse la personne changer tout ce qu'elle veut changer
- son langage n'induit pas la pression ni la culpabilité
- ses feed-back, même négatifs, sont opportuns, justes, et prévisibles (même si une erreur de frappe dans un code peut le rendre inopérant ou créer un chaos monstre, c'est logique, ce n'est pas injuste)
- les échecs sont toujours contrôlables pour peu qu'on développe sa compétence.

Alors si certes, l'ordinateur est bête et qu'il ne satisfait aucunement les besoins de proximité sociale, il n'est pas en tout cas un frein à l'intellect de la personne, il n'humilie pas le génie, il donne matière à réfléchir même à ceux qui sont surdoués, il ne bride pas la personne pour des raisons de jalousie ou de discriminations. Cette porte ouverte que représente l'ordinateur peut alors devenir un refuge, un refuge où même si la personne est rejetée, elle peut se développer tout en développant l'ordinateur lui-même.

À la passion est couplée une certaine façon de penser

Façon de penser qui a pour noyau la pensée systémique, qu'on peut trouver chez le technicien et le scientifique, mais qui s'accouple avec la façon de penser de l'artiste.



C'est un tas d'objets
Ce n'est pas un système.

Rien ne change quand un élément est enlevé ou est enlevé ou ajouté dans cet amas.

C'est un système.

Un changement se produit quand on vous enlevez ou ajoutez un élément à une partie de ce systéme.

INSTITUTE of PLAY
Traduction par HACKING-SOCIAL.COM

Penser de façon systémique, c'est :

- chercher à saisir et comprendre une vision d'ensemble
- chercher les modèles/tendances dans les systèmes
- reconnaître comment la structure d'un système provoque un certain comportement
- identifier les relations de cause à effet
- émettre et tester des hypothèses
- trouver des conséquences inattendues qui pourraient subvenir
- trouver des points changeables qui pourraient changer le système

étudié
- résister à la tentation de tirer des conclusions trop rapides

Q design pack system thinking, Institute of play

On peut reprendre la définition du hacking avec l'analogie entre ces métiers :

Comprendre le(s) système(s) = le technicien qui démonte un objet pour voir ses différentes parties, leurs interactions. Et ensuite être en capacité de le réparer, l'améliorer ou en fabriquer un autre différemment.

Bidouiller le(s) système(s) = le scientifique qui va tester de nouvelles interactions dans le système qui a été déjà un peu appréhendé. Par exemple en psychologie expérimentale, on sait à partir de quel seuil les personnes perçoivent consciemment une image, le scientifique peut donc tester ce qui se passe lorsqu'on assène des images trop rapidement pour être perçues, voir si cela a un effet sur les personnes (et cela donne les études sur les images subliminales).

Détourner le(s) système(s) = l'artiste a compris un système, de façon plus ou moins théorique ou intuitive, par exemple il comprend que la pub est une saloperie, qu'elle ment, qu'elle fait mal aux gens et il a l'idée d'un détournement :

Dans la réalité, les catégories sont moins rigides que tel que nous les présentons, il s'agit là juste de faire l'analogie de certains mécanismes pour cerner la pensée particulière du hacker. Le scientifique peut être artiste et cela parfois par inadvertance : il découvre des propriétés détournées du système étudié par inadvertance ou sérendipité , par exemple la découverte de la pénicilline par Flemming via des moisissures ; la découverte du LSD par Hofmann qui travaillait sur l'ergot de seigle et qui un jour sort de son laboratoire complètement halluciné parce qu'il en a absorbé par hasard ; etc.

Tout comme l'artiste, le technicien ou le scientifique peuvent certes penser de façon systémique ou être reconnu par leur statut, mais ne jamais faire preuve de créativité, ne faire aucune découverte, ne jamais transformer un objet, ne jamais créer une œuvre qui renverse quelconque code.
Le hacker a besoin de ses trois postures, qu'il investira plus ou moins selon son domaine de prédilection.

Des génies ?

Si l'histoire du hacking est parsemée de petits génies qui, sans l'ombre d'un doute, avaient des potentiels intellectuels de base très supérieurs à la moyenne, penser de façon systémique et faire preuve de créativité n'est pas inaccessible au commun des mortels : à partir du moment où l'on veut réparer un objet, comprendre un mécanisme social, qu'on décide de faire quelque chose qui changera le réel d'une façon ou d'une autre, ouvrant des possibilités, changeant des comportements, permettant de nouveaux comportements, on a besoin de comprendre le système sur lequel on s'attelle. C'est à dire, comme l'explique si bien *Quest to learn* à ses élèves, qu'il est nécessaire de voir tous les facteurs dans une situation, leurs relations, leurs failles ou leurs points forts et s'extraire des modes de pensées communes.

Voici une exemple d'un fait qui aurait nécessité une pensée systémique et qui a été résolu en prenant en compte tout un système complexe :

https://www.youtube.com/watch?v=SZImKzAZUv4

Autrement dit, avec la pensée systémique, face à un problème on ne peut pas dire « c'est la faute d'untel, il est trop con », mais « pourquoi untel ne comprend pas ? Est-ce l'objet qui est mal conçu, est-ce qu'il y a des facteurs bloquant sa compréhension, est-ce une question de situation qui le rendrait passablement imbécile ? Et de cette pensée systémique naît assez rapidement des hacks : par exemple si Untel est si bête, c'est peut-être parce que le chauffage est beaucoup trop élevé dans le lieu où il fait preuve de bêtise, et il trouvera son intelligence si on réduit le thermostat. Quand on sort de la pensée commune qui a pour habitude d'accuser les caractéristiques d'autrui comme cause unique de ses comportements, qu'on accepte que regarder le contexte, les situations, ce n'est pas excuser, mais donner les moyens à sa pensée de trouver des solutions (vous comprendrez la référence;D).

Le problème, c'est que la pensée systémique, de près ou de loin, on ne l'apprend pas à l'école, *Quest to learn* reste un ovni dans l'éducation. Les élèves et même les étudiants sont encore considérés comme des réceptacles qui se doivent de recevoir la connaissance passivement, ils sont formés à devenir des automates de la compétence qu'on leur inculque. Soit, ils sont brillants ou suffisamment curieux pour s'émanciper à l'extérieur et leur autodidactisme les sauve de ce manquement, soit ils finissent allégeants, sans cette étincelle de génie qui pourtant fait tout le plaisir de l'apprentissage, tout le plaisir de manier une

compétence, tout le plaisir de la connaissance, tout le plaisir d'œuvrer. Parce qu'au-delà d'apprendre à penser de façon complexe, de voir les systèmes, il ne s'agit pas que d'observer ou appliquer une recette : il faut apprendre à être autonome des recettes, à en trouver d'autres et à les mettre en œuvre.

Et c'est là que l'étincelle de la créativité est nécessaire et qu'on en vient au détournement. Quand on regarde des baguettes chinoises et qu'on persiste à n'y voir que des baguettes chinoises, on ne parviendra pas à les hacker, même si on est un excellent penseur, technicien ou scientifique, car on ne parvient pas à s'extraire des étiquettes et normes.

> « J'aime bien prendre l'exemple des baguettes chinoises [pour expliquer ce qu'est un hack]. A priori, ça sert à manger. Si tu en fais un truc pour tenir une lampe, tu les détournes de leur finalité d'origine. Eh bien voilà, tu as hacké une paire de baguettes chinoises. »
>
> Numendil, dans *Hackers*, Amaëlle Guiton

Le hack demande d'aller au-delà de ce qu'on peut savoir d'un système, de franchir les préjugés (ici d'utilisation, des baguettes chinoises ne servent qu'à manger) pour voir que les parties peuvent être utilisées différemment.
En cela, la curiosité, la flexibilité mentale, c'est-à-dire cette capacité d'accepter le changement, savoir se libérer des automatismes, d'accepter sans crainte le chaos, l'inattendu, l'étranger, être capable de considérer un bug ou une faille non pas comme un obstacle, mais comme une possible opportunité à une nouveauté plus profitable, est aussi nécessaire.
Autrement dit, pour le hacker rien n'est mis en catégorie de façon définitive, tout peut être remis en cause, rien n'est tenu pour acquis.

Critiques

N'est-ce pas réducteur/dogmatique de réduire la mentalité du hacker à un carcan psychologique ?

On peut avoir une mentalité de belliciste dans les jeux vidéo et être doux dans la vie, voire même craintif du conflit dans d'autres situations. Autrement dit, adopter une mentalité pour aborder certaines situations ne dit strictement rien de sa personnalité.

Certes, on pourrait investiguer sur les grandes caractéristiques de la personnalité des hackers, comme certains chercheurs l'ont fait pour les trolls, et il est fort possible que certains traits soit plus récurrents dans cette population (je pense à l'ouverture d'esprit, trait généralement très présent chez les artistes en général),

mais cela n'a que peu d'utilité à mon sens : on ne change pas sa personnalité, à moins de coûteux efforts sur le très long terme pour adoucir certains traits (c'est parfois nécessaire, par exemple pour le névrosisme).

Par contre, une mentalité, on peut l'adopter, s'en défaire, la changer, l'oublier, la retrouver, en cumuler une collection comme autant de cartes à jouer face aux situations. C'est donc une possibilité parmi d'autres, c'est loin d'être un carcan, surtout dans le cas des hackers.

La mentalité du hacker est optée pour œuvrer, tout comme la motivation intrinsèque est un élan et une énergie à se mettre à l'action et la perpétuer. Elle ne dit rien des motifs de celui qui est motivé, rien de son champ de discipline, rien du contexte dans lequel elle a émergé. On pourrait très bien imaginer qu'un cuisinier se mette à adopter une logique de hacker alors qu'il doit faire un repas avec peu de ressources à disposition : la situation complexe qu'il va aborder avec motivation va titiller ses connaissances et ses compétences, il va devoir sortir des recettes déjà éprouvées, il va devoir tester des mélanges qu'il ne connaît pas, mais dont les connaissances lui disent que cela pourrait donner un bon résultat, etc.

La TAD reste également très mystérieuse sur l'objet de la motivation intrinsèque, comment cet intérêt, cette passion s'ancrent chez l'individu. Certaines expériences ont appris aux psychologues comment la susciter, comment éviter de la brider, mais la part de coïncidence, de hasard, de vie est énorme. Des milliers de facteurs entrent en jeu, donc la TAD et ce qu'on a pu dire sur la mentalité du hacker ne sont en rien une recette pour créer un hacker, ce n'est qu'un aperçu pour comprendre cette énergie intellectuelle et créative, énergie qui peut être intermittente, uniquement dédiée à certains domaines ou au contraire à tous (et là on a une personne autotélique), passagère ou durable.

N'est-ce pas superficiel que de tendre vers cette mentalité ?

Dans le *jargon file* (une sorte de lexique alimenté par les hackers depuis des décennies), Éric S. Raymond décrit l'attitude du hacker et rappelle un point fondamental :

> « **5. L'attitude n'est pas un subs**titut à la compétence.
> Pour être un hacker, vous devez développer un certain nombre de ces attitudes. Mais cela seul ne suffira pas à faire de vous un hacker, pas plus qu'un champion sportif ou une rock star. Pour devenir un hacker, il faut de l'intelligence, de l'expérience, de la persévérance et beaucoup de travail.
> Par conséquent, vous devez apprendre à vous méfier des attitudes et à respecter les compétences, quelles qu'elles soient. Les hackers ne se laissent pas impressionner par les poseurs, mais ils apprécient les compétences, particulièrement les compétences de hackers, mais aussi toutes les autres.

> Les compétences dans les domaines exigeants maîtrisées par une élite sont particulièrement appréciées, et plus particulièrement celles qui nécessitent un esprit perçant et une grande concentration.
> Si vous respectez la compétence, alors vous aimerez travailler à vous améliorer sans cesse, et cela sera plus un plaisir qu'une routine. C'est vital pour devenir un hacker. »
>
> *Comment devenir un hacker*,Éric S. RAYMOND http://www.secuser.com/dossiers/devenir_hacker.htm

L'autodétermination comme le hacking ne peuvent se passer d'action, d'ouvrage, sans quoi cela n'est pas de l'autodétermination ou du hacking.

Chez les hackers, il semblerait que la compétence soit au-dessus de tout, tous les autres besoins y sont subordonnés, y compris les besoins de proximité sociale ou d'autonomie. C'est-à-dire que le hacker peut se plier passagèrement à un environnement qui bousille son autonomie pour faire ses armes et augmenter sa compétence ; il peut œuvrer avec motivation même si le soutien social est quasi-nul (moquerie de la famille, pas encore de reconnaissance des pairs…) parce que ce besoin de compétence surpasse tout, son énergie intrinsèque rend endurant et patient : la reconnaissance vient ensuite, elle n'est pas le but, mais la cerise sur le gâteau.

Bien sûr, il y a dans la nébuleuse des hackers, des personnes qui font semblant, qui joue ce rôle de hacker sans l'être. Cela peut être un effet de Dunning-Kruger (les personnes qui ont peu de compétences tendent à les surestimer, justement parce que leur manque de compétence les empêche de distinguer les gens doués des gens incompétents) ; mais cela peut être aussi l'effet d'une norme.

En effet, à présent la société perçoit l'énergie incroyable qu'il y a dans cette motivation intrinsèque et c'est devenu une norme sociale de paraître l'avoir : autrement dit, il est de bon ton de s'afficher passionné, mais sans pour autant l'être (cf https://www.cairn.info/article.php?ID_its=4904+4893+4143+4141+3579+3577+1929+1919+1917+1364+1358+1265+1263+1072+1070+)

Si dans un entretien d'embauche ou dans un dîner mondain, la supercherie peut passer, dans le monde des hackers, non, parce que c'est un monde do-ocratique (le pouvoir à celui qui fait), il ne sert à rien de paraître, de se présenter ou de présenter ses idées, il faut montrer ses productions, ses ouvrages, faire.

En cela, les apparences qu'on se donne n'ont aucune importance dans le monde des hackers et n'offrent pas de reconnaissance de la part des hackers. Évidemment, aucun groupe n'est à l'abri de ces fanfarons qui se donnent une image, mais qui n'œuvrent pas, mais dans l'univers du hacker, ils ont en principe moins de chance de voler de la reconnaissance ou du pouvoir.

Alors si ce n'est pas une recette, à quoi bon chercher à comprendre la mentalité du hacking si cela ne nous donne aucune piste ?

Parce qu'en voyant les rouages de cette énergie qui mène à la création, on voit en négatif ce qui empêche de s'autodéterminer, d'être créatif, d'être un hacker accompli : la motivation extrinsèque est par exemple un poison, agir pour un gain qui se trouve hors de l'objet bloque totalement l'ingéniosité ou la met au service de causes mauvaises pour la société.

[image altair]

C'est ce qui s'est passé avec Bill Gates : c'était dans les années 70 un hacker doué, il savait programmer avec génie, mais il a décidé de faire payer ses premiers logiciels (un interpréteur basic pour l'Altaïr, un des premiers ordinateurs personnels, ci-contre) suite à des copies pirates (habitude déjà ancrée à l'époque) à un prix très cher et , il écrit ceci à l'époque :

> *La majorité des amateurs le sait, la plupart d'entre vous volait le logiciel. On doit payer pour un matériel, mais le logiciel est quelque chose qu'on se partage. Qui se soucie de savoir si les gens qui y ont travaillé sont payés ou non?*
> Gates expliqua que ce « vol » de logiciel empêchait les programmeurs talentueux d'écrire pour des machines comme l'Altair. *Qui peut se permettre de faire pour rien du travail de professionnel? Quel amateur peut consacrer trois ans à programmer, trouver toutes les erreurs, rédiger la documentation de son produit et le distribuer gratuitement?*
> Quoiqu'un peu exaltée, la lettre, relayée par Bunnell, n'était pas un laïus indigeste. Mais elle déchaîna un tollé monstre dans la communauté des hackers.
>
> *L'éthique des hackers*, Steven Levy

Si les justifications de Bill Gates pouvaient se comprendre, cela ne justifiait pas pour autant les prix qu'il demandait (150 dollars par logiciel alors que d'autres créateurs d'interpréteur Basic ne demandaient que 5 dollars).
La suite, on la connaît : c'est le profit qui est devenu le but et pas la création de l'objet lui-même, donc cela donne toute la place aux bugs, aux failles de sécurité, etc.

De même pour l'Apple sans Wozniak (l'inventeur du Apple I et II) : dès lors que l'entreprise n'a fonctionné que par motivations extrinsèques– via Steve Jobs qui n'a jamais été un hacker – cela a donné des appareils bridés par l'absence de connectique, par restriction de l'autonomie de l'usager. Wozniak voulait permettre aux usagers d'augmenter la mémoire de leur ordinateur afin de faire tourner de nouveaux programmes sans réinvestir dans un nouveau matériel, mais Jobs s'est opposé à cette mentalité. Quand la motivation extrinsèque prend le dessus sur les objectifs, on bride, on ferme, on verrouille ou on bâcle : autrement dit, on s'oppose totalement à l'Éthique des hackers.

Observer les mécanismes de la mentalité du hacker permet de se hacker soi-même, se réparer ou se comprendre : cela nous aide à nous-mêmes trouver des pistes pour s'autodéterminer. Face à des décisions, cela rend alerte : « E*st-ce que*

j'accepte ce poste parce qu'il flatte mon égo ou parce que j'y trouve du plaisir dans les actions proposées ? » ; cela peut aider à se poser de bonnes questions : « *Pourquoi je m'empêche de faire cette chose complexe alors qu'elle m'attire ? Quelle pression extrinsèque me tyrannise ?* » *Est ce qu'avant de chercher à être reconnu je ne devrais pas plutôt trouver la compétence qui passionne pour elle-même ? Même si le milieu dans lequel je suis me tyrannise, est-ce que je ne peux pas trouver des hack pour développer des compétences, et que ça profite à tout le monde ?* »
Ce ne sont que quelques questions parmi des milliers qu'on pourrait se poser. Des questions importantes parce qu'elles aident à se développer, à développer ses compétences qui sont tout autant de ponts vers autrui, des possibilités de bien-vivre ensemble, faisant évoluer le monde avec le bonheur d'œuvrer, le bonheur du social, le bonheur de se lever contre les tyrannies et tout ce qui s'oppose au développement de chacun.

***

Nous n'avons parlé ici que du noyau d'énergie des hackers, ce n'est que le terreau de ce qu'ils ont pu développer, il reste foule à dire.
Le prochain article sera directement lié à celui-ci : l'éthique des hackers, vous le verrez, est une extension du flow, de la motivation intrinsèque, des capacités d'autodétermination des hackers.

Pour approfondir les notions dont on a parlé :

- le flow
- la théorie de l'autodétermination et ici Nourrir une motivation autonome et des conséquences positives dans différents milieux de vie : les apports de la théorie de l'autodétermination.
- apprendre la pensée systémique ou la faire apprendre à des enfants
- Tester son autodétermination, aider autrui à être autodéterminé ou voir ce qui l'empêche de l'être : http://selfdeterminationtheory.org/

Sources :

- *L'Éthique des hackers*, Steven Levy
- *L'Éthique hacker*, Pekka Himanen
- *Hacker : au coeur de la résistance numérique*, Amaëlle Guitton
- *Anonymous*, Nicolas Danet et Frederic Bardeau

Autour de L'Éthique hacker de Pekka Himanen :

- Test MAM - 303_fr.pdf
- L.Ethique Hacker.pdf
- Téléchargement de fichier PDF - Cairn.info
- Hacking et management : Microsoft Word - 05-19.doc - f_519398d019e22.pdf

Le manifeste de The mentor, document classique dans l'histoire du hacking : Le manifeste du hacker de Loyd Blankenship - La Revue des Ressources

Milieu du hacking et du libre :

- Éthique et communauté du hacker : un entretien avec Richard
- M. Stallman - Projet GNU - Free Software Foundation
- Richard Stallman - 2012-09-28 - Le logiciel libre et votre liberté (à la HEB-ESI et en français) - YouTube

Jargon file :

- Secuser.com - Comment devenir un hacker?
- How To Become A Hacker - BecomeAHacker.pdf

Presse :

- Les Inrocks - Steven Lévy : «Le sens du mot hacker a considérablement évolué»
- La «hacker attitude», modèle social pour l'ère post-industrielle - Libération
- Snowden to Hackers: Your Tech Skills Can Save Democracy