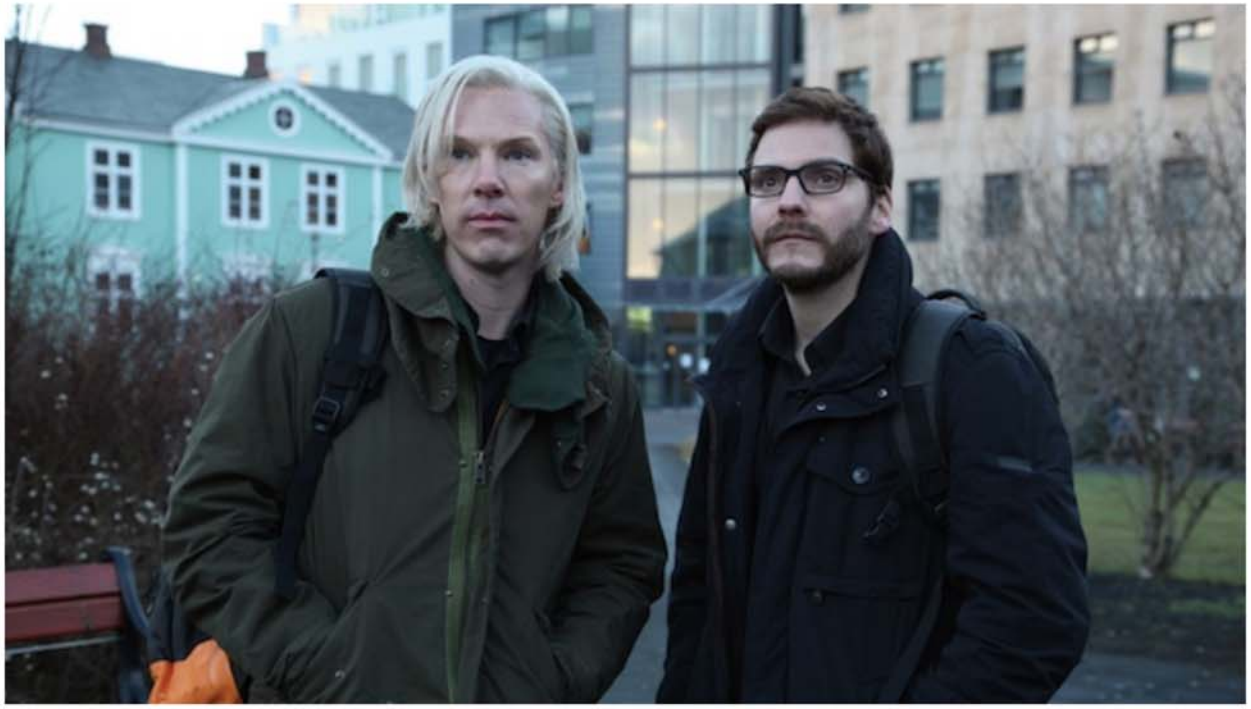
RAGEMAG



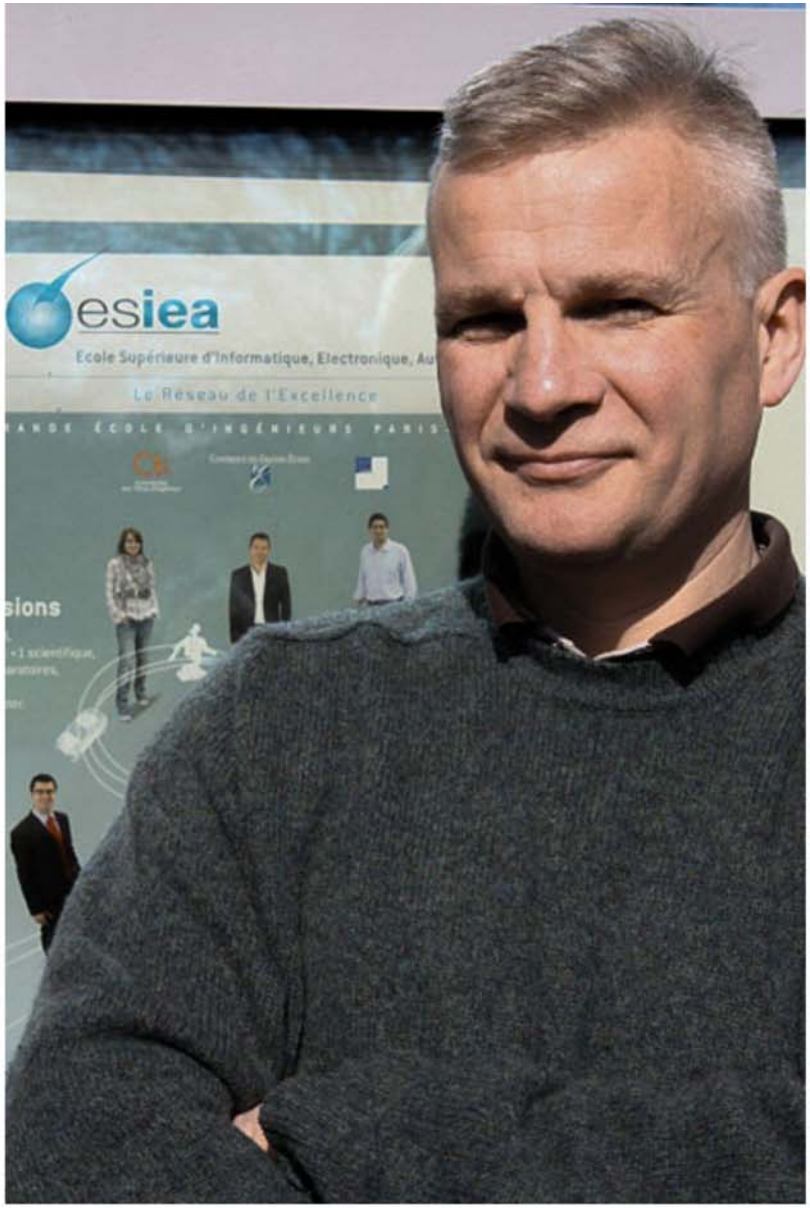
Monde

Éric Filiol : « Mépriser les hackers est une erreur stratégique. »

Publié le 7 mars 2014 à 16:09 par **Adrien Gévaudan** | 0

English version

Y a-t-il une mentalité hacker en France ? À l'occasion de la concrétisation du projet DAVFI (Démonstrateurs d'Antivirus Français et Internationaux), présenté comme un service de sécurité inviolable, nous avons rencontré son concepteur, Eric Filiol. Scientifique diplômé en cryptologie, docteur en informatique et mathématiques appliquées, diplômé de l'OTAN dans le domaine de l'InfoOps et diplômé HDR à l'Université de Rennes, ce corsaire numérique a passé vingt-deux ans dans la Défense en régimen puis près de quinze autres années dans le domaine du renseignement et de l'opérationnel technique.



Éric Filiol, photo CNIS.

Vous considérez-vous comme un hacker ?

Oui, et de plus en plus ! Même si l'approche académique reste intéressante, dans le domaine de la sécurité, surtout si l'on vise une capacité opérationnelle, la seule approche possible est de privilégier les résulta

sur les méthodes (même si les méthodes peuvent être très utiles, même aux hackers), ce que seuls les hackers sont capables de faire. Prétendre faire de la sécurité et ignorer, voire pire, mépriser le phénomène, l'approche et le monde hacker devient une faute professionnelle et une erreur stratégique. Je présente donc de plus en plus mes travaux dans les grandes conférences internationales de hacking (Black Hat, CCC CanSecWest, PacSec, Hack.lu…) car c'est là que tout se passe. La France est la seule à ne l'avoir toujours pas compris. De plus, l'esprit hacker représente un nécessaire contre-pouvoir qui chérit, comme moi l'esprit de liberté et la reconnaissance au mérite, technique mais aussi éthique, contrairement à ce que la majorité des gens pensent). Je vois de plus en plus ce mouvement et cette pensée comme de la résistanc

Vous avez donc travaillé, longuement, pour l'État français. N'y a-t-il pas une difficulté à vouloir concilier une éthique aussi réfractaire à l'autorité que l'est l'éthique hacker et la rigidité inhérente aux différents offices de l'État ?

Absolument pas. Tout d'abord, je viens d'un milieu – le monde militaire – éminemment humain, dans lequel la valorisation permanente de l'autre est à la base des principes du commandement. Je retrouve ces valeurs en partie dans le monde du hacking. Vous ne pouvez pas gérer des hommes sans avant tout les aimer, ce que notre pays a totalement oublié. En France, tout notre système repose sur le conflit et la concurrence permanents entre individus. Dans le monde hacker, la coopération, le partage et l'émulation réciproque sont plus la norme. Mon expérience de certains hackers montre qu'ils n'ont pas un esprit aus réfractaire que certains veulent bien le faire croire (et c'est tellement plus simple de le croire ou de le faire croire, le vieux problème du chien et de la rage).

> « J'ai même rencontré assez souvent plus de sens du bien commun chez les hackers que chez bien des hauts fonctionnaires ou certains politiques. »

J'ai même rencontré assez souvent plus de sens du bien commun chez eux que chez bien des hauts fonctionnaires ou certains politiques. Mais cela s'exprime à leur manière. Comment veut-on que ces jeunes n soient pas désabusés, déçus, voire ne rejettent l'État alors qu'on leur explique qu'ils n'existent pas et n'ont pas droit de cité ? Ils ont un énorme potentiel et cherchent aussi à ce que l'on s'occupe d'eux. Il faut que nous les reconnaissions, les aidions, car ils ont le désir de contribuer au bien commun (je rappelle que dans la grande majorité des cas, ces jeunes pratiquent le *ethical hacking* et qu'il y a un sacré décalage entre le nombre important de hackers en France et dans le monde et le faible nombre de cas de piratage ou de comportements condamnables) et veulent être reconnus pour et par leurs compétences.

L'Histoire montre que lorsque l'État devient mou, se trahit lui-même, sans volonté de défense face à l'agression permanente extérieure, en particulier économique et culturelle, des foyers de résistance naissent spontanément et l'esprit corsaire renaît. L'exemple de l'Allemagne montre qu'il n'y a absolument aucune difficulté à faire travailler hackers et État ensemble. Depuis le début des années 80, notre voisin a su organiser, et surtout s'accorder avec la communauté hacker, travaillant très utilement avec elle, dans le respect mutuel de la culture et des intérêts de chacune des parties.

On a beaucoup parlé du projet DAVFI, devenu Uhuru pour sa valorisation commerciale, notamment dans le cadre du grand emprunt, l'année dernière. Pouvez-vous nous en dire plus ?

Il s'agit de développer un antivirus de rupture, ouvert, et de confiance. La préoccupation principale n'est pas de répondre à un modèle économique déséquilibré mais de placer la préoccupation de sécurité au cœur de la conception et du développement. Ce concept permet de mettre en œuvre les techniques et approches les plus efficaces. L'outil est également pensé pour évoluer en fonction des besoins et demandes des utilisateurs. La confiance que l'on pourra lui accorder en tant qu'outil de sécurité sera garantie par l'ouverture du code : un outil de sécurité ne doit pas lui-même ajouter une incertitude quant au niveau général de sécurisation d'un système.

Surcouf, l'esprit corsaire.

Le projet est réalisé dans le cadre du Programme des Investissements d'Avenir. Il a été labellisé par le pôle de compétitivité System@tic et a reçu le soutien de l'AFUL (Association Francophone des Utilisateur de Logiciels Libres). Comme je n'avais plus de contrainte économique et de *business model* qui devait prendre le pas sur la sécurité, contrairement à l'offre antivirale commerciale, j'ai pu choisir librement les

concepts scientifiques et techniques, ainsi que les modèles de sécurité adéquats (certains d'ailleurs issus des années 50). Cela a donné naissance à une approche totalement nouvelle. Cela représente des années de recherche et de réflexion tant théorique que pratique, et j'avoue profiter de ce projet pour les concrétiser. Ma priorité a été et est de pouvoir lutter pro-activement contre les codes inconnus et les premiers résultats montrent que nous y parvenons efficacement. DAVFI est prévu pour Android (DAVFI Androïd), Linux et Windows.

DAVFI Android a été livré à Nov-It, la société qui sera en charge d'assurer le soutien R&D et le développement commercial, le 17 octobre 2013 (avec un an d'avance, le projet se terminant le 30 septembre 2014). DAVFI sera livré, pour les entreprises, avec certains outils de génération autonome de signatures (un organisme d'importance vital ne peut sous-traiter ses attaques à une société tierce), de gestion de par (MDM), d'infrastructure complète pour des organismes qui veulent être autonomes. Enfin, DAVFI se veut respectueux de l'utilisateur en préservant au maximum sa liberté, dans le respect de la politique de sécurité définie par l'entreprise. En fait, DAVFI a été conçu pour être pleinement configurable à la politique et aux nécessités de sécurité de chaque entreprise.

Le dernier point important concerne l'ouverture du code. Cela va dépendre du système cible. Autant sous Android et Linux, il est facile de tout ouvrir, autant sous MS-Windows, cela peut poser d'autres problèmes, en particulier sur un point juridique avec Microsoft. DAVFI descend si profond dans le système (pour tendre vers un système d'exploitation antiviral en ring 0 et non plus une simple application antivirale en ring 3) qu'il faut étudier tous ces aspects pour ne pas être accusé de contrefaçon par des gens plus attirés par la conservation de leur monopole de fait que par l'innovation.

> « Tant que nous serons dépendants du logiciel propriétaire, et en particulier de Windows, nous ne serons pas véritablement libres. »

Je suis convaincu qu'il est impossible de faire du libre sur du logiciel propriétaire quand on touche au ring 0. Seule la gendarmerie semble l'avoir compris. Donc en ce qui concerne l'ouverture du code DAVFI Windows en totalité, ce n'est pas moi qui déciderai mais je pense que cela n'est pas possible. Tant que nous serons dépendants du logiciel propriétaire, et en particulier de Windows, nous ne serons pas véritablement libres.

Les bâtiments de la NSA.

—

Qu'est DAVDROID par rapport à Uhuru ?

DAVFI Android est la version pour les plateformes Android et pourra s'installer sur tous les téléphones Android compatibles. Il sera open source et destiné à tous les publics. Mais il a été nécessaire de faire plu qu'une application antivirale, en particulier pour lutter contre toutes les attaques possibles (notamment par accès physiques, comme celles que nous avons montrées sur *Envoyé Spécial* et bientôt dans *Zone Interdite* sur M6). On a donc repris un system Android (base cyanogène et source Google) que nous avons nettoyé, durci et sécurisé. En fait, cela est devenu un système d'exploitation antiviral avec chiffremer de voix (VoIP), chiffrement de SMS, VPN, anti-géolocalisation (les applications qui veulent vous localiser sont flouées et renvoient aléatoirement vers l'un des 20 lieux présélectionnés comme la NSA, le FBI, l Kremlin, Buckingham Palace, le GCHQ, la DGSE, le FSB…). Le système de fichier est totalement chiffré, les applications sont certifiées et signées… Bref, tout a été repensé.

Vous déclarez DAVDROID « in-hackable » ; est-ce par provocation, ou le pensez-vous sincèrement ? Avez-vous conscience que de telles prétentions ne peuvent que motiver la communauté hacker à les casser ?

En fait, il faut savoir que le modèle de sécurité sous-jacent est aux antipodes de celui utilisé de nos jours. Je suis parti du principe que ne pouvaient s'exécuter que des ressources expressément autorisées (le res étant bloqué par défaut). Les applications sont analysées selon de toutes nouvelles approches formelles et techniques. En particulier, nous parvenons à identifier des vulnérabilités de type 0-day et à demander a auteurs de l'application de les corriger avant d'être certifiées à la fois sur le plan fonctionnel et sur le plan de la qualité du code.

> « Notre système a déjà été audité par des gens qui pensaient le contourner. Pour le moment, nous les avons tous mis en échec. Nous souhaitons qu'il soit analysé par les hackers du monde entier. »

Dans ces conditions, il est aisé d'apporter la preuve de sécurité souhaitée. Rappelons que les antivirus commerciaux, eux, fonctionnent sur le modèle « tout ce qui n'est pas expressément interdit (par les bases signatures) est autorisé par défaut ». Cela préserve donc l'avantage naturel de l'attaquant. Notre système a déjà été audité par des gens qui pensaient le contourner. Pour le moment, nous les avons tous mis en échec. Le système, nous le souhaitons, sera analysé par les hackers du monde entier. Seul ce type d'épreuves du feu permettra de confirmer la qualité du produit et au final de l'améliorer si besoin était. Mais je reste très confiant.

Le citoyen ou l'internaute lambda peut-il l'adopter ?

Oui, il est prévu que le particulier puisse s'en équiper, et ce gratuitement (sauf s'il souhaite avoir une version pré-installée, dans le cas de DAVDROID, sur le téléphone de son choix, il n'aura que le prix du téléphone majoré du service). Les mises à jour seront également gratuites, il n'y aura donc aucune redevance ou abonnement à payer. Certains services réservés aux entreprises seront en revanche disponibles payant pour le particulier. DAVDROID sera disponible commercialement dès le début avril 2014.

L'affaire des écoutes de la NSA vous a-t-elle surprise ?

Non, pas vraiment. Depuis la fin des années 40, les USA et leurs principaux alliés historiques (Royaume Uni, Canada, Australie et Nouvelle-Zélande, membres fondateurs de l'UKUSA et de l'ANZUS) ont mis en place un véritable système d'espionnage planétaire doublé d'un nécessaire (nécessaire pour mettre en place ce système) contrôle de la technologie (Accords CoCom, Wassenaar, GATT, OMC…). Le résulta est PRISM et ses nombreux sous-programmes. Seuls les naïfs ou les faibles, comme nos politiques, peuvent en être encore étonnés. Le manque de réaction des populations européennes, sud-américaines, asiatiques, et le manque de pression sur leurs gouvernants me surprend beaucoup plus.

Mais peut-on s'offusquer contre l'hégémonie américaine quand on est drogué à ses produits technologiques et culturels ? Comment peut-on espérer que la jeunesse développe un quelconque esprit de résistance et de rejet quand la seule préoccupation de l'écrasante majorité de ces jeunes est la sortie du prochain iPad ou du prochain épisode d'une série US débile ? Au passage, l'hégémonie culturelle des USA sur les jeunes, génération qui sera demain aux manettes, vise en réalité à transformer une acculturation en assimilation. Hollywood a triomphé de Montaigne, l'esprit marchand de la vision humaniste.

NSA, logo parodié depuis PRISM.

Ces dernières années, il semble que les États agissent de plus en plus dans le cyberespace et l'appréhendent désormais comme un nouvel espace stratégique à part entière. Où se situe la France dans ce nouveau concert des puissances ?

Pour paraphraser Staline, je dirais : la France, combien de divisions de hackers ? La France est quasi-inexistante et manque totalement de volonté politique (à part quelques gesticulations destinées à donner le change), alors qu'elle dispose d'un formidable potentiel, probablement l'un des meilleurs avec l'Allemagne, pays auquel je crois plus en termes de puissance dans ce domaine. Nous avons un système éducatif d qualité mais il sort de plus en plus des esprits formatés qui se retrouvent de plus en plus inadaptés à la réalité du cyberespace. Je n'aime pas vraiment ce mot qui ne veut pas dire grand-chose, d'ailleurs. Ce système ne sait pas valoriser TOUS les jeunes qui pourraient apporter un savoir, un savoir-faire et une vision précieux pour la France. La France a juste su en faire une affaire de clientélisme régional en créant un pôle d'excellence cyber-défense en Bretagne uniquement. J'aurais aimé un élan plus national, fédérateur de toutes les compétences et bonnes volontés.

L'analyse de la lettre de mission du ministre montre clairement que les autres régions sont purement et simplement écartées. Quant au volet attaque, développé maintenant par la plupart des pays du G-8 sinon d G-20, il faut encore le chercher, et la principale conséquence en est un abandon total des entreprises, qui se font tailler des croupières à l'international. Avec un peu plus d'esprit corsaire, je pense que l'on aurai pu mieux « lutter » contre les suédois et gagner le marché brésilien pour le Rafale, et je ne parle même pas de la situation en Chine pour nos entreprises ou face aux entreprises US…

Les hackers et le pouvoir

par KheOps

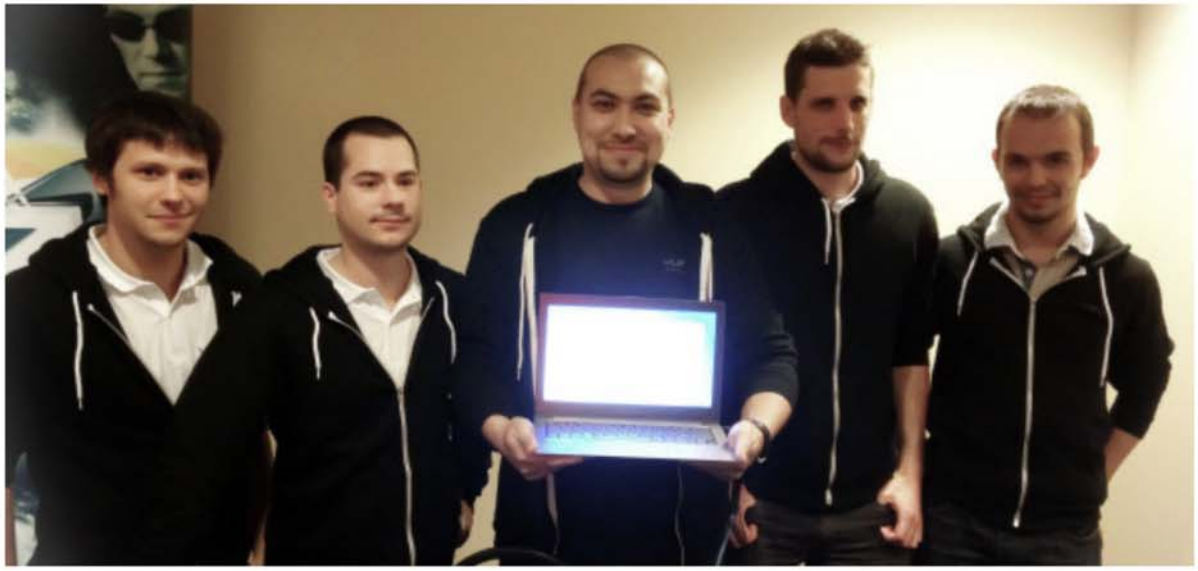
—

Le développement de nouveaux moyens de communication et de propagation du savoir a souvent fait peur aux pouvoirs en place et a souvent donné lieu à des répressions violentes et à des accès obscurantiste: Un bon exemple est l'invention de l'imprimerie, qui remettait en question le pouvoir des moines copistes. Ici, c'est une étape supplémentaire : on remet en question le pouvoir des médias traditionnels, de la stèl sur laquelle les responsables politiques sont placés lorsqu'ils s'expriment, etc. Cela ne peut que créer des frictions, éventuellement violentes, mais il ne fait aucun doute qu'à la fin de cette histoire, on gagne. C'e une étape parmi d'autres pour l'humanité je suppose. La crise passera et le plaisir restera !

Sur une plus petite échelle temporelle, on peut regarder en souriant comment beaucoup de médias parlent de Telecomix comme étant « *venu au secours* » des Syriens et comment ces mêmes médias écrivent d idioties sur les hackers, les dangereux « *pirates de l'internet* » qui menacent la société. L'envie de faire du *storytelling* conduit parfois à de grands écarts risibles.

Et je le répète : nous agissons par solidarité. Il y a des questions à se poser avant de lancer un missile quelque part, pas lorsqu'on aide sans discrimination des personnes à s'informer et à s'exprimer dans des conditions acceptables. S'il y a une réflexion de fond à mener, elle concerne plutôt les outils à mettre en place pour rendre les actions instantanées plus efficaces. L'idéal serait que les actions instantanées ne soient plus nécessaires car tout le monde aurait la connaissance et les outils pour se débrouiller. Et Telecomix pourrait agir pour des idées qu'il ne soutient pas. On ne peut pas discuter des idées et mesurer leur dangerosité si elles ne sont pas visibles publiquement. . Les propos publics doivent être exposés publiquement, d'autant plus s'ils contiennent des idées potentiellement dangereuses.

Extrait de « Entretien avec KheOps »



VUPEN, la PME française au cœur de la tempête.

—

A-t-on des points forts à faire valoir, des points faibles ?

Je pourrais énumérer différents points forts, oui :

- Une ressource humaine et intellectuelle à tous les niveaux (et nous avons besoin de tous les niveaux et de toutes les contributions, et en particulier une communauté hacker riche, inventive, volontaire, motivée).
- Un esprit, voire un génie français pour les sciences et en particulier l'informatique.
- Une capacité d'innovation hors pair mais essentiellement au niveau des TPE/TPI, PME/PMI voire ETI.

Les points faibles seraient alors les suivants :

> « Je considère VUPEN comme un fleuron technologique : la France devrait en avoir plus. C'est un leader mondial dans son domaine. »

- Un manque de volonté politique et de vision stratégique.
- Un manque d'esprit citoyen et une méfiance systématique vis-à-vis de l'État. Je suis toujours sidéré de voir une opinion française se méfier de nos services et de notre État sur des points de détails et e même temps être d'une mansuétude, voire d'une atonie stupéfiante face aux révélations de Snowden. Une des forces des USA est justement cet esprit citoyen.
- Une vassalisation inacceptable aux USA résultant en une perte quasi-totale de souveraineté (le meilleur exemple est le marché Microsoft / Open bar).
- Un esprit trop clientéliste : acheter la paix sociale plus que financer l'innovation.
- Un esprit trop élitiste et jacobin, doublé d'une réelle discrimination des potentiels.
- Un manque de pragmatisme certain et du sens opérationnel.
- Un manque d'humilité sur la scène internationale.
- Notre esprit gaulois qui favorise le déchirement national entre individus et entités au lieu de promouvoir la coopération et l'effort commun.
- Un système éducatif primaire, secondaire, supérieur qui devient de plus en plus inadapté à la chose « cyber » : il n'existe toujours pas de CAPES et d'agrégation en Informatique, et la programmation n'est pas enseignée avant le supérieur. Je suis sidéré par le manque de caractère opérationnel de nos formations mastère spécialisé qui favorise uniquement la théorie souvent stérile car dé-corrélée de la réalité du terrain.

Le déplacement de l'entreprise française VUPEN aux États-Unis a fait bondir de rage beaucoup d'experts du secteur ; pourriez-vous nous expliquer un peu ce cas ?

Il est clair que cela ne fait jamais plaisir de voir partir, du moins potentiellement, à ce jour, un fleuron français dont semble dépendre en partie les USA. Ce cas, certes très emblématique, n'est hélas pas le seul. Mais il ne faut pas oublier qu'une entreprise, ce que semblent ignorer nos politiques qui n'ont jamais mis les pieds dans un tel monde, sauf à vivre des perfusions de l'État, a une obligation de rentabilité, et que rentabilité passe par le chiffre d'affaire. Donc si l'État fait tout pour ne pas aider ces petites sociétés innovantes, voire leur complique la vie, il est normal que pour survivre elles doivent aller là où se trouve le marché. Ces entreprises partent le plus souvent parce qu'on les pousse à le faire, rarement par choix. Ce qui m'a fait le plus bondir c'est la réaction en octobre 2013 de certains hauts fonctionnaires mis au courant de ce risque : « *Et alors ? Ces gens ne nous impressionnent pas !* ». Traduction : ils ne sortent pas du sérail, comment pourraient-ils être intéressants ? La messe est dite.

La mise au point dans *Le Monde* n'est pas nécessairement rassurante. Je la vois plutôt comme un message à nos politiques. Le paragraphe final est plutôt une mise en garde : « *Nous avons des liens forts avec patrie et aucun projet de déménagement aux USA n'est actuellement à l'ordre du jour. Comme toute start-up dans un domaine stratégique, VUPEN suscite l'intérêt de grands groupes, notamment américains. Néanmoins, nous veillons à ce que VUPEN reste une société française – tant que l'environnement, la législation et la réglementation [...] nous permettent de poursuivre sereinement le développement de nos activités de recherche en France, et l'exportation de notre savoir-faire français vers toute l'Europe et l'Amérique.* »

Je considère VUPEN comme un fleuron technologique : la France devrait en avoir plus. C'est un leader mondial dans son domaine. Il investit dans la R&D, même au plan théorique, ce qui prouve qu'outre un niveau technique très élevé, ils ont aussi une vision stratégique à plus long terme. J'avoue que cela serait rageant que les USA se paient à moindre frais ce fleuron, capitalisant sur la nullité de nos décideurs. Normalement, VUPEN et sa technologie devraient être gérés à haut niveau par les commissions spécialisées dans la protection du patrimoine sensible, l'exportation du matériel de guerre ou des techniques à usage dual, et bien sûr le FSI devrait se prononcer, il a été théoriquement fait pour cela, voire la BPI – organismes qui brillent par leur silence. Et dans le cas VUPEN, on peut estimer avoir de la chance, contrairement à des sociétés comme SmartQuantum qui en ont eu moins.

Au delà de cette délicate question de la protection du patrimoine entrepreneurial français, quelles sont les thématiques sur lesquelles il faudrait se concentrer, en France, actuellement ?

La première des mesures – fondamentale et vitale – est de retrouver sa souveraineté nationale voire de créer une véritable souveraineté européennes recentrée. Cela passe par plusieurs aspects et décisions :

- Affirmer et organiser la prééminence voire la priorité d'usage du logiciel libre et donner naissance à une vraie industrie de services autour de lui – il devrait être interdit pour les administrations d'utiliser des logiciels propriétaires, du moins sans en détenir la totalité du code source.
- Sortir de l'OTAN, car être dans l'OTAN oblige à utiliser les produits américains de Cisco, Microsoft , McAfee… et croyez bien que ce ne sont pas les mêmes versions que celles utilisées par l'armée U
- Recréer une véritable industrie européenne dans le domaine des équipements de sécurité et IT, côté routeurs par exemple.
- Enfin, ajouter à l'exception culturelle, celle de l'exception des technologies IT et de sécurité, ce que font les USA en violation des règles de l'Organisation Mondiale du Commerce. Comme aux USA, aucune technologie, équipement, logiciel non européen et non produit par des européens ne devrait être autorisé en Europe, le reste est juste affaire de détail. Il faut d'abord bâtir un cadre cohérent et fort.

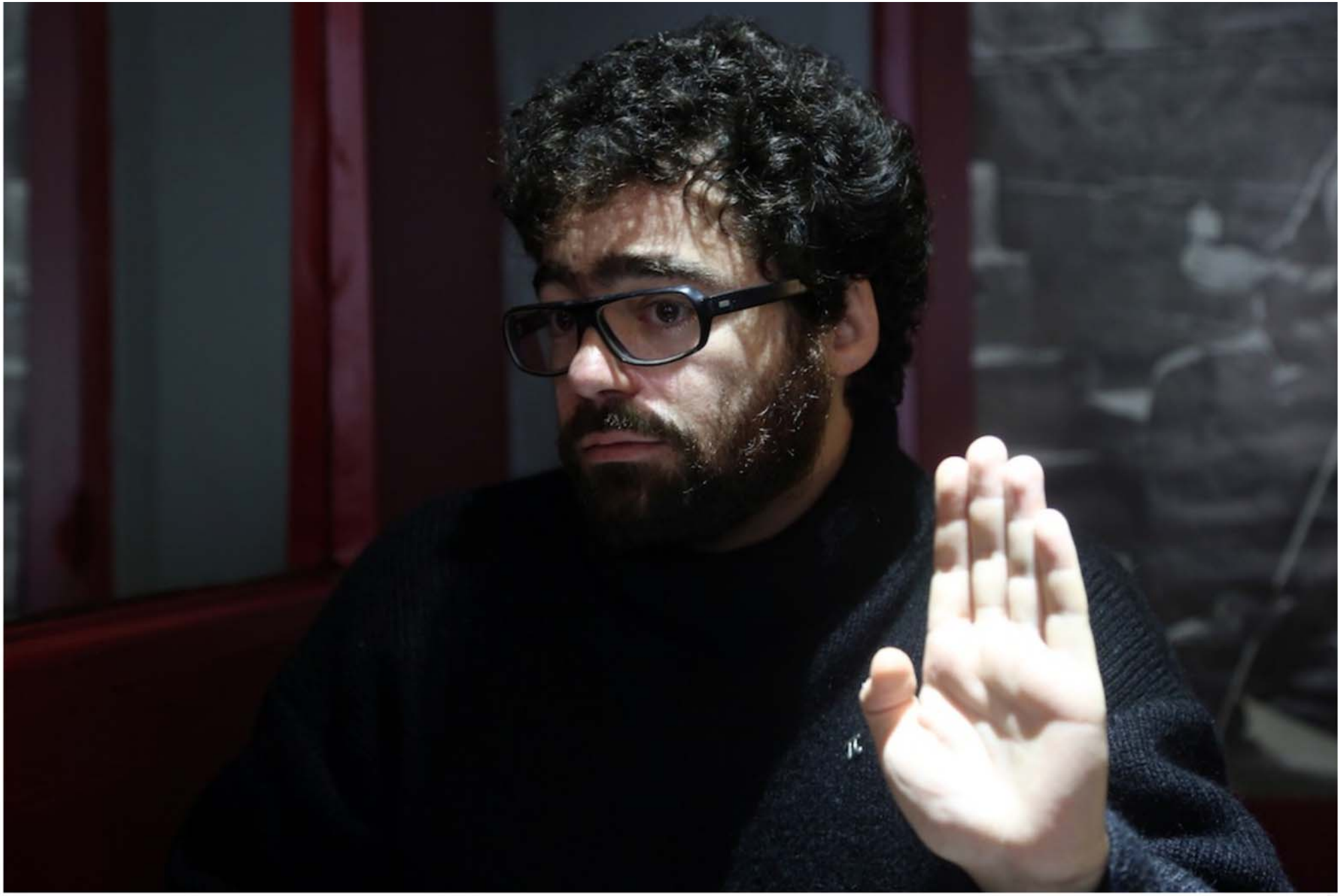
Le monde politique français comprend-il le cyber ?

Je suis convaincu, par mon expérience et pour avoir rencontré certains de ses membres, que le monde politique – et la plupart des hauts fonctionnaires – ne comprend plus grand-chose à quoi que ce soit, et en particulier au « cyber ». La quasi-totalité des décideurs politiques ont une formation littéraire et aucune formation opérationnelle, que ce soit celle des entreprises ou de la société. À force de vivre depuis leur naissance dans une bulle, préservés de la réalité du monde, confortés dans des modèles et des « connaissances » d'un autre temps, ils ne sont plus en phase avec le monde et leurs citoyens.

> « Souvenons-nous que pour un de nos anciens ministres, OpenOffice est un pare-feu. »

Je pense que la plupart seraient tout simplement incapables de vous donner le prix (même approximatif) d'un produit ou d'un service de consommation courante. Alors, comprendre le cyber… Souvenons-nous

que pour un de nos anciens ministres, OpenOffice est un pare-feu. Du coup, le monde politique est la victime des lobbyistes et affairistes qui nous fourguent une technologie non souveraine, et *a minima* non européenne.



Jérémie Zimmermann par Jeanne Frank pour RAGEMAG.

—

Edward Snowden a changé le monde

par Jérémie Zimmermann

—

Wikileaks a ouvert la boîte de Pandore qu'est cette nouvelle utilisation d'Internet pour la diffusion d'information à des fins d'intérêt général. D'une part, ça, ça me semble assez évident : la démarche de Snowden n'aurait peut-être pas été ce qu'elle est s'il n'y avait pas eu Wikileaks avant. D'autre part, on voit clairement que le gouvernement US réagit dans la panique. Quand Wikileaks était la pointe émergée l'iceberg, on se souvient des sénateurs américains qui disaient qu'Assange était un terroriste et qu'il fallait lui envoyer des drones. On se souvient aussi du coup de fil du Département d'État aux entreprises US qui a sans doute conduit à couper les vivres de Wikileaks, notamment Visa, Paypal, etc.

Depuis, on a l'impression que c'est devenu la doctrine du gouvernement américain et on l'a vu avec Snowden : pour que l'avion du président Morales soit à ce point menacé, qu'en Europe tout le monde se mette carpette pour ne pas le laisser passer, cela montre bien que les US avaient l'intention de le descendre. Ce sont des signaux qu'envoie une superpuissance qui est acculée pour dire « voilà, le prochain qui l'ouvre, on le flingue ». On a l'impression que cette chasse aux *whistleblowers* est devenue une doctrine du gouvernement. Cela confirme quelque part le fondement philosophique de Wikileaks théorisé par Julian en 2006, qui disait que lorsque des gouvernements se cachent derrière le secret pour mentir ou commettre des crimes, à ce moment-là, exposer ces secrets ajoute de l'inertie. Leur culture du secret les conduit à une nature paranoïaque, mais on augmente le niveau de paranoïa pour les forcer à l'inertie. On voit la confirmation de cette doctrine-là, j'ai l'impression.

Avec Snowden, on a une preuve évidente qu'une personne seule peut changer le monde. Ce bonhomme a 30 piges, il a un passé scolaire pas très brillant, il était un employé parmi tant d'autres, dans une des centaines de boîtes de sécurité privée (un merdier tentaculaire). Ce bonhomme parmi tant d'autres a changé le monde. Que le *Spiegel* dise cette semaine « Asile pour Snowden ! » sur sa couverture, sans point d'interrogation, que 50 personnalités de la politique et de la culture prennent sa défense dont des vieux conservateurs de 80 piges, que le nid d'espion de la NSA au-dessus de l'ambassade américaine en face de la chancellerie soit exposé en première page du*Spiegel* avec des attaques ultra violentes, que l'Allemagne soit en train d'altérer ses relations diplomatiques avec les US, alors qu'elle était l'un de ses plus fidèles alliés dans l'Union Européenne, c'est quelque chose d'ampleur historique et c'est uniquement grâce au courage de Snowden. Alors coup fatal ou pas fatal, j'en sais rien, mais décisif, c'est sûr. C'est ça qui est important : montrer que les actions d'une personne peuvent changer le monde.

Extrait de « Entretien avec Jérémie Zimmermann »

Que pensez-vous des combats d'*hacktivistes* comme Jérémie Zimmermann de la Quadrature du Net, ou encore de Julian Assange ?

L'hacktivisme est une dimension intéressante voire utile et j'imagine qu'accompagnée d'éthique et de certaines autres valeurs incontournables, comme le respect des autres, il peut constituer une nouvelle dimension politique dont les sociétés modernes ont bien besoin pour renouveler un débat et une vie politique gangrenée par le népotisme, le copinage, le clientélisme et l'idéologie. Maintenant, je pense qu'il ne faut pas confondre des gens comme Zimmerman, que je respecte et admire, et des gens comme Assange et Snowden. Jérémie mène une action positive en utilisant des moyens et approches non seulement légales mais éthiques. C'est un vrai combattant au sens politique et humain du terme et tout ce qu'il fait, toutes ses convictions existent pour le bien des autres.

Des gens comme Assange ou Snowden ne sont absolument pas clairs. Assange a instrumentalisé et mis en danger des personnes qui lui ont fait confiance. Et ce faisant il a mis en danger des gens qui servent – certes quelquefois mal mais avec conviction – leur pays. Snowden est encore plus suspect. Je ne crois pas à sa croisade et à sa posture de chevalier blanc. Il a volé des centaines de milliers de documents et les distille au compte-goutte. Snowden a oublié que la NSA n'était pas les États-Unis. Comme Jérémie Zimmerman le fait, son combat, pour avoir plus de poids, aurait dû être mené sur le sol US. Entre l'Electroni Frontier Foundation, le site Cryptome et l'ACLU, il existe des contre-pouvoirs relativement efficaces aux USA.

Snowden a-t-il fait du bien à ces combats ?

Edward Snowden.

Nous pouvons, dans l'immédiat, imaginer naïvement que oui. Mais à plus long terme, je pense que cela ne fera même pas vaciller les États-Unis qui savent sortir plus fort de ce type d'épreuve. Au final, que va-t-il en rester ? Qu'est-ce qui a réellement changé dans l'opinion et chez nos décideurs ? Fondamentalement, rien. Et *a contrario* des USA, nous, les pays européens, allons en ressortir plus faibles parce que justement nous n'allons rien faire. Je n'oublierai jamais le courage de deux femmes – Dilma Youcef et Angela Merkel – lâchées par la veulerie politique de leurs collègues masculins. C'est le problème avec le *whistleblowing* : dans un contexte politique mou et faible, de peuples composés de consommateurs et non plus de citoyens : cela revient à siffler contre le vent. Au final, les forts en ressortent plus forts et les faibles plus faibles. Les premiers ont juste eu l'occasion de rappeler aux seconds qui sont les maîtres.

Que pensez-vous du *whistleblowing* ?

Il est indéniablement utile mais il doit être encadré pour éviter les débordements et les dommages collatéraux. Il faut certes dénoncer certaines pratiques ou certaines situations mais il faut le faire dans le respect des règles et surtout des personnes qui peuvent être impliquées. On ne peut livrer en pâture des informations brutes voire très sensibles sans mettre en danger des personnes et des entités et au final provoquer l

chaos. Au sortir de la Seconde Guerre mondiale, le Général de Gaulle a dû gérer le problème de tous les fonctionnaires qui avaient collaboré plus ou moins avec l'occupant. Deux solutions s'offraient à lui : tout était révélé, et tous les coupables condamnés, mais l'État et la stabilité du pays ne s'en seraient pas relevé et il aurait manqué un grand nombre de cadres indispensables à la reconstruction nationale – autrement dit, on passait d'un chaos à une autre – ou bien, comme il a choisi de le faire, œuvrer pour gérer cela progressivement, en douceur et discrètement.

Je pense qu'il faut permettre de s'exprimer à des gens qui voient dans leur métier des choses inacceptables et qui, soucieux du bien commun, le ressentent cruellement comme tel. Peut-être faudrait-il créer une juridiction administrativement indépendante (JAI) pouvant recevoir les confessions ou les révélations de ces personnes. Il faudra peut-être envisager de créer des séances d'auditions de ces personnes par des commissions des deux chambres, donner des pouvoirs particuliers à des juges spéciaux… Bref, il faut un cadre, et non favoriser l'anarchie. Il faut que ce cadre protège les *whistleblowers*. Et enfin, il faut que l exactions révélées fassent l'objet de traitements judiciaires, voire de rétorsions fortes.

Certes, l'on peut critiquer les démarches de certains ; mais l'essentiel n'est-il pas de faire sortir les affaires, de crever les abcès ?

Le problème est que cela est fait hors de tout contexte, et les dommages collatéraux sont immenses et souvent à effet retardé. Qui peut dire ce que le cas Snowden va avoir comme conséquence, dans 5, 10 ou même 20 ans ? Au plan géostratégique par exemple. Des données brutes sont difficiles à traiter hors de tout contexte. Il faut le recul de l'expérience, de l'histoire, de la culture pour appréhender un fait ou une somme de faits. De plus, cela met les États en situation de ne pas réagir autrement que par des voies légales.

> « Je crois beaucoup à cette forme d'activisme doux, liée au monde du logiciel libre. Il est parvenu à faire vaciller des géants comme Microsoft, pour lequel les prochaines années vont être difficiles. »

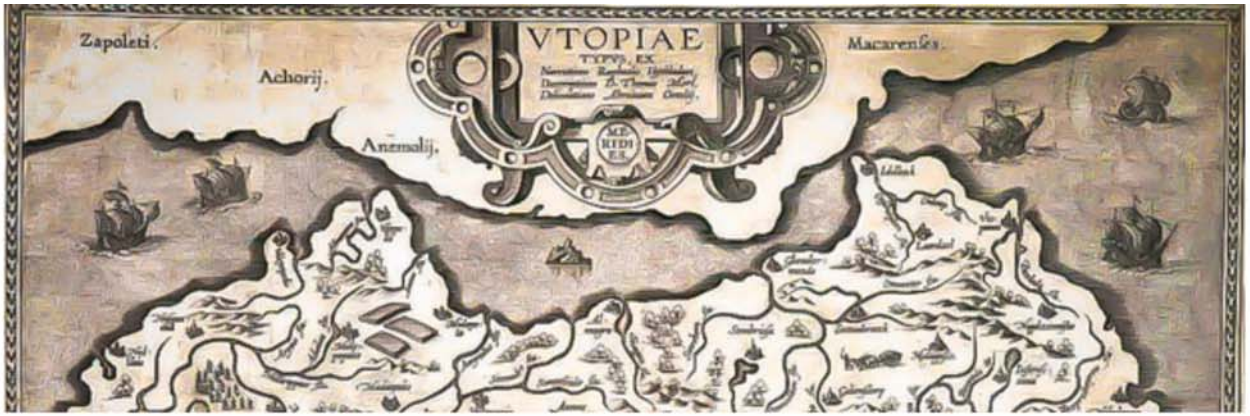
Si cela était resté dans le cadre discret du monde du renseignement, des pays européens auraient pu (ré)agir par des mesures plus fortes, discrètes, mais contre lesquelles les États-Unis n'auraient pu rien faire. Encore une fois, tout ce que nous allons gagner est un renforcement des États-Unis et un affaiblissement des pays européens qui exposent leur inertie, pour ne pas dire plus, à la face du monde. En plus, ces révélations, le plus souvent, ne surprennent que les naïfs et les néophytes – ce qui inclut pas mal de nos politiques.

Que peuvent tous les projets comme DAVDROID, au niveau mondial ? Pensez-vous que l'atomicité des démarches est une force ou une faiblesse, face à toutes les affaires ayant éclatées dernièrement ?

Je crois beaucoup à cette forme d'activisme doux, liée au monde du logiciel libre. Il est parvenu à faire vaciller des géants comme Microsoft, pour lequel les prochaines années vont être difficiles. La variété, corollaire inévitable de cette atomicité, est bonne en toute chose. Elle oppose un front mouvant et difficile à gérer de manière unique, à l'adversaire, qui de plus à la faiblesse de vouloir tout contrôler par l'homogénéisation et les standards. C'est la meilleure façon de lutter face aux incertitudes de l'avenir. Pourquoi est-on condamné pour l'instant à utiliser les mêmes solutions propriétaires ? Parce que pour le moment il n'existe pas de solutions alternatives. Mais elles arrivent et de manière durable. C'est la seule voie possible pour un retour de la souveraineté des pays.

La question du contrôle de la technologie est-elle un enjeu citoyen ?

Oui sans aucun doute. La principale question est : quel type de société voulons nous, nous citoyens, pour demain et pour les générations futures ? Soit on laisse l'État exercer ce contrôle indûment (hors d'un cadre juridique rigoureux), soit les citoyens s'organisent, disent non et font les bons choix. C'est le dilemme entre être citoyen et être consommateur. Les générations actuelles n'ont plus l'esprit militant et encor moins celui de la résistance. En gros, voulons-nous tendre vers une dystopie de type STASI ou vers une utopie telle que décrite par Thomas More ? Le contrôle de la technologie surtout à des fins liberticides n'est aucunement inévitable. Par exemple, si demain, une majorité d'électeurs décident de se déplacer et de voter « blanc », cela fera mal et ne pourra pas être ignoré.



Utopie, par Abraham Ortelius.

Article paginé

Boîte noire

- Démonstrateurs d'Antivirus Français et Internationaux, sur le web ;
- Uhuru, la sécurité made in France ;
- tester Uhuru Mobile, c'est par là ;
- Jérémie Zimmerman, « Edward Snowden a changé le monde » ;
- KheOps, « Hacker, un citoyen qui cherche à améliorer la société avec sincérité. » ;

Mots-clés : assange, attaque, cyberdéfense, Edward Snowden, éric filiol, filiol, géostratégie, hack, hacker, hacking, Julian Assange, lanceur d'alerte, Snowden, whistle blower

À propos de l'auteur

Adrien Gévaudan Géoéconomiste avec un penchant pour la cyberstratégie, je suis également le fondateur d'IntStrat.org, un site d'analyses internationales originales et critiques. Synesthète profondément convaincu qu'il faut parfois une grande intelligence pour ne pas comprendre, j'écris principalement sur les problématiques liées aux Relations Internationales, et à la Géopolitique.

?>