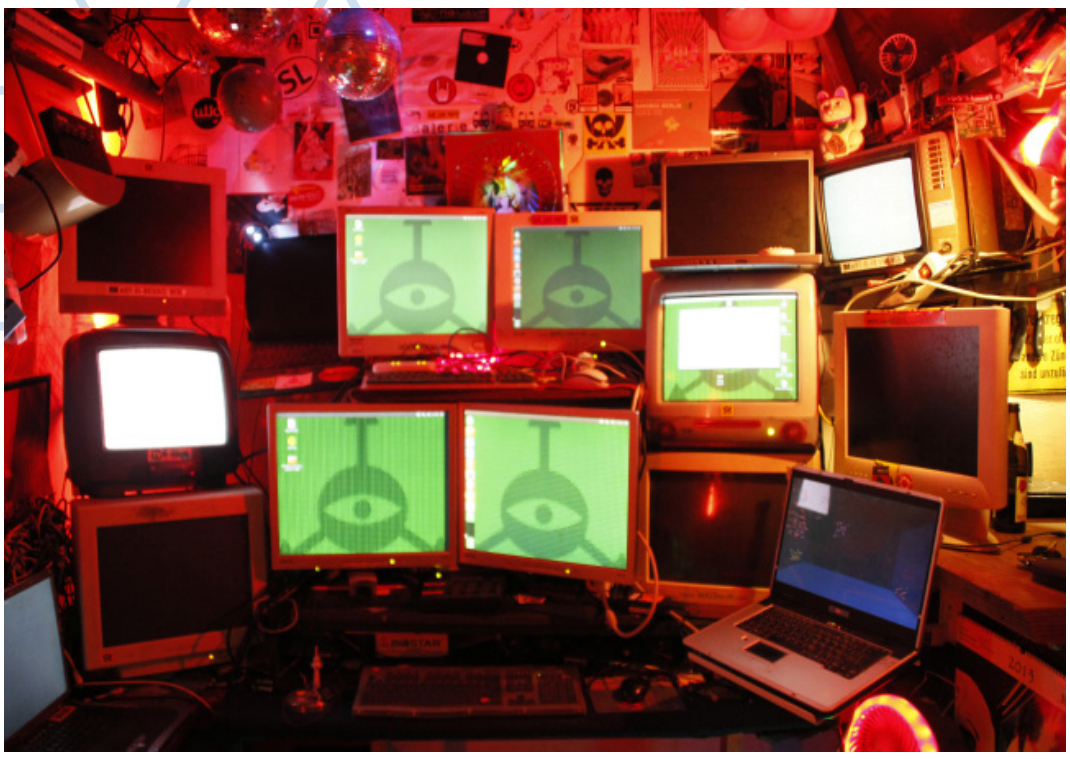
heig-vd

SHOWROOM
HEIG-VD – Route de Cheseaux 1
Horaires : 10h-16h

L'HISTOIRE DU HACKING



Dans l'imaginaire collectif, on associe volontiers les hackers à des pirates, voire à des robins des bois de l'informatique. Mais qu'en est-il réellement ?

Cette exposition montre comment le hacking est intimement lié au développement de l'informatique : il propose une vision atypique et souvent disruptive de la technologie qui a influencé, entre autres, la conception de l'ordinateur personnel et d'Internet.

Les hackers peuvent être des bidouilleurs, des professionnels, des militants, des pirates, mais aussi des femmes – si elles sont peu nombreuses, elles n'en jouent pas moins un rôle important. Ces différentes figures du hacking partagent une même passion pour défricher les terres inconnues et pour l'innovation.

Au cours de son histoire, le hacking a participé à la création de nouvelles technologies et de nouvelles activités professionnelles, comme en témoignent l'Orientation Sécurité informatique et le Pôles Y-Security de la HEIG-VD.

Exposition du 22 octobre au 27 novembre 2020

Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud, Yverdon-les-Bains

heig-vd

LE HACKING, QU'EST-CE QUE C'EST ?

Le terme hacking est dérivé du verbe to hack qui signifie « tailler en pièces ».

Pratiquer le hacking c'est démonter quelque chose pour en comprendre les différents composants – autrement dit de l'ingénierie inversée. Les hackers veulent mettre les mains dans le cambouis, avoir une expérience de première main.

Un enfant qui démonte une radio ou un réveil pour essayer d'en comprendre le fonctionnement, c'est un hacker en herbe !

Les hackers cherchent à comprendre intimement une technique ou une technologie afin de la reproduire ou de la modifier pour l'adapter à leurs besoins. Ils aiment par-dessus tout détourner un objet ou une technique existante pour créer de nouveaux usages. C'est ce qu'ils appellent un « hack ».

Le « hack » ou innover par le détournement

Si le hacking est souvent associé à l'informatique, la philosophie du hack peut être appliquée à de nombreux domaines. Un hack peut être simple ou complexe, l'important c'est le détournement. Il peut s'agir de :

- utiliser une cafetière pour cuire des pommes de terre ;
- transformer un récepteur radio en émetteur ;
- afficher une image en 3 dimensions sur un ordinateur théoriquement incapable de le faire ;
- etc.

L'ordinateur Apple 1 est le premier produit d'Apple et il fut mis en vente en avril 1976

Le Smaky 6, développé en 1978 en Suisse, a été principalement vendu à des écoles de 1979 à 1983. Smaky (SMArt KeYboard) est une famille d'ordinateurs personnels développés par le LAMI à l'EPFL.

Des détournements qui ont façonné l'informatique contemporaine

La philosophie du hack a fortement influencé le développement de l'informatique. Ce sont les détournements des premiers hackers qui ont donné naissance à la notion d'ordinateur personnel et, dans une certaine mesure, à l'architecture décentralisée d'Internet.

heig-vd

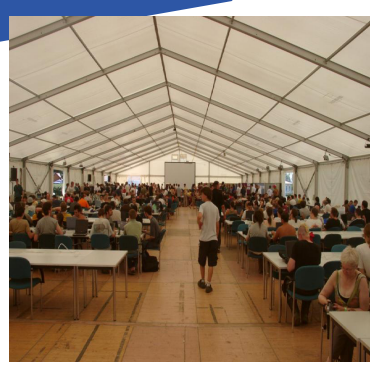
QUI SONT LES HACKERS ?

Il est difficile de définir le terme hacker en raison de sa polysémie. Il peut en effet renvoyer à différents archétypes : l'autodidacte passionné par la bidouille, le hacker professionnel, le militant de la technologie ou le pirate informatique. Et le tableau ne serait pas complet si on oublie la figure peu connue de la femme hacker.

Ces archétypes sont représentés par des logos qui serviront de repères tout au long de cette exposition.

Camp du congrès (2015)

La grande messe du hacking, le Chaos Communication Congress à Hamburg



Tente du « Hackcenter » (2003)

Les hackers autodidactes

Le terme hacker peut désigner des individus passionnés par la technique – et pas uniquement par l'informatique. Ils se basent sur une technologie existante afin d'apprendre son fonctionnement puis cherchent à la bidouiller, que ce soit pour l'améliorer ou la détourner.

Les hackers professionnels

Le hacker peut être un professionnel qui cultive une vision décalée et innovante dans son travail, que ce soit dans l'industrie ou le monde académique. Il est souvent en partie autodidacte et apprécie particulièrement sortir des sentiers battus.

Les hackers militants

Ces hackers développent un rapport idéaliste, voire idéologique à la technique. Ces individus considèrent que la technique n'est pas neutre mais véhicule des valeurs. Ils défendent donc des idéaux, comme l'émancipation à travers la technologie.

Les pirates informatiques

Les pirates informatiques cherchent principalement à s'enrichir : ils peuvent mener des attaques contre des individus ou des organisations, pour leur propre compte ou pour des tiers qui les financent (espionnage industriel par exemple).

Les femmes hackers

Si le hacking compte peu de femmes dans ses rangs, elles en ont pas moins apposé leur marque sur l'histoire de l'informatique. Tout comme les hommes, on retrouve des femmes dans tous les domaines du hacking, bidouille, militantisme ou piratage.

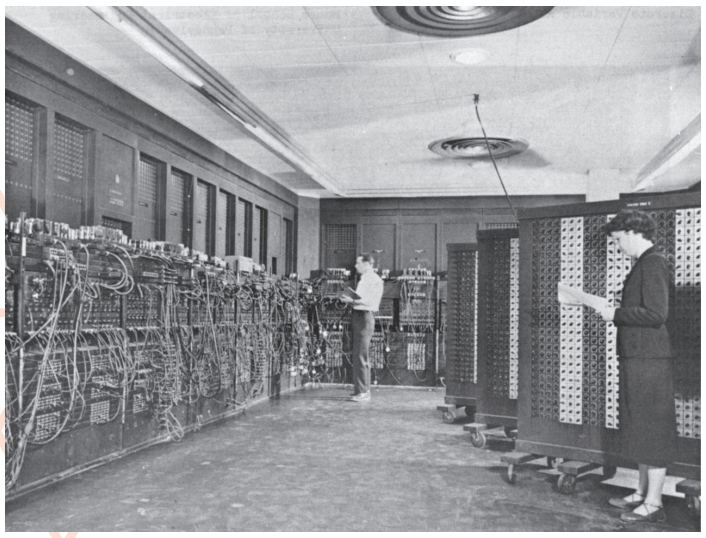
heig-vd

LES DÉBUTS DU HACKING

Pour comprendre les origines du hacking, il faut également s'intéresser aux débuts de l'informatique. Dans les années 1950-1960, l'informatique est une discipline universitaire récente dont les principales applications renvoient au calcul scientifique.

On ne parle d'ailleurs pas encore d'ordinateurs mais bien de calculateurs. Il s'agit de machines volumineuses dont l'accès est réservé exclusivement aux personnes habilitées (chercheurs, ingénieurs, etc.).

La première génération de hackers verra ces calculateurs comme un terrain idéal d'expérimentation et de détournements, quitte à contourner les règles administratives.



Un calculateur ENIAC utilisé par l'armée américaine (c. 1947 à 1955)

Les « premiers hackers » du Tech Model Railroad Club du MIT.

Le Massachusetts Institute of Technology (MIT) est une université de premier plan et réputée pour son rôle pionnier en informatique. C'est également dans ses murs qu'officieront ceux que l'histoire a retenu comme les « premiers hackers ».

Il s'agit à l'origine des membres du Tech Model Railroad Club qui rassemble des passionnés de trains miniatures. Intrigués par les nouveaux calculateurs, comme les fameux TX-0 et PDP-1, ils vont s'approprier ces machines pour voir de quoi elles sont capables.

Afin de contourner les restrictions d'accès, ils n'hésitent pas à investir les locaux de nuit et apprennent à crocheter les serrures, une activité toujours populaire chez les hackers.

QR : Illustration : MIT Guide to Lock Picking

Avec le temps, ils reçoivent le soutien de professeurs intéressés par leur approche peu conventionnelle, à l'instar de Marvin Lee Minsky, fondateur du Groupe d'intelligence artificielle du MIT. Ces premiers hackers vont développer de tout nouveaux usages comme apprendre à un PDP-1 à faire de la musique ou y programmer un des premiers jeux vidéo, Spacewar ! (1962).

Les racines universitaires du hacking laissent une marque durable sur son évolution. Les hackers accordent en effet une grande importance à l'évaluation par les pairs et aux échanges libres et transparents. Cela donnera notamment naissance au mouvement du logiciel libre (cf. affiche « Pour une informatique libre »).

Le PDP-1 est ordinateur qui fut particulièrement apprécié par les premiers hackers du MIT. Vendu à partir de 1959, il s'est écoulé à 50 exemplaires, au prix de 120'000 dollars de l'époque.

QR : Vidéos d'illustration :

Dec PDP-1 Playing Music

heig-vd

LE HACKING ET SES RACINES UTOPIQUES

La pratique du hacking n'est pas exclusive au monde de la recherche. Avec la contre-culture des années 1960, elle sort des murs des universités pour être appropriée par des individus plus politisés.

Manifestation contre la guerre au Vietnam, en avril 1971 à Washington

Le festival Woodstock de 1969, un grand moment de célébration de la contre-culture.

Proche de notre Mai 68, ce mouvement est guidé par des idéaux pacifistes et égalitaristes : oppositions à la guerre du Vietnam, manifestations anti-nucléaires, mouvement pour la liberté d'expression (Free Speech Movement), culture hippie.

Un virus contre le nucléaire

De cette rencontre naît des outils de contestation originaux, à l'instar du virus WANK, pour Worms Againts Nuclear Killers ou Ver contre les tueurs nucléaires. Le principal objectif de ce virus n'était pas de causer des dommages, mais de diffuser un message politique. En plus du message principal (ci-dessous), il affichait sur les machines infectées des messages aléatoires comme « Votez anarchiste » ou « Le FBI est en train de vous observer », etc. Il avait également pour particularité de ne pas infecter d'ordinateurs en Nouvelle-Zélande en raison de l'opposition de ce pays à la politique nucléaire des Etats-Unis.

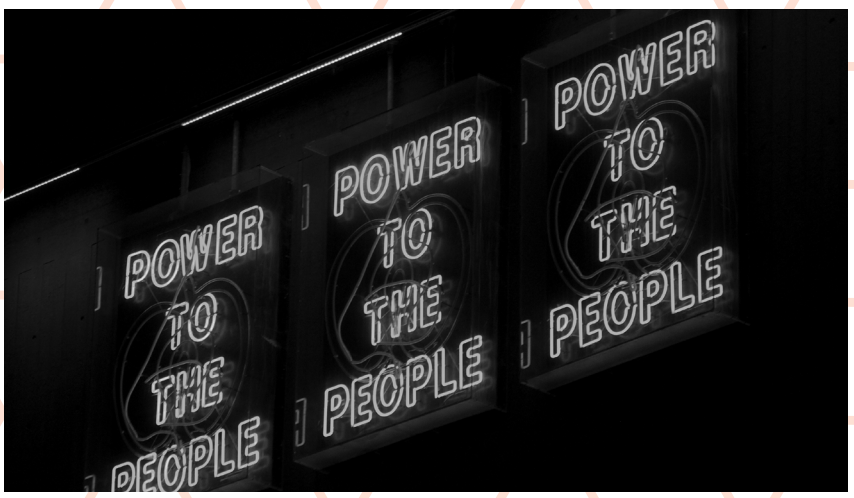
```
 W O R M S   A G A I N S T   N U C L E A R   K I L L E R S
 _____________________________________________________________
 \__  _____  ____  _____  ____  ____  __  ____/
  \ \ \   /\   / /   / /\ \     | \ \  | |    | | / /   /
   \ \ \ /  \ / /   / /__\ \    | |\ \ | |    | |/ /   /
    \ \ \/ /\ \/ /   / _____ \   | | \ \| |    | |\ \  /
     \_\ /__\ /____/ /_____\ \____| |__\ | |____| |_\ \_/
      \_____________________________________________/
       \                                             /
        \    Your System Has Been Officially WANKed  /
         \_____________________________________________/

You talk of times of peace for all, and then prepare for war.
```

Message apparaissant sur les ordinateurs infectés par WANK

Un héritage contre-culturel

Plus largement, la rencontre entre le hacking et la contre-culture impulse une volonté de démocratiser l'informatique, d'en faire un outil de contre-pouvoir. Le motto de cette époque est le fameux « Computer Power to the People ! » ou le pouvoir de l'ordinateur pour le peuple. L'idéal communautaire des hippies inspire également les premières communautés de hackers et plus largement les expérimentations autour de l'idée de communauté virtuelle.



heig-vd

LA CONTRE-CULTURE DES ANNÉES 1960

La contre-culture des années 1960 se développe tout d'abord dans le monde anglo-saxon (Etats-Unis, Grande-Bretagne), avant de se diffuser plus largement.

Chez nous, ce mouvement contre-culturel se manifesta à travers le fameux Mai 68.

Une contre-culture a pour principale caractéristique de contester le pouvoir en place et de proposer des valeurs alternatives. La contre-culture des années 1960 se diffusera principalement au sein de la jeunesse et des universités, mais aura également des échos au sein des mouvements ouvriers.

Les principales valeurs portées par cette contre-culture sont :

- l'émancipation vis-à-vis des formes d'autorité traditionnelles, à l'instar de l'« autorité du père » ;
- le pacifisme (opposition à la guerre au Viêt Nam ou à la guerre d'Algérie) et une opposition au nucléaire ;
- l'égalité entre femmes et hommes et des mœurs sexuelles plus libres, ainsi que l'égalité entre les « races » ;
- de nouvelles formes de vie en communauté, principalement promues par les hippies.

heig-vd

LA PASSION DES HACKERS POUR LES TÉLÉCOMMUNICATIONS

Les hackers voient très tôt le potentiel de l'informatique dans le domaine des télécommunications. Ils s'inspirent de ce qui se passe sur les réseaux téléphoniques et développent de nouvelles manières de communiquer collectivement.

Le phreaking ou le hacking des réseaux téléphoniques

Dès la fin des années 1950, les phreakers font parler d'eux. Ces fous/mordus (freak) du téléphone (phone) cherchent à explorer et à contrôler les réseaux téléphoniques, sans grands égards pour les entreprises du secteur.

Le hacking et le phreaking se sont influencés mutuellement. Par exemple, Stewart Nelson, est considéré à la fois comme un des premiers hackers du MIT et un des premiers phreakers, lorsqu'il réussit à connecter un calculateur PDP-1 au réseau téléphonique d'AT&T.

John Draper, alias Captain Crunch, est une légende du phreaking. Il découvre qu'un sifflet en plastique distribué dans des boîtes de céréales Capt'n Crunch permet d'effectuer gratuitement des appels à longue distance et des appels internationaux. En effet, ce sifflet produisait un son à 2600 Hz, une fréquence utilisée pour le pilotage de la centrale téléphonique.

John Draper, alias Captain Crunch, au festival Maker Faire 2015 à Berlin.

Le sifflet Capt'n Crunch produisant un son à 2600 Hz.

Leslie Lynn Doucette (1954-..., USA), alias Kyrie, phreakeuse.

A recruté et formé des adolescents afin de former un réseau qui comptera jusqu'à 150 complices. A 35 ans et mère de deux enfants, elle organise en tant que tête du réseau des campagnes de fraudes téléphoniques contre une vingtaine d'entreprises. Elle sera finalement appréhendée et condamnée à 27 mois de prison.

Le phreaking ne fait qu'anticiper le goût des hackers pour la maîtrise des réseaux de télécommunications et les questions de sécurité.

heig-vd

LA PASSION DES HACKERS POUR LES TÉLÉCOMMUNICATIONS (SUITE)

Le projet Community Memory :
l'informatique comme outil de communication

L'idée d'Internet a existé bien avant Internet, comme l'illustre le projet Community Memory. En 1973, un collectif de hackers mettent un terminal informatique à disposition du public de Berkeley. Quiconque pouvait y poster des messages ou consulter les messages d'autrui, sans modération ou contrôle – l'anonymat était garanti.

Le terminal du projet Community Memory, qui fut mis à disposition du public de Berkley de 1973 à 1975.

Le projet est né de la rencontre entre l'informatique et la contre-culture, comme l'illustre les portraits de certains de ses fondateurs, Lee Felsenstein et Judith Milhon.


Lee Felsenstein (Berkeley, 2010)

Lee Felsenstein est un ingénieur américain, passionné de technologies. Il est également militant gauchiste (New Left Radical) et participe au Mouvement pour la liberté d'expression (Free Speech Movement). Il participera à la fondation d'un autre lieu emblématique du hacking, le Homebrew Computer Club.
(cf. affiche « Pour une informatique libre »).

Judith Milhon, dite « St. Jude », est considérée comme la première hackeuse et la « Sainte Patronne » des hackers : une ardente défenseuse du droit des femmes à accéder à la technologie et à la cyberculture, une pionnière du droit à l'anonymat sur Internet. Elle invente le terme cypherpunk – de cypher (chiffrement) et de punk – dans lequel se reconnaissent des hackers comme Julian Assange.

Judith Milhon, alias St. Jude (1965)

Pour St. Jude, le hacking c'est *« contourner de manière astucieuse les limites imposées, qu'elles le soient par votre gouvernement, vos propres compétences ou les lois de la physique ». C'est aussi « un art martial – un moyen de défense contre les politiciens politiquement corrects, les lois trop intrusives, les bigots et les personnes imperméables à toute forme de persuasion »*.

heig-vd

POUR UNE INFORMATIQUE LIBRE

Les hackers ont une conception libertaire de l'informatique : ils voient d'un mauvais œil tout ce qui limite les échanges et la réutilisation du code informatique (ou de matériel), à l'instar de la propriété intellectuelle (copyright). Si aux débuts du hacking, cette liberté s'exprime essentiellement à travers des échanges « sauvages », le mouvement du logiciel libre se structure progressivement et permet d'établir un commun en informatique.

Qu'est-ce qu'un commun ?

Un commun est une ressource partagée, gérée et maintenue collectivement par une communauté ; celle-ci établit des règles dans le but de préserver et pérenniser cette ressource tout en fournissant la possibilité et le droit de l'utiliser par tous. Les communs impliquent que la propriété n'est pas conçue comme une appropriation ou une privatisation, mais comme un usage. (Wikipédia)

La notion de commun peut être appliquée à la gestion :

- De ressources naturelles pas ou peu renouvelables : terres cultivables, ressources en gibier, en poissons, en bois, et en eau potable ou d'irrigation notamment.
- D'infrastructures et de machine.
- Des biens immatériels (connaissances, culture).

Plus concrètement, un commun peut se concrétiser à travers des coopératives pour la gestion des terres agricoles, des machines agricoles ou d'un bâtiment (locatif, lieu de production). On peut également citer un exemple historique avec l'usage collectifs des fours à pain, le plus souvent au niveau d'un village.

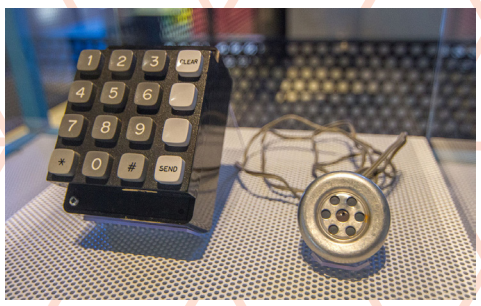
Gordon French, co-fondateur du Homebrew Computer Club avec Fred Moore, au Living Computer Museum de Seattle en 2017

Le Homebrew Computer Club : la liberté d'échanger et de créer

Fondé en 1975, ce club mythique accueille aussi bien des professionnels, des amateurs que des individus politisés, tous passionnés par la technique. Un de ses fondateurs n'est autre que Lee Felsenstein (cf. affiche « La passion des hackers pour les télécommunications »), qui incarne parfaitement la rencontre entre technique et contre-culture.

Le mot d'ordre est l'échange libre et réciproque d'idées et de matériel, parfois sans l'accord des entreprises qui les ont développés. Ainsi, obtenir une copie d'un logiciel passe par l'obligation d'en faire d'autres copies.

Parmi ses membres on retrouve John Draper, alias Captain Crunch. Il fait profiter les autres membres d'une de ses inventions, la Blue box. Selon le point de vue, une Blue box permet d'explorer les réseaux téléphoniques ou de frauder les télécommunications. Bref, un jouet de rêve pour hacker.



Une Blue Box exposée au Powerhouse Museum, à Ultimo en Australie.

heig-vd

POUR UNE INFORMATIQUE LIBRE (SUITE)

Les UNIX WARS et la naissance du logiciel libre

Le code informatique s'est tout d'abord développé dans le monde académique où il s'échangeait librement. Les entreprises, qui vendaient surtout du matériel (hardware) à cette époque, participaient également à cet échange libre de code informatique.

Les choses commencèrent à changer avec l'apparition d'une industrie du logiciel et la décision du gouvernement américain de faire entrer le code informatique dans le régime de la propriété intellectuelle (copyright) en 1980.

Rien n'illustre mieux les conséquences de ce changement que les « Unix Wars ». Très populaires dans les années 1970-1980, les systèmes d'exploitation UNIX pouvaient contenir du code informatique développé à la fois par des entreprises et des universités. Les tentatives de commercialisation de différentes versions d'UNIX aboutirent donc à des conflits autour de la propriété du code informatique et à des procès entre des entreprises et des universités.

Richar Stallman, promoteur du logiciel libre et fondateur du projet GNU (Oslo, 2009).

En réaction à cet épisode, Richard Stallman, hacker et chercheur au MIT, décide de « hacker » la propriété intellectuelle afin de défendre l'idéal de libre échange du code. Avec le professeur de droit Elben Molgen, ils créent la General Public Licence (GPL) qui non seulement autorise la réutilisation du code informatique mais oblige à mettre sous GPL tout logiciel réutilisant du code protégé par cette licence (clause virale ou copyleft).

Grâce à ce détournement de la propriété intellectuelle, les chercheurs et les hackers peuvent continuer à échanger librement du code informatique tout en étant protégé sur le plan juridique. Cela a également permis la naissance de nombreux logiciels libres, soutenus par des communautés réunissant développeurs et utilisateurs.

heig-vd

EXEMPLES DE LOGICIELS LIBRES

Il existe des milliers de logiciels libres aux dimensions et aux ambitions extrêmement diversifiées. Certains d'entre eux ont joué un rôle particulièrement important pour la constitution et la diffusion d'un commun en informatique.

Tout d'abord, la création de versions libres des outils de base permettant de faire fonctionner un ordinateur et de développer de nouvelles applications. On peut notamment citer :

- Les systèmes d'exploitation Linux (Debian, Ubuntu, etc.) qui représentent la principale (et essentielle) alternative à Windows et à Mac OS.
- Des outils permettant de faire fonctionner le Web, comme les serveurs Apache (serveur le plus populaire jusqu'en avril 2019) ou NGINX (serveur le plus utilisé), ou encore l'application PhpMyAdmin pour la gestion de bases de données MySQL, etc.
- Des langages de programmation et des environnements de développement, à l'instar de Python.
- Etc.

Afin de toucher le grand public, des alternatives libres aux programmes les plus utilisés ont été développées, comme :

- Le navigateur Mozilla Firefox, comme alternative aux navigateurs proposés par les GAFAM (Internet Explorer, Microsoft Edge, Opera, Safari, Google Chrome, etc.).
- Le logiciel de traitement de texte LibreOffice, comme alternative aux suite Microsoft Office et iWork.
- Le lecteur de médias VLC Media Player, comme alternative à Windows Media Player.
- Etc.

Enfin, on peut encore citer certains logiciels libres utilisés en ingénierie :

- Le langage de programmation et logiciel libre R destiné aux statistiques et à la science des données.
- GNU Octave et Scilab, des logiciels libres de calcul numérique (alternative à MALAB).
- Etc.

heig-vd

HACKING ET CONCEPTION D'INTERNET

Aujourd'hui, Internet est littéralement partout et permet des échanges à une échelle et à une rapidité jamais vue dans notre histoire.

Au vu de son importance, des acteurs étatiques et des grandes entreprises comme les GAFAM – les géants du Web, Google, Apple, Facebook, Amazon, et Microsoft – cherchent à y exercer une forme de contrôle (profilage, censure, etc.).

Ces efforts rencontrent un succès mitigé car, à l'origine, Internet a été conçu pour être un réseau décentralisé, accordant un contrôle important à ses utilisateurs. En effet, la contre-culture du hacking a laissé sa marque sur le réseau des réseaux.

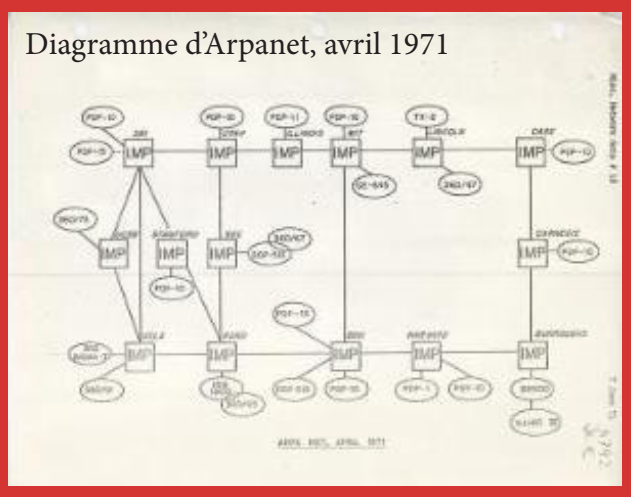
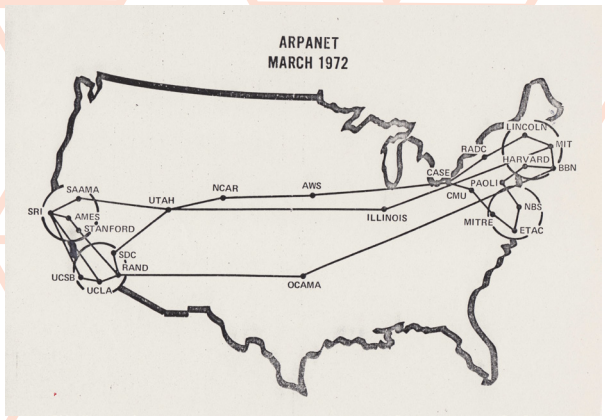


Diagramme d'Arpanet, avril 1971



Carte d'Arpanet, mars 1972

Financements militaires et Arpanet

Le premier réseau informatique, Arpanet, a été lancé en 1969. S'il fut financé par la DARPA, l'Agence pour les projets de recherche avancée de défense, il a été développé au sein du monde universitaire.

Le réseau se développe rapidement aux Etats-Unis : il relie 15 institutions en avril 1971 et 25 en mars 1972

Protocole TCP/IP et neutralité d'Internet

Ancrée dans le monde universitaire, la conception d'Internet va être marquée par la contre-culture et le hacking. Les universitaires développent un protocole spécifique, le protocole TCP/IP, de manière horizontale et ouverte. Le développement se fait via des demandes de commentaires (requests for comments ou RFC) ouvertes à la « communauté d'Internet » qui, à l'époque, est principalement composée de chercheurs, d'ingénieurs et de hackers.

QR : Illustration : le RFC 1122 qui spécifie le protocole TPC/IP

Internet représente une rupture dans la manière de penser un réseau de télécommunications. Lancé en 1983, le protocole TCP/IP définit une architecture décentralisée dite de bout-en-bout (end-to-end). Le contrôle est placé aux extrémités du réseau, chez les utilisateurs, et non centralisé chez un opérateur comme cela est le cas pour les réseaux téléphoniques – le modèle dominant à l'époque.

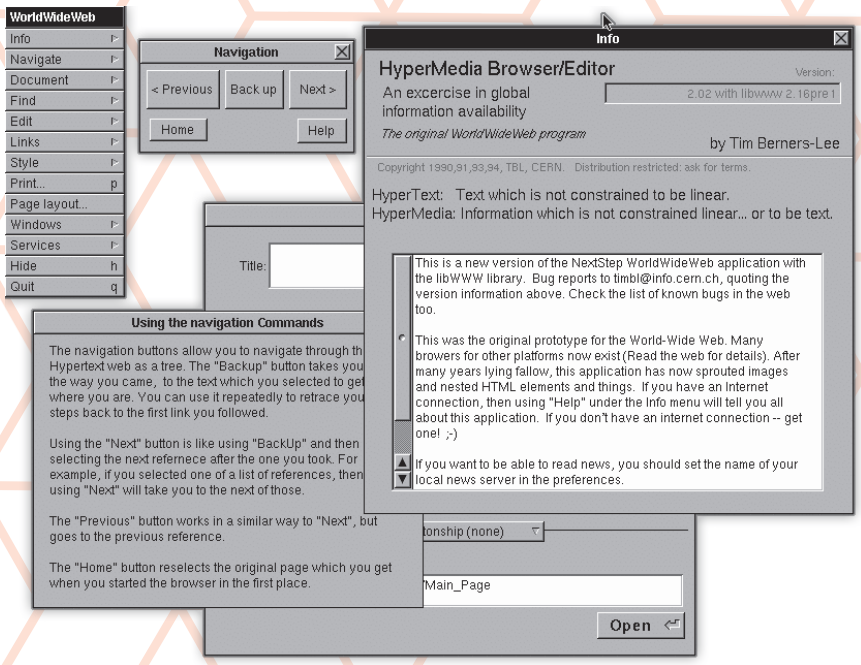
C'est cette décentralisation qui permet à Internet de garantir une certaine neutralité dans les échanges, un principe que les hackers continuent à défendre activement aujourd'hui (cf. affiche « Liberté et anonymat sur Internet »).

heig-vd

HACKING ET CONCEPTION D'INTERNET (SUITE)

La démocratisation d'Internet

Si les hackers investissent les réseaux informatiques dès leurs débuts, Internet se démocratise à partir des années 1990. Avec la diffusion des ordinateurs personnels, chaque individu peut potentiellement accéder à Internet et devenir également un contributeur, un créateur de contenu.



Mais c'est surtout les débuts Web (World Wide Web) en 1990 – développé par Tim Berners-Lee et Robert Cailliau au sein du CERN –, qui fera exploser les usages.

Le Web permet de consulter à partir d'un navigateur des sites hébergeant un ensemble de pages, la navigation de pages en pages se faisant grâce à des hyperliens.

Le premier navigateur du web, développé par Tim Berners-Lee.

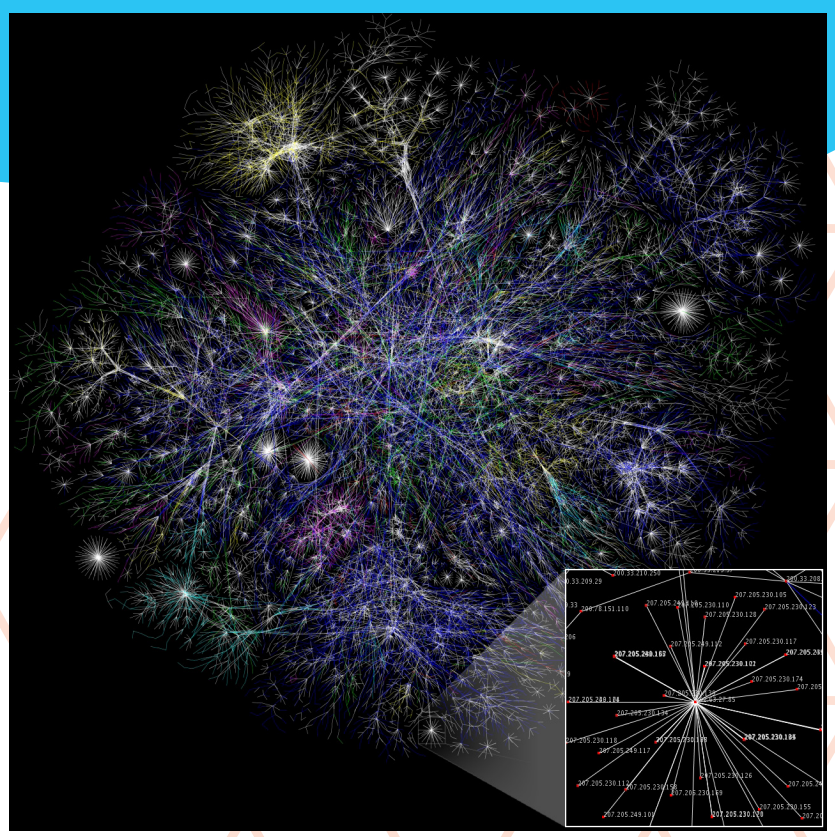
La différence entre Internet et le Web

Internet désigne l'infrastructure matérielle (les câbles p.ex.) et le code informatique (protocole TPC/IP p.ex.) qui permettent d'interconnecter des réseaux (d'institutions, d'entreprises, etc.) et des ordinateurs entre eux. C'est pour cette raison qu'on le nomme fréquemment le réseau des réseaux.

Le World Wide Web (la « toile mondialement étendue »), appelé communément Web, est une couche rajoutée sur Internet qui permet de créer, d'afficher et de consulter du contenu textuel et audio-visuel. Le Web est également une toile, c'est-à-dire un réseau de documents, d'images, de fichiers, de pages web, etc. qui sont reliés entre eux par des liens hypertextes (selon le protocole HTTP).

Internet est un support à de nombreux flux d'informations. Parmi les nombreuses applications qui utilisent Internet, on peut mentionner le courrier électronique (protocole SMTP) ou le transfert de fichier (protocole FTP).

Ci-contre une carte partielle d'Internet en janvier 2005.



heig-vd

LES DIFFÉRENTS VISAGES DU HACKING CONTEMPORAIN

Si le hacking a pu se maintenir et se diversifier jusqu'à aujourd'hui, c'est grâce à :

- Des logiciels libres permettant d'apprendre et de s'outiller librement ;
- Un réseau Internet décentralisé, difficile à contrôler pour une autorité centrale ;
- Un tissu de communautés plus ou moins anciennes et structurées.

Toujours vivace, le hacking contemporain a gardé ses multiples visages.

Un panneau d'affichage de la Silicon Valley qui promeut différents lieux ancrés dans la philosophie du hacking.

Des communautés de passionnés

Les hackers, qu'ils soient passionnés par la technologie, le logiciel libre ou le «Do It Yourself» (faites-le vous-mêmes) aiment se rencontrer dans des communautés virtuelles ou réelles.

Depuis 2006, des associations ayant pignon sur rue, les hackerspaces, ouvrent partout sur la planète. En février 2020, 1392 hackerspaces actifs sont référencés sur le site hackerspace.org. On peut y pratiquer l'informatique, l'électronique, la biologie (bio-hackerspace), le travail sur bois ou textile, etc.


Des passionnés de hacking se rencontrent au NYC REsistor, un hackerspace de New York

QR : Lien : carte des hackerspaces actifs

De nouvelles activités professionnelles

Beaucoup de hackers ont une âme de pionniers, il n'est donc pas rare qu'ils développent de nouvelles techniques. Parfois, ils créent même de nouvelles activités professionnelles. Le « hacking éthique » en est un bon exemple. Depuis 10-15 ans, des hackers mettent leurs compétences en intrusion à profit dans le domaine du conseil et de l'audit (cf. affiche « Le hacking comme art de l'intrusion »).

heig-vd

LES DIFFÉRENTS VISAGES DU HACKING CONTEMPORAIN (SUITE)

L'hacktivisme : se battre pour une cause

Dans la continuité de la contre-culture des années 1960, des hackers se dédient à ce qu'on nomme communément l'hacktivisme (contraction entre hacking et activisme).

Si leur première grande cause a été le logiciel libre, ils ont pris à bras le corps d'autres causes avec le temps :

- la liberté d'expression sur Internet, qui est notamment notamment défendue par l'Electronic Frontier Foundation (EFF) (cf. affiche « Liberté et anonymat sur Internet ») ;
- la protection des données privées et le droit à l'anonymat, un domaine où l'on trouve Jacob Appelbaum, le réseau Tor (cf. affiche « Liberté et anonymat sur Internet »), ou encore la mouvance Anonymous.
- la transparence des institutions et la protection des lanceurs d'alerte, qui ont acquis une forte visibilité avec Julian Assange et son projet Wikileaks, lancé en 2006.

Le piratage informatique

Aujourd'hui, le petit génie qui se lance seul dans le piratage renvoie plus à un mythe qu'à une réalité. Le piratage est pratiqué par des groupes, voire des réseaux de plus en plus structurés et perfectionnés.

Les pirates informatiques peuvent s'enrichir directement, en organisant des campagnes massives d'hameçonnage ou de rançongiciels. Ils peuvent également vendre leurs services aux plus offrants, qu'il s'agisse d'entreprises ou de gouvernements. Ils pratiquent alors la désinformation, l'espionnage ou l'attaque d'infrastructure critique.

Conseils et bonnes pratiques en matière de sécurité informatique à la HEIG-VD :

heig-vd

PORTRAIT D'HACKTIVISTES

Rena Tangens est une artiste et pionnière de l'Internet allemande. Elle fait partie des fondatrices des Haecksen, une association de plus de 200 femmes membres du Chaos Computer Club – le plus ancien groupe de hackers organisés au monde –, co-organisatrice des Big Brother Awards en Allemagne. Elle participe au développement du programme de messagerie sécurisé Zerberus ainsi qu'à l'adoption par le grand public du logiciel libre de chiffrement Pretty Easy Privacy (« la vie privée plutôt facile »).

Jacob Appelbaum se fait connaître sous le pseudonyme « ioerror » au sein du Cult of the Dead Cow, un collectif de hacking et un média indépendant. Il est également développeur Debian (une distribution Linux), et devient chercheur en sécurité informatique, employé notamment sur le Projet Tor qu'il promeut activement en tant que : « part of an ecosystem of software that helps people regain and reclaim their autonomy » . Il intervient régulièrement dans les grandes conventions de hacking et s'engage pour soutenir Julian Assange, puis Edward Snowden. En 2007, il fonde Noisebridge avec Mitch Altman, un célèbre hackerspace de la Baie de San Francisco.

Julian Assange fait ses premières armes dès 1987 dans l'underground informatique, et plus particulièrement dans un groupe qu'il participe à fonder, les International Subversives. Sous le pseudonyme de « Mendax » il acquière une certaine réputation pour sa capacité à pénétrer dans différents réseaux gouvernementaux, universitaires ou de grandes entreprises. Il développe également différents logiciels libres, dont Rubberhose un outil cryptographique destiné à Linux. Ses actions sont motivées par la conviction que des informations importantes sont cachées aux citoyens. Il se fera du

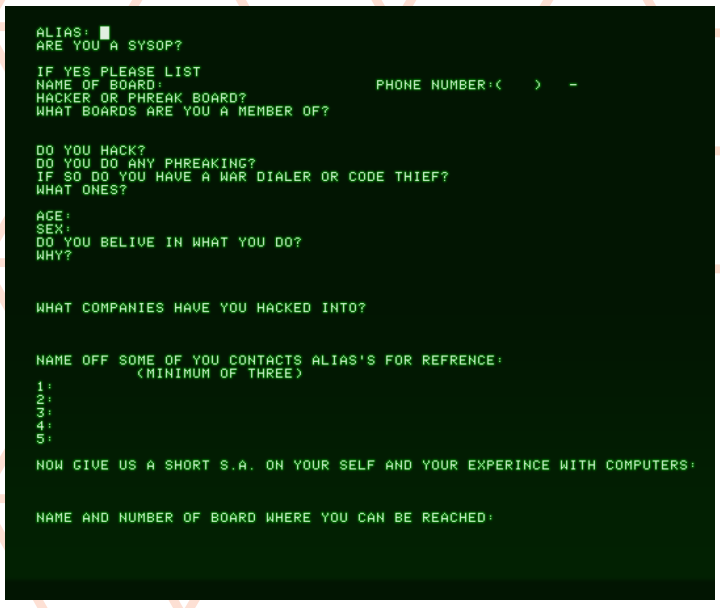
heig-vd

LIBERTÉ ET ANONYMAT SUR INTERNET

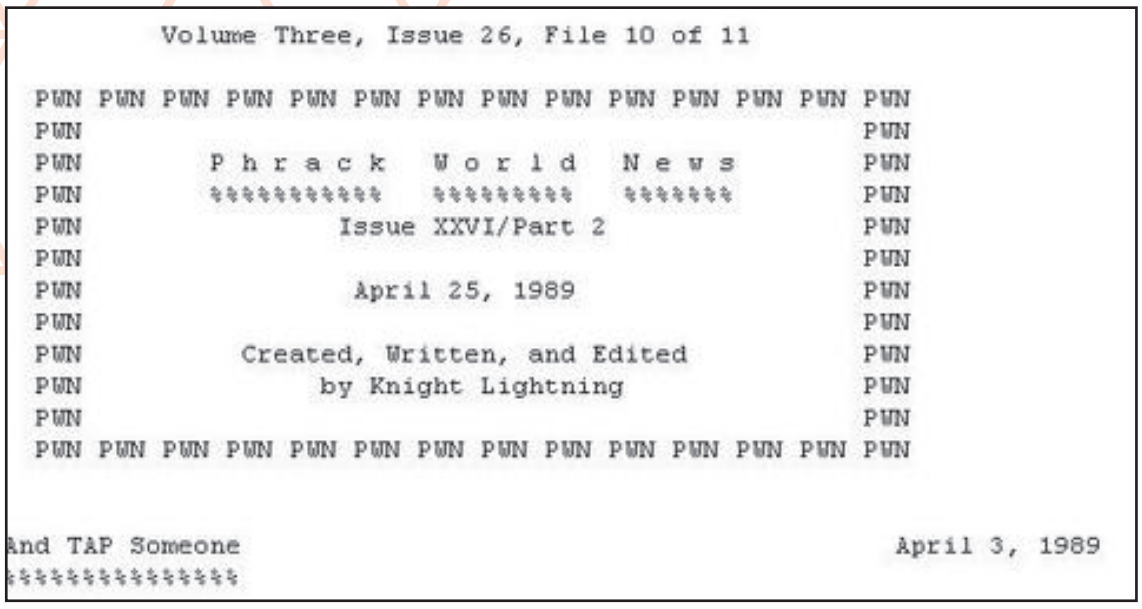
Les hackers voient dans l'informatique un formidable outil de communication.

Avant le web, ils communiquaient via les fameux BBS ou « systèmes de bulletins électroniques » (bulletin board system) qui furent populaires entre la fin des années 1970 et le début des années 1990.

Les BBS ont permis à des individus, à des communautés et même à des revues underground comme Phrack de bénéficier d'un espace d'échanges autonome.



Ecran d'accueil d'un BBS (Neon)



Page d'accueil de Phrack World News, avril 1989

Pionniers dans l'âme, les premières générations de hackers étaient souvent peu regardantes sur l'aspect légal. Toutefois, les autorités durcirent le ton lorsque l'informatique devint un rouage important de l'économie. Au tournant des années 1990, les pays les plus répressifs, comme les Etats-Unis et la France, organisent des descentes de police ciblant indistinctement pirates et hackers politisés. L'opération Sundevil voit même l'implication des services secrets américains et aboutira à la fermeture (temporaire) de Phrack et à un procès injustifié contre Steve Jackson Games.

L'Electronic Frontier Foundation

L'opération Sundevil marqua les esprits et amena des chercheurs, des entrepreneurs, des hackers à se mobiliser pour fonder l'Electronic Frontier Foundation (EFF), afin d'apporter un soutien financier et juridique aux personnes mises en accusation par les autorités américaines. L'EFF a publié un guide d'Autodéfense contre la surveillance et est toujours très active dans la promotion et la défense de la liberté d'expression sur Internet.

heig-vd

LIBERTÉ ET ANNONYMAT SUR INTERNET (SUITE)

Le chiffrement à disposition du public

Le droit de protéger sa vie privée est un contentieux de longue date entre les hackers et les autorités, comme l'illustre l'histoire de Pretty Good Privacy (PGP).

En 1991, Phil Zimmermann publie PGP sur Internet, un outil permettant de chiffrer les courriers électroniques.

Phil Zimmermann, créateur de PGP

Il est attaqué en justice, car il contrevint à une loi interdisant l'export de munitions – les technologies de chiffrement sont considérés comme telles par les USA. Il n'en faut pas plus pour que de nombreux hackers se mobilisent pour s'assurer que le code de PGP se diffuse le plus largement possible, parfois via des méthodes inattendues : le code est imprimé dans des ouvrages envoyés ensuite par la poste ou tatoué sur le corps avant de partir en voyage à l'étranger, etc.

TorProject.org

Le réseau Tor

Avec le temps, les hackers ont promu des outils de plus en plus performants à l'image des réseaux d'anonymisation, dont le représentant le plus connu est probablement Tor.

Ces logiciels permettent de créer des petits réseaux chiffrés et anonymisés qui sont souvent qualifiés, à tort, de « darknet » au singulier.

Ce type d'outils peut être utilisé aussi bien par des réseaux criminels que par des militants politiques vivant dans des pays totalitaires.

Guide d'Autodéfense contre la surveillance de l'EFF :

heig-vd

LES AUTORITÉS FACE À L'UNDERGROUND INFORMATIQUE

L'underground informatique a pu être perçu comme une menace dans certains pays, car il accueille toute une gamme de pratiques subversives (médias indépendants, contestation politique, etc.), voire des pratiques illégales stricto sensu (piratage informatique pour des raisons idéologiques ou bassement pécuniaires).

Tous les pays n'ont pas adopté la même attitude face à l'underground informatique. Les Etats-Unis et la France font partie des pays les plus répressifs qui ont mené des actions policières ciblant indistinctement les pirates et les pratiques contestataires.

D'autres pays, à l'instar de l'Allemagne et des Pays-Bas, ont adopté une attitude plus conciliante vis-à-vis de l'underground informatique et n'ont réprimé que les pirates. Ainsi, les hackers allemands ont pu développer un tissu associatif très vivace avec le fameux Chaos Computer Club et ses nombreuses antennes régionales. Les hackers hollandais organisèrent la première rencontre internationale en 1989, The Galactic Hacker Party, et ont pu devenir un acteur central de l'accès Internet haut débit et bon marché dans leur pays.

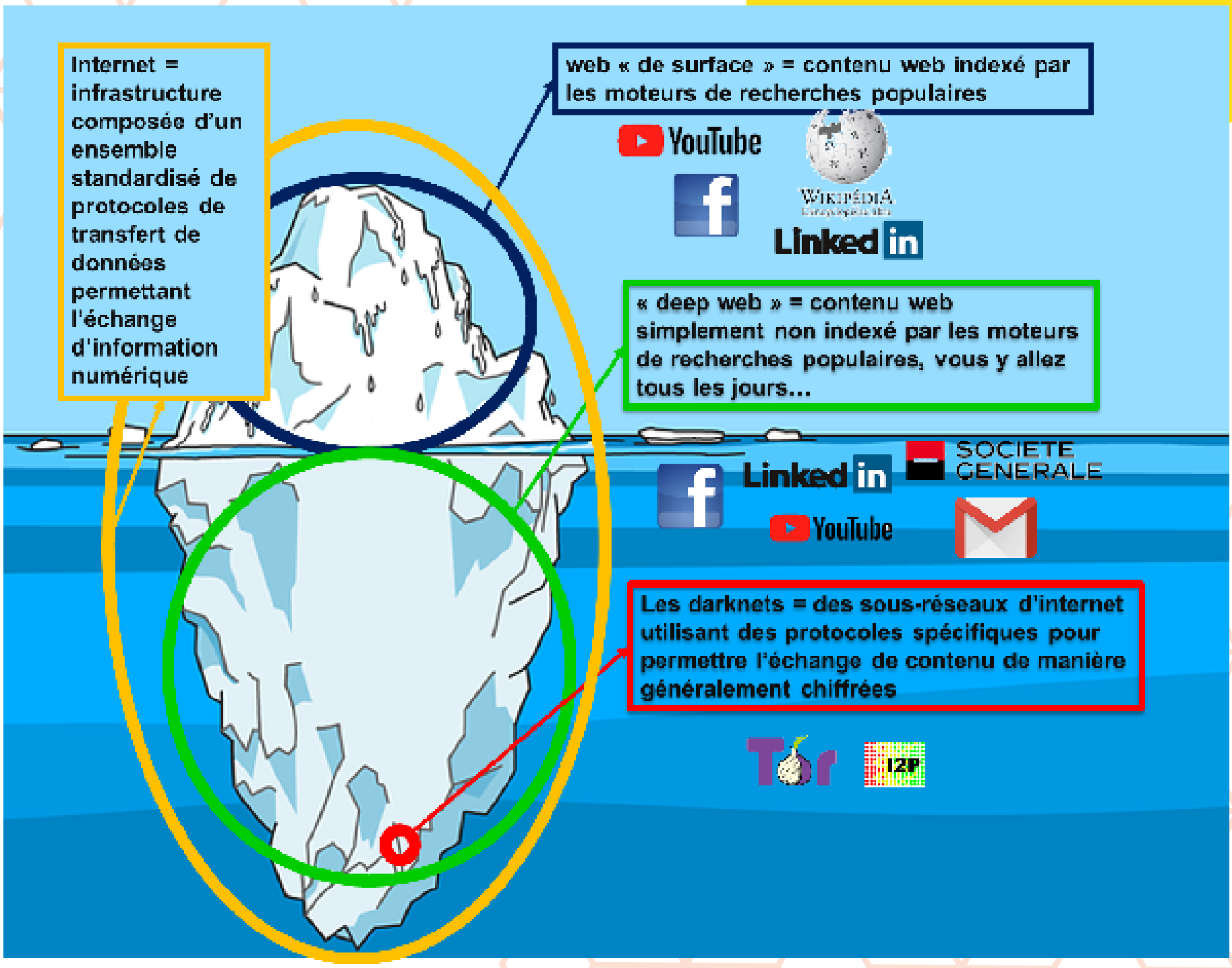
heig-vd

WEB, WEB PROFOND ET INTERNET CLANDESTIN

Le web surfacique ou référencé représente le contenu accessible via les moteurs de recherche généralistes, à l'instar de Google search. Cela représente qu'une petite fraction du contenu circulant sur le web.

La grande majorité du contenu non indexé par les moteurs de recherche se trouve dans le web profond (deepweb). Les raisons pour lesquelles du contenu en ligne ne peut pas être indexé sont nombreuses (accès protégé, format non indexable, etc.) et cela peut concerner des données très différentes : un e-mail, un Google document, un script informatique, etc.

Enfin, l'internet clandestin (darknet) est composé de sous-réseaux protégés par des mesures de chiffrement et d'anonymisation, à l'instar de Tor.



Le net vu comme un iceberg : une illustration d'Internet, du web, du deepweb et des darknets

heig-vd

LE HACKING COMME ART DE L'INTRUSION

Les réseaux téléphoniques connaissaient déjà leurs « intrus » avides d'exploration et de challenge technique, les phreakers (cf. affiche « La passion des hackers pour les télécommunications »).

Les hackers ont repris le flambeau sur les réseaux informatiques et ont développé un art de l'intrusion qui, aujourd'hui, peut prendre plusieurs visages.

Le goût du défi et de la prouesse technique était très répandu aux débuts d'Internet qui était alors une terra incognita encore peu sécurisée.

Des motivations idéologiques ou politiques peuvent se traduire par une volonté à extraire et à révéler des informations « cachées » aux citoyens.

L'intrusion est très utile dans le domaine de l'espionnage, qu'il soit pratiqué par des pirates ou des agences gouvernementales.

Plus récemment, l'intrusion est devenue une compétence professionnelle dans le domaine du hacking éthique, notamment pour la conduite d'audit de sécurité.

L'intrusion technique

L'intrusion technique fait appel à une expertise pointue : il s'agit d'exploiter des failles techniques afin de pénétrer et contrôler un réseau informatique.

Aujourd'hui, il s'agit d'un domaine de haut vol, hors de portée des amateurs et amatrices. C'est un terrain principalement investi par des entreprises, des agences gouvernementales et des réseaux criminels.

Présentation de Kevin Mitnick à la conférence Cyber Incursion en 2018, sur la question de l'ingénierie sociale et de ses risques pour les utilisatrices et utilisateurs.

L'ingénierie sociale

L'ingénierie sociale vise à pénétrer un réseau ou une organisation grâce à des techniques de manipulation. Pour Kevin Mitnick, un précurseur de cette pratique, il s'agit d'utiliser les « failles humaines » pour contourner les mesures de sécurité. A une époque où les réseaux informatiques sont de plus en plus sécurisés, l'ingénierie sociale a le vent en poupe.

L'ingénierie sociale recouvre de nombreuses méthodes, certaines classiques comme l'imposture, d'autres plus exotiques. Les hackers américains ont par exemple popularisé l'art du trashing, autrement dit le fait de fouiller les poubelles afin de récupérer des informations.

Portrait de femme : Susan Headley (1959-…, USA), dite « Susy Thunder » et « Susan Thunder » : elle débute avec le phreaking et réussit à hacker le système téléphonique américain à 17 ans. Active dans le groupe Cyberpunks, elle se spécialise dans l'ingénierie sociale – elle a notamment collaboré avec Kevin Mitnick. Elle finit par abandonner le hacking pour devenir joueuse professionnelle de pocker, puis est élue « City Clerk » de la ville de Californie.

heig-vd

LES HACKERS ET LEURS DIFFÉRENTS « CHAPEAUX »

Le hacking peut recouvrir des pratiques diverses, des plus légitimes au plus illégitimes. Les hackers eux-mêmes ont développé une classification à base de chapeaux de couleur, afin d'y voir un peu plus clair.

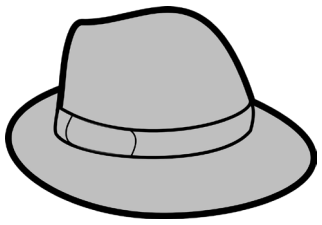
Pourquoi des chapeaux ? En hommage à un code du western qui veut que les gentils portent un chapeau blanc et les méchants un chapeau noir. Si ces catégories offrent des repères utiles, il faut garder à l'esprit que la réalité est souvent plus complexe – un individu peut porter plusieurs chapeaux au cours de sa vie.

Les chapeaux blancs

Aussi surnommés chevaliers blancs, les chapeaux blancs sont des hackers qui restent du bon côté de la loi, voire qui aident directement les autorités à appréhender les hackers moins scrupuleux. Les hackers éthiques (cf. affiche « Le hacking comme art de l'intrusion ») en sont un exemple typique.

Les chapeaux noirs

Les chapeaux noirs désignent les pirates informatiques qui utilisent leurs compétences pour s'enrichir ou nuire à autrui ou à des organisations. A l'heure actuelle, ils sont particulièrement actifs dans l'extraction d'informations et la guerre économique.



Les chapeaux gris

Les chapeaux gris se situent dans un entre deux : ils agissent parfois de manière éthique, parfois non. Lorsqu'ils agissent en dehors de la légalité, ils le font moins par appât du gain que par goût du défi ou pour des raisons idéologiques.

Les chapeaux bleus

Le chapeau bleu est une variante du chapeau blanc qui aide les organisations à améliorer leur sécurité en leur signalant leurs failles. Ils peuvent le faire de leur propre initiative ou dans le cadre des fameuses chasses aux bugs, où des récompenses sont promises par des entreprises.

heig-vd

SCÈNES DE L'UNDER-GROUND INFORMATIQUE

La scène Warez

Le terme warez est une déformation du mot wares, désignant des marchandises en anglais. Cette scène est surtout connue pour le piratage et la diffusion de contenus numériques protégés par le droit d'auteur, qu'il s'agisse de produits culturels ou de logiciels. Les prouesses, comme « cracker » des protections élaborées, y sont valorisées, de même que les attitudes ludiques et anti-système (« Fuck You Microsoft ! »). Fréquenter cette scène peut relever de motivations pécuniaires ou plus idéologiques, comme le libre accès à la culture. Ciblée régulièrement par des opérations policières, elle n'en reste pas moins active. Ces pratiques sont très difficiles à juguler en raison de serveurs existants dans des pays n'ayant pas de lois permettant de les pénaliser.

Manifestation en faveur du partage de fichiers et du piratage de logiciels, à Stockholm en 2006. Le Parti Pirate est fondé la même année en Suède.

Partie du code du virus Blaser avec un message adressé à Bill Gates : « billy gates pourquoi rends-tu ça possible ? Arrêt de te faire de l'argent et corrige ton logiciel !! ». Blaster est un virus qui s'est répandu en août 2003 sur les systèmes d'exploitation Windows XP et Windows 2000.

La scène vX (Virus eXchange)

L'histoire des milieux des virus informatiques est très proche de celle du hacking. Les débuts sont marqués par l'exploration et les expérimentations. Par la suite, les fronts se durcissent entre les acteurs du développement de virus et d'antivirus, tout particulièrement aux États-Unis. Dans les années 1990 se développe la scène vX (Virus eXchange ou échange de virus) qui regroupe clandestinement des programmeurs et des collectionneurs de virus informatique.

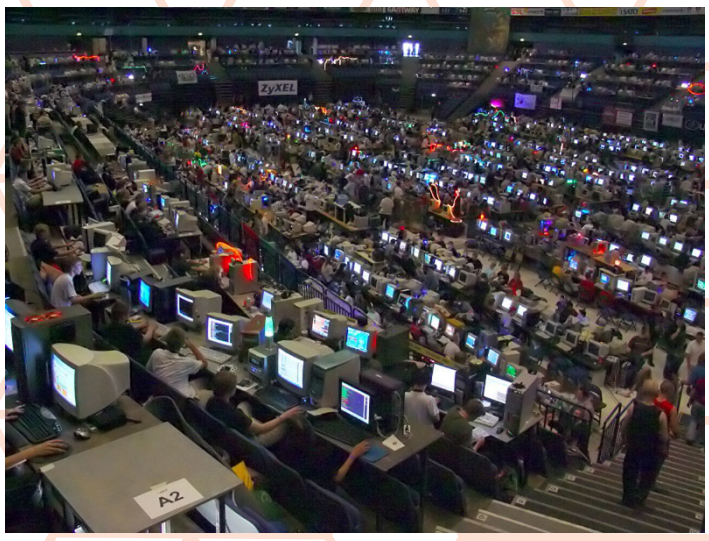
Les virus peuvent être conçus pour différentes raisons : pour détruire les systèmes infectés, pour la « blague », comme outil de recherche, pour véhiculer un message politique (anti-nucléaire, anticapitaliste), etc.

Portrait de femme : Kim Vanvaeck (Belgique), dite « Gigabyte » : elle a créé des virus haut de gamme dédiés à la destruction d'informations sensibles (Coconut-A, Sahay-A, Sharp-A, etc.). Elle acquiert le respect de ses pairs et des virus incluant des messages d'admiration ont été découverts (« HECHO EN ADMIRACION A GIGABYTE »). Elle est arrêtée après avoir mené une guerre contre un professionnel de la sécurité informatique qu'elle jugeait arrogant et sexiste. Suite à cet épisode, elle quitte la scène des virus et devient une professionnelle en sécurité des réseaux.

QR : Lien : virus Coconut

La scène démo (demoscene)

Les acteurs de la scène démo cherchent à dépasser les limites inhérentes à des machines peu performantes, par exemple en affichant de la 3D sur un ordinateur n'ayant théoriquement pas la capacité de le faire. A la virtuosité technique s'ajoute souvent une recherche esthétique. Les productions (démos) de cette scène sont souvent distribuées via des copies pirates de jeux ou de logiciels. La France a connu une scène démo très active.



Le hall principal d'Assembly en 2004, une des demoparties les plus populaires. La première édition de cette manifestation a eu lieu en 1992 en Finlande.

heig-vd

LE HACKING ET LES FEMMES

Si les hackers sont en grande majorité des hommes, des femmes sont présentes dès les débuts. Grace Hopper (1906-1992, USA) est souvent considérée comme la « mamie du hacking ». Elle est la première à avoir développé un langage de programmation « compilé », c'est-à-dire proche du langage humain. Son travail a été fondateur pour le langage COBOL, toujours utilisé aujourd'hui dans le secteur bancaire.

A l'instar de leurs homologues masculins, elles peuvent investir différents aspects du hacking. Certaines vont privilégier la technique, d'autres le militantisme.

Grace Hopper opère un UNIVAC, le premier ordinateur commercial réalisé aux Etats-Unis (c. 1960)

Des femmes virtuoses

Stephanie Wehner (1977, Allemagne), physicienne et informaticienne, professeure de l'Université de technologie de Delft et spécialiste reconnue en cryptographie quantique et en communication quantique. Avant d'intégrer le monde académique, elle fait ses armes en tant que hackeuse dès 15 ans et acquiert une réputation lui permettant d'être embauchée par des pairs à l'âge de 20 ans. Elle rentre à l'université quelques années après, alors qu'elle travaille en tant que spécialiste en sécurité des réseaux. Son intérêt pour l'informatique quantique est lié à son désir de réinventer Internet.

Joanna Rutkowksa (1981-…, Pologne), experte en sécurité informatique connue pour ses recherches sur la sécurité à bas niveau et les rootkits : lors de la conférence Black Hat Briefings en 2006, elle démontre devant un large public comment pirater le noyau de Windows Vista. Ses recherches amènent le magazine eWeek à l'intégrer à la liste des « cinq hackers qui ont marqué 2006 ».

Joanna Rutkwoska présente ses travaux à la LinuxCon Europe de 2014, à Düsseldorf

Parisa Tabriz (1983-…, USA), la Security Princess de Google : elle dirige l'équipe d'ingénieurs « hackers » qui lance des attaques préventives contre les logiciels et applications de Google. En 2012, le magazine Forbes l'inclut dans la liste des « 30 personnes âgées de moins de 30 ans à surveiller de près dans l'industrie des technologies ».

Parisa Tabriz, la Security Princesse de Google

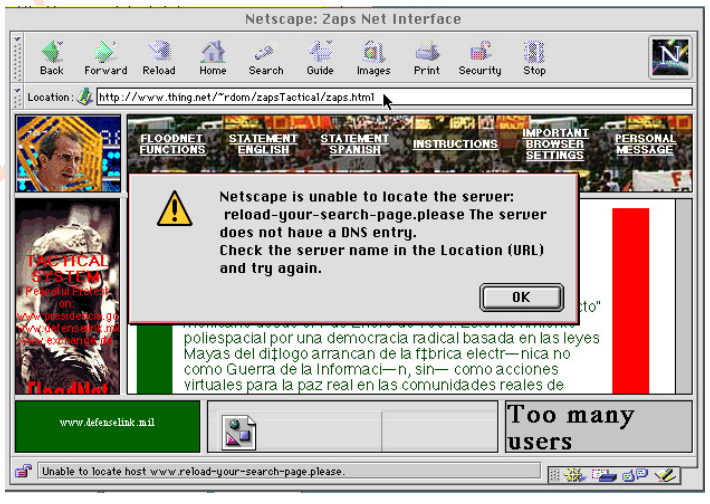
Xia Tian (1989-…, Chine) : encore étudiante en TIC, elle fonde le groupe China Girl Security Team qui réunit rapidement plus de 2000 femmes. Ce groupe s'inscrit dans la continuité du « hacking patriotique » chinois qui est apparu à la fin des années 1990.

LE HACKING ET LES FEMMES (SUITE)

Des femmes engagées pour une cause

Natasha Grigori (USA) : elle se fait connaître dans les années 1980-90 pour ses activités et anime un BBS pour les programmeurs amateurs et les hackers. A la fin des années 1990, elle se lance dans une croisade contre la pédopornographie en ligne (antichildporn.org) et développe des techniques – encore utilisées aujourd'hui – pour aider les autorités à trouver et condamner les distributeurs de pédopornographie.

Carmin Karasic (1954, USA) est une artiste spécialisée dans les technologies de l'information et co-fondatrice du collectif Electronic Disturbance Theater en 1997, qui a été précurseur dans le domaine de la contestation politique en ligne. Dans ce cadre, elle a participé au développement de FloodNet, une application permettant d'organiser un « sit-in virtuel », c'est-à-dire l'équivalent en ligne d'une manifestation visant à bloquer un axe routier ou l'entrée d'une usine, repris plus récemment par la mouvance Anonymous. Elle devient par la suite professeure adjointe à l'Université de Lesley.



Capture d'écran d'une performance de FloodNet, le 9 septembre 1998.

Naomi Wu (Chine), aussi connue comme Sexy Cyborg, est active dans la mouvance Do It Yourself. Elle s'est faite l'avocate des femmes dans les MINT, du transhumanisme, du matériel libre et des modifications corporelles. Elle cherche à bousculer aussi bien les stéréotypes genrés que ceux associés à la technologique.

Naomi Wu en train de configurer un Raspberry Pi 2, un nano-ordinateur à carte unique.

Ying Cracker (Chine), hackeuse qui aime se définir comme une enseignante : elle s'est fait connaître et reconnaître pour ses multiples publications qui enseignent les bases du hacking. A côté des cours gratuits qu'elle propose, elle gagne sa vie en développant des progiciels visant à protéger les données sensibles d'entreprises et d'institutions.

heig-vd

CRÉDIT POUR LES ILLUSTRATIONS

Les icônes

Icône pour les hackers autodidactes : user-cog, fontawesome.com, licence CC BY 4.0

Icône pour les hackers professionnels : Briefcase 7, simpleicon.com, licence CC BY 3.0

L'histoire du hacking

3D Hackespace Berlin_MG_3804, Berlin in 3D (Flickr), CC BY 2.0

Qu'est-ce que le hacking

Appel Computer 1, Ed Uthman (Flickr), CC BY 2.0

Epsitec Smaky 6, Rama & Musée Bolo (commons.wikimedia.org), licence CC BY-SA 2.0 FR

Les débuts du hacking

PDP-1, m.haswkey (Flickr) licence CC BY 2.0

Qui sont les hackers ?

Orage au-dessus du Chaos Communication Camp 2015, Robert Anders (Flickr), licence CC BY 2.0

« Hackcenter » du Chaos Communication Camp 2003, Hagbard (de.wikipedia), licence CC BY-SA 3.0

Le hacking et ses racines utopiques

Manifestation contre la guerre au Vietnam à Washington DC avril 1971, Leena A. Krohn (commons.wikimedia.org), licence CC BY-SA 3.0

Foule à Woodstock, Derek Redmond (commons.wikimedia.org), licence CC BY-SA 3.0

Power To The People, Nick Webb (Flickr), licence CC BY

La passion des hackers pour les télécommunications

Captain Crunch, Sebaso (commons.wikimedia.org), licence CC BY-SA 4.0

Le sifflet Capt'n Crunch, 1971markus (de.m.wikipedia.org), licence CC BY-SA 4.0

Le terminal du projet Community Memory, Kathryn Greenhill (Flickr), licence CC BY-SA 2.0

Lee Felsenstein, cellanr (Flickr), licence CC BY-SA 2.0

Judith Milhon, Trescabehling (commons.wikimedia.org), licence CC BY-SA 4.0

Pour une informatique libre

Gordon French, Cromemco (commons.wikimedia.org), licence CC BY-SA 4.0

Blue Box, Maksym Kozlenko (commons.wikimedia.org), licence CC BY-SA 4.0

Richard Stallman, Anders Brenna / tekniskbeta.no, licence CC BY 3.0 NO

Hacking et conception d'Internet

Arpanet avril 1971, ULCA Library | Digital Collection, licence CC BY-SA 4.0

Arpanet mars 1972, ULCA Library | Digital Collection, licence CC BY-SA 4.0

Internet Map, The Opte Project (en.wikipedia.org), licence CC BY-SA 2.5

Les différents visages du hacking contemporain

On travaille dessus !, Dave Jenson (Flickr), licence CC BY-SA 2.0

NYCResistor Group, Openfly (wiki.hackerspaces.org), licence CC BY-SA 3.0

Photokaos – Thème : Hacking/TAZ/Utopies – Borderline Biennale 2011, Thierry Ehrmann (Flickr), licence CC BY 2.0

heig-vd

CRÉDIT POUR LES ILLUSTRATIONS

Portrait d'hacktivistes

Rena Tangens, pixel.fabian (Flickr), licence CC BY-SA 2.0

Jacob Appelbaum, re:publica (Flickr), licence CC BY 2.0

Julian Assange (image recadrée), David D. Silvers (Flickr), licence CC BY-SA 2.0

Liberté et anonymat sur Internet

Neon2, Massacre (Flickr), licence CC BY-SA 3.0

Phrack, Phrack World News (commons.wikimedia.org / urbandictionary.com), licence CC BY 3.0

Phil Zimmermann, créateur de PGP, Phil Zimmermann (commons.wikimedia.org / philzimmermann.com), licence CC-BY-SA 3.0

Logo de Tor, Tor Project (commons.wikimedia.org / media.torproject.org), licence CC BY-SA 3.0

Web, web profond et Internet clandestin

Internet, web, deepweb et darknets illustrés, Pierreangy (commons.wikimedia.org), licence CC BY-SA 4.0

Le hacking comme art de l'intrusion

Cortana scripting language, Christiaan Colen (Flicrk), licence CC BY-SA 2.0

Présentation de Kevin Mitnick à la conférence Cyber Incursion en 2018, Urbanista32 (commons.wikimedia.org), licence CC BY-SA 4.0

Scènes de l'underground informatique

Manifestation pour le partage de fichiers à Stockholm, Jon Åslund (commons.wikimedia.org / web.archive.org), licence CC BY 2.5

Virus Blaster, Ismail saber (commons.wikimedia.org), licence CC BY-SA 3.0

Assembly demo party, ZeroOne (commons.wikimedia.org), licence CC BY-SA 2.0

Le hacking et les femmes

Grace Hopper et UNIVAC, Inconnu / Smithsonian Institution (Flickr), licence CC BY 2.0

Joanna Rutkowska, Krd (commons.wikimedia.org), licence CC BY-SA 3.0

Parisa Tabriz, Google Chrome Developers (Youtube / commons.wikimedia.org), licence CC BY 3.0

Capture d'écran d'une performance de FloodNet, le 9 septembre 1998, Bret Stalbaum (commons.wikimedia.org), CC BY-SA 4.0

Naomi Wu, Naomi Wu (commons.wikimedia.org), licence CC BY-SA 4.0