



ChrisHarrison.net

# INTERNET – UN RÊVE ENFIN RÉALISÉ OU LE DÉBUT DU CAUCHEMAR ?

Janvier 2018



Cyber-espace: une hallucination consensuelle  
vécue chaque jour par des dizaines de millions de  
participants volontaires répartis sur toute la  
planète.

(William Gibson)

qq citations

# UN CONSTAT

La première réalité  
d'Internet est **qu'il n'y a**  
**plus de frontières** : le  
monde est un village !



# UN SECOND CONSTAT

”

Je n'ai pas de réponse en 140 caractères à la cybersécurité.

#AssisesSI

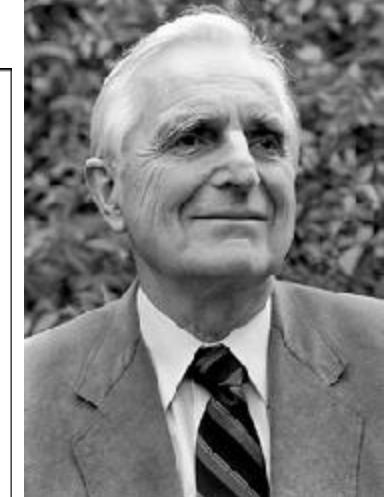
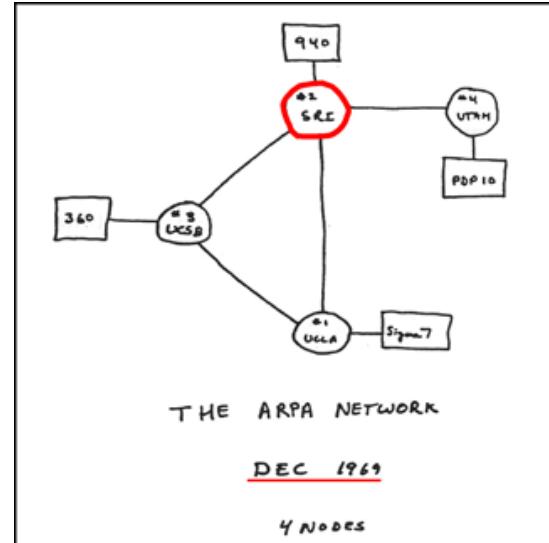
**GUILLAUME POUPARD**

Directeur de l'ANSSI



# INTERNET ?

Un des pionniers : Douglas Engelbart  
(1925-2013)



- A l'intuition d'internet<sup>1</sup> dès les années 1950 (son laboratoire –SRI- participe à la première liaison en 1969 avec l'UCLA)
- Démontre la première vidéoconférence (1968) « *The Mother of All demos* »<sup>2</sup> (Le 1<sup>er</sup> Skype)
- Invente la souris (1968)

<sup>1</sup>Augmented Human intellect:

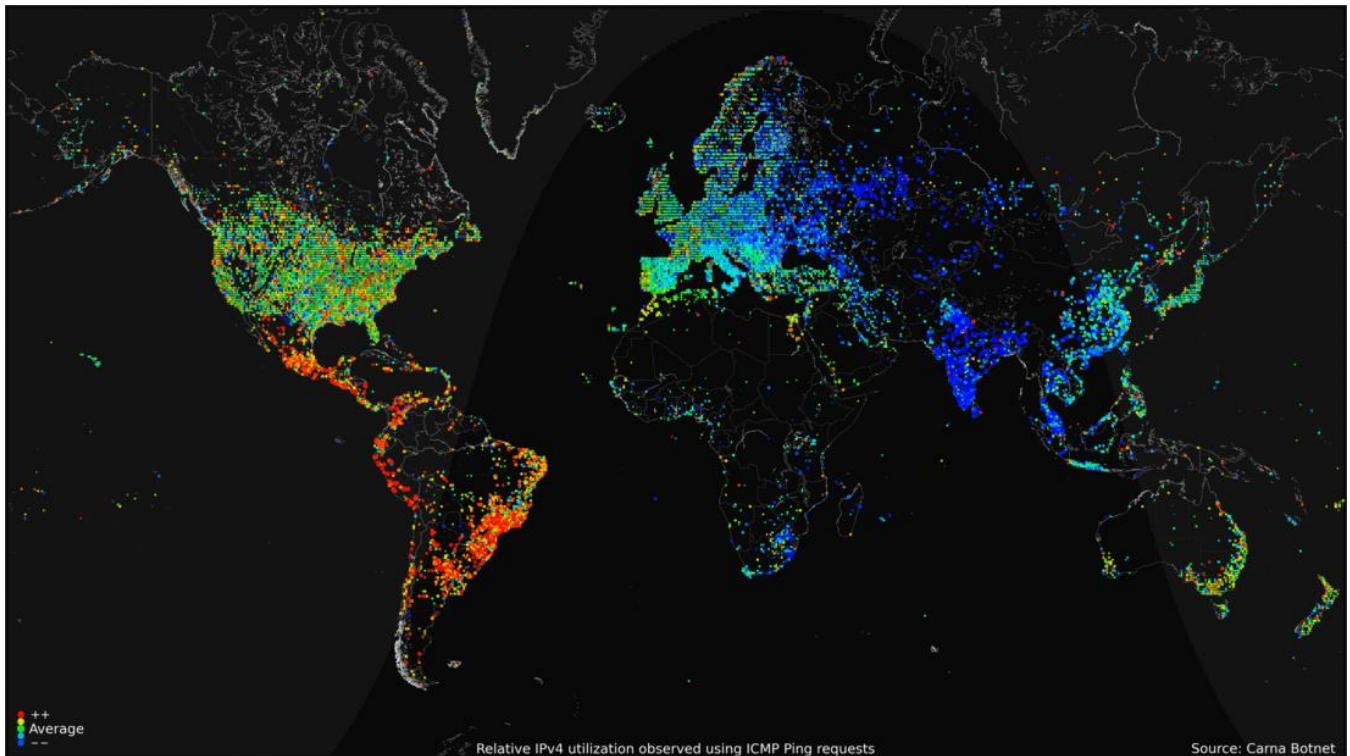
<http://www.douengelbart.org/pubs/augment-3906.html>

<sup>2</sup>The Mother of All demos,

<http://www.douengelbart.org/firsts/dougs-1968-demo.html>

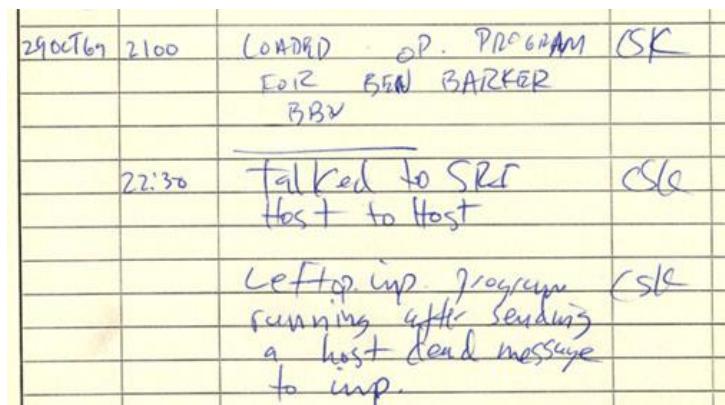
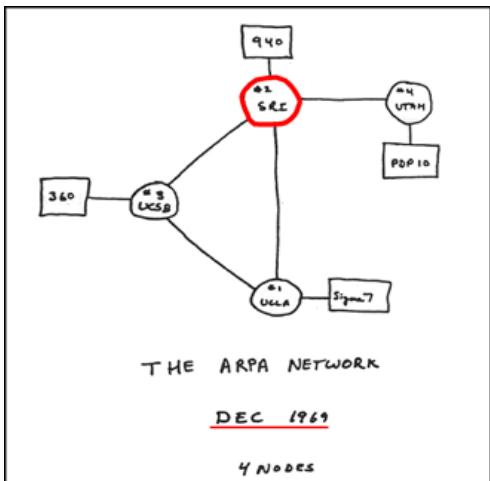


# INTERNET ?



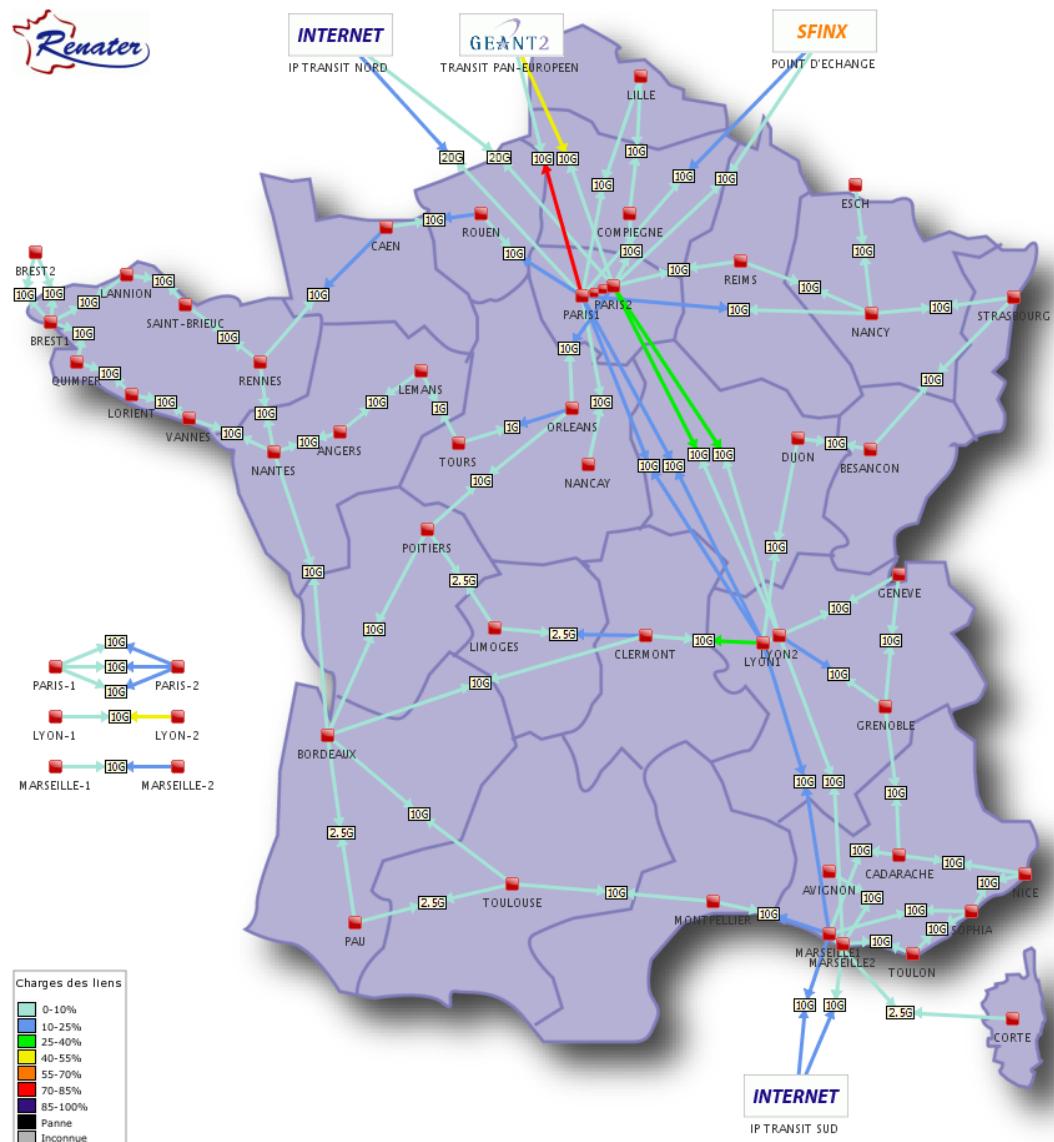
<http://motherboard.vice.com/blog/this-is-most-detailed-picture-internet-ever>

Internet est ... un réseau de réseaux (Vous en avez un morceau à la maison !)



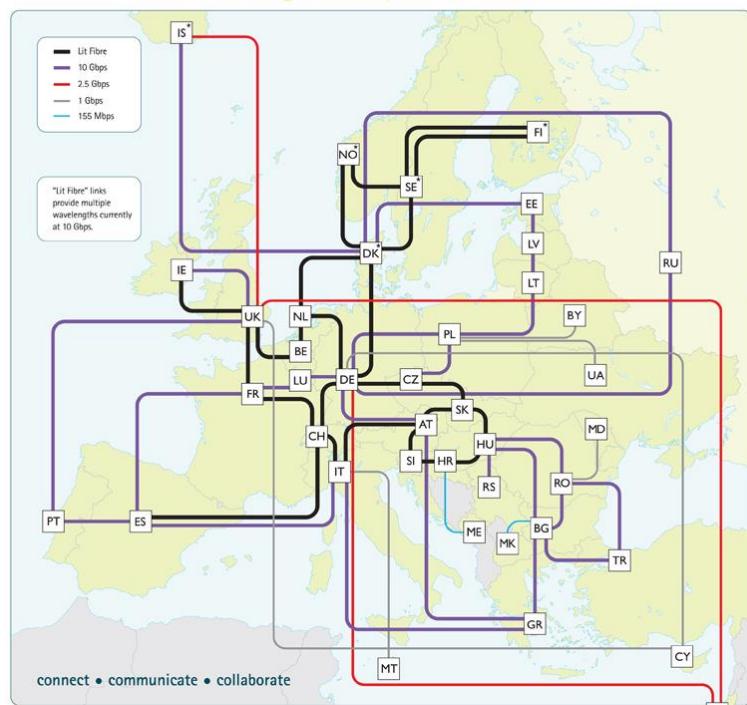
[http://www.computerhistory.org/internet\\_history](http://www.computerhistory.org/internet_history)

# INTERNET ?

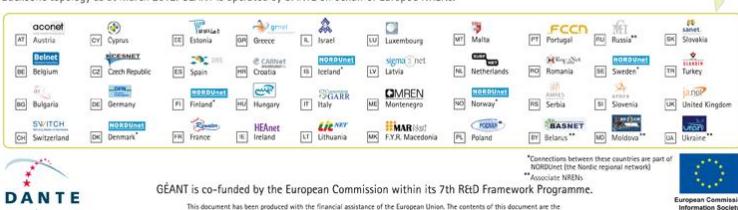


Last update: Tue Apr 17 10:11:03 CEST 2012

# GÉANT the pan-European research and education network



Backbone topology as at March 2012. GÉANT is operated by DANTE on behalf of Europe's NRENs.



\*\* Associate NRENs

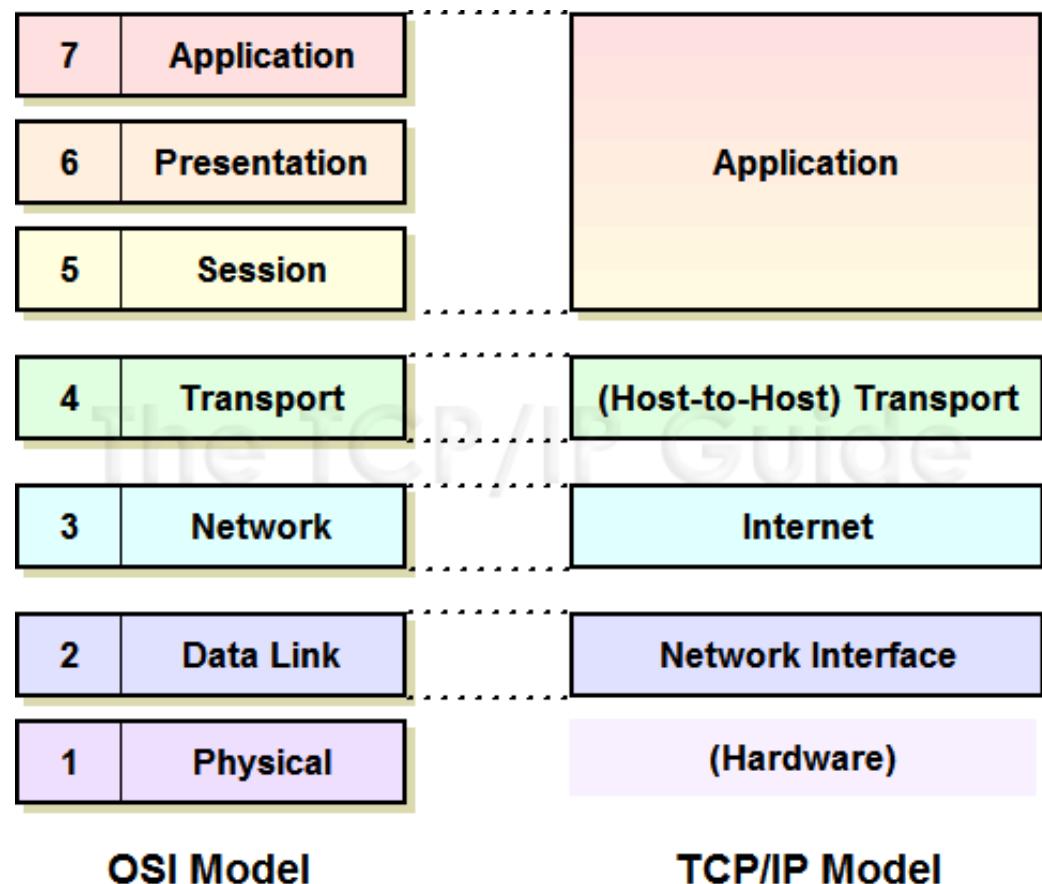
This document has been produced with the financial assistance of the European Union. The contents of this document are the

# INTERNET ?

internet ... est un ensemble de protocoles (1969/1972)

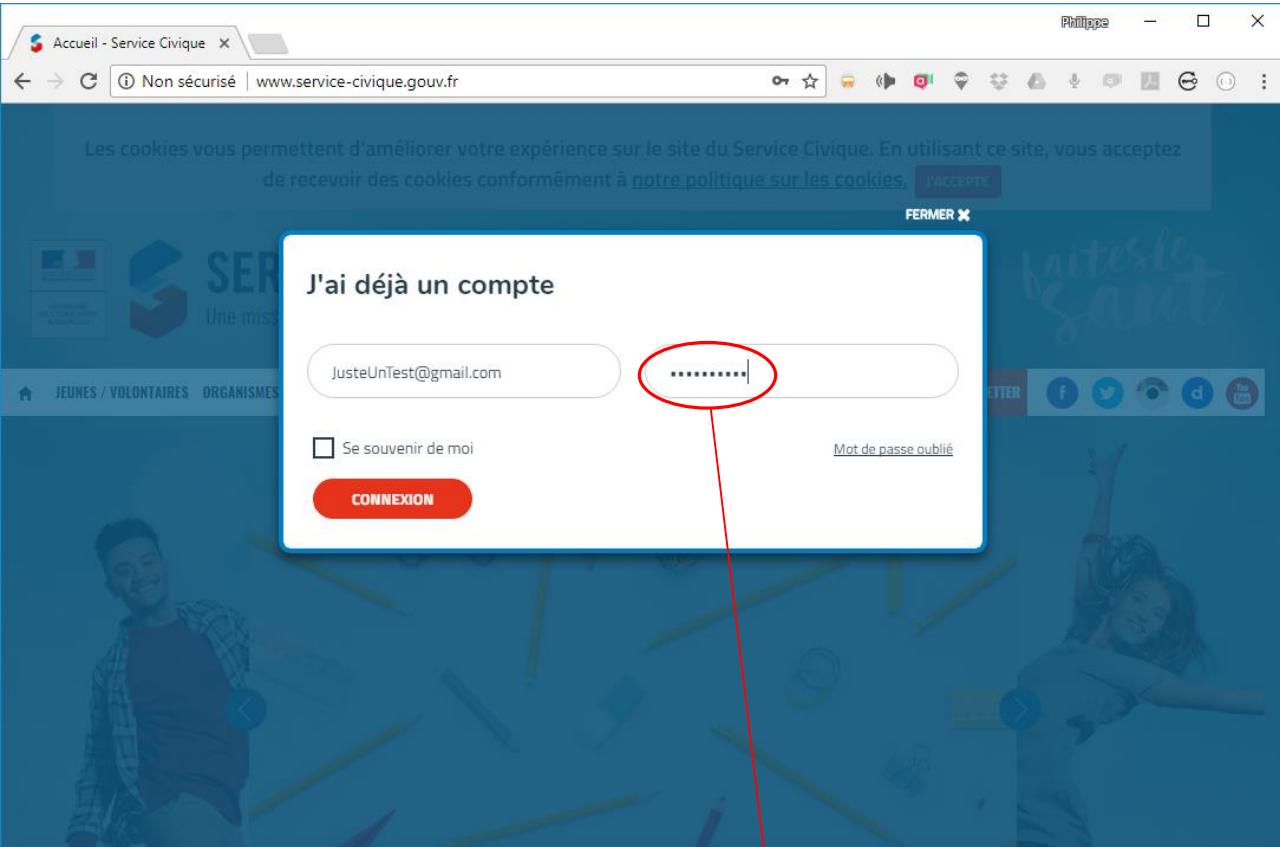
IP “Internet Protocol”  
(réseau)

TCP “Transport Control Protocol” (transport)



internet n'a PAS été pensé pour la sécurité mais pour le partage des données

<http://www.tcpipguide.com/free>



```
File Data: 128 bytes
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "_csrf_token" = "p4kjrCjydidapFGnfbKeUfJrdPeopPnnr69PUvtxLUM"
  > Form item: "_username" = "JusteUnTest@gmail.com"
  > Form item: "_password" = "CEstUnTest"
  > Form item: "_submit" = "Connexion"

0030 fa f0 79 3e 00 00 50 4f 53 54 20 2f 6c 6f 67 69 ..y>..PO ST /logi
0040 6e 5f 63 68 65 63 6b 20 48 54 54 50 2f 31 2e 31 n_check HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 73 65 72 76 ..Host: www.serv
0060 69 63 65 2d 63 69 76 69 71 75 65 2e 67 6f 75 76 ice-civi que.gouv
0070 2e 66 72 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a .fr..Con nection:
0080 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e keep-alive..Con
0090 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 31 32 38 tent-Len gth: 128
00a0 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a ..Cache- Control:
00b0 20 6d 61 78 2d 61 67 65 3d 30 0d 0a 4f 72 69 67 max-age =0..Orig

The full requested URI (including host name) (http.request.full_uri)
Paquets: 379 · Affichés: 10 (2.6%) · Perdus: 0 (0.0%) || Profil: Default
```

# INTERNET ... ?

internet n'a PAS été pensé **pour la sécurité**  
mais pour le **partage** des données

## Sécuriser ?

- Quoi ?
- Comment ?

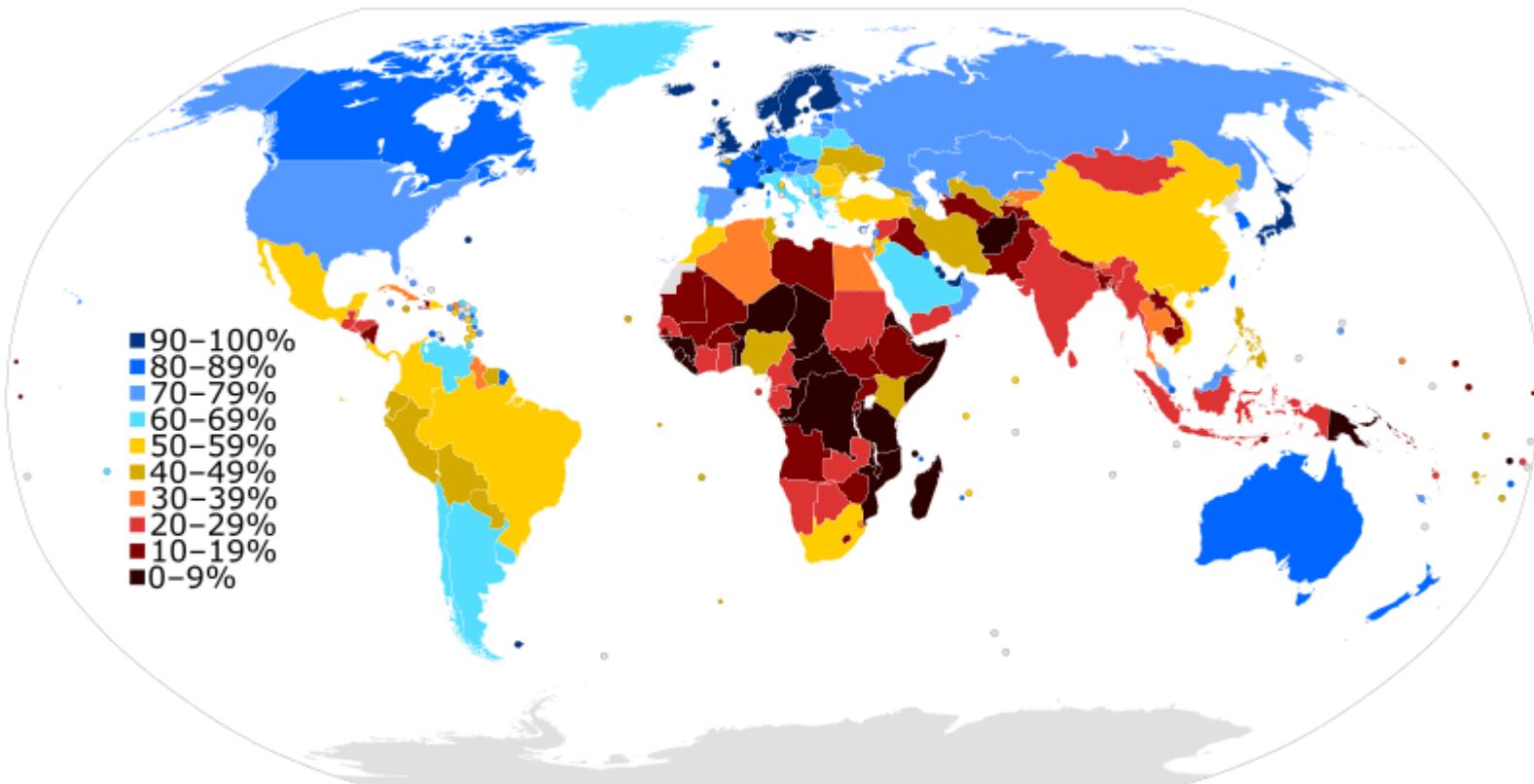


“Le seul système informatique vraiment sûr est un système éteint et débranché, enfermé dans un blockhaus sous terre, entouré par des gaz mortels et des gardiens hautement payés et armés.

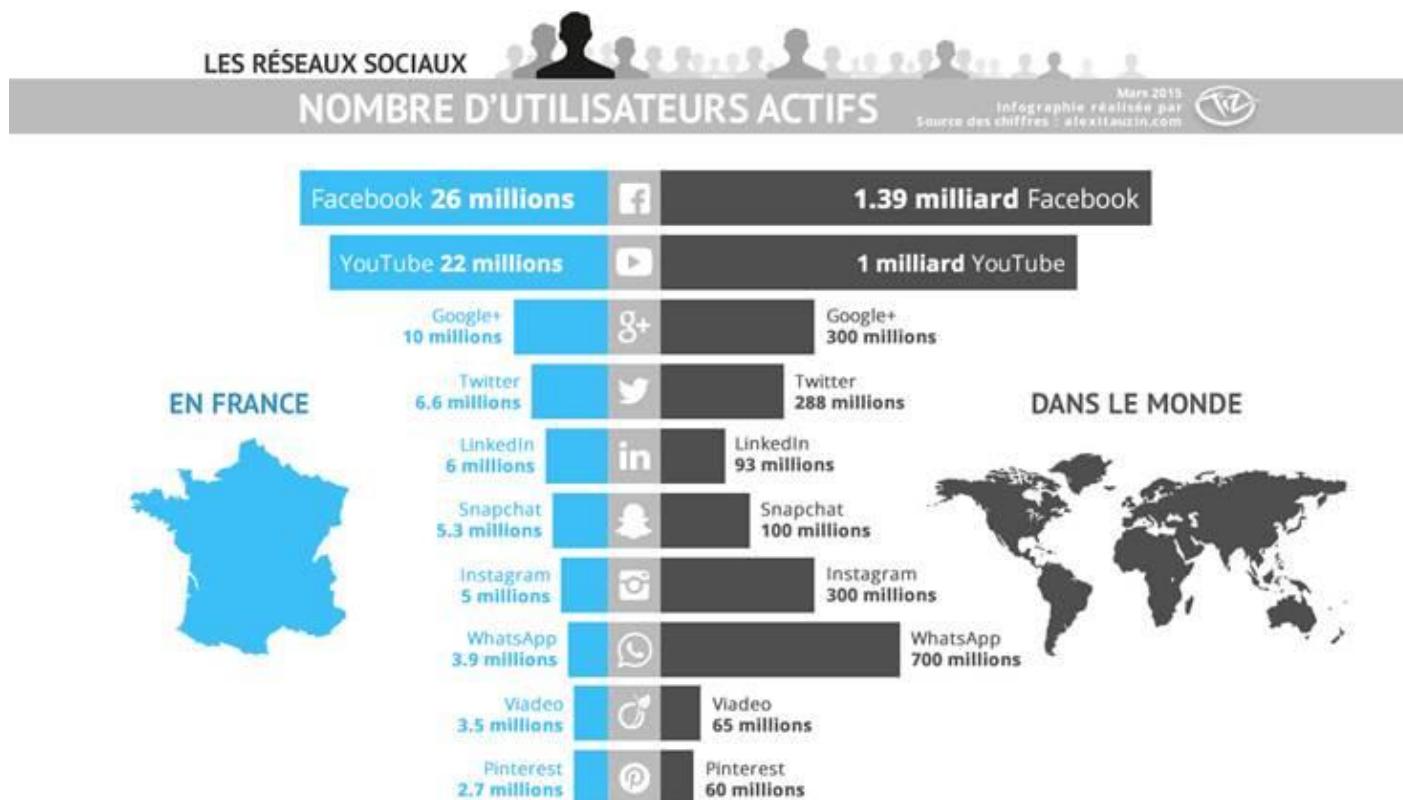
Même dans ces conditions, je ne parierais pas ma vie dessus.”

Pr .Eugene Spafford  
Purdue University

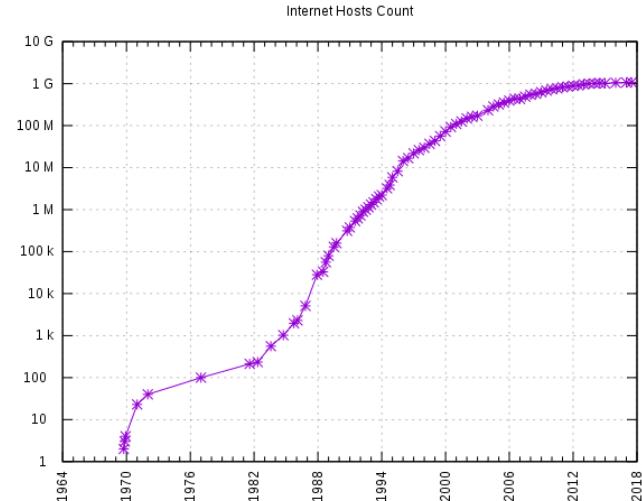
# INTERNET ? DES CHIFFRES (2015)



# INTERNET ? DES CHIFFRES



# INTERNET ? DES CHIFFRES



[https://en.wikipedia.org/wiki/Global\\_Internet\\_usage#/media/File:Internet\\_Hosts\\_Count\\_log.svg](https://en.wikipedia.org/wiki/Global_Internet_usage#/media/File:Internet_Hosts_Count_log.svg)

## 3,43 milliards d'internautes

- 144 milliards d'emails envoyés par jour (2/3 sont des spams)

1 site internet sur 500 est infecté par un virus ou un malware

- Google bloque 10 000 sites /jour

# ÇA A L'AIR SIMPLE ...

Beaucoup d'attaques sont liées à internet (devenu **LE** réseau mondial qui relie **TOUT** – les gens, les transports, ...)

Les utilisateurs sont souvent le point de départ ... ou l'objectif final !

## Pourquoi ?

- Pour vous nuire (diffamer, nuire à votre commerce)
- Voler votre argent !



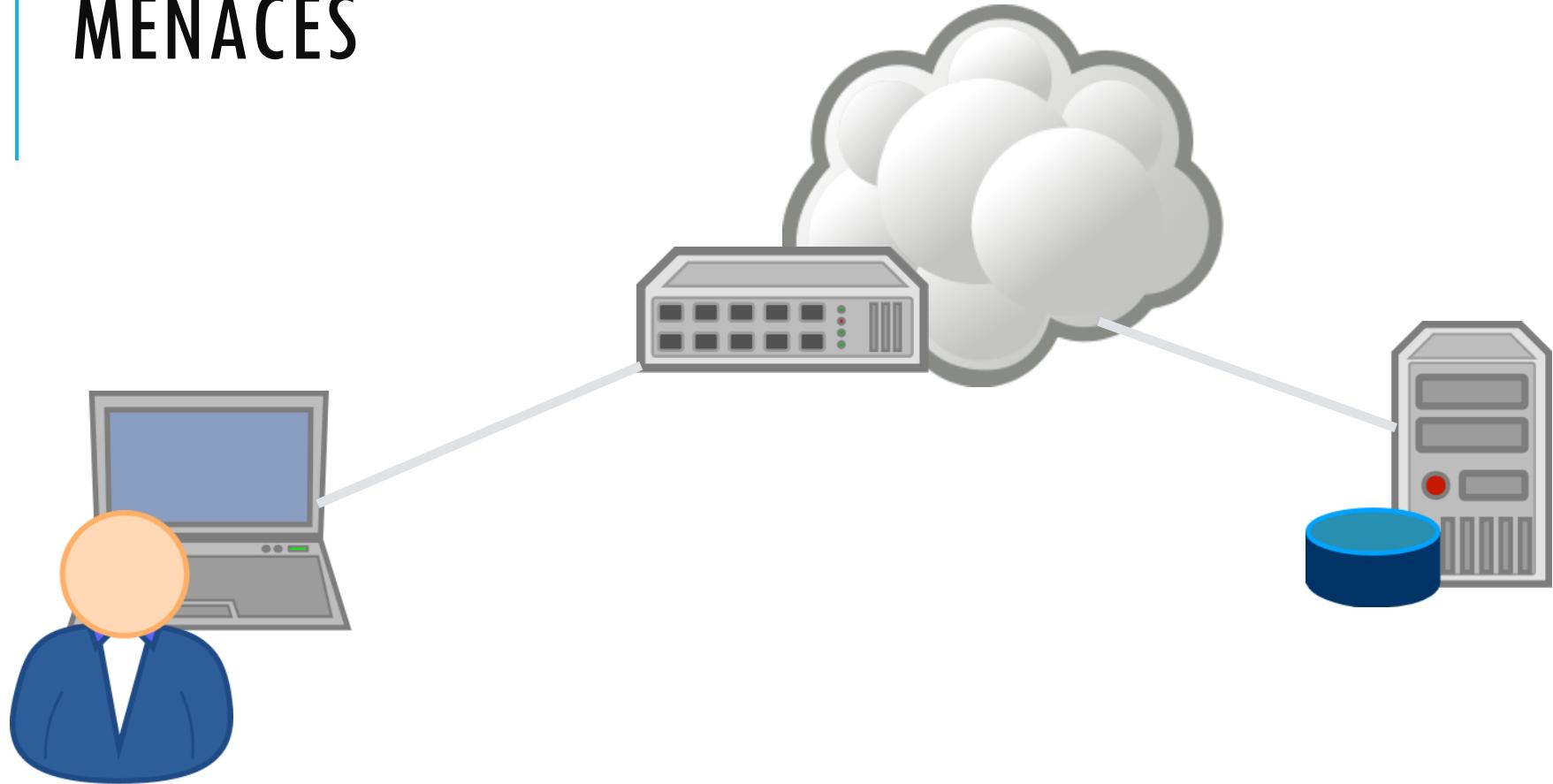
# D'OU VIENNENT LES PROBLÈMES ?

Beaucoup de « **fantasmes** »

La plupart des attaques sont simples et sont effectuées par des « *script kiddies* » (des gens qui ne connaissent pas grand-chose à l'informatique voire des enfants)



# MENACES

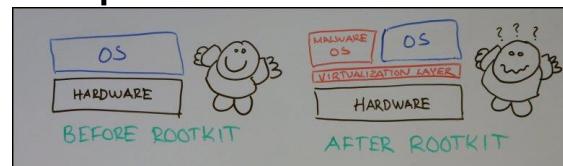


- 1 <http://openclipart.org/detail/171417/laptop-by-cyberscooty-171417>
- 2 <http://openclipart.org/detail/171423/server---database-by-cyberscooty-171423>
- 3 <http://openclipart.org/detail/171432/user-1-by-cyberscooty-171432>
- 4 <http://openclipart.org/detail/152311/internet-cloud-by-b.gaultier>
- 5 <http://openclipart.org/detail/171420/switch-hub-by-cyberscooty-171420>

# MENACES

- **sur les serveurs**

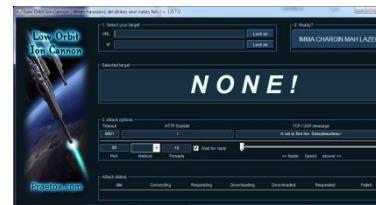
- Le « pirate » prend la main sur tout ou partie de la machine qui délivre des services
  - Ex: par intrusion (cassage de mots de passe, injection SQL, ...)
- Il compromet des services
  - Ex : modification de pages web, ...
- Et/ou ouvre « des portes dérobées » pour revenir plus tard
  - Ex : usage de rootkits, bootkits, ...
  - Attaque de type « cheval de Troie »
  - Ou via les « objets IoT » (Ex. de 未来)



# MENACES

- sur la communication
  - Le pirate écoute les communications
    - Ex : sidejacking (HTTP session jacking)
  - Détourne les communications en se faisant passer pour un autre
    - Ex : Fake hotspot, ARP Poisoning, ...
  - « Attaque » des serveurs en le saturant de demandes
    - Ex : Dénie de Service Distribué (DDoS)

<http://sourceforge.net/projects/loic>  
<https://map.httpcs.com/>



## CYBERTHREAT REAL-TIME MAP EN

Download Trial

MAP STATISTICS DATA SOURCES BUZZ WIDGET



## FRANCE

# 6 MOST-ATTACKED COUNTRY

|     |        |
|-----|--------|
| OAS | 632184 |
| ODS | 525759 |
| MAV | 7832   |
| HAV | 323157 |
| IDS | 537708 |
| VUL | 20666  |
| KAS | 951939 |
| BAD | 0      |

Detections discovered since 00:00 GMT

[More details](#)

Share data



MAV HAV IDS VUL KAS BAD

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on [more information](#).

ACCEPT AND CLOSE

# MENACES



<http://nakedsecurity.sophos.com/2012/11/21/prince-william-photos-password/>

# EN RÉSUMÉ ...

Menace 1 : on parle beaucoup ... trop !



## Menace 2 : on clique beaucoup ...

### Rançongiciel une prise d'otage informatique

#### 1 Envoi d'e-mails infectés

Exploitant une faille du système informatique, des pirates envoient des millions d'e-mails avec, en pièce jointe, un virus de type rançongiciel.



#### 2 Contamination de l'ordinateur

L'internaute visé ouvre le fichier infecté qu'il a reçu en pièce jointe sans se douter de sa dangerosité.



#### 3 Cryptage des fichiers

Le logiciel malveillant chiffre tous les fichiers (disques durs externes, clés USB...) pour les rendre inutilisables.



#### 4 Demande de rançon

Un message apparaît sur l'écran avec une demande de rançon.



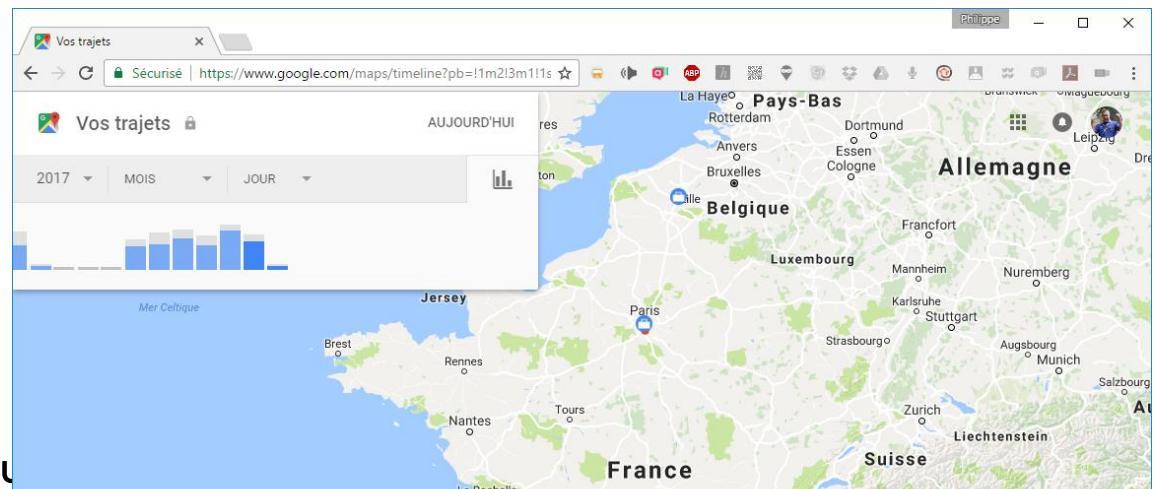
#### Paiement de la rançon

Si l'utilisateur accepte le chantage, il paie en bitcoin, une monnaie virtuelle et anonyme, et peut espérer récupérer ses fichiers.

#### 5 Refus du paiement

Si l'utilisateur ne paie pas, ses données restent inutilisables. Il peut toutefois réinitialiser son ordinateur au prix de la perte de toutes ses données.

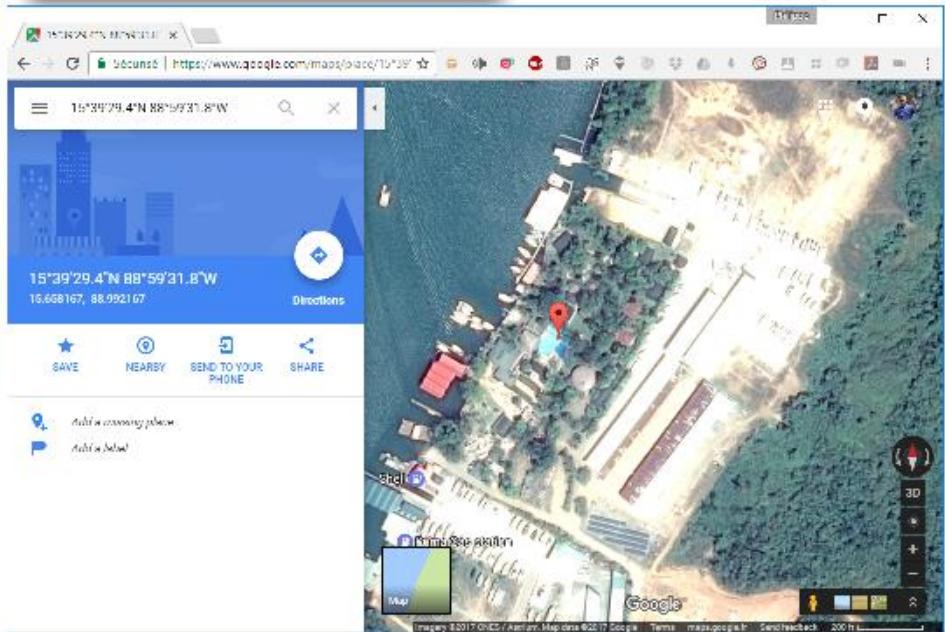




### Menace 3 : on laisse beau



exif:GPSImgDirection: 54424/255  
exif:GPSImgDirectionRef: T  
exif:GPSLatitude: 15,39,49N  
exif:GPSLongitude: 88,59,53W  
exif:GPSTimeStamp: 2012-12-03T18:25:26Z

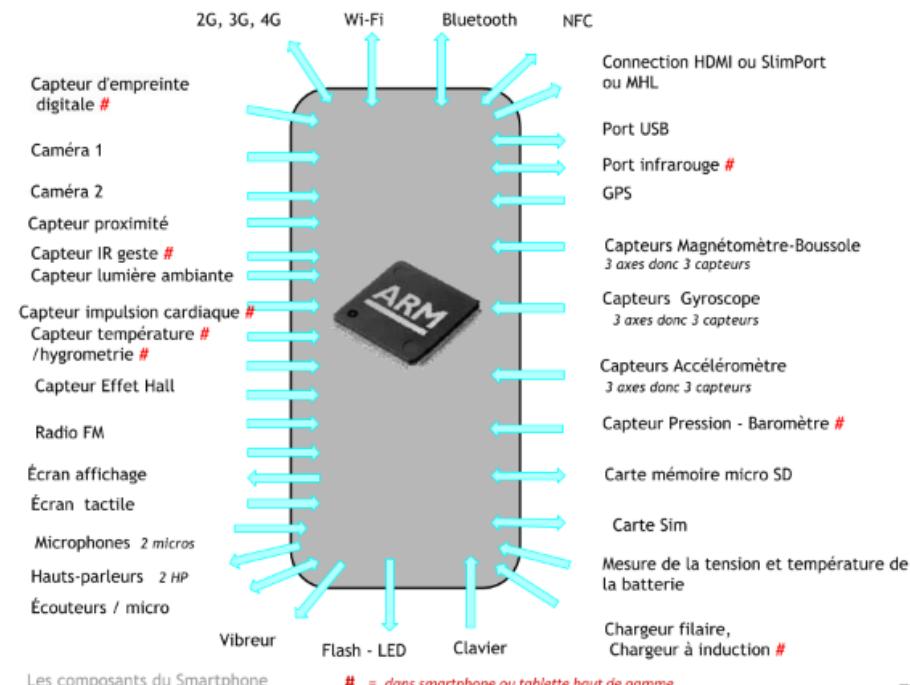


## Menace 4 : on a un « double » numérique ... Le smartphone !

- Il contient vie privée et vie publique
- Bourré de capteurs
- Facile à pirater

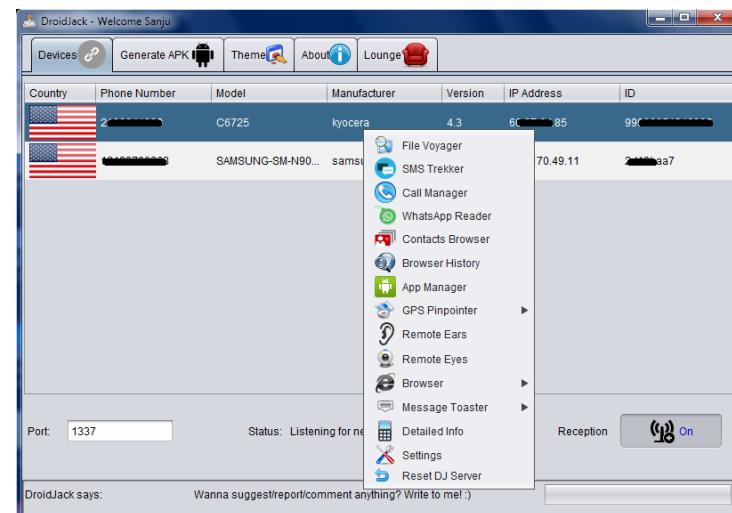


Un SmartPhone = Un SuperOrdinateur



# AVEC DES RAT REMOTE ADMINISTRATION TOOL

DROIDJACK : <http://droidjack.net>



AndroRAT : <https://github.com/wszf/andrорат>

```
public class MyService extends Service {  
    private static final b b;  
    private boolean c;  
  
    static {  
        MyService.b = new b("127.0.0.1", 1300);  
    }  
  
    public MyService() {
```

# AVEC DES OUTILS D'INTRUSION (PARFOIS GRATUITS)

<https://www.metasploit.com>

<https://www.pwnieexpress.com>



<https://www.zimperium.com/zanti-mobile-penetration-testing>

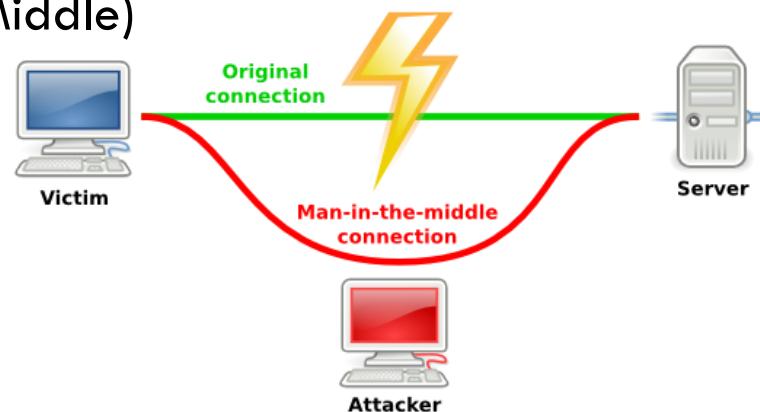


# AVEC DES LEURRES ...

Des hotspots (WiFi Gratuit par exemple ...)



Attaques MiTM (Man in The Middle)

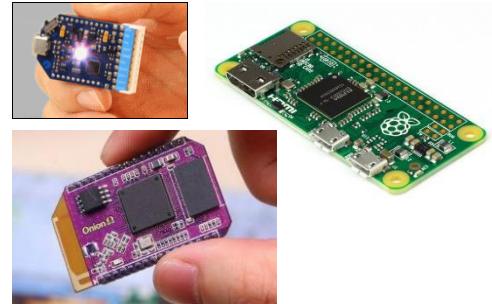


...

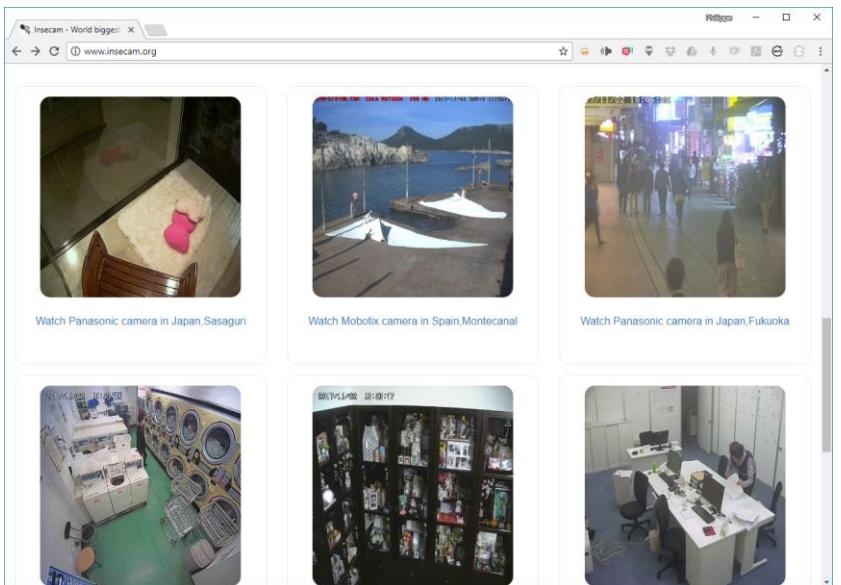


# ET FACILITÉ PAR L'IOT !

## IoT : Internet des Objets



- Plusieurs milliards d'ici 2020
- Assez peu / pas protégés (Attaque du BotNet 未来)



## Menace 5 : la désinformation

- Amplifié par les réseaux sociaux
- Tout se dit et son contraire ...

Largement utilisé ...

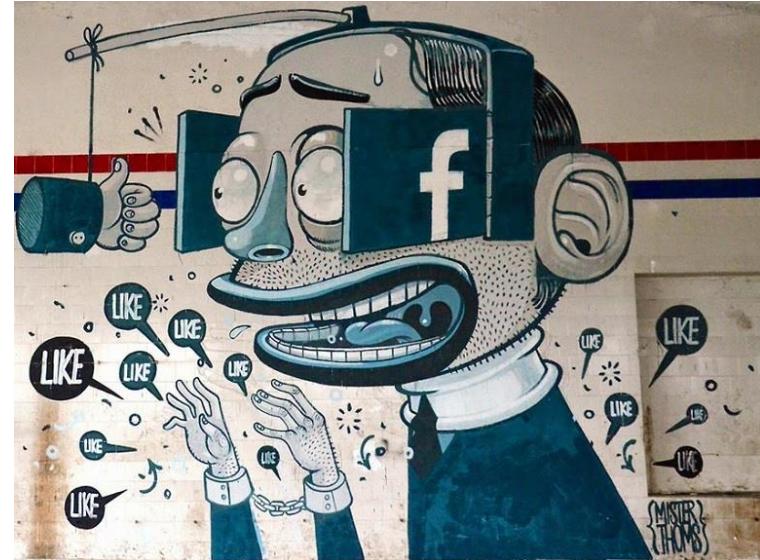
Business

Russian propaganda effort helped spread 'fake news' during election, experts say



Most Read

- 1 AT&T just unveiled its answer to the cord-cutting wars
- 2 Trump's populism is about to face a rude awakening
- 3 A single chart everybody needs to look at before Trump's big fight over bringing back American jobs



Decodex  
Proposé par Les Décodeurs / Le Monde ★★★★ (45) | Réseaux sociaux et communication | 13 417 utilisateurs

+ AJOUTER À CHROME

PRÉSENTATION AVIS ARTICLES SIMILAIRES

Comment vérifier la fiabilité d'un site en 3 clics

DÉCODEX

Comment vérifier la fiabilité d'un site en 3 clics

D D D D D

Compatibilité avec votre appareil

Avec le Décodex, évaluez en un clin d'œil si les sites que vous consultez sont fiables.

Un service innovant pour vous aider à vérifier l'information sur Internet.

Le Décodex est un service proposé par Les Décodeurs du Monde. Cela empêche vous d'indiquer en temps réel et pendant votre navigation si un site est fiable ou non.

Signaler un abus

Informations supplémentaires

Version : 1.1.2

Langue : Français

Taille : 365KB

"Ne croyez pas tout ce que vous lisez sur internet juste parce qu'il y a une photo et une citation à côté."

Charles de Gaulle

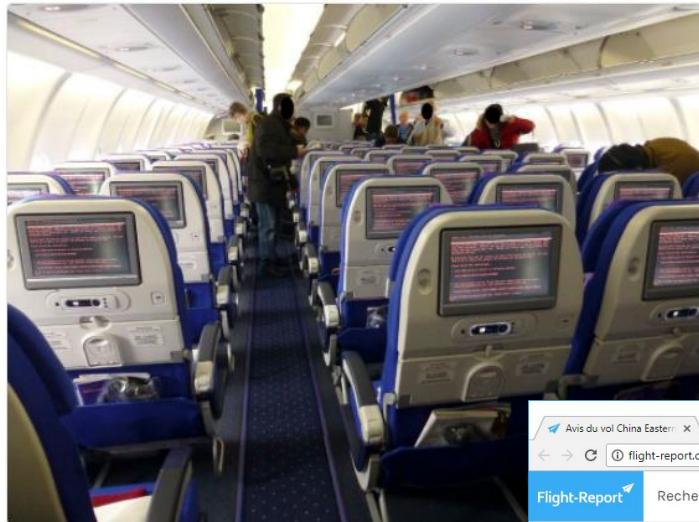


hackndo  
@HackAndDo

Suivre

Emergency landing after #ransomware  
#Petya infects a plane ! 😱

À l'origine en anglais



18:57 - 27 juin 2017

281 Retweets 217 J'aime



30 281 217

Recherche Google

https://www.google.fr/search?tbm=isch&q=DDb5J...AEDphw.jpg

Google

avion avec écran

Tous Images Maps Shopping Plus Paramètres Outils

Environ 25 270 000 000 résultats (0,72 secondes)

Taille de l'image :  
800 × 600

Trouver d'autres tailles de l'image :  
Toutes les tailles - Moyennes - Grandes

Hypothèse la plus probable pour cette image : [avion avec écran](#)

VIDÉO. Tiré au sort, un homme est violement expulsé d'un avion ...  
[www.leexpress.fr/...video-un-homme-violement-expulse-d-un-avion-united-airlines...](http://www.leexpress.fr/...video-un-homme-violement-expulse-d-un-avion-united-airlines...)  
10 avr. 2017 - Capture d'écran de la vidéo mise en ligne par l'un des passagers du vol 3411 de la ...  
L'avion a finalement décollé avec deux heures de retard.

Choisir un avion avec écran individuel vers les États-Unis ...  
[https://voyageforum.com/...Thèmes/Compagnies-aériennes/...](http://voyageforum.com/...Thèmes/Compagnies-aériennes/...)  
14 juil. 2010 - Ma question est donc: y a t'il un moyen de pouvoir choisir telle compagnie ou tel avion avec écran individuel. Si oui, quelle compagnie et quel ...

Images similaires

Avis du vol China Eastern

flight-report.com/fr/report/3290/China\_Eastern\_MU554\_Paris\_CDG\_Shanghai\_PVG

Flight-Report Recherche Bons plans Classements Blog Connexion

Compagnie China Eastern Classe Economique Avion Airbus A330-200 Décollage CDG Arrivée à PVG Temps de vol 11:35

5MM%2538http%25253A%25252F%25252Fflight-rep...

# CONCLUSION



**La technologie possède deux faces :**

- Une qui nous permet de rester en contact, de partager, de découvrir le monde
- Une qui permet aux malfrats, mafias, terroristes ... de voler, trafiquer, ...

**Soyons conscients de nos actes,  
Nous pouvons tous agir.**

**Tirons le meilleur de la technologie !**

# CONTACT

**Site web / mél** <http://www.irit.fr/~Philippe.TrUILLET>

[Philippe.TrUILLET@univ-tlse3.fr](mailto:Philippe.TrUILLET@univ-tlse3.fr)

## Réseaux sociaux



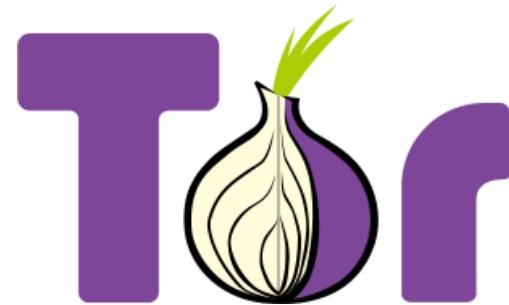
Philippe Truillet (Profil Professionnel)



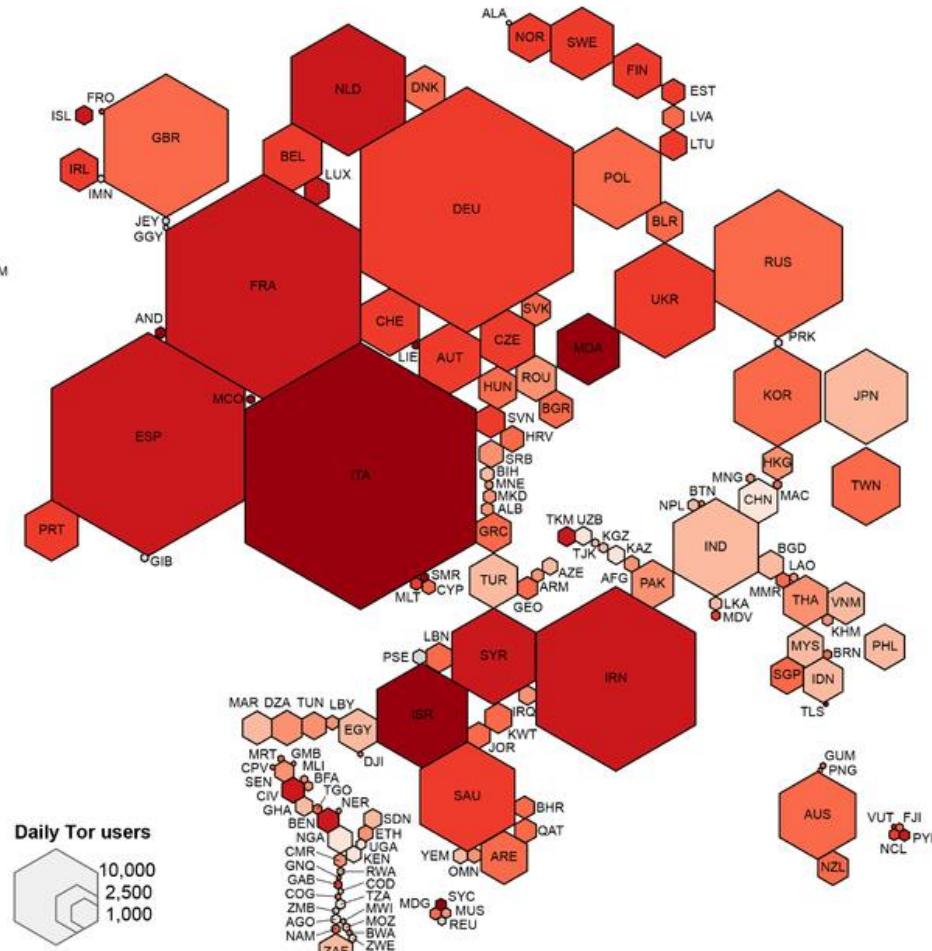
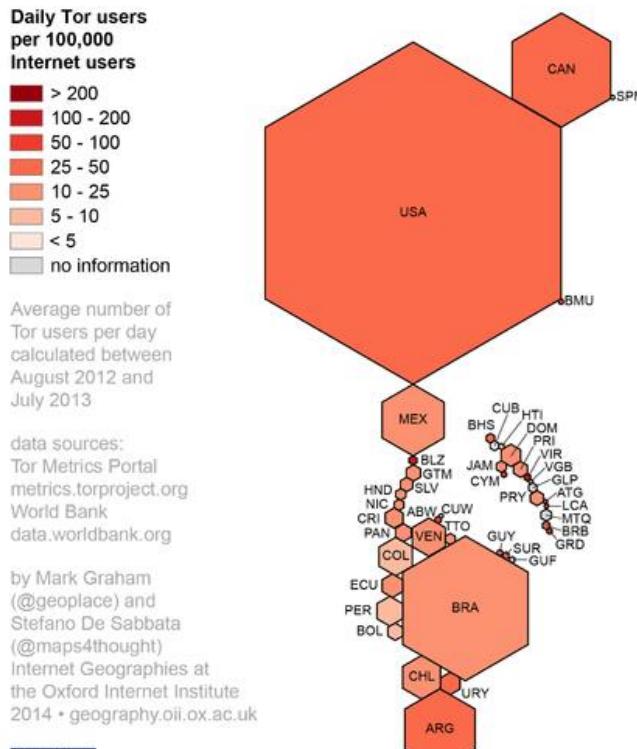
Suivre

@phtruillett

**TOR**



# The anonymous Internet



Average number of  
Tor users per day  
calculated between  
August 2012 and  
July 2013

data sources:  
Tor Metrics Portal  
[metrics.torproject.org](http://metrics.torproject.org)  
World Bank  
[data.worldbank.org](http://data.worldbank.org)

by Mark Graham  
(@geoplace) and  
Stefano De Sabbata  
(@maps4thought)  
Internet Geographies at  
the Oxford Internet Institute  
2014 • geography.oiil.ox.ac.uk

# TOR ET NOUVEAU MARCHÉ

## What is Satan?

Apart from the mythological creature, Satan is a ransomware, a malicious software that once opened in a Windows system, encrypts all the files, and demands a ransom for the decryption tools.

## How to make money with Satan?

First of all, you'll need to [sign up](#). Once you've sign up, you'll have to log in to your account, create a new virus and download it. Once you've downloaded your newly created virus, you're ready to start infecting people.

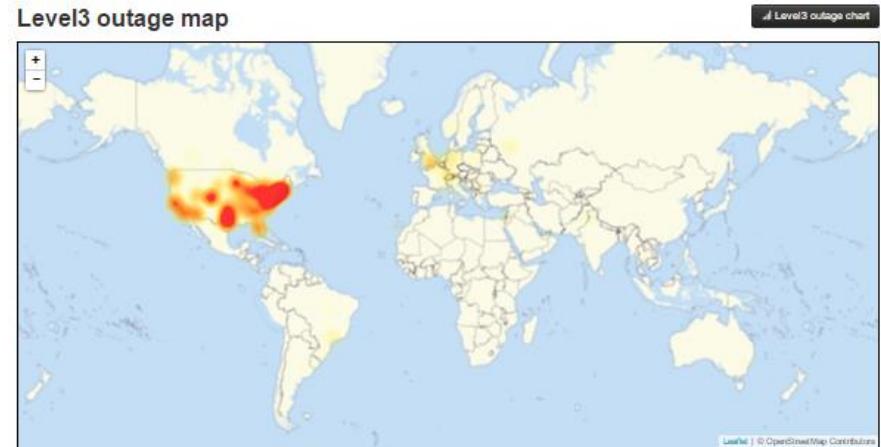
Now, the most important part: **the bitcoin paid by the victim will be credited to your account**. We will keep a 30% fee. If you specified a 1 BTC ransom, you will get 0.7 BTC and we will get 0.3 BTC. The fee will become lower depending on the number of payments you have.

The screenshot shows a web-based interface for managing a ransomware operation. At the top, there's a navigation bar with links for Satan, Malwares, Droppers, Translate, Account, Notices, and Messages (0). A user is logged in under 'Satan'. The main area displays account statistics: Malwares (0), Infections (0), Paid (0), and a Balance of 0.0000000 BTC. Below this is a 'First time logging in' section with a secret token: TcflyC9zKldSOLkdSSbbmTaabnwaeo. A 'Create a malware' form is at the bottom, with fields for Ransom (Ransom in BTC (min 0.1)), Multiplier (Optional), Multiplier (Days) (Optional), and Note (Optional). The note field includes a note: "Notes are private, and used only to keep track of your victims."

# MIRAI BOTNET - 未来

<https://github.com/jgamblin/Mirai-Source-Code>

This screenshot shows the GitHub repository page for 'jgamblin/Mirai-Source-Code'. The page includes a brief description: 'Leaked Mirai Source Code for Research/IoC Development Purposes'. It displays basic repository statistics: 6 commits, 1 branch, 0 releases, and 3 contributors. A timeline of recent commits is shown, all made by 'jgamblin' 29 days ago, with commit messages like 'Merge pull request #30 from peterkshultz/master' and 'Trying to Shrink Size'. The repository has 374 stars and 2,227 forks.



# MOTEURS D'OBJETS

<https://www.insecam.org>

<https://www.shodan.io>

The screenshot shows the Shodan search interface with a dark theme. The top navigation bar includes links for 'Shodan', 'Developers', 'Book', and 'View All...'. The main search bar contains the query 'Webcam'. Below the search bar, there are buttons for 'Explore', 'Enterprise Access', and 'Contact Us'. A 'Login or Register' button is also present. The main content area features sections for 'Featured Categories' (Industrial Control Systems, Databases) and 'Top Voted' (Webcam, Cams). The 'Recently Shared' section lists an entry for 'AXIS IP Cams'.

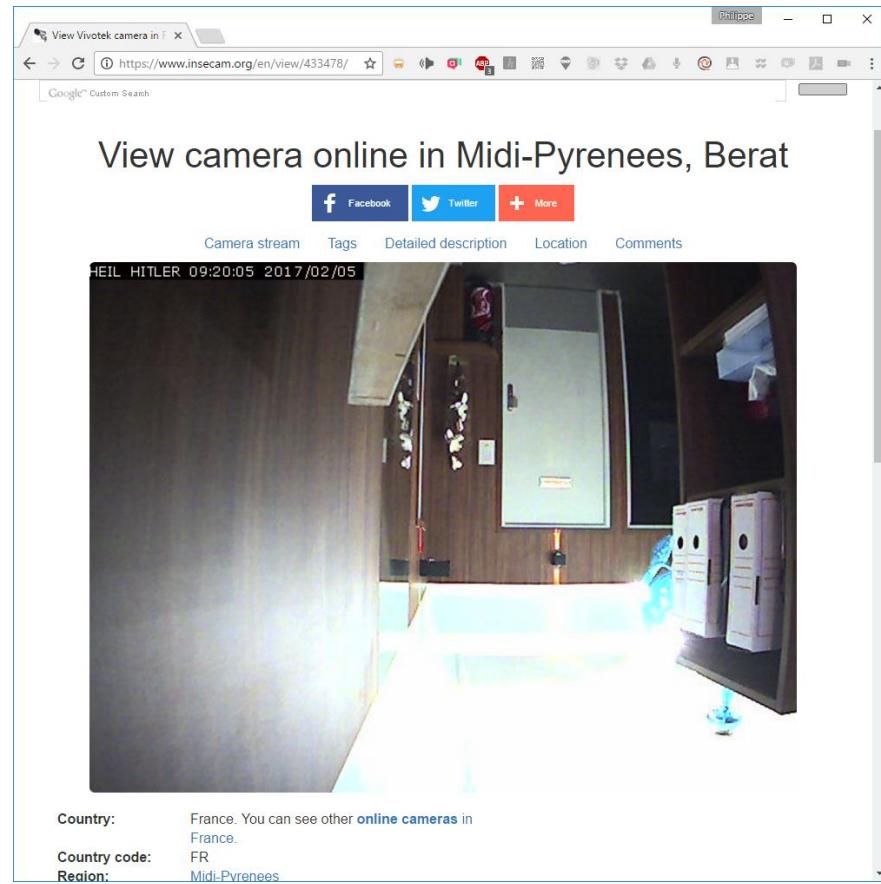
Country: France. You can see other [online cameras](#) in France.  
Country code: FR  
Region: Midi-Pyrénées

Welcome to Insecam project. The world biggest directory of online surveillance security cameras. Select a country to watch live street, traffic, parking, office, road, beach, earth online webcams. Now you can search live web cams around the world. You can find here Axis, Panasonic, Linksys, Sony, TP-Link, Foscam and a lot of other network video cams available online without a password. Mozilla Firefox browser is recommended to watch network cameras.

The following actions were made to Insecam for the protection of individual privacy:

- Only filtered cameras are available now. This way none of the cameras on Insecam invade anybody's private life.
- Any private or unethical camera will be removed immediately upon e-mail complaint. Please provide a direct link to help facilitate the prompt removal of the camera.
- If you do not want to contact us by e-mail, you can still remove your camera from Insecam. The only thing you need to do is to set the password of your camera.
- You can add your camera to the directory by following next [link](#). It will be available only after administrator's approval.

The coordinates of the cameras are approximate. They point to the ISP address and not the physical address of the camera. This information is accurate only to a few hundred miles. The coordinates are provided for the convenience of the user and are not intended to be used for navigation purposes. We are not responsible for any errors or inaccuracies in the coordinates provided.



The screenshot shows the Insecam website homepage with a dark theme. The top navigation bar includes links for 'Welcome', 'Most popular', 'Manufacturers', 'Countries', 'Places', 'Cities', 'Timezones', 'New online cameras', 'FAQ', and 'Contacts'. The main content area features a heading 'Network live IP video cameras directory Insecam.com' and a welcome message about the project's purpose and privacy policy.