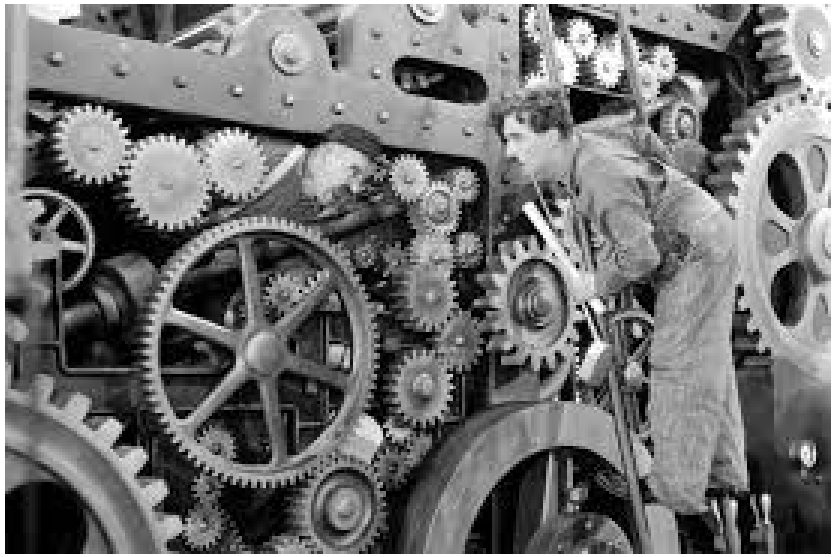
Les grandes désillusions des temps modernes

G[al] Jean-Louis Desvignes *(voir aussi autre texte illustré)*

Prof. Jean-Jacques Quisquater



Cheval de Troie

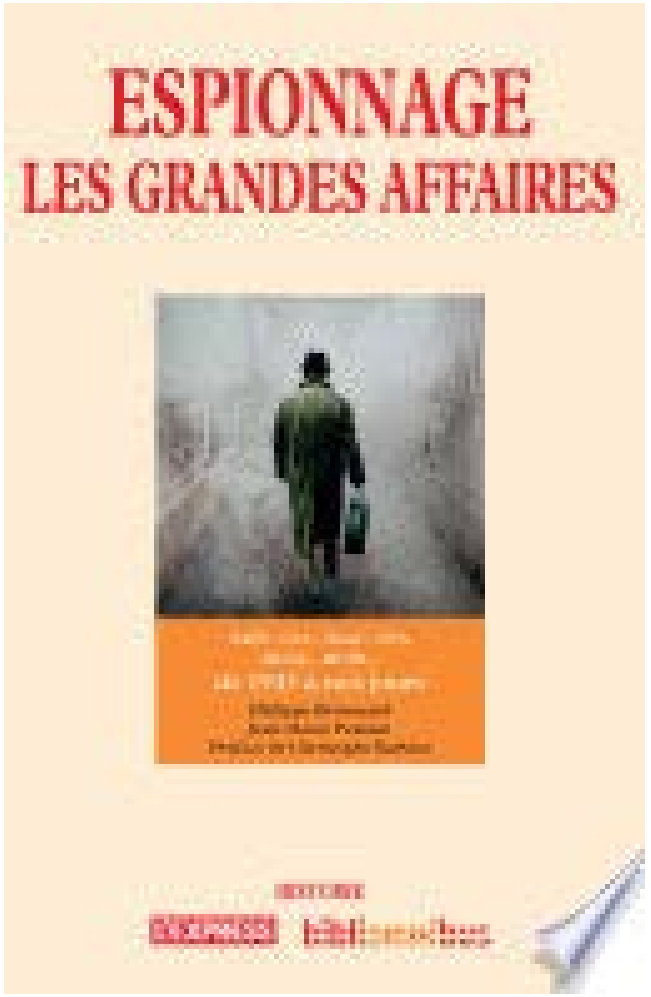
- Mythe tenace
- Problème constant (backdoor)

Les téléscripteurs français (Quai d'orsay) de l'ambassade à Moscou (1983)

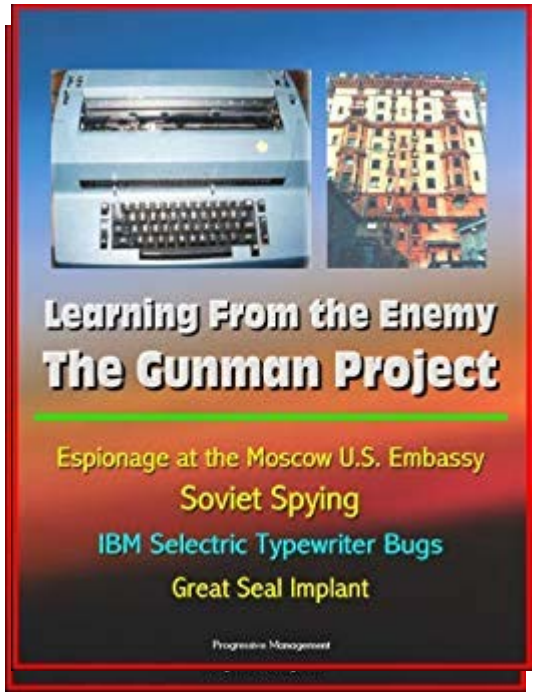
- Grâce à *Jour,* probablement, les nouveaux téléscripteurs installés à l'ambassade de France à Moscou, entre octobre 1976 et février 1977, furent «écoutés» pendant six ans. L'ambassade de France à Moscou était depuis longtemps une cible favorite du KGB, et le livre raconte comment dans les années 60 de charmantes Mata Hari soviétiques entreprirent de séduire l'ambassadeur, Maurice Dejean, et l'attaché de l'air, le colonel Louis Guibaud. …

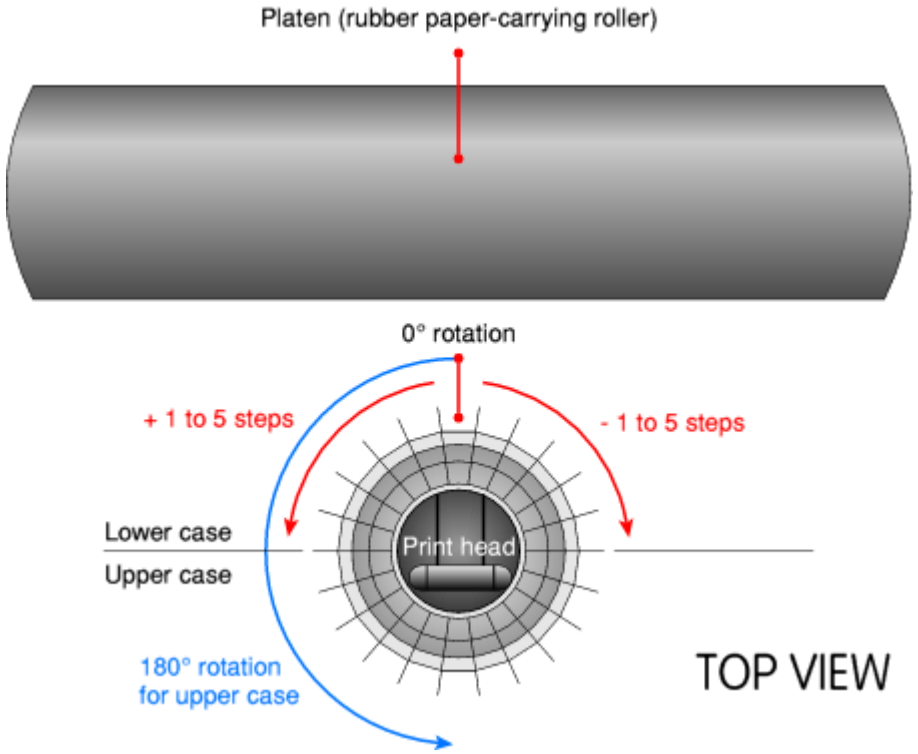
- « Jour » est une recrue du KGB (actif entre 1945 et 1983), employé du chiffre au Quai d'Orsay, Paris, …

- **Voir la présentation de Jean-Louis Desvignes**

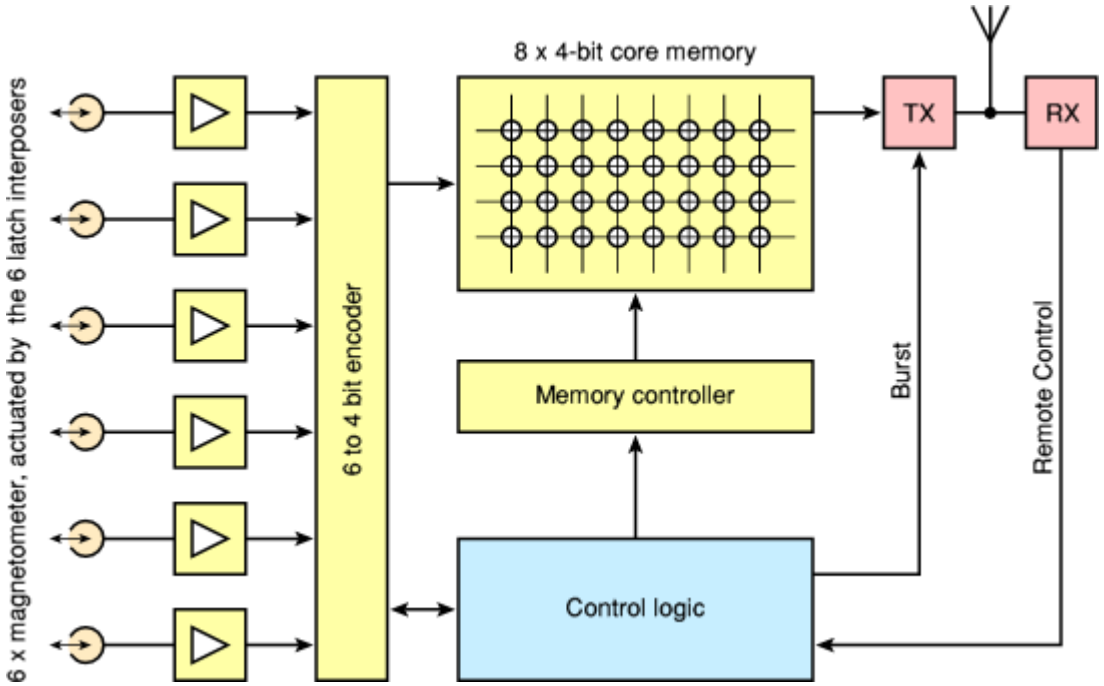


Ambassade USA à Moscou (1984)
https://www.cryptomuseum.com/covert/bugs/selectric/



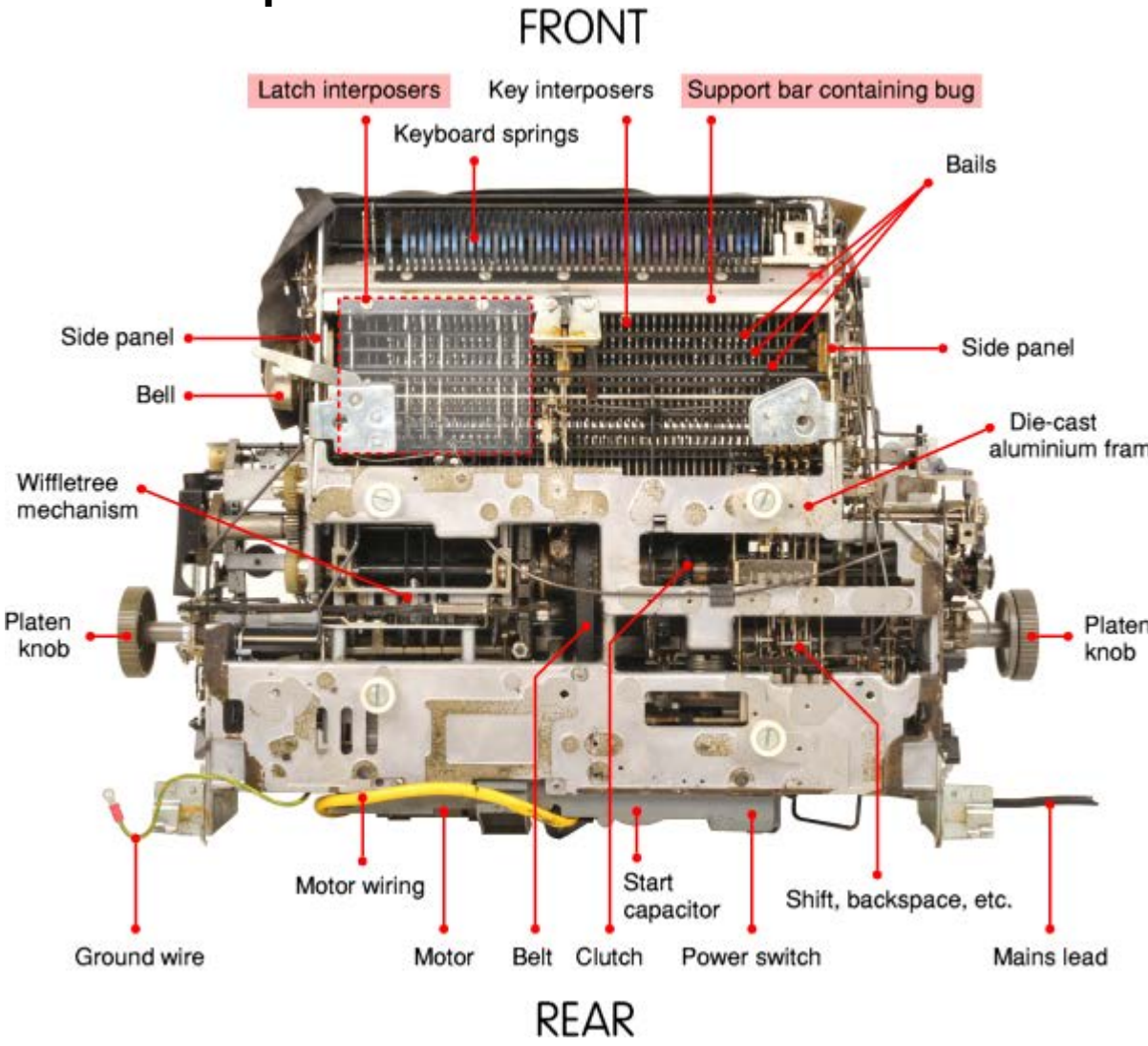


Circuits de codage des magnétomètres

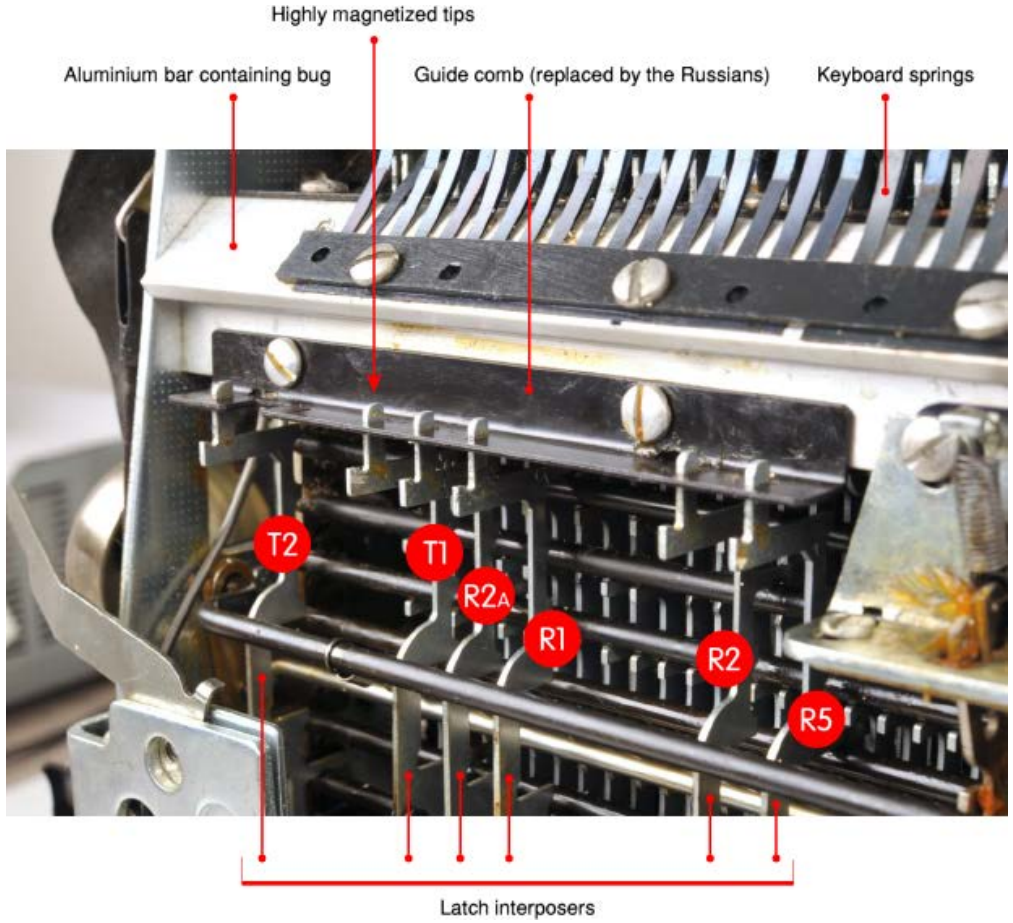


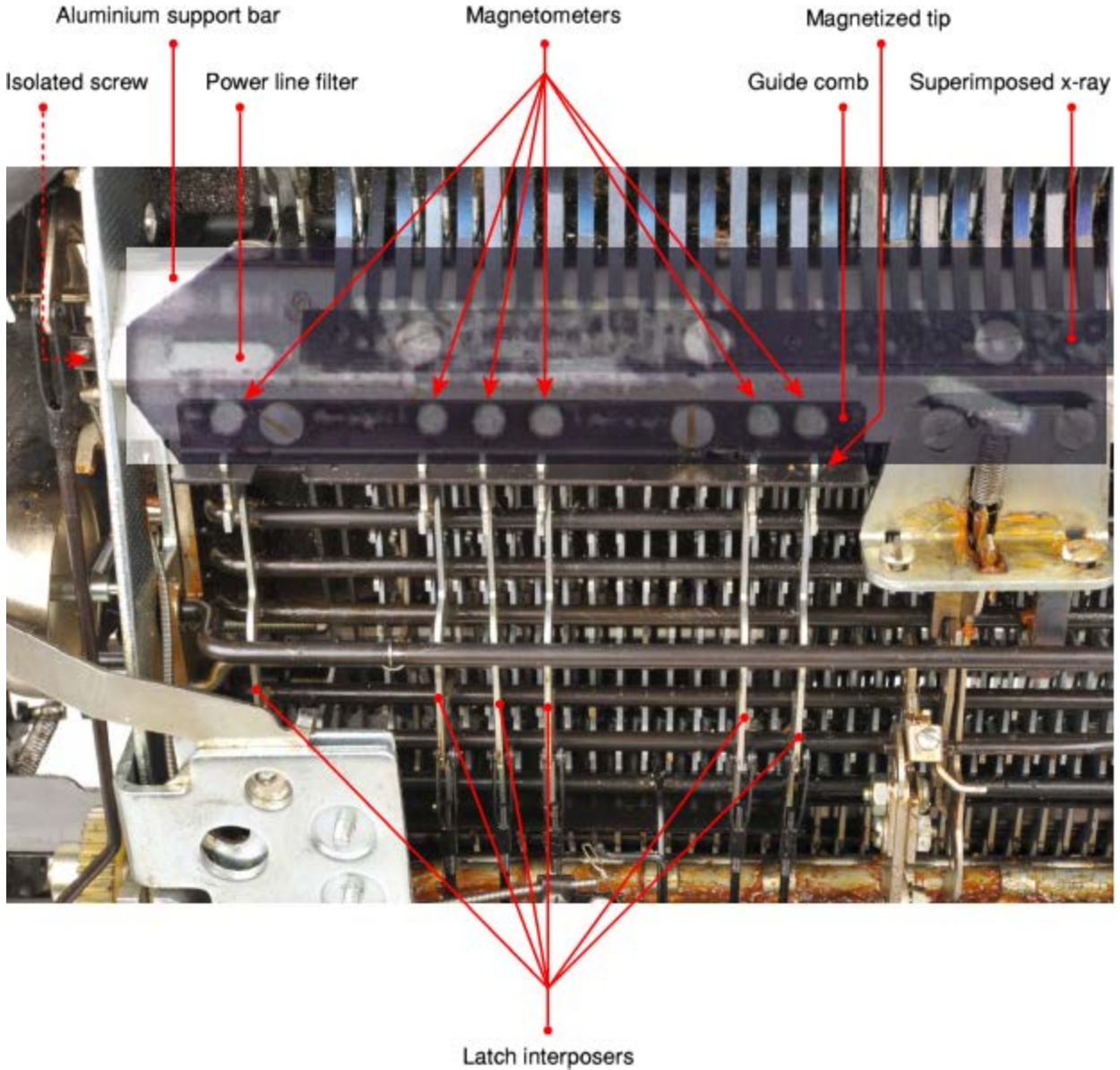
Utilisé de 1976 à 1984 pour espionner US

- Encore plus longtemps que pour l'ambassade de France,
- 6 magnétomètres par machine + circuit (bug),
- 16 tonnes de matériel saisi,
- 16 machines infectées (aussi à Léningrad),
- USA averti par les Français !

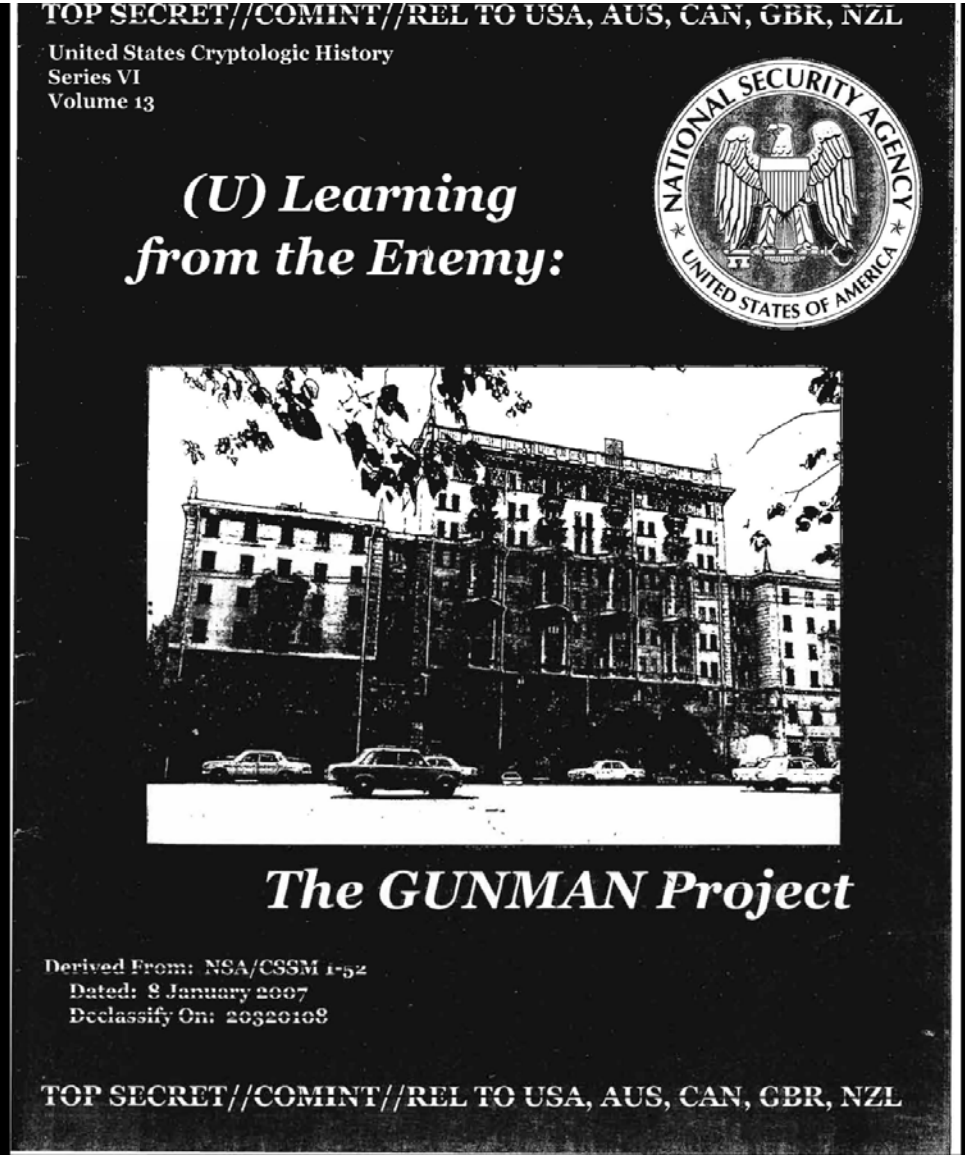


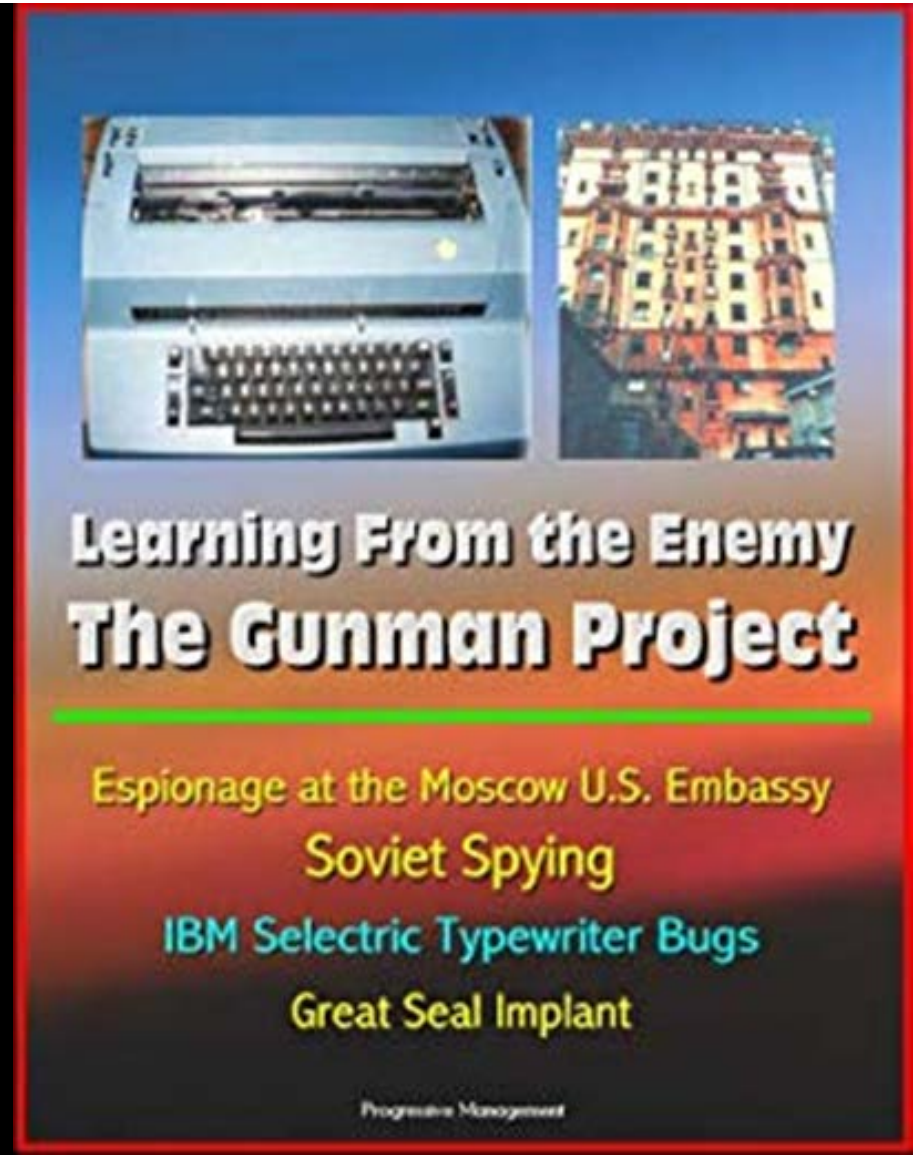
Les endroits infectés





Rapport de la NSA (version interne) + livre





Affaire Humpich (1997) :
voir surtout exposé de Jean-Louis Desvignes

Le Monde

Consulter le journal

J. QUISQUATER

ACTUALITÉS ÉCONOMIE VIDÉOS OPINIONS CULTURE M LE MAG SERVICES

ARCHIVES

Favoris Partage

Les faiblesses de la puce sont connues depuis longtemps

Par Hervé Morin • Publié le 10 mars 2000 à 13h24 - Mis à jour le 10 mars 2000 à 13h24

Lecture 4 min.

Article réservé aux abonnés

LE MYTHE français de l'inviolabilité de la carte bancaire à puce a vécu. Serge Humpich, un informaticien ingénieux, l'a prouvé à ses dépens *(lire ci-dessous)*. Il

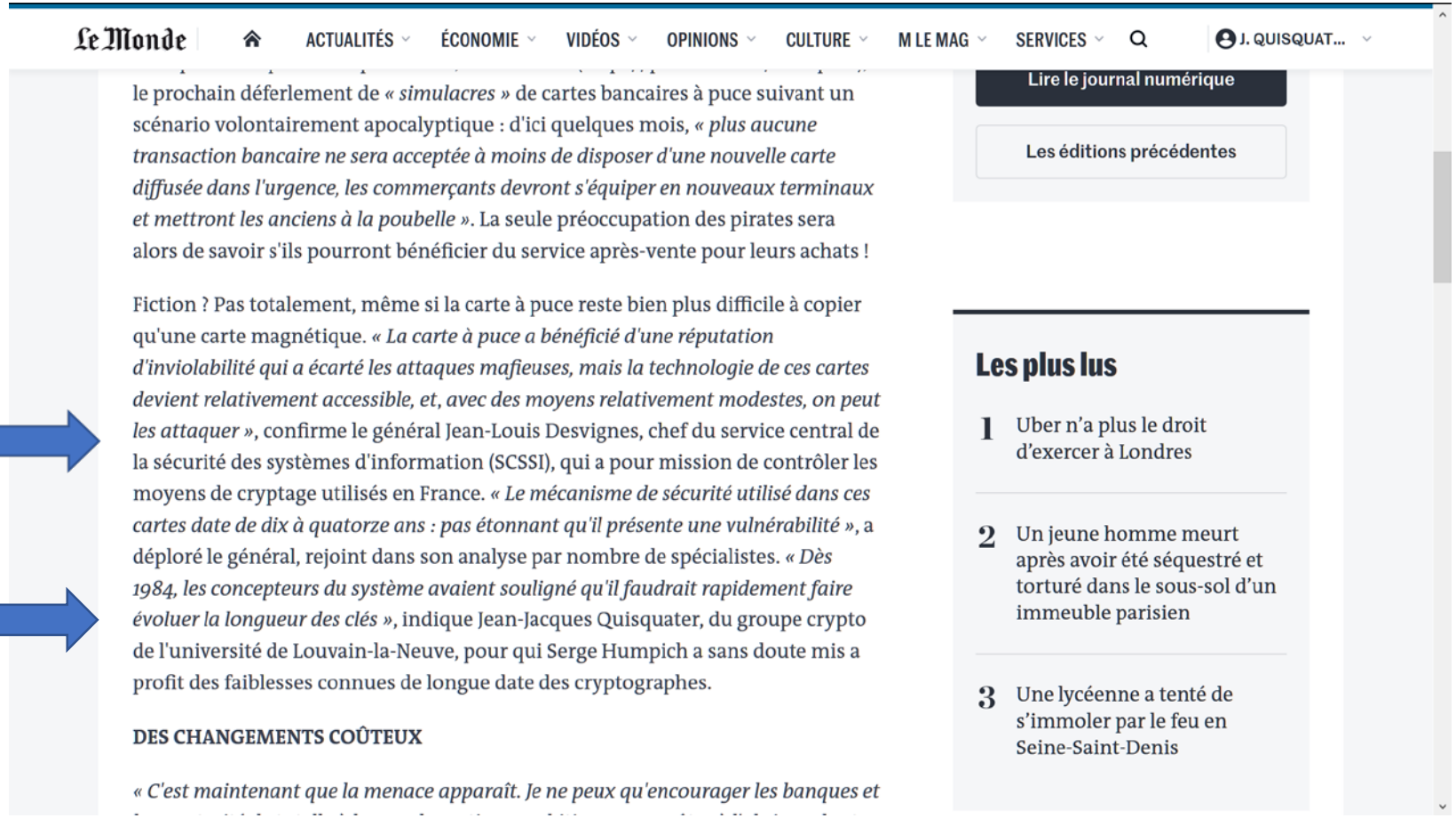
Édition du jour

Daté du mardi 26 novembre

Le Monde

Un nouvel arsenal législatif contre les féminicides

Le Monde (suite) : les deux orateurs …



Le Monde | ACTUALITÉS | ÉCONOMIE | VIDÉOS | OPINIONS | CULTURE | M LE MAG | SERVICES | J. QUISQUAT…

le prochain déferlement de *« simulacres »* de cartes bancaires à puce suivant un scénario volontairement apocalyptique : d'ici quelques mois, *« plus aucune transaction bancaire ne sera acceptée à moins de disposer d'une nouvelle carte diffusée dans l'urgence, les commerçants devront s'équiper en nouveaux terminaux et mettront les anciens à la poubelle »*. La seule préoccupation des pirates sera alors de savoir s'ils pourront bénéficier du service après-vente pour leurs achats !

Fiction ? Pas totalement, même si la carte à puce reste bien plus difficile à copier qu'une carte magnétique. *« La carte à puce a bénéficié d'une réputation d'inviolabilité qui a écarté les attaques mafieuses, mais la technologie de ces cartes devient relativement accessible, et, avec des moyens relativement modestes, on peut les attaquer »*, confirme le général Jean-Louis Desvignes, chef du service central de la sécurité des systèmes d'information (SCSSI), qui a pour mission de contrôler les moyens de cryptage utilisés en France. *« Le mécanisme de sécurité utilisé dans ces cartes date de dix à quatorze ans : pas étonnant qu'il présente une vulnérabilité »*, a déploré le général, rejoint dans son analyse par nombre de spécialistes. *« Dès 1984, les concepteurs du système avaient souligné qu'il faudrait rapidement faire évoluer la longueur des clés »*, indique Jean-Jacques Quisquater, du groupe crypto de l'université de Louvain-la-Neuve, pour qui Serge Humpich a sans doute mis a profit des faiblesses connues de longue date des cryptographes.

DES CHANGEMENTS COÛTEUX

« C'est maintenant que la menace apparaît. Je ne peux qu'encourager les banques et

Lire le journal numérique

Les éditions précédentes

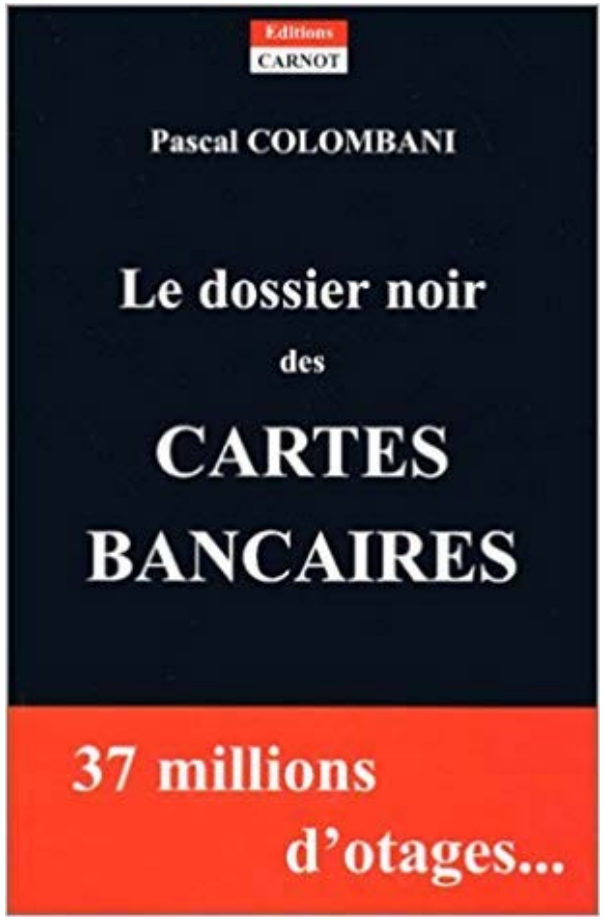
Les plus lus

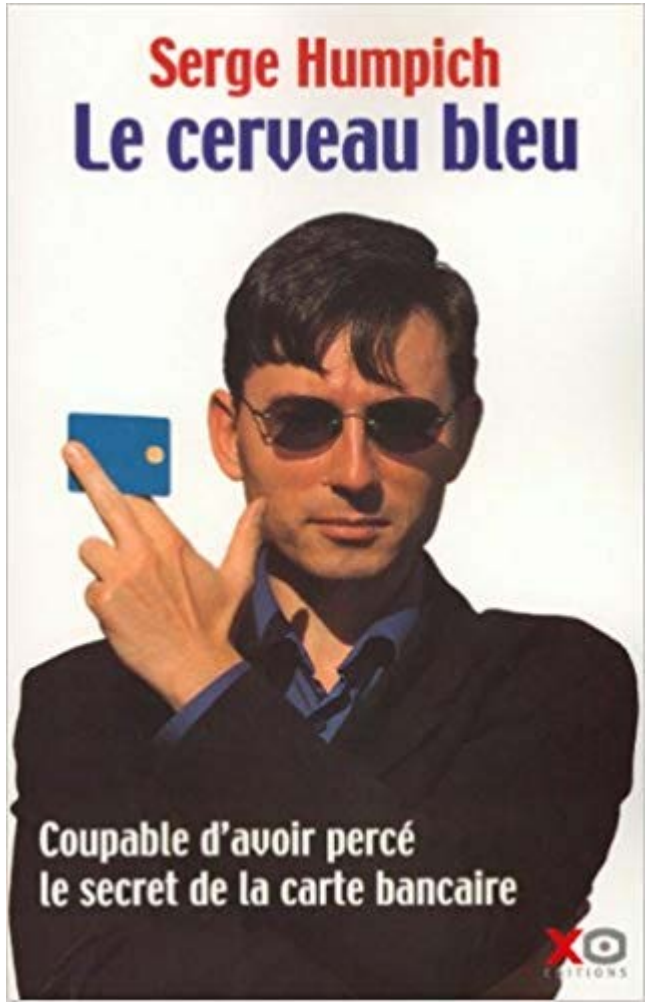
1 Uber n'a plus le droit d'exercer à Londres

2 Un jeune homme meurt après avoir été séquestré et torturé dans le sous-sol d'un immeuble parisien

3 Une lycéenne a tenté de s'immoler par le feu en Seine-Saint-Denis

livres


Editions
CARNOT
Pascal COLOMBANI
Le dossier noir
des
CARTES
BANCAIRES
37 millions
d'otages...


Serge Humpich
Le cerveau bleu
Coupable d'avoir percé
le secret de la carte bancaire
XO
EDITIONS

English Italiano Español Russian Polish Português Norsk Japanese Dansk

L'affaire des cartes bancaires

Depuis que Serge Humpich a démontré que les cartes bancaires à puce françaises sont falsifiables, la vérité éclate peu à peu sur cette affaire de la sécurité des cartes bancaires et des moyens de paiement électroniques.

Ce site fait toute la lumière sur les multiples failles persistantes du système des cartes bancaires (notamment au niveau des terminaux de paiement électroniques chez les commerçants).

Le GIE cartes bancaires (cartel réunissant 175 banques), qui a poursuivi injustement Serge Humpich, est sur la sellette du fait de sa position monopolistique (puisqu'il diffuse la quasi totalité des 37 millions de cartes bancaires en France) et des lacunes de sa politique sécuritaire. Sa responsabilité et sa crédibilité est directement en cause.

Il s'agit maintenant de réorganiser la politique sécuritaire des moyens de paiement électronique en adoptant des normes techniques transparentes et ouvertes.

Ce portail indépendant donne ainsi les dernières nouvelles en matière de monétique, et les commente. Il propose des dossiers sur les problèmes juridiques, techniques, de l'évolution du piratage, de fraude, politiques, concurrentiels sans oublier les conséquences au niveau du commerce électronique avec les systèmes Cyber-comm et de Porte-monnaie électronique.
Les rôles des différents acteurs sont précisés.

22/05/2000 Documents exclusifs : Politique de lobbying européen et français du cartel des banques.

30/04/2000 Document exclusif : Lettre de la Banque de France au Directeur Général de la Police Nationale pour demander des mesures de surveillance et de protection adaptées autour de l'affaire Humpich.

16/04/2000 : critique du système propriétaire "cyber-comm" de transactions soit disant "sécurisées" par Internet qu'on veut nous "imposer" au prix d'une propagande intense actuellement.

Changement de propriétaire !!!!
Revenez bientôt !!!

Détournement de marque

Logos cartes pirates
Des détournements de marque et des logos pour décorer votre Yescard

antipub.net
Site de militants contre la pub.

Je Boycotte ~~DANONE~~
Site appelant au boycott de la multinationale du yaourt qui non seulement licencie du personnel pour faire monter son cours en bourse mais veut baillonner les gens qui s'en émeuvent

Humour

Quizz du malfaiteur
Progressez en math pour diriger le gang

rigoler.com
Le web pour rigoler

Prix Darwin
Récompense chaque année les accidents les plus absurdes

Parodies de site

Rapts Bancaires
Parodie de la page d'accueil du Groupement des Rapts Bancaires

ZiPiZ.com
Parodie de site à la gloire des hackers. Le nom ressemble à celui de zataz.com, site sur l'actualité des hackers.

Loft Poury
Le cauchemar de vos rêves, parodie de Loft Story

CNN
Parodie du site de CNN

Les bêtes du web
Parodie de sites animaliers

Insolite

Kangourou
Tout sur le slip kangourou

Jacky
The Jacky touch, le top des décorations ridicules pour les voitures.
Voir aussi le guide du parfait Nanard

Peter Plante
L'histoire extraordinaire de Peter Plante

Cafard Warez
Il y a plein de cafards sur ce site et c'est vraiment insupportable

Bruler la paillotte
Enfile vite ta cagoule pour mettre le feu à la paillotte !
Attention, la mission est très difficile, alors pas de dérapage !

Politique

Abracadabrantesque !
Coupable mais intouchable !

Elysee.org
Site officieux de la Présidence de la République Française. (Site officiel : elysee.fr)

Ministère de l'injustice

Parodies de chansons

www.parodyland.net
Le site référence sur les parodies de chansons

Parodies Choum
Toutes les parodies de Choum.

Parodies Cauet
Toutes les parodies de Cauet

Parodies de film

Les guignols
Parodies de film

Nuit de l'invasion des nains de jardin
Le film, les animations et les photos du tournage

Canular

hacking : Une fausse carte bancaire pour les nulles

Tintin est vivant
Parodies et fausses BD de Tintin

HoaxBuster
Enquêtes sur la désinformation et les canulars sur le Web

Parodie de parodie !

Parodie.com (Laurent Pelé)

- Hélas, le site a changé de main, quelle confiance dans la parodie ?
- Il y a un site merveilleux, archive.org qui nous permet de revenir dans le passé d'internet (wayback) …
- Explorez !

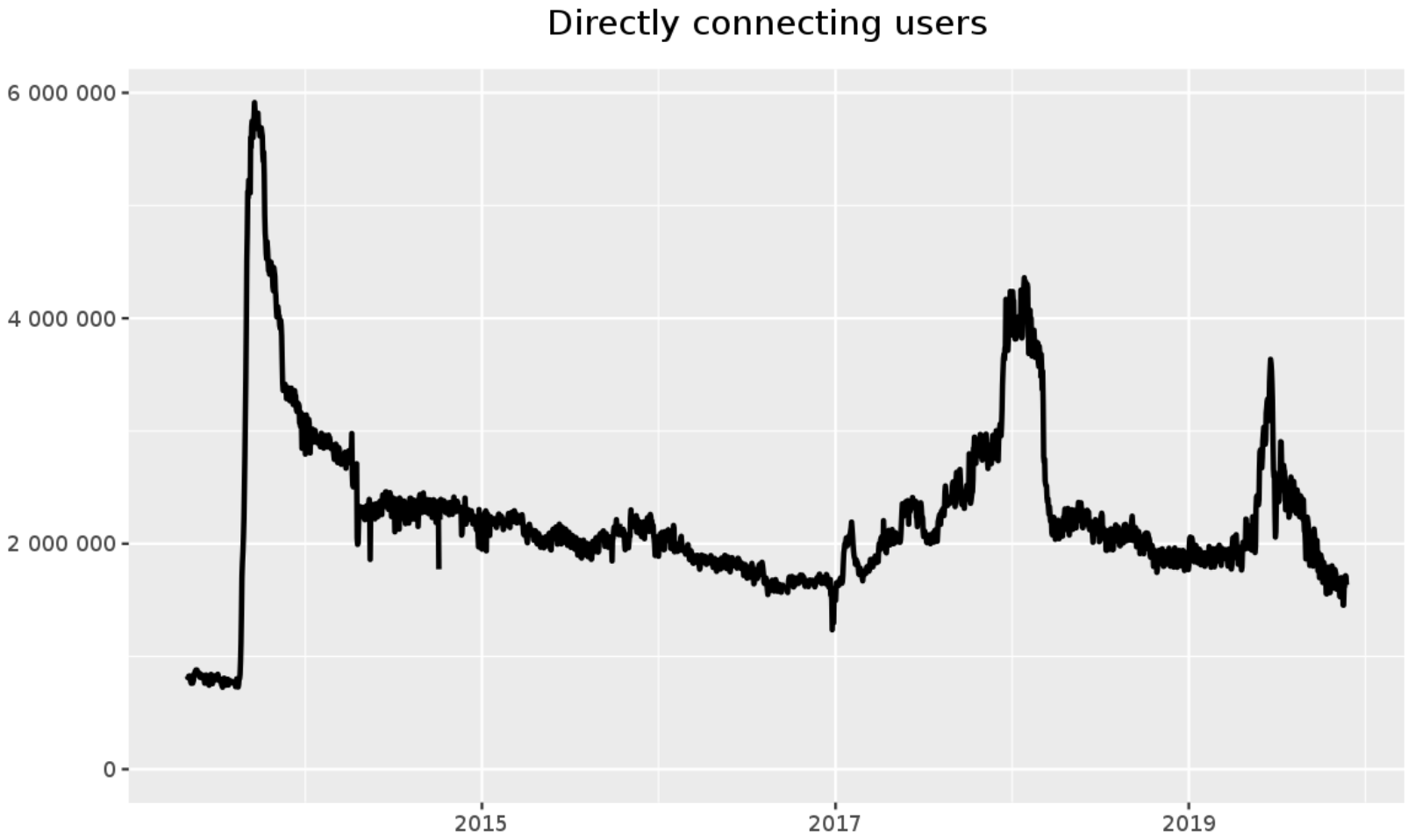
Commentaires

- D’autres personnes ont aussi factorisé les fameuses clés,
- Le Gie Cartes Bancaires n’a pas voulu écouter,
- Louis Guillou et moi-même avions dit très tôt et avec insistance que les clés RSA étaient bien trop courtes,

Edward Snowden (5 juin 2013)

- Révélations de documents internes à la NSA,
- Pas la seule fuite,
- Loin d'avoir tout publié, sans doute environ 2 % des documents,
- Les journalistes en charge (de moins en moins nombreux) filtrent les documents pour éviter de mettre en danger des personnes, y compris eux-mêmes.

Tor : effet Snowden
de 1 à 6 millions d’utilisateurs journaliers



The Tor Project - https://metrics.torproject.org/

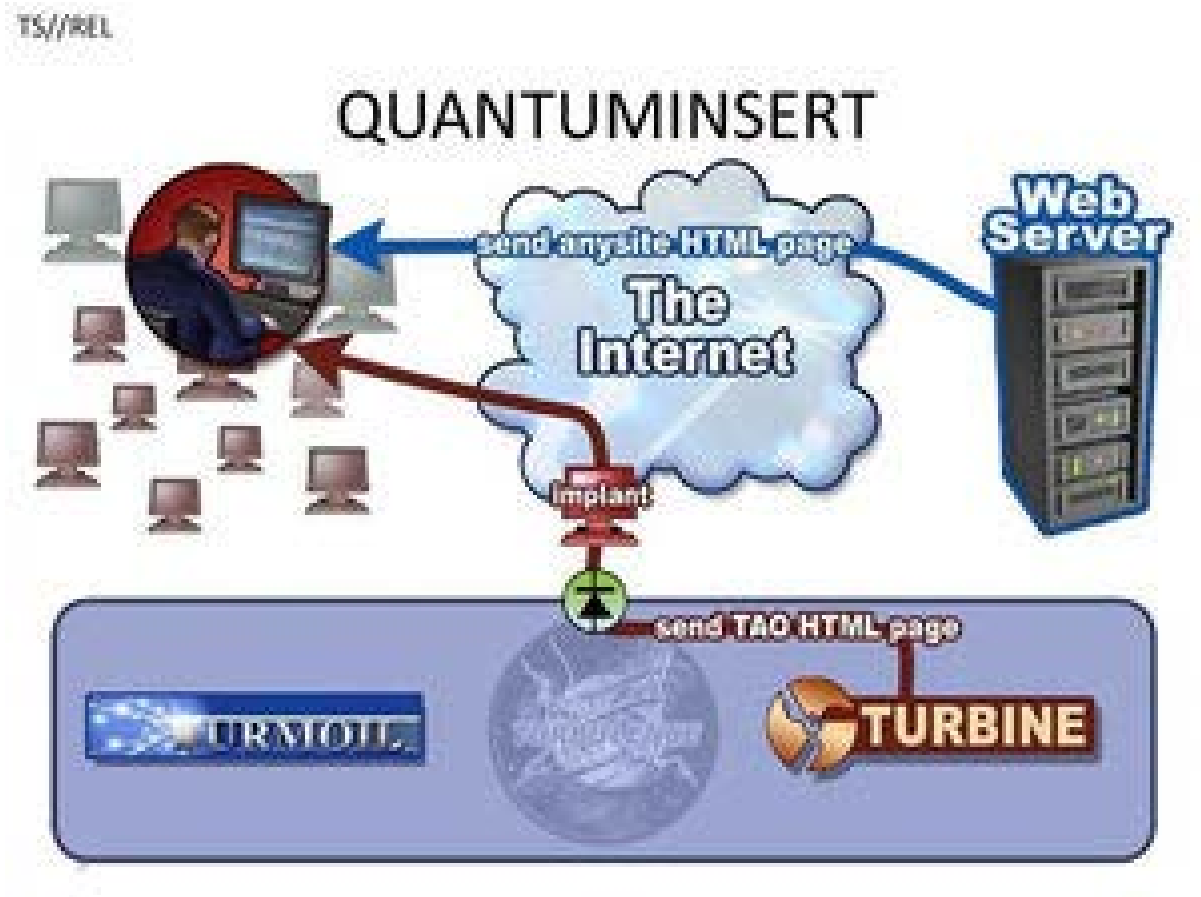
Attaque de Belgacom – 15 septembre 2013

- Suite à une fuite, l'information sur l'attaque passe dans la presse,
- Oui, ce sont la NSA via le GCHQ,
- L'attaque dure depuis au moins deux ans,
- Pourquoi ? Grand réseau mondial, surtout roaming (alors le 5^{e}),
- On fouille dans les fichiers de Snowden et on y découvre une description minute par minute de l'attaque (ce n'est pas la seule : voir aussi Gemplus),
- Rupture de confiance en Belgique avec des Alliés.

Attaque JJQ (2014)

- Semble avoir été effectuée le 15 septembre 2013,
- Je suis averti en novembre,
- Découverte par l'OTAN,
- Relié à Belgacom (pourquoi ?),
- Utilise Quantum Insert et linkedin (comme pour Begacom),

Quantum insert



Entreprises & Start-up

Le génie belge du cryptage espionné par la NSA

Belga

Publié le samedi 01 février 2014 à 07h30 - Mis à jour le lundi 03 février 2014 à 23h35

Le Belge Jean-Jacques Quisquater, professeur à l'UCL et expert internationalement reconnu de la protection des

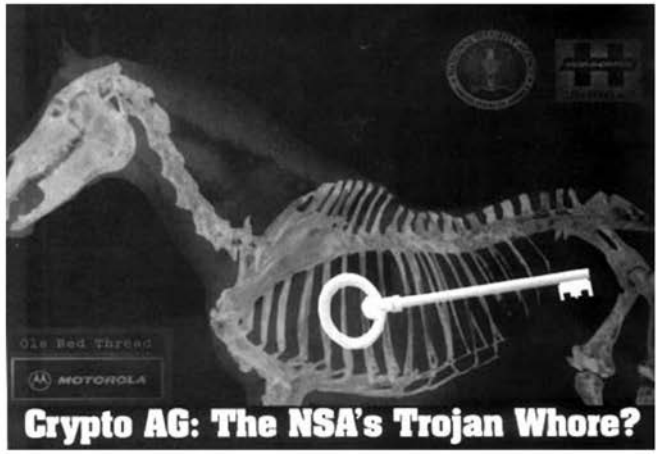
Backdoors

- Utilisé par l’espionnage depuis longtemps (voir CRYPTO AG),
- Plus récemment générateur d’aléas basé sur les courbes elliptiques,

CRYPTO AG (mars 1992) – accord avec la NSA

MediaFilter.org

CAQ CovertAction Quarterly



by Wayne Madsen

FOR AT LEAST HALF A CENTURY, THE US HAS BEEN INTERCEPTING AND DECRYPTING THE TOP SECRET DOCUMENTS OF MOST OF THE WORLD'S GOVERNMENTS

It may be the greatest intelligence scam of the century: For decades, the US has routinely

(NSA) and Crypto AG, they might as well have been hand delivering the message to

Et maintenant … ?

- Débats,
- Huawei ?
- APT (malware ciblé),
- Internet ?
- GAFAMI ?
- Chine ?
- Etc, …