Le contrôle des technologies de l'information: un bien ou un mal ?

Etat des lieux, enjeux et perspectives

Eric Filiol
ESIEA
efiliol@netc.fr

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

Introduction

Introduction : le contexte

- L'impact des révélations de Snowden
- L'ancien modèle de nos sociétés (vertical, hiérarchisé…) versus le nouveau modèle de société en émergence (horizontal, collaboratif, individualiste…)
- L'espionnage des citoyens par leur propre Etat (ex. bonnets rouges) trahit la faiblesse et la peur de ces Etats.
- TTIP, CETA et ISDS : le pouvoir futur est aux entités privées (rapport CIA à 30 ans)

Questions clefs

- **Quelles sont la nature et les évolutions actuelles du contrôle des technologies de l'information ?**
- **Est-ce un bien ou un mal ?**
- **Que nous réserve l'avenir ?**
- **La cryptologie est LA dimension critique**
  - Qui contrôle la cryptologie contrôle tout le reste

Le contrôle de la technologie

Histoire et état des lieux

Bloomberg News Quick Markets Personal Finance Tech U.S. Politics Sustainability Luxury Vide

Microsoft Bugs

In addition to private communications, information about equipment specifications and... **Read More**

Microsoft Corp. (MSFT), the world's largest software company, provides intelligence agencies with information about bugs in its popular software before it publicly releases a fix, according to two people familiar with the process. That information can be used to protect government computers and to access the computers of terrorists or military foes.

Redmond, Washington-based Microsoft and other software or Internet security companies have been aware that this type of early alert allowed the U.S. to exploit vulnerabilities in software sold to foreign governments, according to two U.S. officials. Microsoft doesn't ask and can't be told how the government uses such tip-offs, said the officials, who asked not to be identified because the matter is confidential.

Frank Shaw, a spokesman for Microsoft, said those releases occur in cooperation with multiple agencies and are designed to give government "an early start" on risk assessment and mitigation.

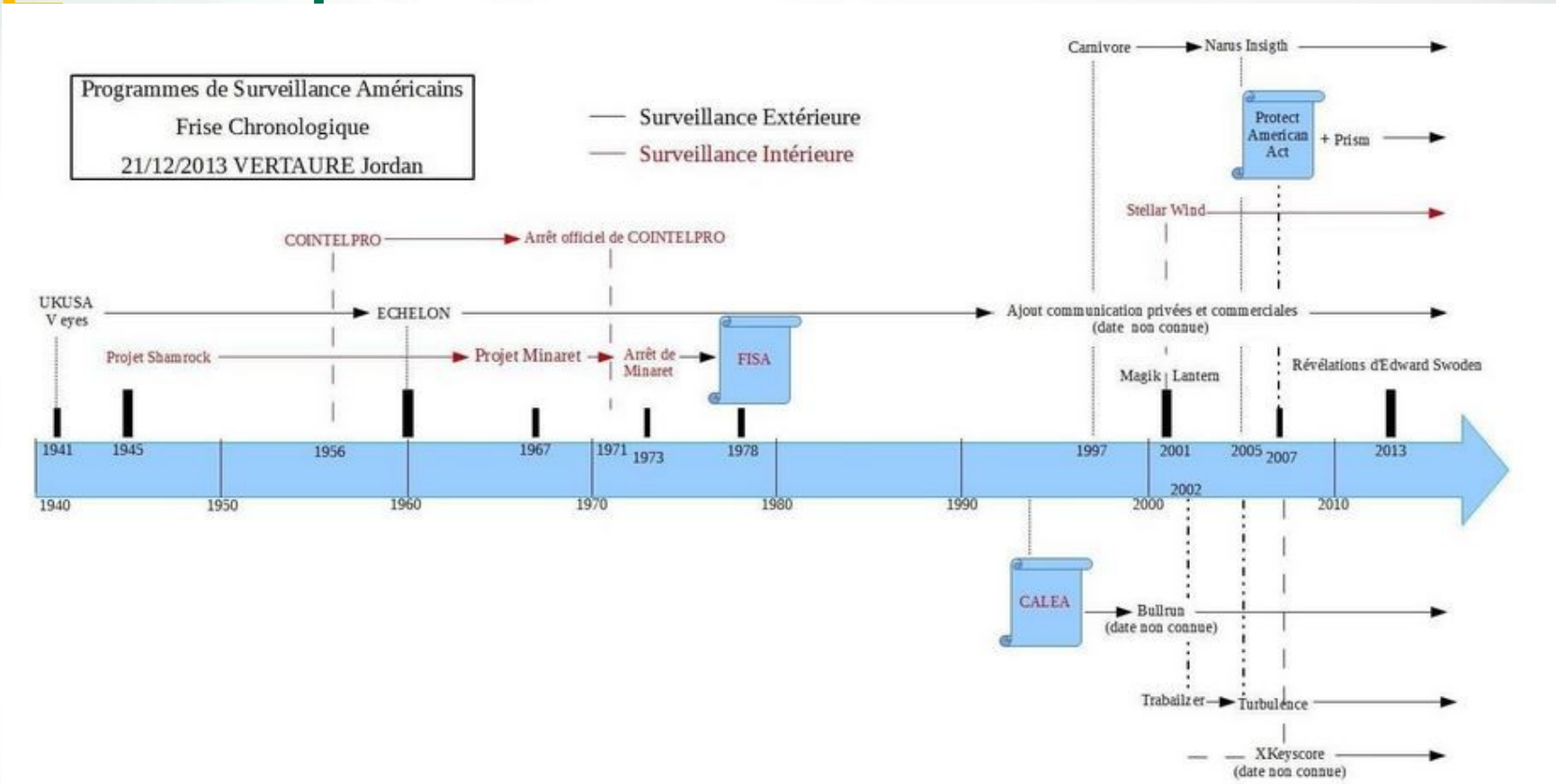
In an e-mailed statement, Shaw said there are "several programs" through which such information is passed to the government, and named two which are public, run by Microsoft and for defensive purposes.

Photographer: Scott Eells/Bloomberg

Microsoft Corp., the world's largest software

Heartbleed appears to be one of the biggest flaws in the Internet's history, affecting the basic security of as many as two-thirds of the world's websites. Its discovery and the creation of a fix by researchers five days ago prompted consumers to change their passwords, the Canadian government to suspend electronic tax filing and computer companies including **Cisco Systems Inc.** to Juniper Networks Inc.

Quelques faits



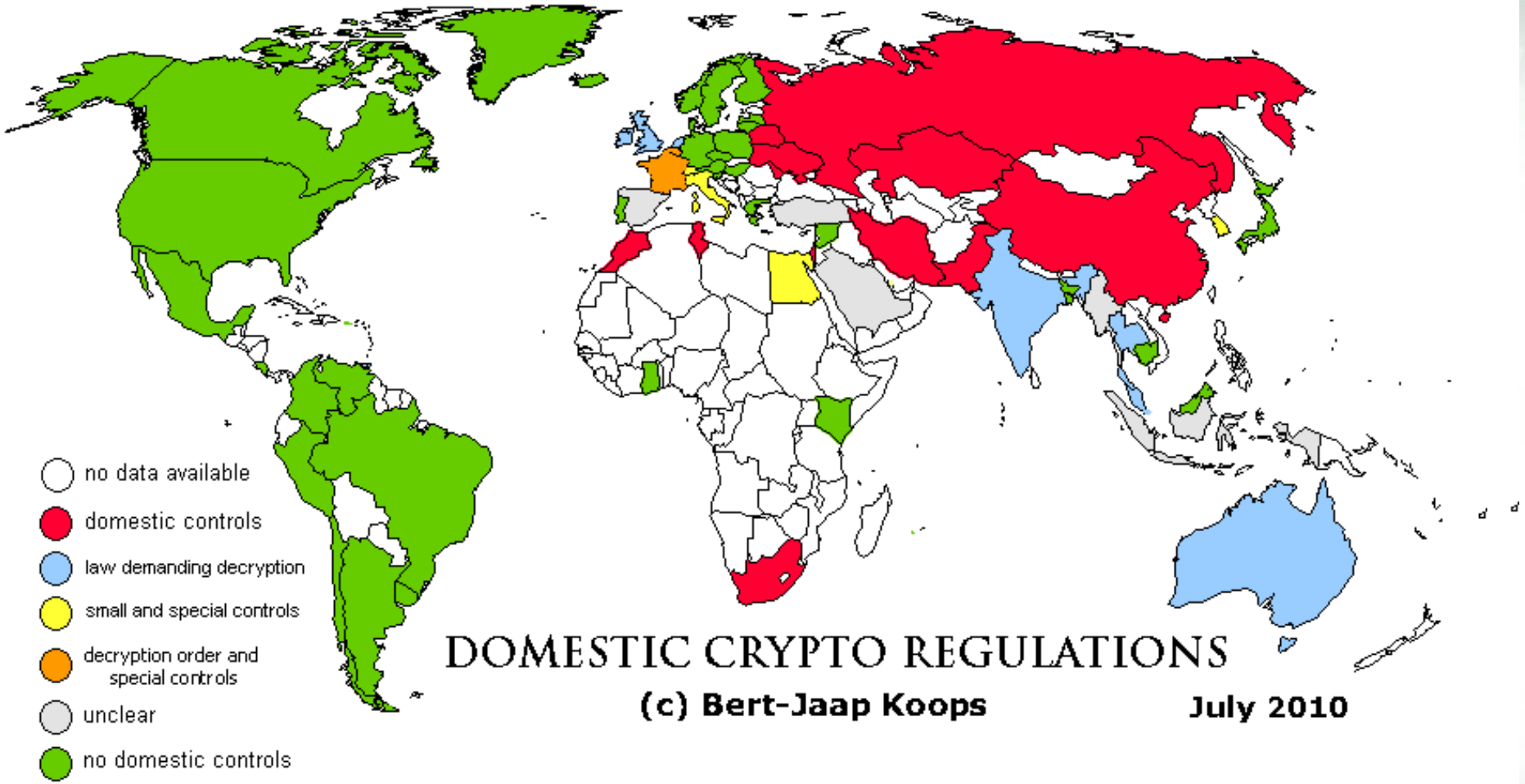
70 ans de contrôle

- **Depuis la fin de WWII, la cryptologie est sous contrôle. Ce contrôle se renforce mais de diverses manières**
- **UKUSA (5 eyes)/9 eyes/14 eyes – SIGINT Seniors Europe…**
- ***International Traffic in Arms regulations* (ITAR, part 121) et lois suivantes (Wassenaar I & II…)**
  - Une cryptologie « libre » signifie une cryptologie sous contrôle.
  - Année clef : 1997 (la cryptologie sort de l'ITAR)
  - Débuts 2000 : le monde devient connecté. Le contrôle devient plus facile et multi-niveaux (ordinateurs, OS, réseaux…)

Cinq phases de contrôle

- **Préhistoire (1945 – 1975) : CoCom, ITAR**
- **Phase de mutation (1975 – 2001): Wassenaar, contrôle du monde académique…**
- **Phase de globalisation (2001 – 2012) : *Patriot Act*, WTO, ISO…**
- **Phase légale (2010 - …): brevets, licences, standards, PIPA, ACTA, TTIP, CETA, ISDS…**
- **Phase d'assimilation culturelle (maintenant): cibler la jeunesse par le consumérisme (TV, marketing, produits US…). Le but est que la prochaine génération aime/pense US.**

Le contrôle de la cryptologie



- ht
- 42
- La
- Pr
- L'a
- La
- M

reflets.info

Technos Politique France Economie Monde Sagas Entretiens Photos On s'en fou

Par bluetouff 10 janvier 2014 2 Commentaires

La vente de 0day rentre dans l'arrangement de Wassenaar

Le commerce de l'exploitation des vulnérabilités informatiques fait officiellement son entrée dans l'arrangement de Wassenaar. Cet accord relatif aux ventes d'armes et aux outils à usage dual règlemente le commerce international de certains produits. Une quarantaine d'états, dont la France, l'Italie ou le Royaume-Unis, 3 états en pointe dans le commerce des vulnérabilités informatiques à destination des forces de police, des armées, ou des services de renseignement sont donc maintenant soumis à un contrôle plus strict à l'export... il était temps.

Ces outils tombent malheureusement souvent dans les mains de régimes dont les aspirations démocratiques sont relativement limitées. On se souvient de FinFisher au Bahreïn : la suite offensive de Gamma International était notamment utilisée à l'encontre d'opposants politiques, comme l'avouait un document officiel des services de renseignements locaux. Gamma avait alors argué que le Bahrein avait utilisé une version « de test » de sa suite.

Avec les outils de surveillance d'Internet qui permettent aujourd'hui de capturer d'énormes flux de données et de contrôler, altérer, modifier ou interdire l'accès à l'information, les outils d'intrusion à distance sont maintenant considérés comme des armes à part entières.

Exportation et transfert de moyens de cryptologie depuis la France

Moyen de cryptologie (la catégorie signalée fait référence aux annexes du décret n° 2007-663)	**TRANSFERT VERS UN ÉTAT MEMBRE DE LA COMMUNAUTÉ EUROPÉENNE**	**EXPORTATION VERS SEPT ÉTATS IDENTIFIÉS (1)**	**EXPORTATION VERS D'AUTRES ÉTATS**
- assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité - de type : cartes à puce (carte bancaire, gsm, décodeur tv...), récepteurs de télévision ou de radiodiffusion, protection contre la duplication, lecteurs dvd... (catégories 1 à 7 de l'annexe 1)	LIBRE		

CATEGORIE : 13
Moyens de cryptologie ne mettant en oeuvre aucun algorithme cryptographique présentant l'une des caractéristiques suivantes :
a) un algorithme cryptographique symétrique employant une clé de longueur supérieure à 56 bits ;
b) un algorithme cryptographique asymétrique fondé soit sur la factorisation d'entiers de taille supérieure à 512 bits, soit sur le calcul de logarithme discret dans un groupe multiplicatif d'un corps fini de taille supérieure à 512 bits ou dans un autre type de groupe de taille supérieure à 112 bits.

- employant des clés cryptographiques de grande taille (catégorie 1 de l'annexe 2)	DECLARATION	DECLARATION [Licence générale communautaire]	AUTORISATION [Licence individuelle ou globale]
- permettant la cryptanalyse	AUTORISATION [Licence individuelle ou globale]		

(1) Australie, Canada, États-Unis d'Amérique, Japon, Nouvelle-Zélande, Norvège et Suisse

Second niveau de contrôle

- USA versus le reste du monde
- « *La puissance d'un pays réside dans sa capacité à imposer des normes* »

  Bernard Carayon
- Hégémonie des standards cryptologiques US (e.g. Linky)!
- Le but est de contrôler les normes et standards (ISO) et de standardiser les esprits

Troisième niveau de contrôle

- Utiliser le monde académique comme caution scientifique et comme écran de fumée
  - Complexité/combinatoire rendent toute avancée opérationnelle impossible de nos jours
  - Ce qui est « académiquement » cassé ne l'est pas d'un point de vue opérationnel
  - Promotion de orthodoxie scientifique
- Les algorithmes sont choisis par le binôme {Etats, industriels} en réalité.
- Contrôle de la communauté académique
  - Par les comités de programmes (sujets à la mode) et l'effet « *publier ou périr* »
  - Par le financement (NSF, FP7, NSA...)

Les différentes approches techniques

Type	Data	NSA Programs	Techniques	Examples
Connected	Plaintext	PRISM, Xkeyscore…	Data collection, wiretapping, eavesdropping, agreements with industry/providers….	Google, Facebook, Apple, Microsoft (including Skype)…
	Ciphertext	Bullrun/Edgehill…	Malware, 0-day exploitation, random generator control, security standards control, controlling CAs, bugging software, applied cryptanalysis…	Heartbleed, RSA, Google/ANSSI, Mail.ru, Alibaba…
Connected by private network	Ciphertext	Cottonmouth, Godsurge, TOR attack, Quantum, Foxacid, Firework, Bulldozer…	Malware, 0-day exploitation, random generator control, controlling CAs, security standards control, bugging software, hardware bugs, mathematical trapdoors…	TOR network, Gasprom, Petrobras, French MFA, Aeroflot, Total. Airbus, SWIFT…
Non-connected (offline)	Ciphertext	TAO, still unknown projects???	Tempest techniques, mathematical backdoors, hardware bugging, Humint	Hans Buehler Case (1995). Gov, MIL, Sensitive companies

Le contrôle est nécessaire

Top 10 Facts About Modern Slavery

FREE THE SLAVES

- Slavery: forced to work without pay under threat of violence and unable to walk away.
- 27 million slaves in the world today.
- Slavery is not legal anywhere but happens everywhere.
- The majority of slaves can be found in India and in African countries.
- At least 14,500 slaves are trafficked into the US each year.
- Slaves work in fields, brothels, homes, mines, restaurants -- anywhere slave owners can feed their greed.
- Human trafficking is the modern-day slave trade.
- $90 is the average cost of a human slave around the world.
- Slave owners use many terms to avoid the word slavery: debt bondage, bonded labor, attached labor, restavec, forced labor, indentured servitude, and human trafficking.
- It is possible to end slavery in 25 years. Everyone has a role to play - government, business, international organizations, consumers, YOU.

www.freetheslaves.net

Photo d'illustration. © Gaetan Bally / Keystone / Maxppp

Home > Docket USC-RULES-CR-2014-0004

Proposed Amendments to the Federal Rules of Criminal Procedure

Docket ID: USC-RULES-CR-2014-0004

ABSTRACT:

The Judicial Conference Advisory Committee on Criminal Rules has proposed amendments to the Federal Rules of Criminal Procedure and requested that the proposals be circulated to the bench, bar, and public for comment. On August 15, 2014, the public comment period opens for the proposed amendments to Criminal Rules 4, 41, and 45. The public comment period closes on February 17, 2015.

RIN: Not Assigned

Type: Rule Making

PRIMARY DOCUMENTS

VIEW ALL (2)

PUBLIC HEARINGS OF THE JUDICIAL CONFERENCE ADVISORY COMMITTEES ON...

Notice | Posted: 08/15/2014 | ID: USC-RULES-CR-2014-0004-0002

PRELIMINARY DRAFT OF PROPOSED AMENDMENTS TO THE FEDERAL RULES OF ...

Proposed Rule | Posted: 08/14/2014 | ID: USC-RULES-CR-2014-0004-0001

Les dangers & dérives d'un contrôle

Qui contrôle les « contrôleurs » ?

← Italian Researchers Find Women And Men Drastically Differ In Symptoms For Heart Attacks, Cancer, and Liver Disease

Dr. Jeff Pettis, USDA Scientist, Says Bee Apocalypse Is 'One Poor Weather event or High Winter Bee Loss' Away →

Is This The Early Signs of Fascism? : NSA, CIA, & FBI Have Secret Agreements With Microsoft, McAfee, and Other Tech Companies For 'National Security'

JUN 16 Posted by Emergingtruth

http://www.dailymail.co.uk/news/article-2341758/U-S-security-agencies-swap-data-thousands-tech-finance-manufacturing-firms-secret-agreements.html

U.S. security agencies 'swap data with thousands of tech, finance and manufacturing firms under secret agreements'

- U.S intelligence organizations including the NSA, CIA and FBI 'have secret agreements with companies including Microsoft and McAfee'
- Companies 'believe they are helping to protect the nation'
- In return for their help, 'firms are lavished with gratitude and attention'

By Lydia Warren

PUBLISHED: 11:09 EST, 14 June 2013 | **UPDATED:** 12:44 EST, 14 June 2013

Thousands of tech, finance, and manufacturing companies have secret agreements with U.S. security agencies to swap sensitive data in return for classified intelligence, sources have

GO

RECENT POSTS

- Are We Close to The Collapse of The U.S. Dollar and A New World Reserve Currency?
- Has Morsi and The Muslim Brotherhood Done More Harm Than Good In Egypt? In the Last Three Days, Over 700 People Have Died In Violent Riots In Cairo
- Innocent 10 Year-Old Christian Girl In Egypt Was Shot Dead On Her Way Home From Bible Study Class
- Video: 666 In Ancient Religions - Part 1 Truth about God, Devil, Symbols, etc.
- Pew Research Study Reveals Not All Americans Support Anti-Aging and Life-Extending Medical Treatments
- Researchers Say New Mothers In Urban Areas Are More Likely To Develop Postnatal Depression Than New Mothers Who Live In Rural Areas
- IBM Reveals Cutting-Edge New Computer Chip Architecture That Will Allow Future PCs To Work Like The Human Brain
- Iran's New President Says "U.S. is looking for excuse" to Confront Iran Over Their Nuclear Program
- NASA Warning: Sun's Magnetic Field Is about to Flip in 3-4 Months, Which Will "Have Ripple effects Throughout the Solar System"
- Survey Conducted By The Iraq Afghanistan Veterans of America (IAVA) Reveals 45% of Veterans Know a Soldier Who Has Tried To Commit Suicide

01/05/2012 à 18:36

Browse Privacy Topics

Privacy Rights Clearinghouse Releases Study:

Vie privée

- Numérama, le 17/05/2014 : Et maintenant Google lit vos factures

Fermeture

- CNIL, le 03/01/2014 : Exemple de sanction de la CNIL à l'encontre de Google
- 01Net, le 23/11/2012 : Sécurité : le cloud est plus dangereux que les virus
- CNIL, le 25/06/2012 : Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing
- INRIA, le 13/12/2013 : Quand les terminaux mobiles jouent les mouchards de poche
- INAGlobal, le 04/02/2014 : Facebook, n'en fais pas une affaire de données personnelles!
- Rue89, le 03/02/2013 : A qui appartiennent vos données sur Internet ? Mauvaises nouvelles et conseils
- Atlantico, le 16/06/2014 : Quelle cible publicitaire êtes-vous?
- Nextinpact, le 22/07/2009 : Des ouvrages d'Orwell supprimés du Kindle par Amazon
- Rue89, le 18/11/2013 : Google, Facebook, Apple... : ces superpuissances ont privatisé Internet
- Liberation.fr, le 07/03/2014 : La fin du porno sur Vine, un espace de liberté en moins
- Liberation.fr, le 14/03/2014 : Apple censure un roman français pour cause de seins nus
- Rue89, le 29/05/2014 : Chantage : Google, Apple et Amazon, les tontons écrabouilleurs
- Numerama, le 09/08/2014 : Quand Facebook est en panne, le trafic des sites baisse
- NextInpact, le 22/08/2014 : Quand Twitter déraille avec la timeline de ses utilisateurs

- LDN, le 17/04/2014 : Je n'ai rien à cacher
- Numerama, le 26/09/2014 : Même si vous dites rien, Facebook sait où vous passez votre lune de miel
- Journal du Net, le 16/07/14 : Soyons honnêtes, la quantité d'informations que Google rassemble à notre sujet est effrayante

Je viens de voir que

peuvent être trouvé

t serveurs touchés,

PRC Privacy Rights CLEARINGHOUSE

- Nearly three-fourths, or 72%, of the apps we assessed presented medium (32%) to high (40%) risk regarding personal privacy.
- The apps which presented the lowest privacy risk to users were paid apps. This is primarily due to the fact that they don't rely solely on advertising to make money, which means the data is less likely to be available to other parties.

Le

- Le est
  que
  « Qu *du*
  plus *ire*

Perspectives

Voyage prospectif dans le futur

Quid de l'avenir ?

- **La captation va devenir généralisée (internet des objets, mobilité)**
- **L'inertie globale des citoyens va faciliter cette évolution**
  - Les révélations de Snowden n'ont pas fondamentalement changé grand chose
  - Finalement tout le monde y trouve son intérêt… à part quelques (h)ac(k)tivistes
  - Allons-nous nous vers un monde de moutons/veaux connectés ?

Quid de l'avenir ?

- **Toutefois l'Histoire est par nature non linéaire**
  - Or cette évolution repose sur une vision linéaire (sans perturbations)
  - Exemple : deux séismes majeurs en 2014 (Heartbleed et Shellschock)
  - Beaucoup de technologies IT font reposer leur sécurité sur des principes non éprouvés (RSA, ECC [2014]…)
- **Nous pouvons aussi aller vers un monde beaucoup plus chaotique et incertain**

Conclusion

Quelques points clefs

Conclusion

- **La dimension majeure n'est pas technique mais économique/politique**
  - La force des Etats dominants (USA, Chine) réside dans leur monopole sur la technologie (Huawei, Cisco, Intel, Microsoft…), les services (Facebook, Google, FedEx…) et leur place dominante dans le business (le marché IT US représente près de 45 % du marche IT mondial).
  - Le véritable pouvoir réside dans le commerce et la volonté politique.

Conclusion

- **Le poids des standards (ISO, ANSI, IEEE…) est fondamental**
- **L'Europe doit peser plus sur les processus de standardisation voire faire émerger de nouveaux standards/organisations de standardisation.**
- **Elle doit donner naissance à un nouveau marché mondial structuré (Europe + Fédération de Russie ?)**
- **Avenir : certification du respect de la vie privée et de la confidentialité des données**
  - Il y a une formidable opportunité pour le marché de la confiance

INSPIRING A SAFE AND SECURE CYBER WORLD.

Questions & réponses
Merci de votre attention