



Jean-Nicolas Piotrowski
Fondateur et Président ITrust

Ancien responsable sécurité de la salle des marchés de la BNP
Intervenant expert sécurité cloud sécurité à l'Assemblée nationale
Pilote du thinkTank PRISSM

Twit : jcopiotro

75 %

8 sur 10

Possédaient les basiques de la sécurité
Firewall, Antivirus, Backup...

90 %

Ne savaient pas qu'elles étaient attaquées (Itrust)

100 %

des réseaux analysés contiennent des
malwares (Cisco)

Une entreprise perd en moyenne **4,5%** de ses clients
lorsqu'il est découvert qu'un incident a touché l'intégrité de
ses données (IBM)

15 millions de cartes blues volées

Recent Hacking Incidents around the

CREDIT CARDS & CUSTOMER INFO

HACKED

TARGET 40 million
customer accounts hacked

27
NOV 2013

USA

15
DEC 2013



USINE DIGITALE > AÉRONAUTIQUE - DÉFENSE

Airbus Helicopters victime d'une cyberattaque qui proviendrait des Etats-Unis

Par Julien Bonnet - Publié le 13 novembre 2014, à 16h25

► [Aéronautique - Défense](#), [Aéronautique](#), [Airbus Group](#), [Airbus Helicopters](#), [Cybersécurité](#),



Le Caracal d'Airbus Helicopters en lice dans un appel d'offres en Pologne. © jfhweb - Flickr - C.C

D'après LaTribune.fr, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a ouvert une enquête pour savoir si Airbus Helicopters a été victime d'un piratage informatique qui pourrait être lié à un important appel d'offres en Pologne. Le journal en ligne, qui cite des sources concordantes, indique que le constructeur "nourrit 'de fortes suspicions' vis-à-vis des Etats-Unis". Les entreprises américaines Sikorsky et Boeing sont actuellement engagées en Pologne dans une véritable bataille commerciale avec le constructeur européen.

Malgré les retombées de l'affaire Snowden, les Etats-Unis continueraient de pratiquer l'espionnage de leurs alliés. C'est en tout cas ce que laisse entendre cette information révélée par le site de La Tribune : l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a ouvert une enquête pour savoir si Airbus Helicopters a été victime de piratage informatique. Il pourrait être lié à un important appel d'offres en Pologne. Et d'après le journal en ligne, qui cite des sources concordantes, le constructeur "nourrit 'de fortes suspicions' vis-à-vis des Etats-Unis".

"LES ATTAQUES SONT FRÉQUENTES DANS NOTRE SECTEUR"

Interrogée par l'AFP, l'Anssi s'est refusée à confirmer l'ouverture d'une enquête "pour ne pas stigmatiser les victimes". "L'Anssi accompagne les acteurs publics et privés en phase préventive ou en cas d'attaque", a simplement déclaré une porte-parole à l'agence de presse.

NSA Details Chinese Cyber Theft of F-35, Military Secrets

Chinese hackers pillaged U.S. defense, contractor networks for critical data



F-35 / AP



BY: **Bill Gertz** Follow @BillGertz

January 22, 2015 3:55 pm



China obtained more than 50 terabytes of data from U.S. defense and government networks, notably the Joint Strike Fighter's stealth radar and engine secrets, through cyber espionage, according to newly disclosed National Security Agency documents.

A NSA briefing **slide** labeled "Top Secret" and headlined "Chinese Exfiltrate Sensitive Military Data," states that the Chinese have stolen a massive amount of data from U.S.

government and private contractors.

The document was made public by the German magazine *Der Spiegel* in a two articles detailing how NSA in the mid-2000s was capable of conducting global cyber intelligence-gathering by tapping into the networks of foreign intelligence services and stealing the data they were collecting from others.

The unique capability of spying on the spies was described in a series of documents that were stolen in 2013 by former NSA contractor Edward Snowden, currently a fugitive in Russia.

Faire sauter la banque

Publié le : Lundi 16 Février 2015 - 15:06

Dernière mise à jour : Mardi 17 Février 2015 - 12:13

Banques: près de 1 milliard de dollars volés par des pirates informatiques

Une bande de cybercriminels russes, ukrainiens et chinois ont trouvé le moyen de pirater des centaines d'établissements bancaires en infiltrant les réseaux de ces derniers. Montant du butin de ces attaques débutées en 2013 et toujours en cours: jusqu'à un milliard d'euros.



Piratage de Sony : démission de la coprésidente Amy Pascal

Emportée par le piratage de Sony Pictures et la publication d'emails à caractère raciste, la patronne du groupe a annoncé sa démission.



La patronne de Sony Pictures, Amy Pascal, lors de l'avant-première de "L'interview qui tue !". © Frazer Harrison / Getty Images North America/AFP

[Home / USA /](#)

Texas college hacks drone in front of DHS

Published time: June 27, 2012 18:30

Edited time: June 28, 2012 22:38

[Get short URL](#)

US Navy handout photo of a RQ-4 Global Hawk drone (REUTERS/U.S. Navy)



622



43



There are a lot of cool things you can do with \$1,000, but scientists at an Austin, Texas college have come across one that is often overlooked: for less than a grand, how'd you like to hijack a drone?

Tags
[Planes](#), [USA](#)

Cambriolage, espionnage et contrefaçon : le « polar noir » de Cuir, PME carvinoise

PUBLIÉ LE 23/07/2011 À 05H13

Fabriquante de machines à imprimer et à découper le carton ondulé, Cuir CCM subit depuis quelques années des cambriolages en rafale. Et elle poursuit d'autres sociétés pour piratage de son outil de production et concurrence déloyale. La justice lui a donné raison mais les procédures ne sont pas terminées.



| - A + | 

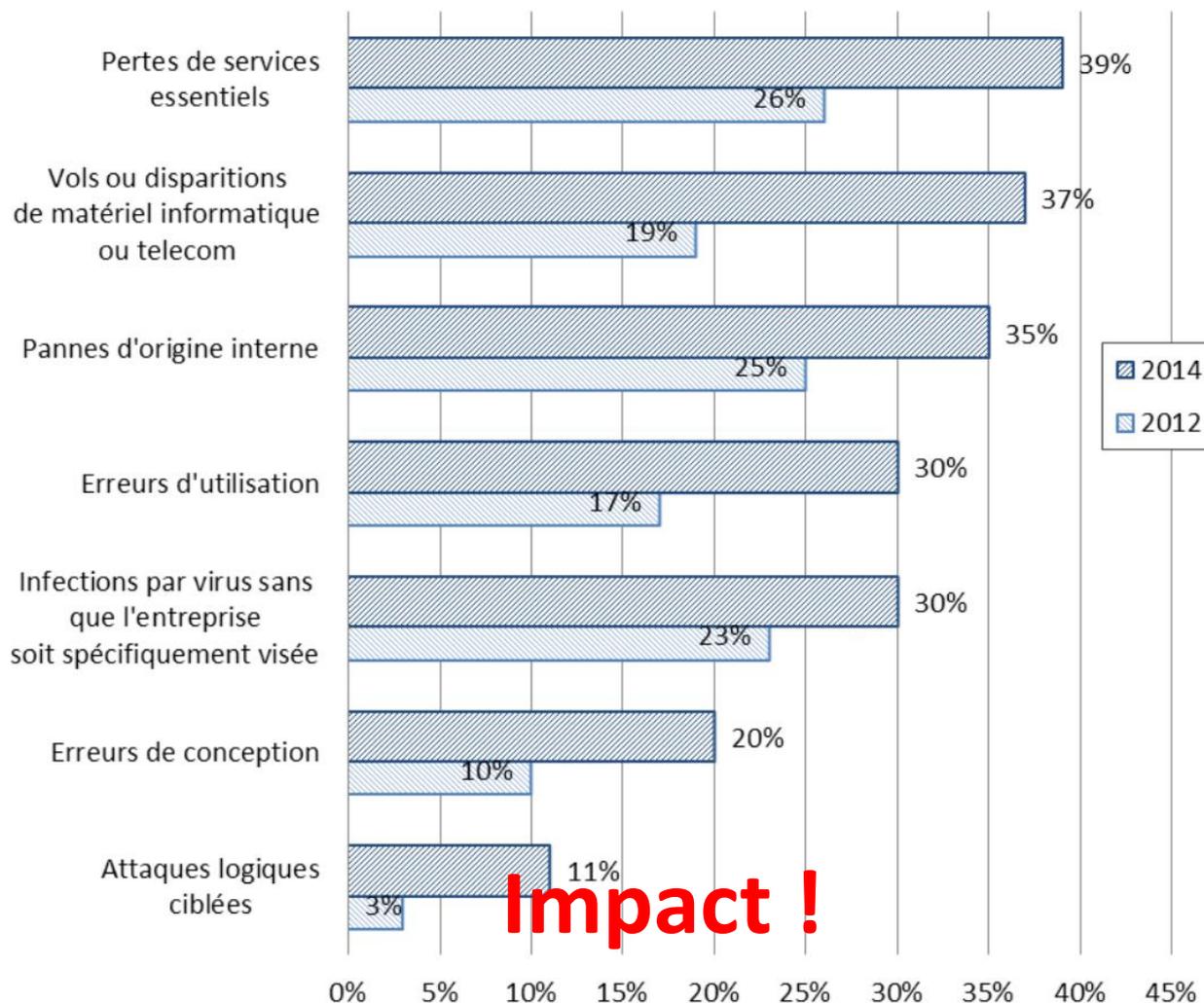
PAR CHRISTOPHE LE COUTEUX

henin@info-artois.fr



On oserait un mauvais jeu de mots, on dirait qu'il vaut mieux avoir le cuir épais pour travailler dans cette PME carvinoise. Le 5 juin au midi, le vigile d'une société privée passe pour la deuxième fois de la journée. En l'espace de trois heures, des vandales ont eu le

Au cours de l'année passée, votre entreprise a-t-elle subi des incidents de sécurité de l'information consécutifs à...



Incidents 2014 (Clusif)

Figure 36 : Typologie des principaux incidents de sécurité

- 4 interventions sur des attaques inconnues
- 20 entreprises de l'aéro-space piratées en 2014
- 90% taux de réussite sur les audits externes (!!)
- 5 interventions forensiques en urgence sur des malversations humaines internes
- Les problèmes ne sont JAMAIS ébruités
- Tous types d'entreprise : de la TPE au Cac40
- 4 Cas de virus inconnus et indétectés
(Statistiques ITrust sur les 2 dernières années)

1

PROFESSIONNALISME du PIRATAGE

- LES ATTAQUES SONT DÉSORMAIS CIBLÉES
- > LES OUTILS DE PROTECTION actuels SONT OBSOLÈTES
- > TROP DE BRUIT pour IDENTIFIER une malveillance

2

L'ENTREPRISE est ETENDUE

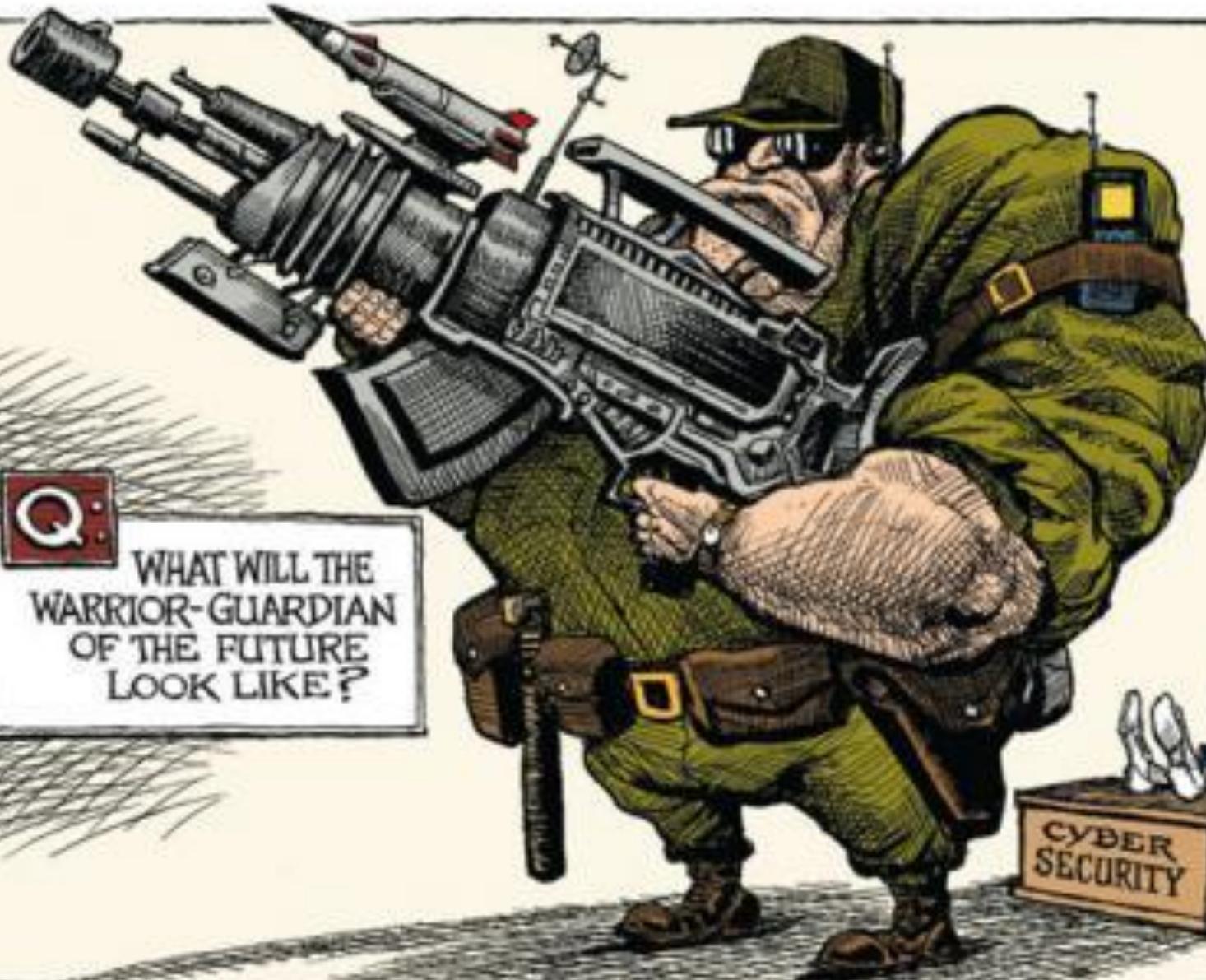
Cloud, BYOD, NOMADISME, « EXTRANET », données Privées/Professionnelles





“The next Pearl Harbor we confront could very well be a **cyber attack**”

US Secretary of Defense and former CIA Director Leon Panetta, at a Senate hearing in August 2011



YO! DUDE.
BACK
HERE



WHAT WILL THE
WARRIOR-GUARDIAN
OF THE FUTURE
LOOK LIKE?

CYBER
SECURITY

- **Extraction de données** (Phishing et APT)
- **Attaques sur les infrastructures et applications**
- **Bombe logique / Malware** (sur mobile ou embarqué)
- **Ransomware**
- **Malveillance interne**
- **Attaque sur systèmes embarqués et MtoM**
- **Arnaque aux transferts financiers**
- **Erreurs de sauvegardes et de MCO** (disponibilité des services)
- **Deni de service**

**Hors, des solutions simples
existent ...**

40 **principes** essentiels permettent d'augmenter à **99 %**
le niveau de protection

10 failles techniques essentielles représentent 99% des
vecteurs d'attaques et malveillance

La bonne application d'une Politique de sécurité
réduit l'exposition aux risques de **50 %**

Le budget cybersécurité doit être compris entre **3 et 10%**
du budget informatique

1 Firewall et **1** antivirus ne suffisent pas !

Empiler des technologies non plus ...

3500 professionnels cybersécurité en MPY,
60 entreprises expertes en cybersécurité

Merci de votre attention

Merci