Petits-Déjeuners Persyval-Minalogic

Les défis de la cybersécurité

15 Mai 2018

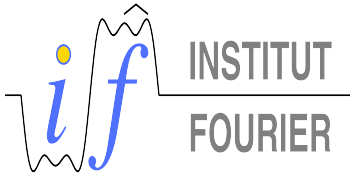
Philippe Elbaz-Vincent

philippe.elbaz-vincent@univ-grenoble-alpes.fr

Cybersecurity Institute
Univ. Grenoble Alpes

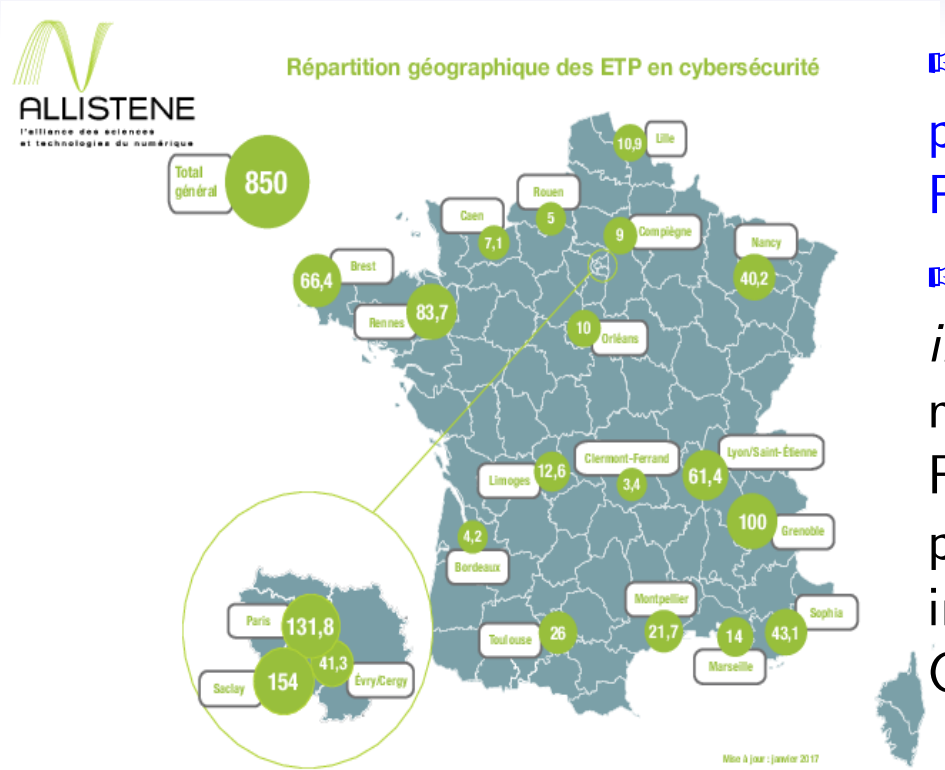
financé par
IDEX Université Grenoble Alpes

https://www-fourier.ujf-grenoble.fr/~pev/ELBAZ_defi_cyber2018.pdf



Univ. Grenoble Alpes
University of innovation

La Cybersécurité à Grenoble (national et international)



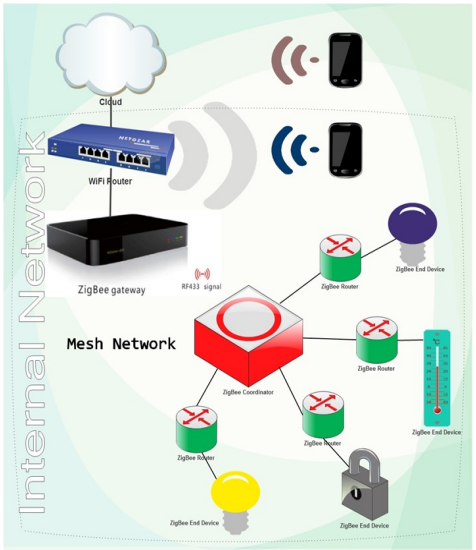
☞ Un site important en France pour la cybersécurité. 160 ETP en Rhône-Alpes dont 100 à Grenoble.

☞ *Des équipes reconnues et impliquées nationalement* : GDR nationaux, organisations JC2'14, RESSI'17, ISA'18, nombreux projets de recherche et à caractère industriel (ANR, PIA, FUI, DGA, CIFRE).

☞ *Des équipes reconnues et impliquées internationalement* :

- 8 projets européens (dont un lauréat du prix Eureka) ; Spacios, Diamonds (*), D-mils, Success (16-18), Citadel, GAINS, Serene-IoT (17-20), UPRISE-IoT.
- conférences internationales de «hacking» CSAW (depuis 2017, plus de 300 visiteurs, collab avec NYU), GreHack (depuis 2012, plus de 400 participants en 2017). Présents au FIC2018 et FIC2019...

Des enjeux socio-économiques mondiaux !



☞ Un objet connecté du quotidien (des millions d'utilisateurs) !

☞ Une faille exploitant ; une cryptanalyse, une attaque sur le matériel, des failles dans l'architecture de sécurité, une vulnérabilité du firmware.

☞ Des conséquences graves : «blackout».

Quel cadre réglementaire ? Quelles garanties pour le citoyen ?

☞ Attaques du réseau électrique en Ukraine (2015)

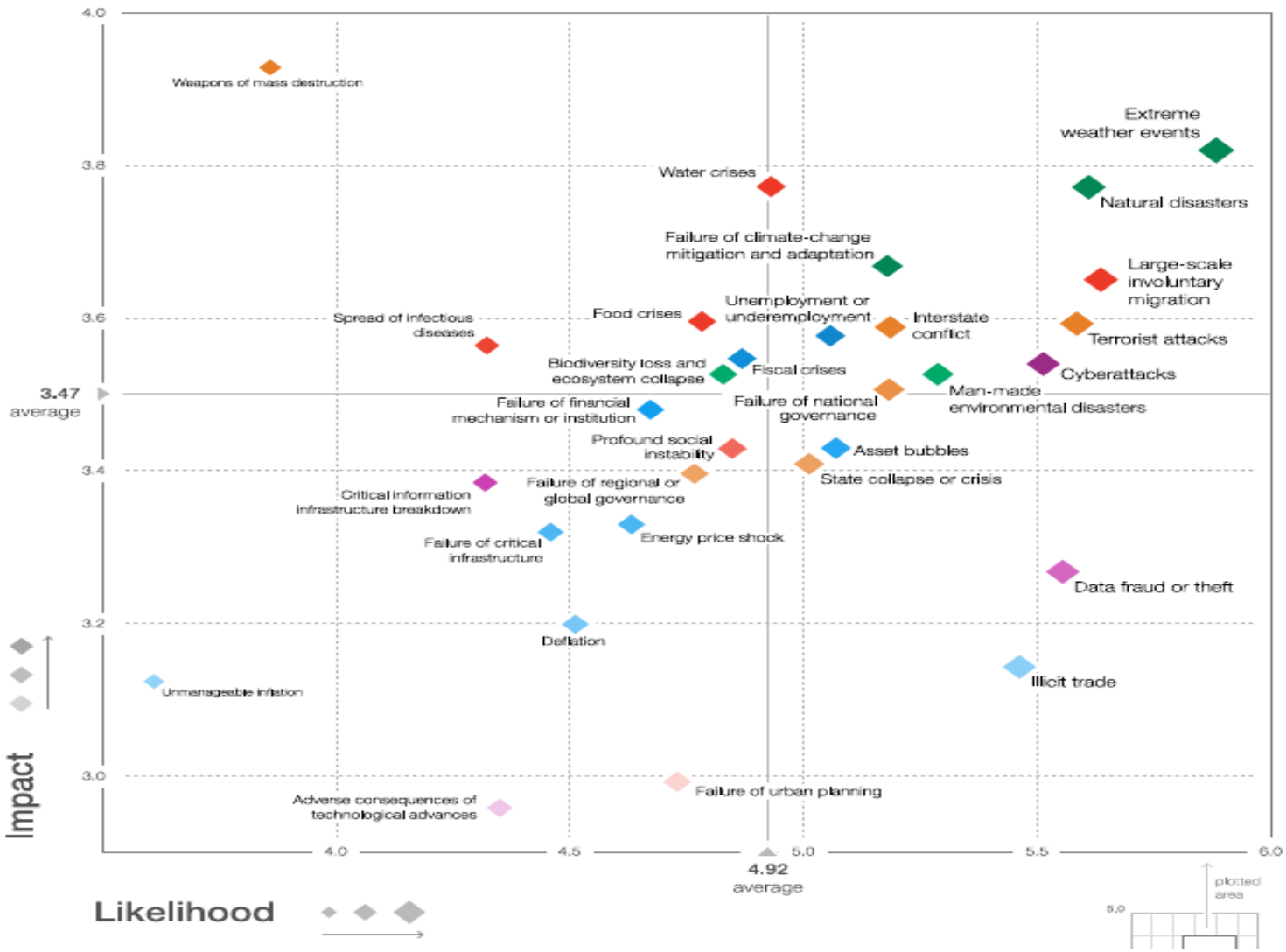
☞ Infection WanaCry (2017), des centaines de sites de production arrêtés pour plusieurs heures, voir jours (e.g., Renault). Des milliers d'entreprises et de secteurs sensibles impactées (e.g., Hôpitaux).

☞ Erreur d'implantation dans des cryptopuces Infineon (Nov. 2017), près de 100 millions de produits impactés (dont 70 millions de ID).

(Forbes, 2017) : estimation du coût de la cybercriminalité en 2021 ; 6000 Milliards de dollars.

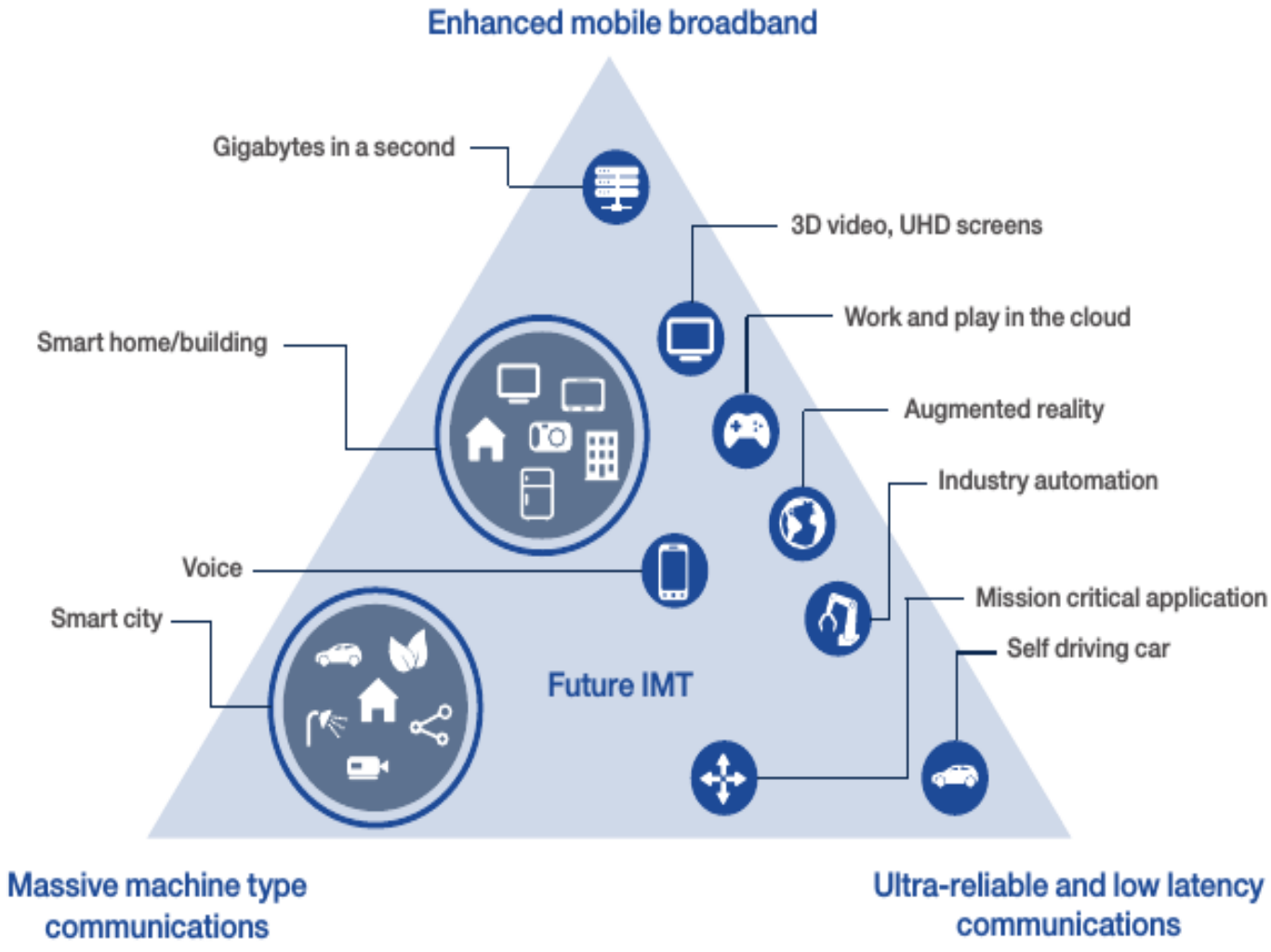
Quel avenir pour nos sociétés numériques hyperconnectées ?

Cybersecurity and the Global Risks



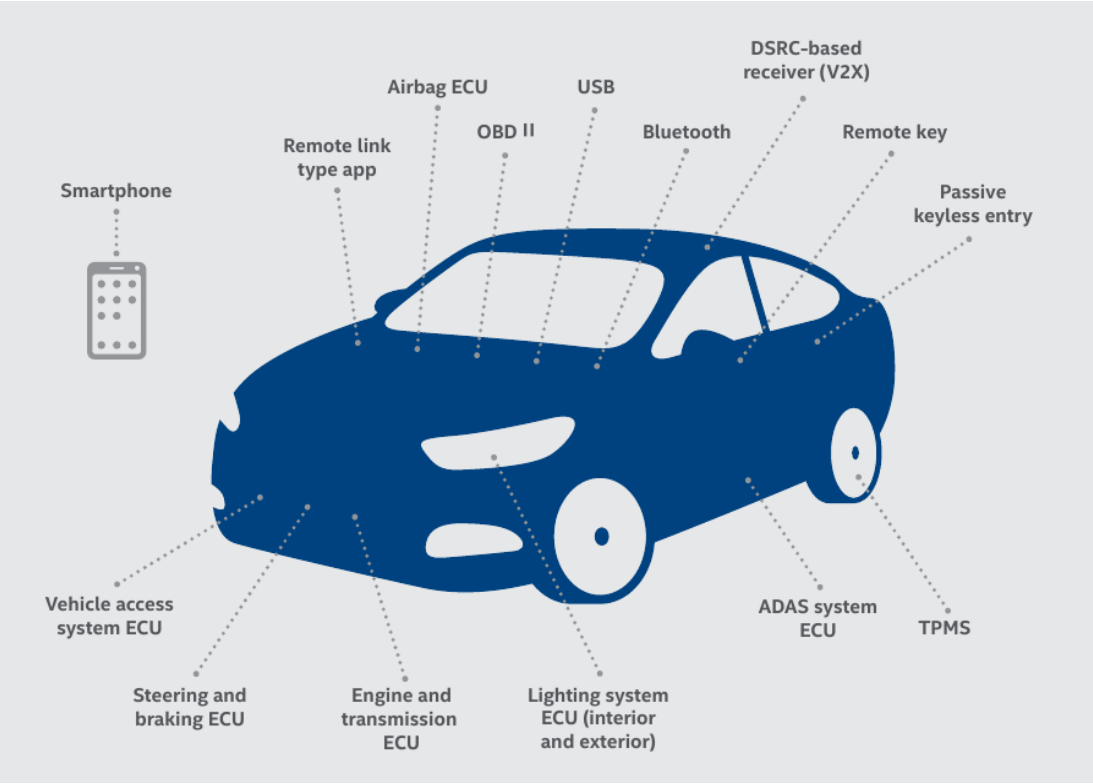
(c) World Economic Forum 2017. The Global Risks Report 2017. 12th Edition

Cybersecurity Everywhere ?



(c) ITU 2015

Illustration with the Automotive systems



(c) McAfee Labs 2016

☞ 220 millions of connected cars by 2020, 12% directly connected to Internet, more than 12 potential attacks entry points...

Failles Intel, AMD et autres CPUs

- Faille dans le Intel Management Engine (2017) ; besoin d'un patch au niveau du BIOS de la carte mère (indépendant de l'OS). Problématique en termes de déploiement industriels.
- Failles «Spectre» et Meltdown» (2017,2018) ; utilisation du «prédicteur de branchement» des CPUs «modernes» pour accéder des zones mémoires protégées. Exploitation possible sur des structures clouds ou via des navigateurs (indépendant de l'OS). Patch au niveau de l'OS (impact potentiel sur les performances).
  `https://spectreattack.com/`

☞ **Impact colossale de telles failles, difficile à corriger, coûts importants.**

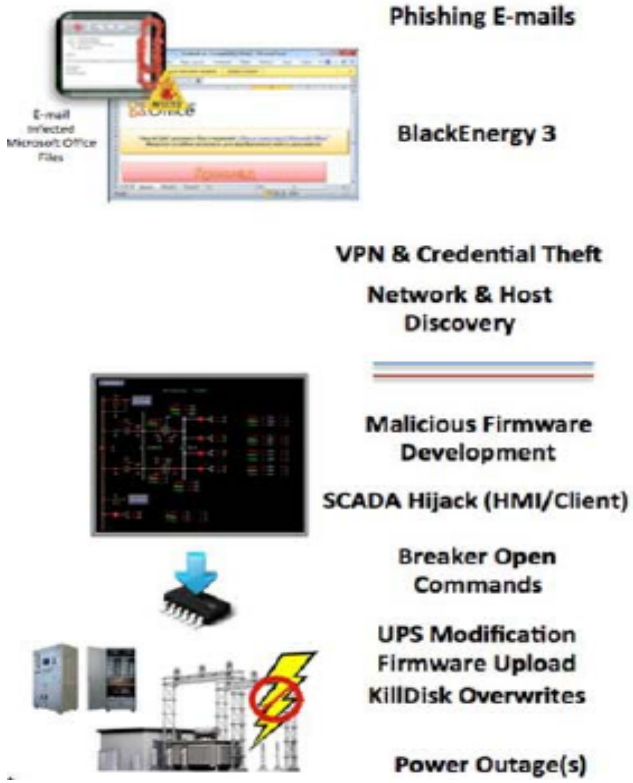
Problèmes des backdoors

☞ de nombreux dispositifs sont préinstallés avec des «login/passwd» par défaut et les utilisateurs n'en ont pas toujours connaissances. Permet une exploitation facile par des cybercriminels.

☞ Illustration avec les dispositifs «My Cloud» de Western Digital (2017-2018) : un login «caché» est crée en usine pour ces familles de matériels (NAS pour utilisation individuel et entreprises). C'est «mydlinkBRionyg» avec un mot de passe par défaut «abc12345cba» !

☞ La présence de «backdoor» est toujours à l'avantage des intentions malveillantes. C'est une mauvaise stratégie !

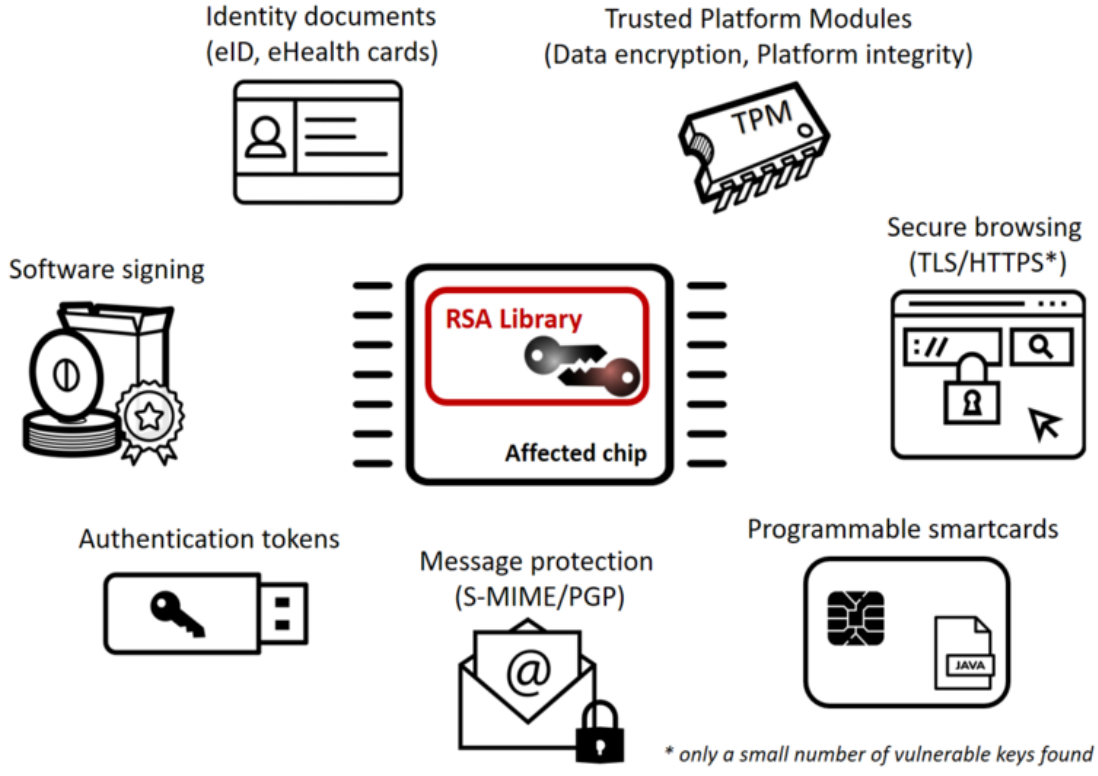
Cyberattacks on Critial Infrastructures



(c) SANS ICS et E-ISAC 2016, «Analysis of the Cyber Attack on the Ukrainian Power Grid», Mars 2016

☞ The Cyberattack was deployed from March 2015 to December 2015 (date of the power outage) ! A recent Symantec's report shows that the situation on US critical infrastructures is worrying (linked to "Dragonfly espionnage group").

☞ **Une erreur d'implantation ou d'algorithmes dans un firmware peut compromettre la sécurité de millions de personnes à travers le monde... !**



(c) Cryptas IT-Security GmBH November 2017

☞ **Conséquences :** Toutes les ID en Espagne et en Letonie sont compromises... !

Different Categories of Attacks

- Generic massive attacks usually non-targeted (phishing, ramsonware, ...),
- Targeted economic attacks,
- Targeted ideological attacks (“hacktivists”, terrorists, “States guided attacks”).

Exemple d'attaque ciblée simple : «Fraude au président ou FOVI»

(c) Police Nationale

☞ Exemple le plus célèbre : Michelin 2014 pour 1,6 Millions d'euros !

L'écosystème du cybercriminel

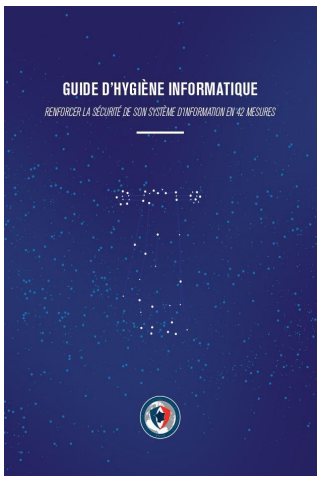
Il existe une économie parallèle (avec son propre réseau de distribution) où l'on peut acheter en ligne des vulnérabilités logiciels, ou réseau, des données volées (pour fraude, usurpation d'identitée), des outils «clef-en-main». En particulier,

- Achat en ligne de kit de phishing, facile a installer sur un serveur, afin de collecter des données et de les revendre via le «boncoin» du cybercriminel ou des forums spécialisés,
- Achat de vulnérabilités, d'exploits, de ransomware, etc (de quelques dollars à des milliers de dollars),
- Location de machines zombies pour attaques réseaux (DDOS), mise en place de botnets,
- Service de cassage de mots-de-passe sur une base de données,
- Achat ou vente de données volées (compte bancaire, messageries, identités, photos/vidéos, PI).

Des solutions ?

- **Nouvelles contraintes sur la protection des données** ; Mise en place du RGPD (EU). *Exposé de C. Lauradoux*.
- **Détection de vulnérabilités, utilisation de composants certifiés** ; *Exposé de J. Fournier*.
- **Bonne pratique de «sécurité» au sein de l'entreprise**

☞ **GUIDE D'HYGIÈNE INFORMATIQUE de l'ANSSI** :



Prix du livre Cyberdéfense au FIC 2018

☞ *Cyberattaques. Prévention-réactions : rôle des Etats et des acteurs privés*, K. Bannelier et T. Christakis (Univ. Grenoble Alpes), éditions Les cahiers de la Revue Défense Nationale.