CYBERSÉCURITÉ

Panorama des menaces cybernétiques sur les états, les entreprises, les particuliers

« Un beau matin les hommes découvriront avec surprise que des objets aimables et pacifiques ont acquis des propriétés offensives et meurtrières »

Qiao Liang et Wang Xiangsui, La guerre hors limites

Introduction – Panorama du monde moderne

Une explosion numérique mondiale

- Des usages personnels qui explosent: informatisation, mobilité (BYOD), objets connectés, cloud computing…
- Une course technologies permanente
- Le numérique est devenu un enjeu vital pour les entreprises et les états.

Un monde multipolaire

- La fin d'un modèle mondial et de la domination occidentale.
- Des règles du jeu définies par pôle.
- Une forte interaction des états et des entreprises.
- Une concurrence acharnée.

Des Conséquences pour les individus

- Sécurité versus libertés individuelles ?
- ➢ Confiance numérique

Cybersécurité, Cyberdéfense: ce qui a changé en France

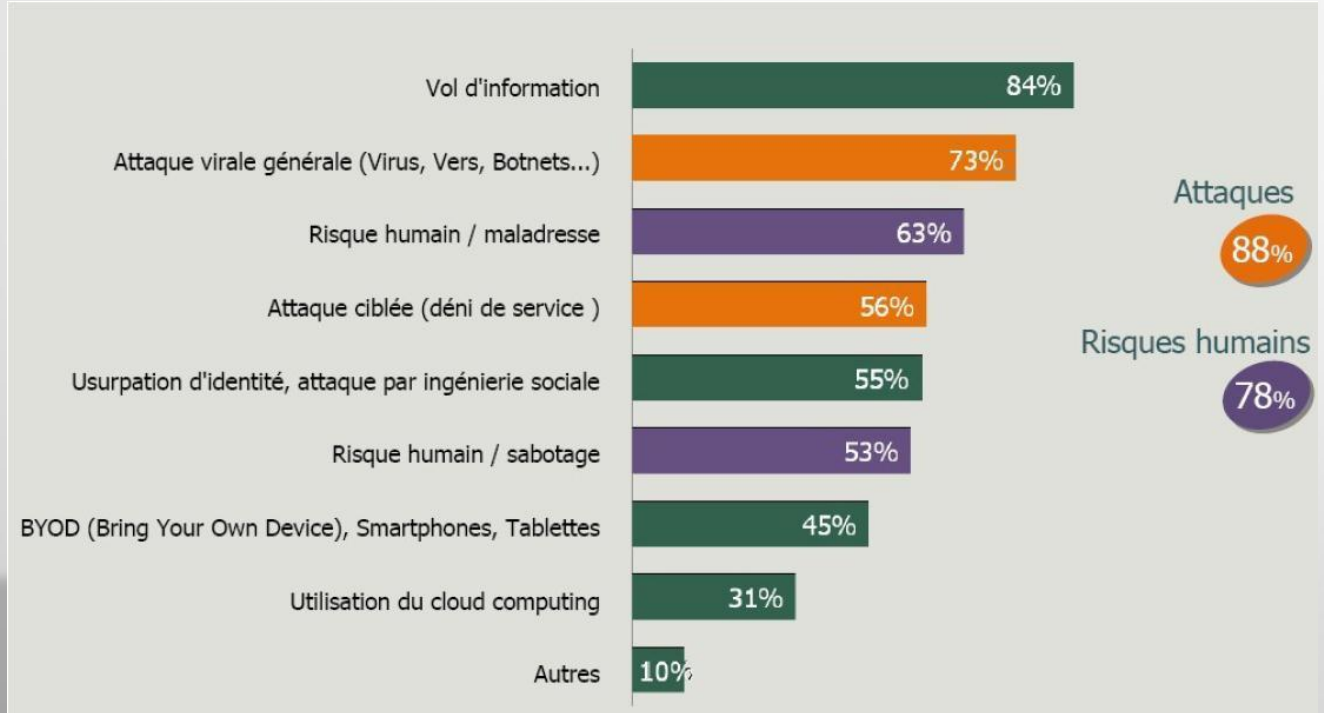
- **Le Rapport du député Pierre Lasbordes** (« La Sécurité des Systèmes d'Information: un enjeu majeur pour la France », 2006)
- **Le cas STUXNET** (2010)
- **Le Rapport du sénateur Jean-Marie Bockel** (« La cyberdéfense : un enjeu mondial, une priorité nationale », 2012)
- **Le Livre Blanc sur la Défense et la Sécurité Nationale** (2012)
- **Rapport « APT1 » de la société de sécurité *Mandiant*** (2013)
- **Révélations d'Edward Snowden sur le programme PRISM** (2013)
- **Loi de programmation militaire** (2013)
- **Rapport du député Jean-Jacques URVOAS («** Evaluation du cadre juridique applicable aux services de renseignement », 2013)
- **Projet de loi sur le renseignement** (2014, 2015)

Les cybermenaces en quelques chiffres

- **42,8 millions** de cyber-attaques dans le monde en 2014 soit1,35 attaque par seconde (*PwC*)
- **200%** d'augmentation des actes de cyber-espionnage en 2014 (*Rapport Verizon 2014*)
- **25 %** des entreprises européennes ont signalé un vol de données confidentielles en 2013 contre 18% en 2012 (*CA Technologies*)
- **78% des entreprises** ont connu des coupures des applications critiques. 63% estiment que les pertes ainsi engendrées vont de quelques centaines de dollars à plus de 5 millions. (*Unitrends)*
- **Cybercriminalité: 7,6 millions de dollars** par an et par entreprise en moyenne (*Ponemon Institute)*
- **190 milliards d'euros**: valeur économique pillée par la cybercriminalité en 2013 (Conseil des Industries de Confiance et de Sécurité).
- **315 milliards d'euros**: marché des données personnelles européennes (2012), 1000 milliards en 2020 (*Boston Consulting Group*)

Evolutions des cybermenaces sur la période 2000 - 2015

2015:



(Source : baromètre annuel CDSE-OpinionWay)

Des premières cyber-armes aux cyber-armées

- StuxNet, DuQu, Flame ….
- Le cyberespace: 5 ° champ de bataille
- Le cyber-renseignement: rapport Mandiant
- Des organisations spécifiques de lutte défensive – et offensive.
- Même les organisations terroristes ont leur pendant Web !

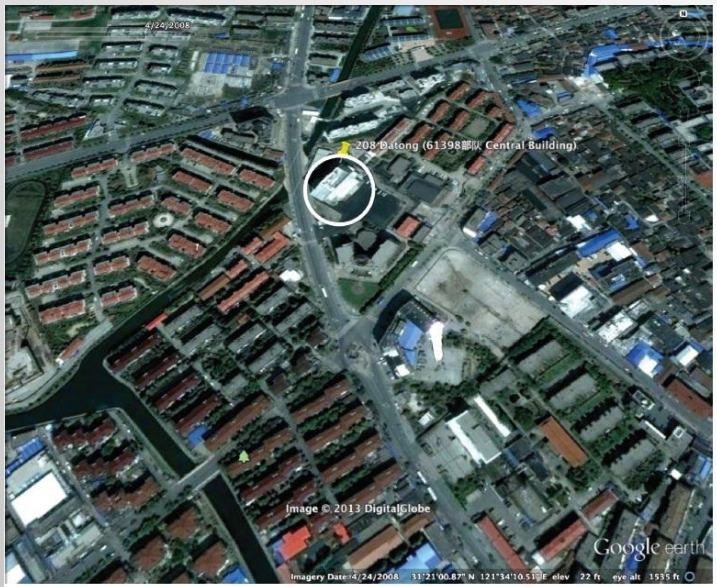


FIGURE 5: Datong Circa 2008 (Unit 61398 Center Building visible at 208 Datong) Image Copyright 2013 DigitalGlobe

Du programme Echelon à Prism: le pillage économique des entreprises

« ... Les affrontements économiques se durcissent de plus en plus. Face à cette situation, le constat est très clair. Les économies les plus conquérantes et les mieux organisées sont celles qui ont su trouver une articulation entre l'intérêt privé et l'intérêt de puissance... »

Christian Harbulot, directeur de l'Ecole de Guerre Economique

TOP SECRET//SI//ORCON//NOFORN

Gmail facebook Hotmail YAHOO! Google skype paltalk.com YouTube AOL mail

SPECIAL SOURCE OPERATIONS

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

PRISM

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.

International Internet Regional Bandwidth Capacity in 2011
Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

Les nouvelles menaces visant les organisations

- Des escroqueries sophistiquées
- Le « *Rançonwares* »
- Les APT: « *Advanced Persistent Threat* »
- Les manipulations et détournements de données officielles
- Le cyber-terrorisme, visant à provoquer une catastrophe.

Et des menaces « classiques » qui persistent et se développent:

- Déni de service
- Virus, malwares
- Phishing
- « Defacement» de sites Internet (SQLi, Attaques force brute, …)

8 Aout 2014: les sites du groupe Les Nouvelles sont piratés par des « hacktivistes » propalestiniens

Conséquences sur les usages et la vie privée des individus

- **Risques accrus** sur les données personnelles
- Une émergence notable des malwares « mobiles »
- Un contrôle, sur surveillance renforcée, une sensation de « flicage »
- Une confiance numérique à évaluer – mais un besoin devenu essentiel.

➢ **Choisir ses outils et la manière dont on les utilise.**

Santé

18 Aout 2014: Un groupe de hackers chinois subtilise 4,5 millions de données médicales au Community Health Centre (CHS), le deuxième réseau hospitalier américain.

Contacts, Adresses

18 avril 2014: 1,3 millions de données de clients et prospects est dérobée à l'opérateur ORANGE.

Emails

Janvier 2014: de nombreux identifiants et mots de passes de la messagerie Yahoo! sont piratés.

… en Nouvelle-Calédonie ?

- L'ile n'en est plus une du point de vue du Cyberespace
- Hors du champs de compétence de l'ANSSI
- Présence de ressources étatiques: Gendarmerie, DGSI, ….
- Peu de compétences locales, peu de ressources, pas d'indicateurs des incidents ou d'échelle de risques.
- La politique économique est de compétence du Gouvernement de la Nouvelle-Calédonie:

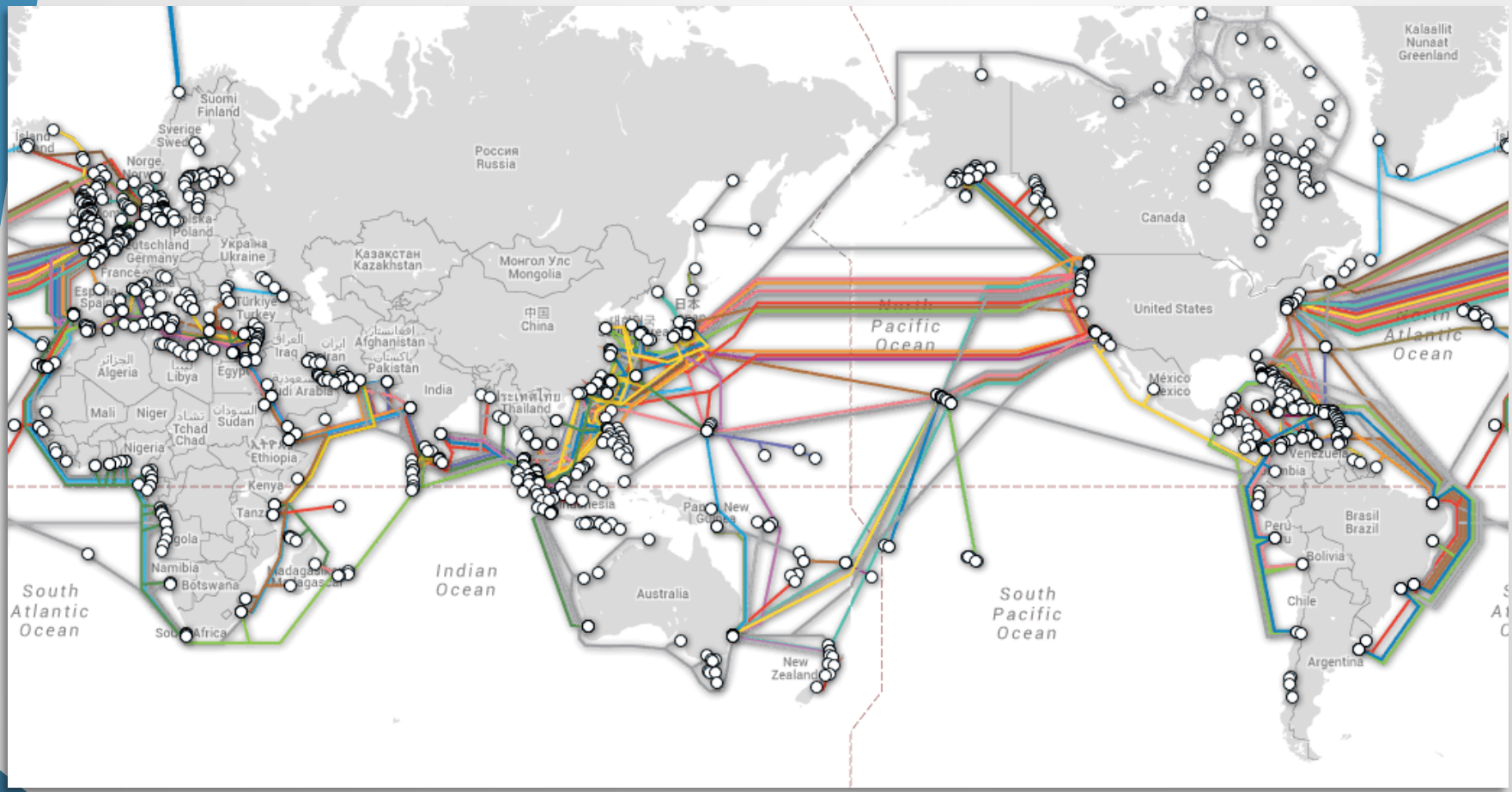
Vers la **Confiance Numérique**.

Conclusion

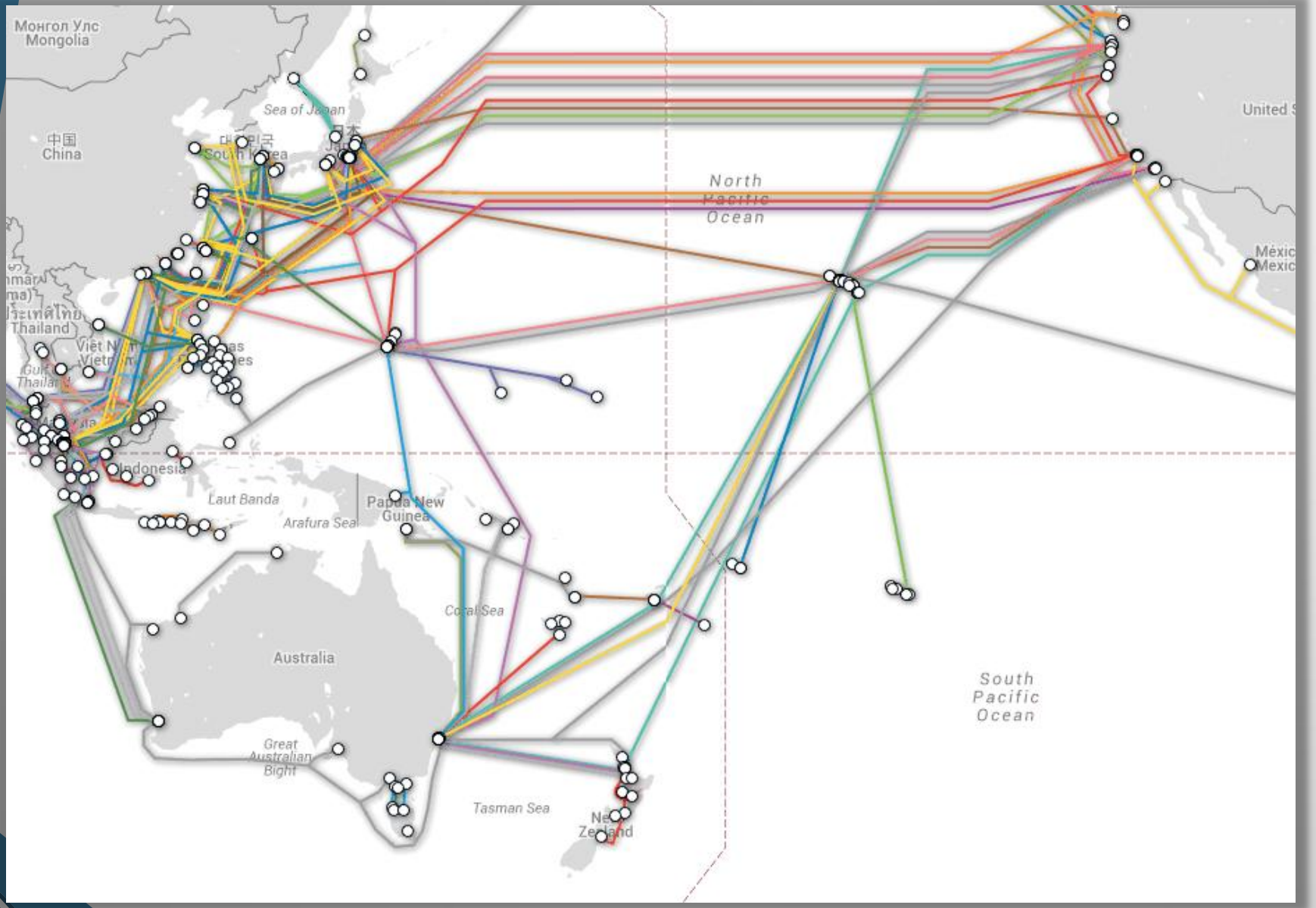
Nous n'avons pas d'amis, nous n'avons pas d'ennemi.
Nous n'avons que des partenaires aux intérêts changeants.

Merci pour votre attention

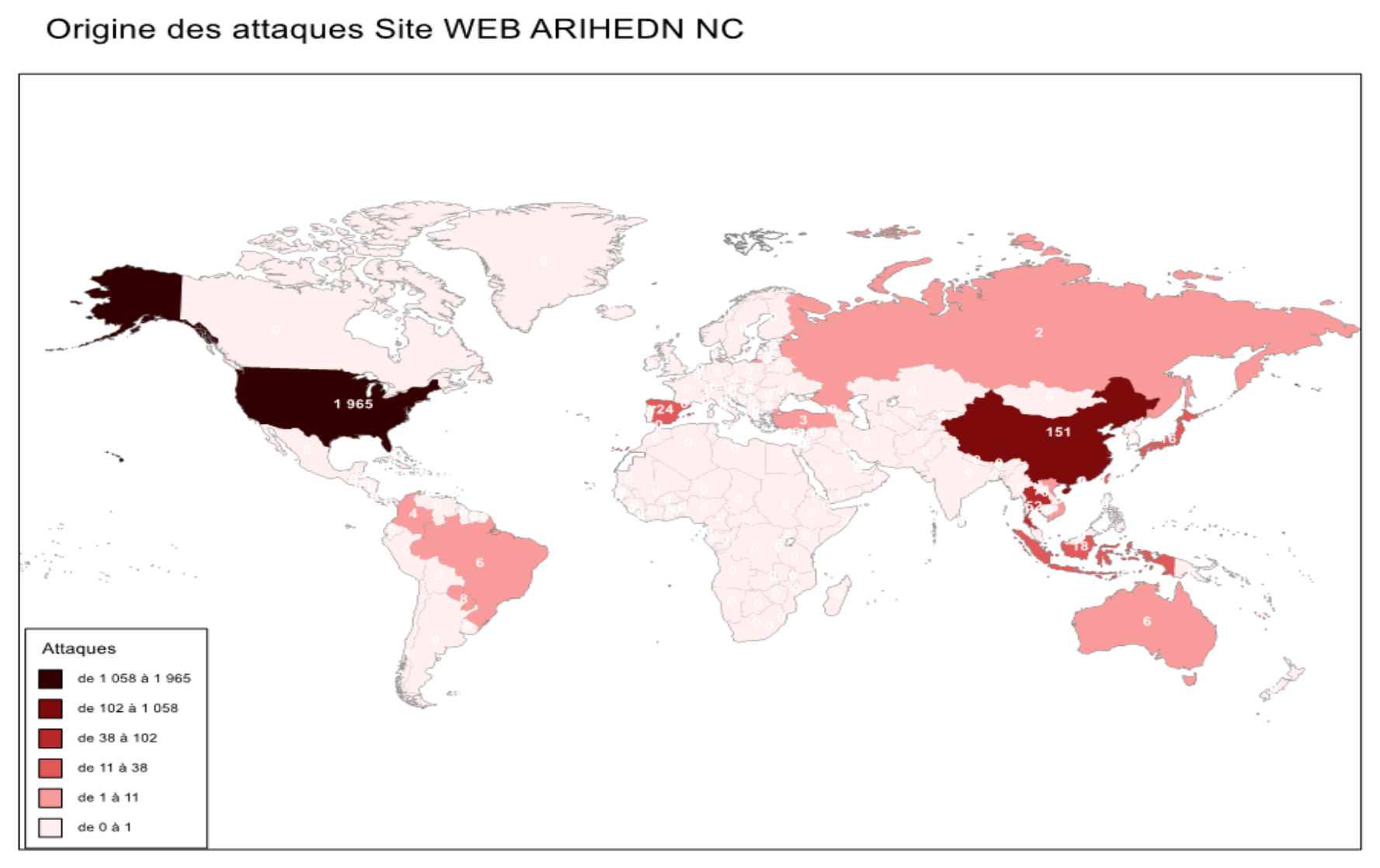
Annexe 1: Câbles sous-marins dans le Monde



Annexe 2: Câbles sous-marins dans le pacifique

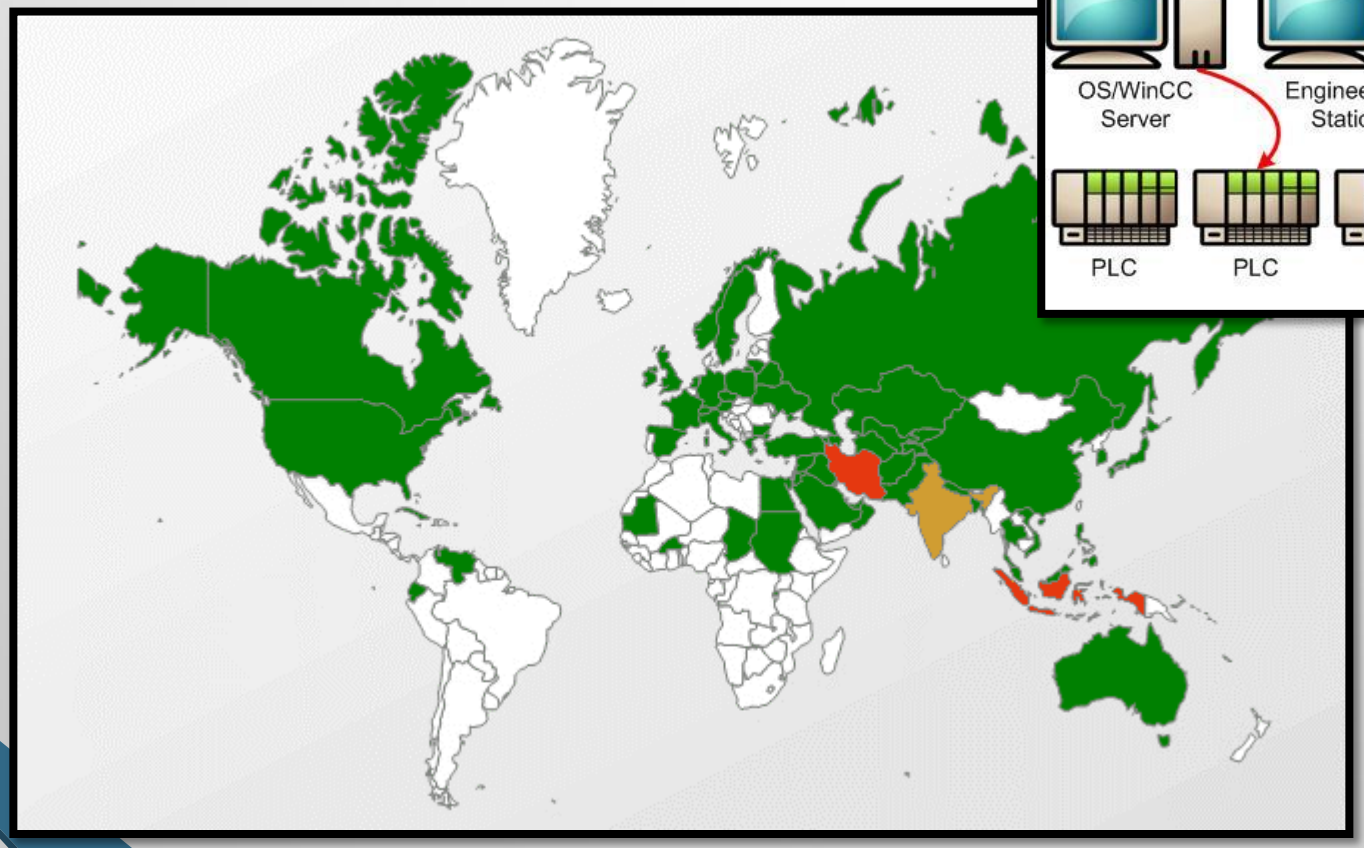


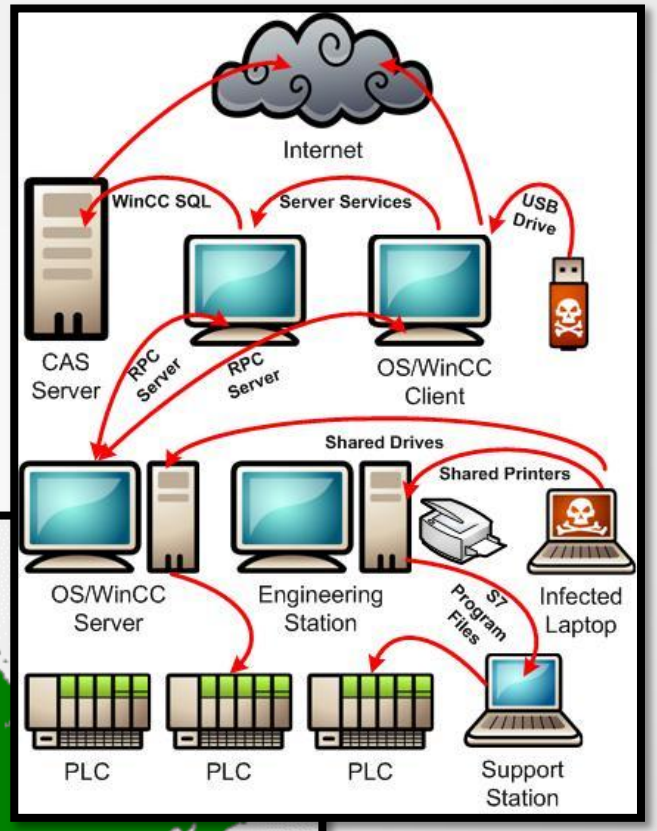
Annexe 3: Attaques sur le site Internet de l'ARIHEDN NC (Aout 2013)



Annexe 4: STUXNET

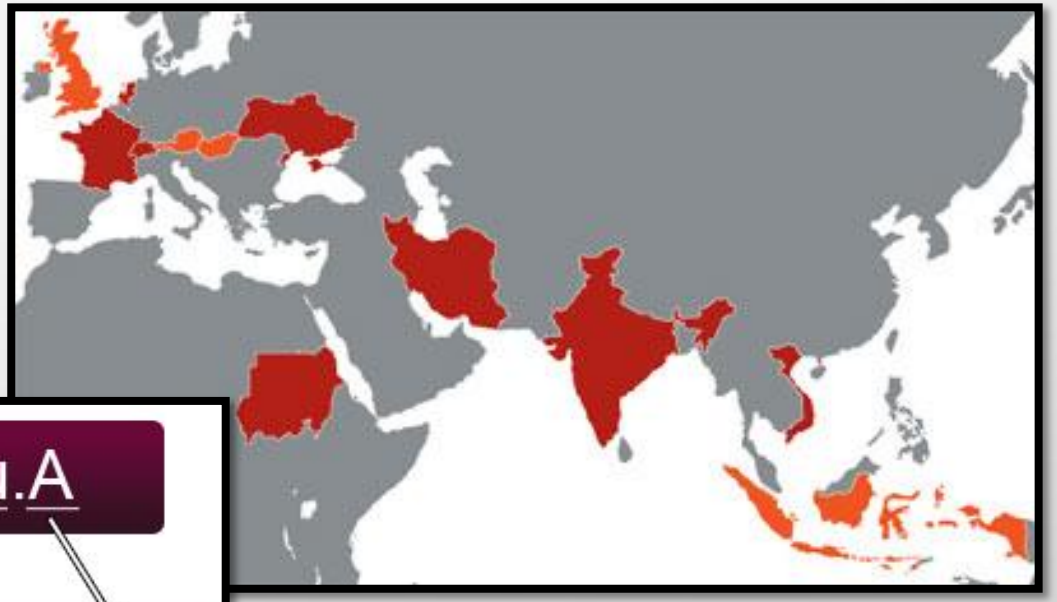
- Vise les systèmes SCADA.
- Origines probables.
- Le cas Iranien.

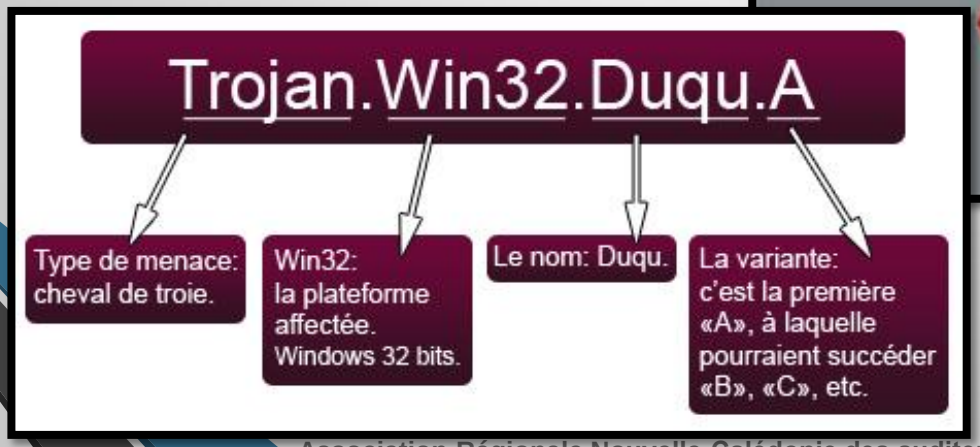




Annexe 5: DUQU

- Très proche de STUXNET dans la structure.
- Exploite une faille zero-day de MS.Word
- Prévoit des vols d'informations, écoutes….
- Opération visiblement avortée avant son lancement.





Annexe 6: FLAME

- Vol de données
- Dessins Autocad, fichiers PDF, textes
- Ecoutes (activation de micro à distance)
- Cible principale: données du programme nucléaire Iranien, données financières des pays arabes.
- Autodestruction après 4 ans d'activités des son repérage par Kaspersky.


```
if not __LIB_FLAME_PROPS_LOADED__ then
    __LIB_FLAME_PROPS_LOADED__ = true
    flame_props = {}
    flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
    flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
    flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
    flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
    flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CH
    flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
    flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUE
    flame_props.BPS_KEY = "BPS"
    flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
    flame_props.getFlameId = function()
      if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
        local l_1_0 = config.get
        local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
        return l_1_0(l_1_1)
      end
```