Etat de la menace
Stratégie nationale de cybersécurité

http://www.ssi.gouv.fr
http://www.certa.ssi.gouv.fr
http://www.securite-informatique.gouv.fr

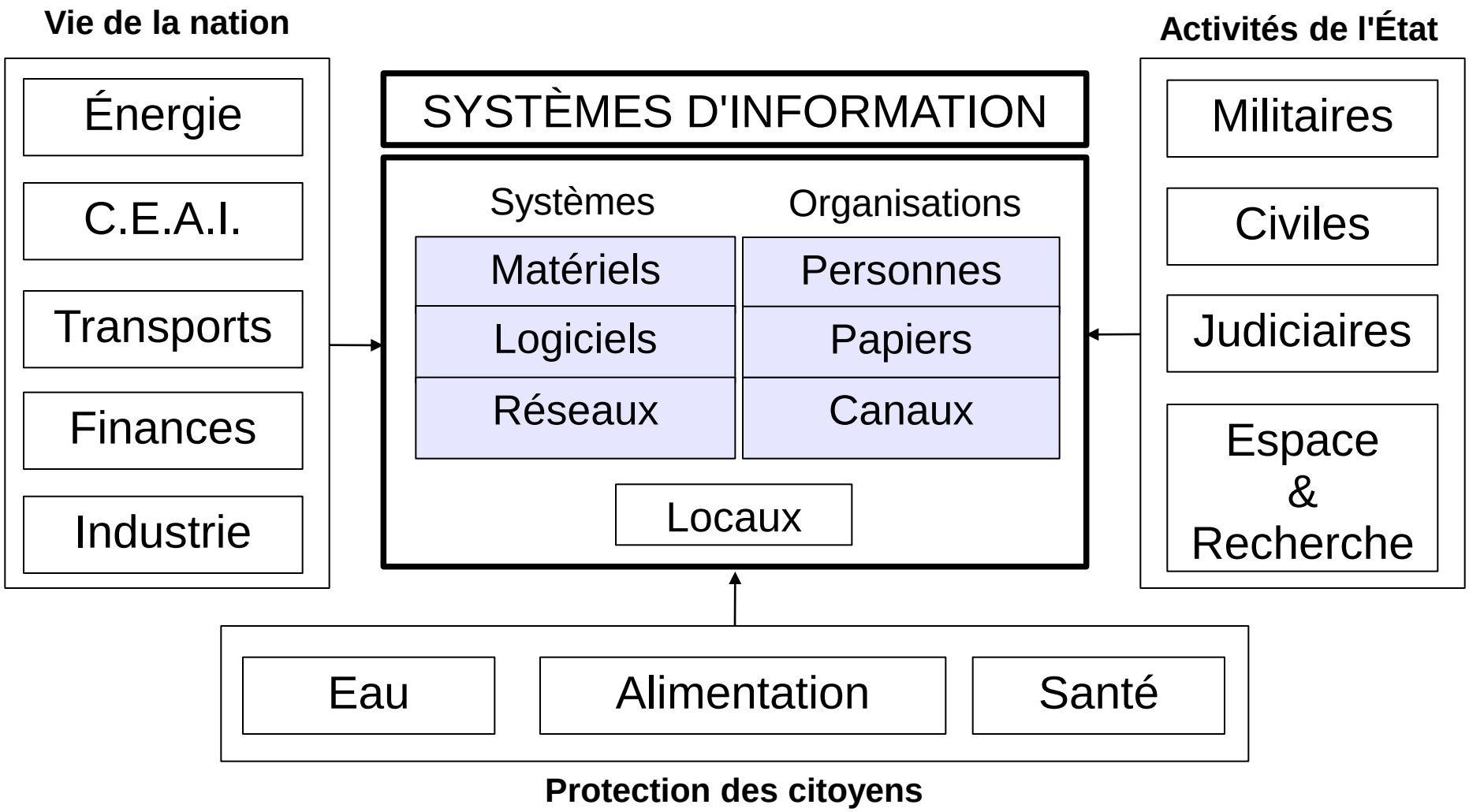
David CROCHEMORE
Mercredi 28 novembre 2012

Menaces cyber contemporaines

- I - Des attaques contre les SI
- II - Six menaces contemporaines
- III - Stratégie nationale de cyber-sécurité
- IV – L'agence nationale de la sécurité des systèmes d'information

I – Des attaques contre les SI

Cibles / richesses - Surface / Périmètre
Enjeux



Chemins d'attaque

VOIE INFORMATIQUE

- Ver, virus, cheval de Troie...
- Keylogger, porte dérobée...
- Paquet spécialement forgé
- Bombe logicielle
- Saturation réseau

...

VOIE COGNITIVE

- Manipulation
  - à distance
    - ciblée
    - de masse
  - au contact (interne)

...

VOIE PHYSIQUE

- Effraction (salle serveur)
- Destruction (cables)
- Piégeage (PABX)

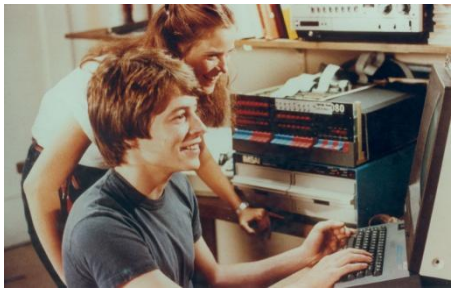
...

Motivations et profils

LUCRATIVE
Cybergangs
Cybermercenaires
Officines

POLITIQUE
Hacktivistes
Cyberpatriotes
Cyberterroristes

MILITAIRE
Unités spécialisées



LUDIQUE
Adolescent désoeuvré

TECHNIQUE
Hacker

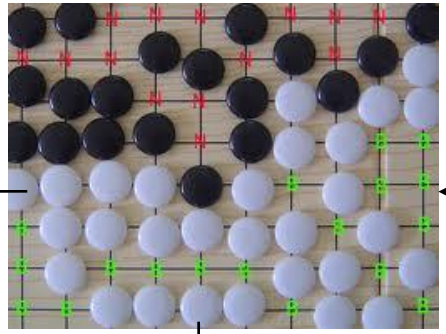
PATHOS
Employé mécontent

Opérations malveillantes

Espionnage

Agit-prop

Invasion



Sabotage

Fraude massive

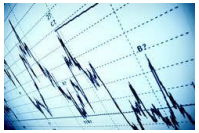
Saturation

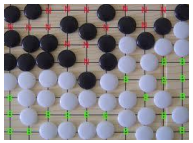
Rappel : spécificités du terrain

- Cyberespace : espace artificiel planétaire sans frontières
  - Construction humaine, infrastructure technique != espace naturel
  - Traverse et relie les espaces
  - Problèmes de frontières (entre pays, entre civils et militaires, public et privé)
- Double dimension, usages multiples, interdépendance généralisée
  - Virtuelle : espace logiciel et de connaissances, politique, économique
  - Physique : sert des services critiques : eau, énergie, transport, défense…
- Durée et espace contractés, mouvement et extension perpétuels
- Asymétrie structurelle en faveur de l'attaquant
  - Disproportion de moyens requis entre attaque et défense
  - Difficulté de détection
  - Difficulté d'attribution
  - Difficulté de riposte

II – Six menaces contemporaines

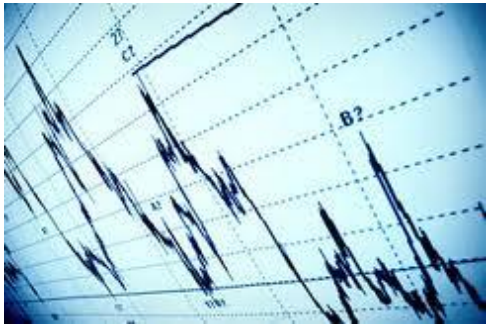
Six menaces contemporaines





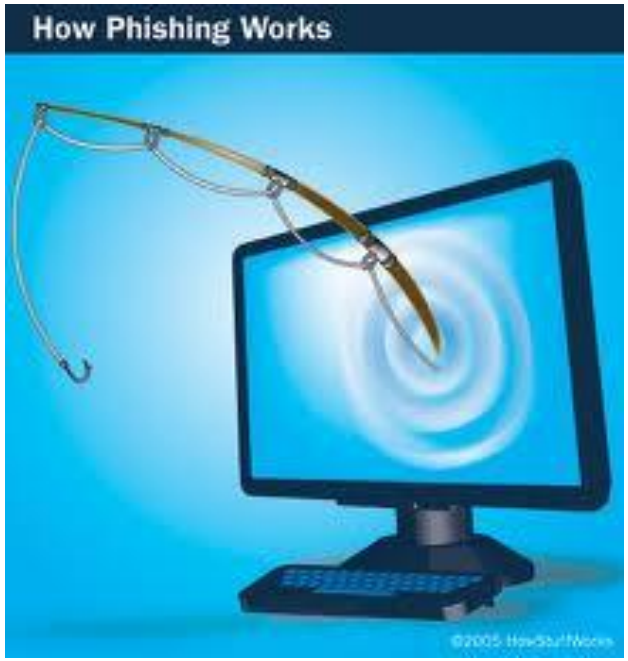
1. Fraude massive
    1. Bourse CO2
2. Espionnage
    1. APT / PHO
3. Espionnage + Sabotage
    1. Stuxnet, Duqu & Co
4. Agit-Prop + Saturation
    1. Estonie, Géorgie, Iran
5. Espionnage + Agit-Prop + Saturation
    1. Wikileaks, Lulzec, Anonymous
6. Invasion
    1. Conficker

1. Bourse CO2



Fraude massive

2010 : 15 places de marchés ciblés



- Courriel de phishing ciblé
  - Envoyé aux entreprises affiliées au registre européen
  - Usurpation d'adresses courriels d'autorités émettant les certificats + faux site de la CE
  - Au moins 15 pays européens touchés (dont France)

IMPACT

Fermeture du marché par la CE

Au moins 3 millions d'euros de certificats allemands dérobés

Montant total « exfiltré » : inconnu

2011 – Les attaques continuent

- Keylogger déposé par pièce jointe piégée
- Attaque directe contre les serveurs de la bourse autrichienne

IMPACT

Nouvelle fermeture du marché pendant une semaine

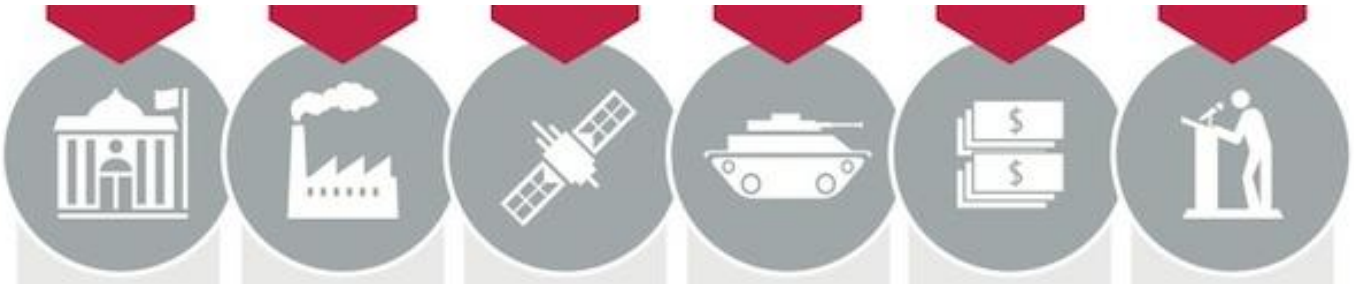
Au total, près de 50M€ de certificats dérobés

Impact sur l'image du marché (déstabilisation)

2. APT / PHO

Espionnage

APT / PHO : généralités



- Acronyme APT créé en 2006 par l'US Air Force
- Désigne des campagnes d'attaques
  - **P**ersistantes : depuis au moins 2003, cibles récurrentes
  - **H**étéroclites : principe de consommation minimale
  - **O**rganisées : plusieurs équipes coordonnées
- But : espionnage massif (pillage stratégique)
- Secteurs ciblés : défense, énergie, aéronautique, spatial, diplomatie, media, ONG…

APT/PHO : caractéristiques détaillées

- **Persistantes**
  - une cible le reste, quoiqu'elle fasse (poursuite d'un PR)
  - les attaquants peuvent se maintenir des années
- **Hétéroclites**
  - Large palette d'outils et techniques utilisés en fonction du besoin
  - Chevaux de Troie/Backdoor observés peu sophistiqués à ce jour
  - Mais exploitation « *zero month* » régulières et experts sur demande
- **Organisées**
  - Organisation du travail (perceurs/exploitants/analystes…)
  - Synchronisation avec l'actualité (cf : négociations de contrats en cours, sommets internationaux à venir…)
  - Multiples cibles traitées en simultanée (campagnes)

3. Stuxnet, DuQu & co

Espionnage + Sabotage

2010 - Stuxnet

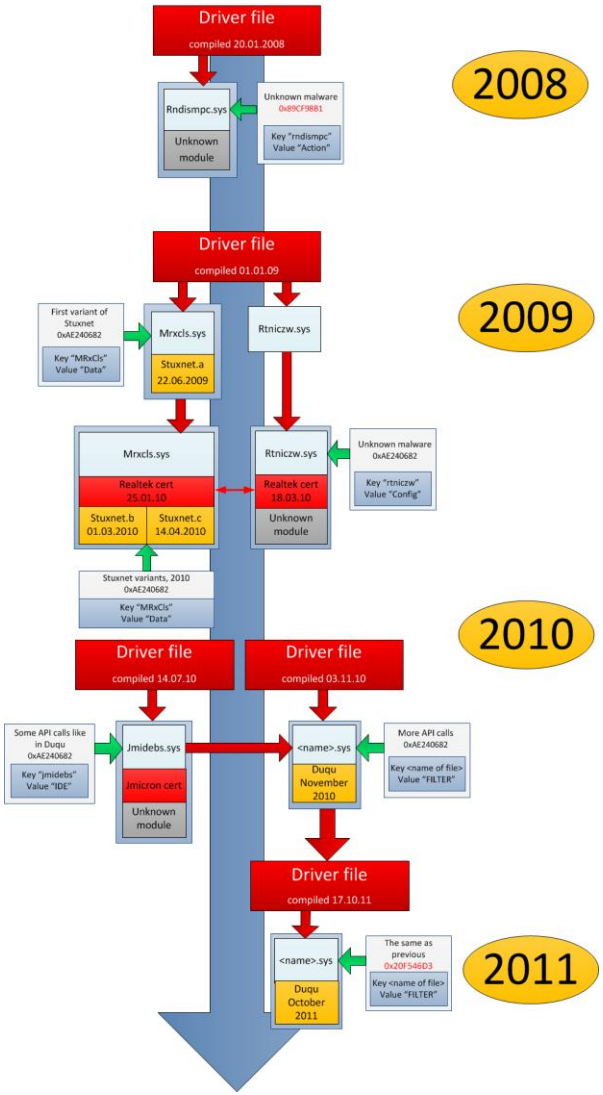
Découvert en juin 2010

- Technicité très élevée
- Charge active ciblant des PLC
- Simulateur de normalité SCADA
- Plusieurs zero-day exploitées
- Emploi de certificats dérobés
- Forte furtivité

D'après le NYT (juin 2012), opération conjointe US / IL

- Conçue pour saboter l'installation nucléaire de Natanz
- Développée et conduite sur des années
- Code déployé via clé USB par agents ou utilisateurs piégés
- A atteint ses objectifs (retarder le programme nuc. iranien)

2011 - DUQU



Outil de cyberespionnage

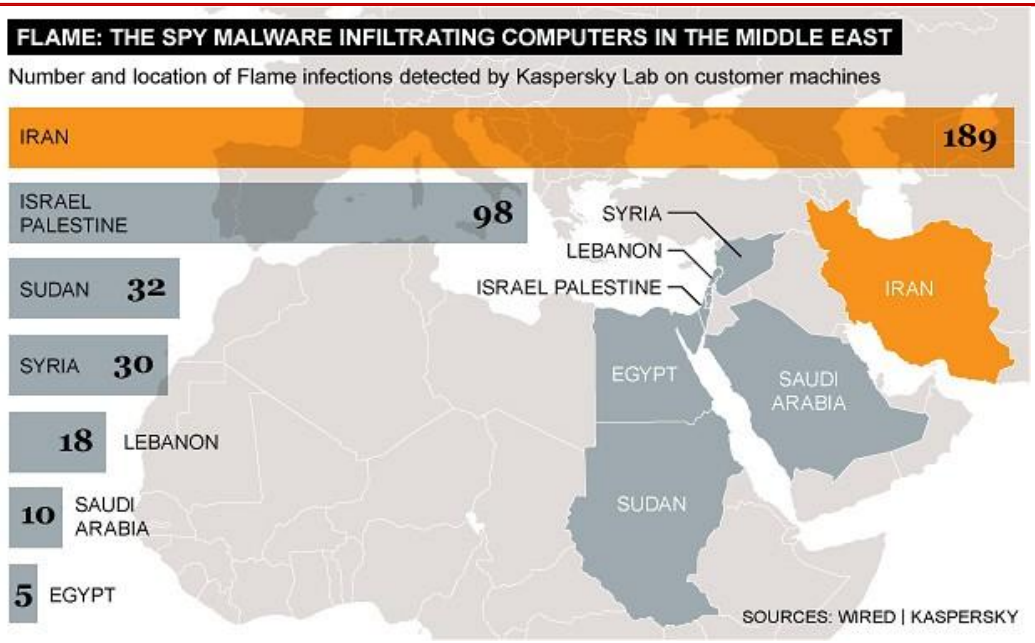
Découvert chez des :

- éditeurs/utilisateurs de systèmes de contrôle industriel
- autorités de certification

Partage avec Stuxnet :

- Blocs de code commun
- Installation via *zero day*
- Camouflage via certificat dérobé
- Peu d'infections détectées
- Pays sensibles sur-représentés

2012 – FLAME



- Trousse à outils modulaire de cyberespionnage
- Découvert suite à attaque de type effacement de données
- Exploitation d'une vulnérabilité de conception MS
- En activité depuis au moins depuis 2008
- N'était détecté par aucun produit de sécurité
- Intérêt particulier pour les fichiers Autocad (CAO)

4. Estonie, Georgie, Iran

Agit-Prop + Saturation

2007 : Estonie

- Avril 2007 : le déplacement d'une statue militaire soviétique déclenche une crise
- Attaques massives en déni de service et défigurations de sites officiels
- Emploi de réseaux de machines zombies
- Revendiquées par des cyberpatriotes
- Attribuées à l'État russe par l'Estonie

IMPACT

Saturation des réseaux de télécommunication
Services étatiques, bancaires, d'urgence... touchés
Vie de la Nation déstabilisée pendant plusieurs jours
Coût conséquent de retour à la normal

2008 : Géorgie

- Attaques massives
  - en déni de service
  - par défiguration
  - détournement de trafic
- En amont d'opérations conventionnelles
- Revendiquées par des « cyberpatriotes »
- Attribuées à l'État russe par la Géorgie

IMPACT

Réseaux civils perturbés en temps de crise
Difficulté de communication de l'État (interne/population)
Propagande ennemie relayée sur ses propres sites

2009 : Iran

I want all hackers to take down ALL sub-sites for http://www.khamenei.ir/ #gr88 #iranelection
11:52 AM Jun 16th from Seesmic Desktop

It seems that http://www.pagereboot.com/ is "blocked" when doing it 4 http://farsi.khamenei.ir
11:51 AM Jun 16th from Seesmic Desktop

WTF!"Your IP, location and other information has been recorded!-Security Defence Team!" gr83
11:49 AM Jun 16th from Seesmic Desktop

TAKE DOWN THESE SITES NOW! http://is.gd/13GpE http://bit.ly/E0kOu http://bit.ly/BHMzh #GR88
11:46 AM Jun 16th from Seesmic Desktop

TAKE DOWN THESE SITES http://www.khamenei.ir/ http://www.iribnews.ir/ http://www.irib.ir/English/ #gr88
11:43 AM Jun 16th from Seesmic Desktop

- Contexte : élections présidentielles iraniennes
- Agitation sur les réseaux sociaux
- Attaques informatiques massives
  - Défiguration et déni de service
- Assistance technique anti-censure (TOR)
- Revendiquée par hacktivistes et diaspora
- Attribuée aux États-Unis et Israël par l'Iran

IMPACT

Alimentation de troubles politiques à un moment clé
Propagande adverse massivement relayée (effet de *buzz*)
Aggravation de l'image dans le monde

5. Wikileaks, Anonymous, Lulzsec

Espionnage + Agit-Prop + Saturation

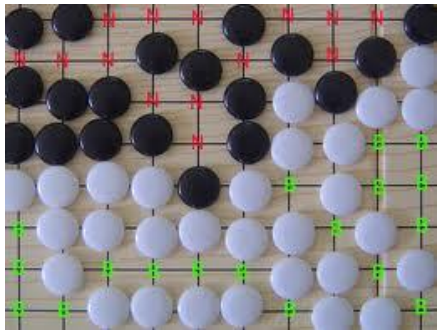
Wikileaks (2010/11)

- Fuites massives de documents classifiés US
  - « Collateral Murder »
  - « War logs »
  - « Cablegate »
- Attribué à un attaquant interne
- Relayé par l'ONG Wikileaks
- Impact :
  - risques sur opérations
  - compromission de sources
  - déstabilisation diplomatique
  - image dans le monde
  - déclenchement d'enquêtes

Anonymous/Lulzec (2011/12)

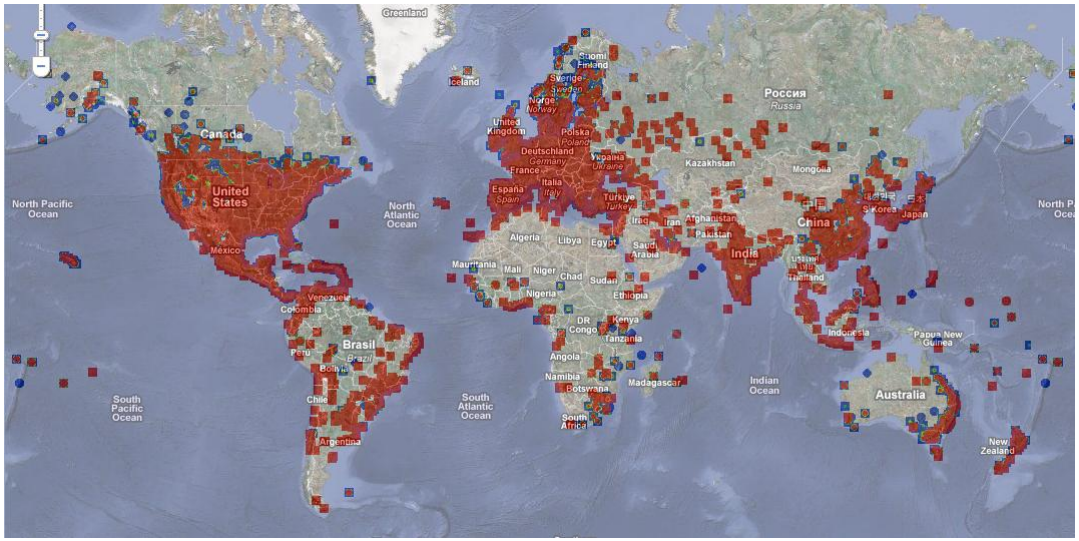
- Mouvance dite « libertaire »
- Sans « tête » apparente
- Se développe nettement suite de l'affaire Wikileaks
- Attaques combinées et répétées contre des cibles variées
  - Défiguration et déni de service (Mastercard, Paypal, Printemps arabe)
  - Espionnage suivi de divulgation (HB Gary, Sony)
- A conduit à une opération d'infiltration du F.B.I.
- Profils concernés : hacker, kiddie, grand public, faux-nez…

6. Conficker



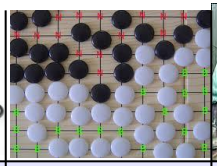
Invasion

2009 - Conficker



- Ver informatique sophistiqué reposant sur un type de *zero day* rare
- Des millions de PC infectés de par le monde en quelques semaines
- Capacité de pilotage opérationnel des attaquants remarquable
- Perturbations dans tous les secteurs stratégiques
  - transports, santé, énergie, activités civiles et militaires…
- Pourtant… pas de charge active téléchargée
- But : délinquance, exercice, dissuasion, pré-positionnement ?

Récapitulatif des menaces

	Espion	Sabotage	Invasion	Agit-prop	Saturation	Fraude
						
Campagnes APT/PHO	✓					
Stuxnet, DuQu & co	✓	✓				
Estonie, Georgie, Iran				✓	✓	
WL, Anon. Lulzec	✓			✓	✓	
Conficker			✓			

III – Stratégie nationale de Cyber-sécurité

Définition de la cyber-sécurité (1/2)

La **cybersécurité** est « l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. »

Définition de la cyber-sécurité (2/2)

Quatre dimensions conditionnent la cybersécurité :

1. La sécurité des systèmes d'information fait appel à des techniques de protection pour concevoir et rendre les systèmes d'information et de communication moins vulnérables aux attaques.
2. Elle s'appuie sur la lutte contre la cybercriminalité, qui en constitue le volet répressif.
3. Elle nécessite la mise en place d'une cyberdéfense qui s'appuie sur une organisation, des outils de prévention et de surveillance et sur des chaînes opérationnelles réactives.
4. Elle repose sur une maîtrise des systèmes d'information qui doivent être administrés et tenus à jour par des opérateurs de confiance, mobilisés pour en assurer la résilience, et rattachés à un responsable identifié, qu'il soit public ou privé.

La SSI : Priorité du Livre Blanc

Livre Blanc sur la Défense et la Sécurité nationale, publié en 2008.

<< *La France doit garder un domaine de souveraineté, concentré sur les capacités nécessaires au maintien de l'autonomie stratégique et politique de la Nation : la dissuasion nucléaire, le secteur des missiles balistiques, les sous-marins nucléaires d'attaque,* ***la sécurité des systèmes d'information*** *font partie de ce premier cercle.* >>

Révision du Livre Blanc en cours. Le rôle primordial de la SSI sera au moins confirmé.

STRATÉGIE FRANÇAISE DE CYBERSÉCURITÉ (1/2)

Publiée en février 2010, la stratégie de la France en matière de défense et de sécurité des systèmes d'information repose sur **quatre objectifs stratégiques** :

1. Être une puissance mondiale de cyberdéfense
2. Garantir la liberté de décision de la France par la protection de l'information de souveraineté
3. Renforcer la cybersécurité des infrastructures vitales nationales
4. Assurer la sécurité dans le cyberespace

STRATÉGIE FRANÇAISE DE CYBERSÉCURITÉ (2/2)

Afin de remplir les quatre objectifs stratégiques, **sept axes d'effort** ont été retenus :

1. Anticiper, analyser ;
2. Détecter, alerter, réagir ;
3. Accroitre et pérenniser nos capacités scientifiques, techniques, industrielles et humaines ;
4. Protéger les systèmes d'information de l'Etat et des opérateurs d'importance vitale ;
5. Adapter notre droit ;
6. Développer nos collaborations internationales ;
7. Communiquer pour informer et convaincre.

IV – L’agence nationale de la sécurité des systèmes d’information (ANSSI)

PRÉSENTATION

Créée le 7 juillet 2009, l'ANSSI :

- est l'**autorité nationale en matière de défense et de sécurité des systèmes d'information**
  - décret n° 2009-834 du 7 juillet 2009
  - modifié par le décret n° 2011-170 du 11 février 2011
- est rattachée au Secrétaire général de la défense et de la sécurité nationale, en lien direct avec le cabinet du Premier ministre
- est un réservoir de compétences au profit des administrations et des opérateurs d'importances vitales
- développe et acquiert des produits de sécurité essentiels à la sécurité des réseaux les plus sensibles de l'Etat.

Un effectif à terme de 360 personnes.

LES MISSIONS DE L'ANSSI

L'ANSSI a une mission de **prévention** :

- Réglementation en matière de SSI ;
- Aide et conseil à destination de services de l' État et des OIV;
- Inspections des SI de l'État ;
- Délivrance d'agréments ;
- Négociations internationales et liaison avec ses homologues étrangers ;
- Formation dans le domaine de la SSI ;
- Réalisation et exploitation de moyens de communications sécurisés.

LES MISSIONS DE L'ANSSI (2)

L'ANSSI a une mission de **défense des systèmes d'information**, afin de protéger nos systèmes d'information vitaux :

- Système de détection et gestion d'incident ;

En cas d'attaques majeures contre les systèmes d'information de l'État, l'ANSSI par délégation du Premier ministre :

- Décide des mesures de protection à faire appliquer ;
- Met en œuvre la réponse aux crises.

LES PRIORITÉS D'ACTION

Une cyberdéfense active en profondeur

- une capacité de détection précoce des attaques
- une réaction rapide
- une protection intrinsèque des systèmes
- la surveillance en temps réel des réseaux les plus critiques

Des systèmes et produits sécurisés

- promouvoir le développement et l'utilisation des produits de sécurité
- construire, mettre en place et opérer des SI de confiance au sein du gouvernement

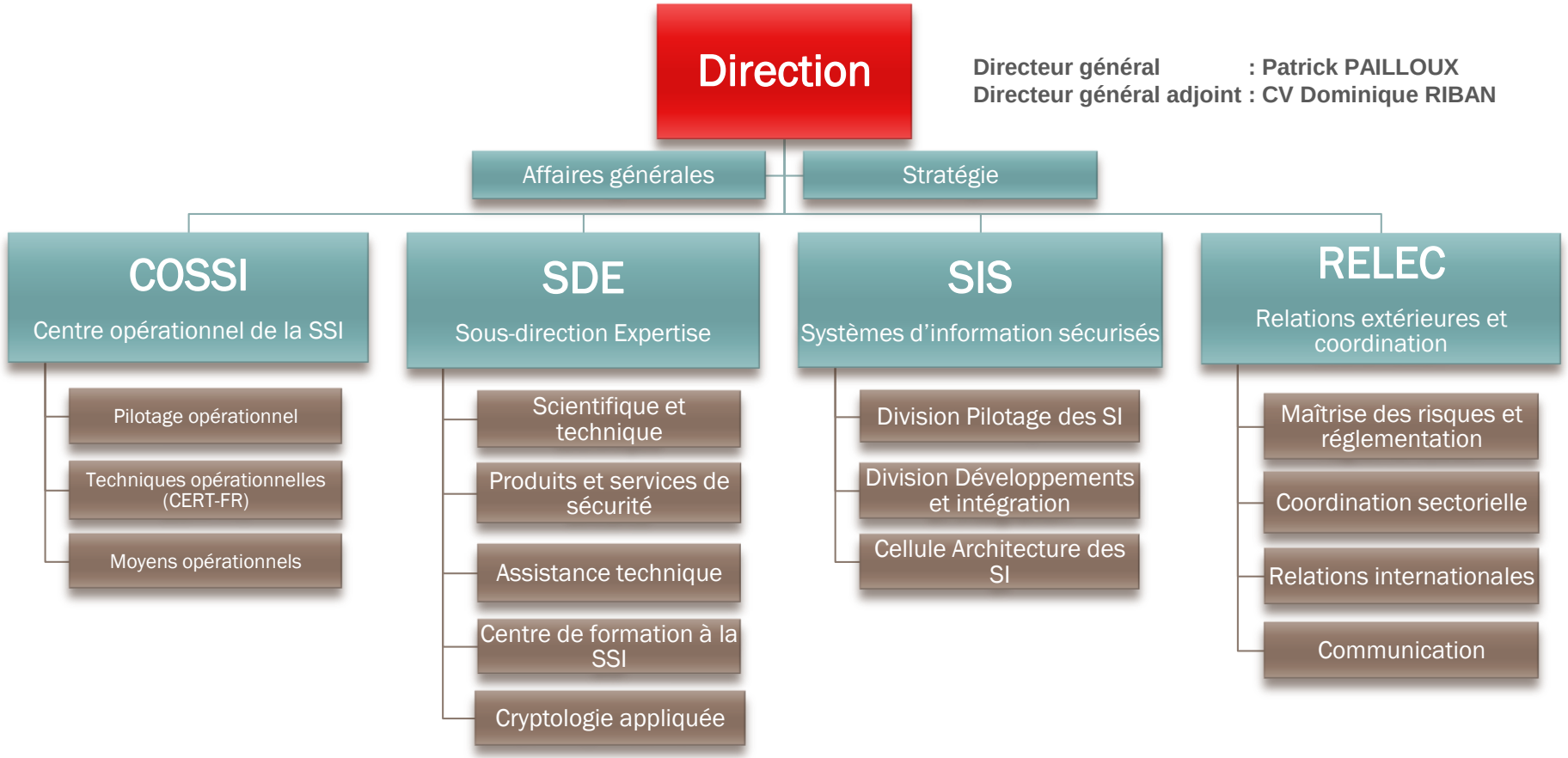
Prise en compte des infrastructures vitales

- soutenir les opérateurs d'infrastructures vitales dans l'amélioration de leur niveau de sécurité
- vérifier par des audits le niveau de protection

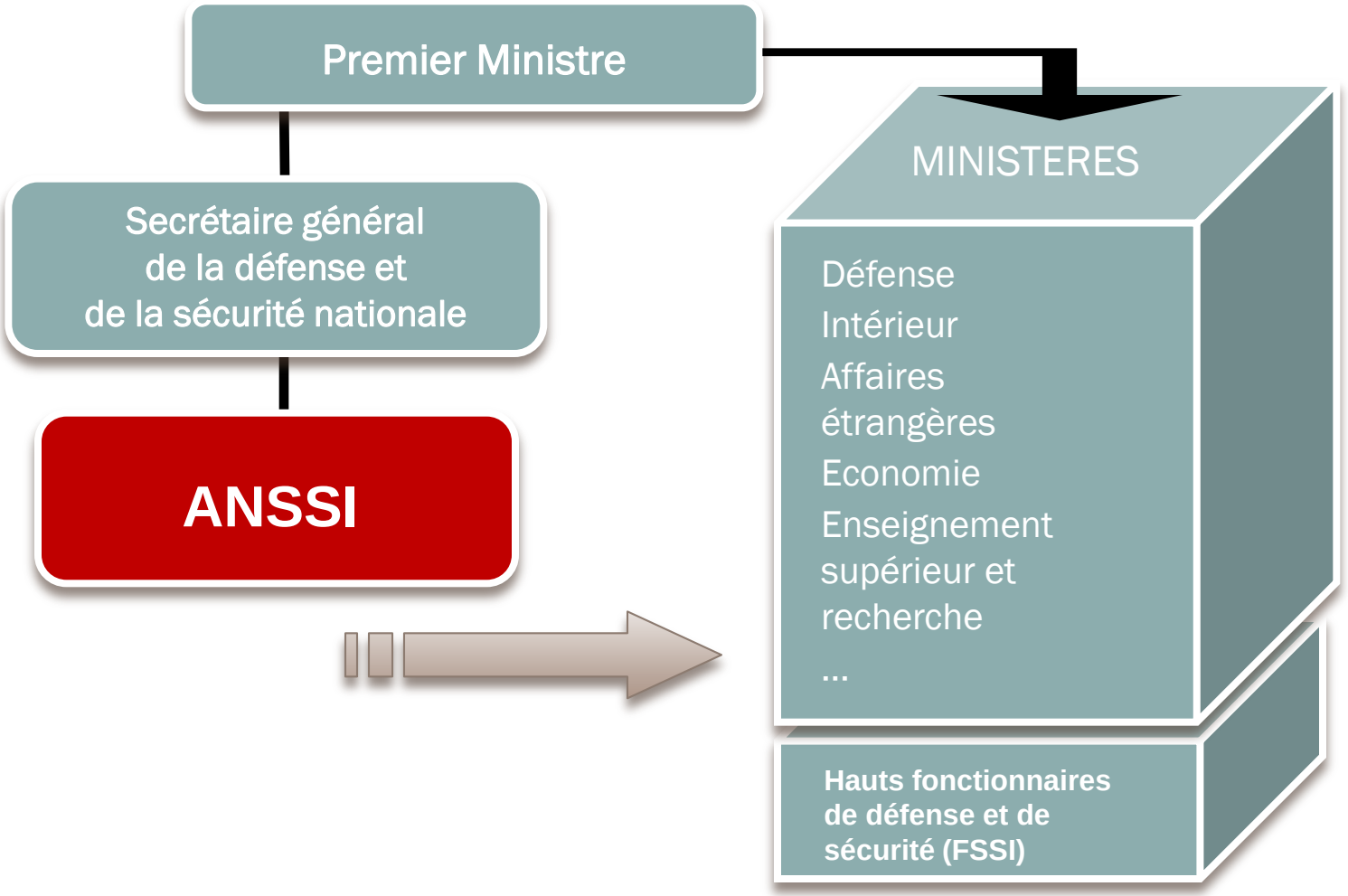
Résilience et internet

- l'Internet est une infrastructure vitale
- améliorer la résilience des SI est une priorité

ORGANISATION DE L'ANSSI



POSITION INTERMINISTÉRIELLE



OBSERVATOIRES ZONAUX DE LA SSI

- Le livre blanc a souligné l'importance de disposer de relais sur l'ensemble du territoire pour **sensibiliser les principaux acteurs de la société de l'information et diffuser les mesures de protection préparées par l'ANSSI.**

- Un réseau territorial d'experts a donc été mis en place au sein **d'observatoires zonaux (OZSSI) placés auprès des préfets de zone.**