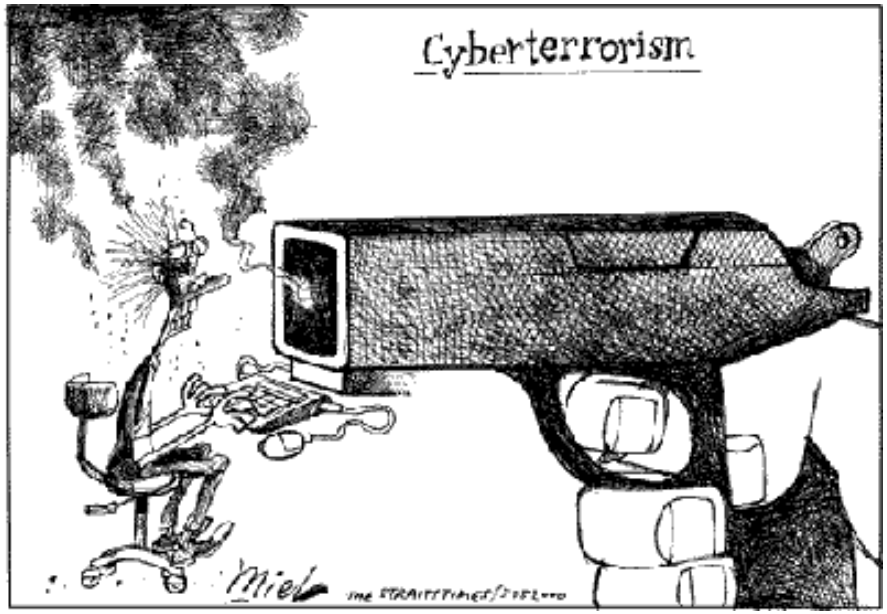
Cyber-terrorisme

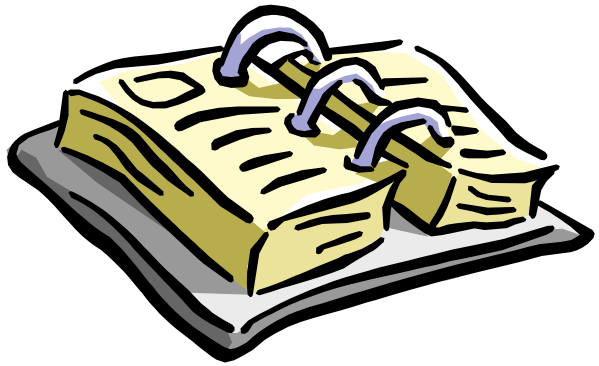
Mythe ou réalité ?



Patrick CHAMBET http://www.chambet.com
EdelWeb http://www.edelweb.fr

Planning

- Généralités
  - Qu'est-ce que le cyber-terrorisme ?
  - Qui sont les cyber-terroristes ?
  - Historique
- Cibles et moyens
  - Cibles et impacts potentiels
  - Les armes des cyber-terroristes
  - Communications, recrutement et formation
- Principes de défense
- Conclusion



Généralités (1/4)

- **Définitions**
  - **Convergence entre le terrorisme traditionnel et les réseaux**
  - **« Action délibérée de destruction, dégradation ou modification de données, de flux d'informations ou de systèmes informatiques vitaux d'Etats ou d'entreprises cruciales au bon fonctionnement d'un pays, dans un but de dommages et/ou de retentissement maximum afin de susciter la peur, pour des raisons politiques, religieuses ou idéologiques »**

Généralités (2/4)

- **Paradoxe du cyber-terrorisme**
  - **Il préoccupe, mais aucune action de grande ampleur avec impact stratégique majeur n'a encore eu lieu**
- **La peur est le mot clé**
  - **Un cyber-attentat peut causer le même choc sur une population que l'explosion d'une bombe**
  - **Une attaque qui couperait l'électricité pendant plusieurs jours ou détruirait les données de la Bourse aurait un tel effet**
- **Attentat conventionnel et attaque informatique combinés**
  - **Amplificateur d'effets**
  - **Réciprocité des effets**

Généralités (3/4)

- **Différences par rapport aux autres phénomènes numériques**
  - **Cyber-crime**
    - **Objectif purement crapuleux**
  - **« Hacktivism »**
    - **Simples messages idéologiques ou politiques**
  - **Cyber-combat (guerre numérique)**
    - **Caractère militaire des cibles**

Généralités (4/4)

- **Avantages du cyber-terrorisme**
  - **Coût d'accès réduit**
  - **Pas de présence physique localement**
  - **Impacts importants à l'aide de moyens faibles**
  - **Effet boule de neige (attentat et attaque informatique combinés)**
  - **Large couverture par les médias (sujet « à la mode »)**
  - **Fierté de montrer sa capacité à effectuer des actes « high tech »**
  - **Attaque des pays « développés » par leur point faible**
  - **Moindre vulnérabilité des pays émergents**

Qui sont les cyber-terroristes ?

- **Trois grands types**
  - **Sous-groupes de groupes terroristes traditionnels**
  - **Sympathisants de groupes terroristes et hackers « patriotes »**
  - **Etats**

Qui sont les cyber-terroristes ?

Le Tchétchène Shamil Basayev (photo : kavkazcenter.com)

Historique (1/2)

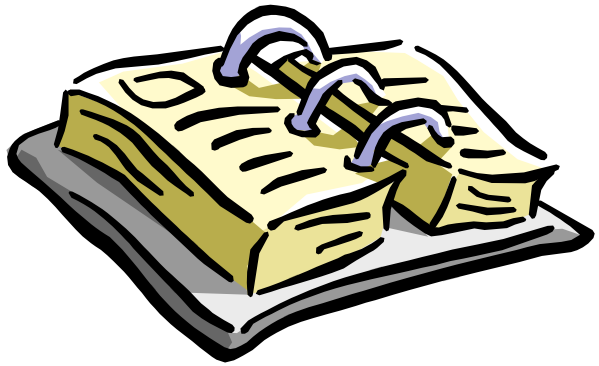
- 1996
  - Première « promesse » de cyber-terrorisme aux USA par un militant raciste
- 1997
  - Attaque du gouvernement mexicain par les zapatistes
  - Plantage du contrôle aérien à l'aéroport de Worcester (USA)
- 1998
  - Attaque d'un ISP américain par des Espagnols anti-ETA
  - Attaque des ambassades sri-lankaises par la guerrilla tamoule
  - Détournement des appels au 911 aux USA
- 1999
  - Attaque des ordinateurs de l'OTAN par des sympathisants serbes
  - Attaque de sites gouvernementaux américains par des Chinois suite au bombardement de l'ambassade chinoise à Belgrade
- 2000
  - En Australie, un attaquant libère de l'eau polluée dans une rivière

Historique (2/2)

- **2001**
  - **Attaque d'un ordinateur d'une centrale électrique aux USA**
  - **Attaques réciproques (directes ou par vers/virus) entre la Chine et les USA suite au détournement d'un avion espion américain**
- **2002**
  - **Des documents retrouvés en Afghanistan montrent qu'Al Qaïda étudiait la faisabilité de cyber-attentats**
- **2003**
  - **Lors de la panne de courant générale aux USA et au Canada, une étude du rôle suspecté de certains vers/virus dans le déroulement de la panne a été effectuée**
- **2004**
  - **Lors d'une conférence aux USA, présentation d'une étude des attaques informatiques ayant eu lieu en permanence entre Israël et la Palestine**

Planning

- Généralités
  - Qu'est-ce que le cyber-terrorisme ?
  - Qui sont les cyber-terroristes ?
  - Historique
- Cibles et moyens
  - Cibles et impacts potentiels
  - Les armes des cyber-terroristes
  - Communications, recrutement et formation
- Principes de défense
- Conclusion



Cibles (1/2)

- **Installations de gestion des télécommunications**
  - **Centraux téléphoniques, bornes GSM**
  - **Réseaux filaires, relais hertziens et satellites**
- **Sites de génération et de distribution d'énergie**
  - **Centrales nucléaires, thermiques**
  - **Sites de régulation EDF**
- **Transports**
  - **Aéroports (*avions !*), ports, contrôle aérien et maritime**
  - **Gares ferroviaires et routières, autoroutes**
  - **Systèmes de régulation des feux rouges des grandes villes**
- **Installations de raffinage, stockage et distribution de produits pétroliers**
- **Centres de gestion du courrier postal**
- **Sites de production, stockage et distribution d'eau**

Cibles (2/2)

- **Institutions financières et bancaires**
  - **Bourses nationales, réseau SWIFT**
  - **Home banking, réseaux de distributeurs de billets**
- **Services d'urgence, de santé et de sécurité publique**
  - **Police, pompiers, SAMU, hôpitaux**
- **Services gouvernementaux**
  - **Sécurité sociale, assurance maladie**
  - **Sites institutionnels, sites de défense**
- **Médias**
  - **Chaînes de télévision, groupes de presse**
  - **Fournisseurs de contenus divers**
- **Eléments symboliques d'une société**
  - **Grande distribution, industries représentatives, ...**

Impacts potentiels

- **Attaques combinées sur plusieurs cibles simultanément**
- **Attaques concomitantes d'événements politiques ou militaires**
- **Impacts**
  - **Economiques**
  - **Sociaux**
  - **Environnementaux**
  - **Vitaux**

Quelques scénarios (1/4)

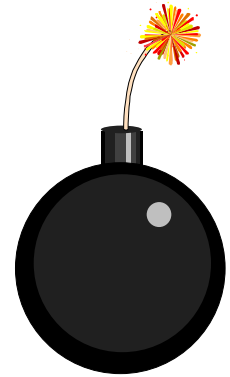
Aéroport d'Orly

Quelques scénarios (2/4)

Quelques scénarios (3/4)

Quelques scénarios (4/4)

Les armes des cyber-terroristes



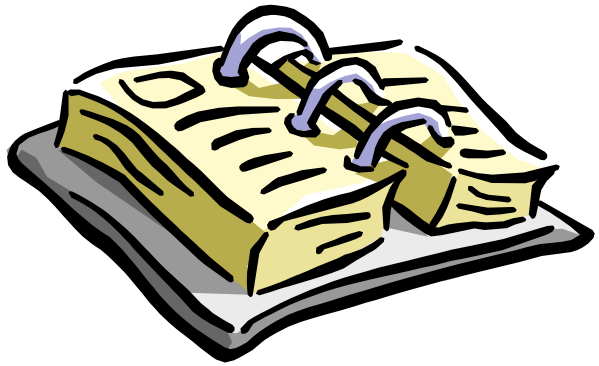
- Armes logiques (“cyber-armes”)
  - Défiguration de sites Web et "attaques sémantiques"
  - Dénis de service simples (DoS) ou distribués (DDoS)
  - Attaques de l’infrastructure d’Internet (DNS, routeurs)
  - Vers / virus
  - Intrusions classiques
  - Modification furtive de données
  - Implantation de bombes logiques internes
- Si possible, perturber autant que possible le fonctionnement des opérations de riposte (militaires ou autres)
- Mais une fois utilisés et leurs techniques révélées, les outils d’attaque ne sont plus très utiles

Communications, recrutement, formation

- Utilisation intensive d'Internet
  - Sites Web de propagande et de vente (cassettes vidéo de propagande)
  - Listes de diffusion
  - IRC
- Multiplication des cyber-cafés dans le monde entier
- Communications noyées dans la masse
  - Trafic licite
  - Sans même besoin de chiffrement et/ou de stéganographie
  - Efficacité de Carnivore ?

Planning

- Généralités
  - Qu'est-ce que le cyber-terrorisme ?
  - Qui sont les cyber-terroristes ?
  - Historique
- Cibles et moyens
  - Cibles et impacts potentiels
  - Les armes des cyber-terroristes
  - Communications, recrutement et formation
- Principes de défense
- Conclusion



Recommandations

- Maintenir un état de vigilance élevé
- Effectuer ou faire effectuer une veille technique
- Mettre à jour les systèmes d'exploitation et les applications
- Minimiser le nombre de services offerts sur les serveurs
- Sécuriser les configurations
  - Mots de passe, principe du moindre privilège
- Mettre en place un filtrage d'accès
  - En entrée, mais aussi en sortie
- Installer des anti-virus et les mettre à jour très souvent
- Activer les systèmes de journalisation, centraliser, analyser et sauvegarder les logs régulièrement
- Effectuer des sauvegardes régulières
- Faire procéder à des tests d'intrusion

Conclusion (1/2)

- **Bien qu'aucune action de grande ampleur n'ait vraiment eu lieu, la probabilité d'un cyber-attentat est de plus en plus préoccupante**
  - **DDoSNets de plus en plus élaborés**
  - **Vers de plus en plus intelligents**
  - **Frappes physiques de plus en plus menées en parallèle avec des frappes logiques**
- **Mais la menace est plus facile à contrer qu'un attentat conventionnel**
- **Il est important de s'y préparer et d'évaluer les vulnérabilités *réelles***

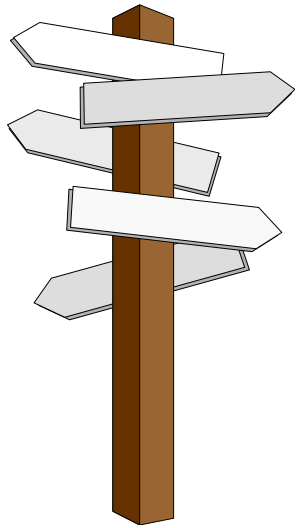
Conclusion (2/2)

- La sécurité doit être appréhendée de manière globale
  - Sécurité organisationnelle
  - Sécurité technique (physique, logique)
  - Évolution de la sécurité vers la défense en profondeur des SI

- L'Europe a commencé à réagir
  - Projet de Cyber Security Task Force
  - Etude des vulnérabilités de notre société de l'information par la Rand Corporation Europe
  - Objectivité de ce cabinet américain ?

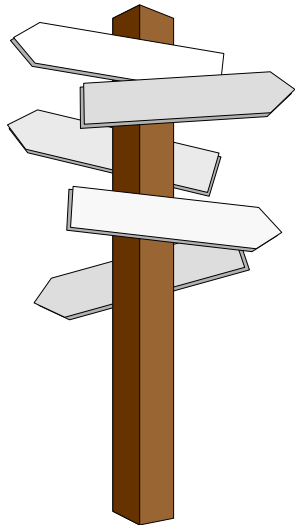
Pour aller plus loin… (1/2)

- http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
- http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm
- http://www.terrorisme.net/lecture/2002/008_cyberterror_dunnigan.htm
- http://www.terrorisme.net/info/2002/025_cyberterrorism.htm
- http://www.geopolitis.net/geopol/geo/article/pouvoirs/arti1026492623aaacRpjhYXuF-Jhn.html
- http://www.defense.gouv.fr/das/etudes/etude/infoguerre/synthese.htm



Pour aller plus loin… (2/2)

- **Cyber Jihad and the Globalization of Warfare: Computer Networks as a Battle Ground in the Middle East and Beyond (Conférence BlackHat USA 2004)**
  - **http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-geers.pdf**
- **Propagande**
  - **http://www.tibyan.net/home.asp**
  - **http://www.faharis.net/fatwa.shtml**
- ***MISC* (premier journal technique français sur la sécurité des SI)**
  - **http://www.miscmag.com**
  - **Le cyber-terrorisme http://www.chambet.com/publications/Cyberterrorisme.pdf**



Questions