

Club des Vigilants

Pour apprivoiser l'avenir



Cyberguerre en Estonie

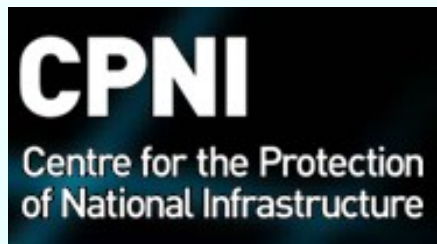
[http:// bruno . kerouanton . net](http://bruno.kerouanton.net)

Rump Session SSTIC 2007
31 mai - Rennes, France

Protection des infrastructures critiques nationales



Quelques exemples :



Royaume-Uni : **CNPI**
(Centre for the Protection of National Infrastructure)

USA : **NIAC**
(National Infrastructure Advisory Concil). Department of Homeland Security.



Canada : **NCIAP**
(National Critical Infrastructure Assurance Program).



Club des Vigilants

POUR APPRIVOISER L'AVENIR



Cyberguerre



27 avril 2007 : Incident majeur entre Estonie et Russie

L'Estonie déplace une statue commémorative russe.

Réaction négative du Kremlin

Début d'émeutes à Tallin :

- ➔ 1 mort
- ➔ 150 blessés
- ➔ Près de 1000 arrestations

Début de la **première Cyberguerre « officielle »**



Attaques par Déni de Service Distribué (botnets) contre l'Estonie :

Vise exclusivement :

- ➔ Sites gouvernementaux et publics,
- ➔ Banques, média (presse, télévision, etc.)

(Sources : International Herald Tribune, AFP)



Club des Vigilants

POUR APPRIVOISER L'AVENIR



Cyberguerre



27 avril 2007 à 15h00

⇒ Sites indisponibles :

- Gouvernement (www.valitsus.ee)
- Premier ministre (www.peaminister.ee)
- Parlement (www.riigikogu.ee)
- Ministère des Communications et de l'Economie (www.mkm.ee)
- Ministère des Affaires Etrangères (www.vm.ee)
- Ministère de l'Intérieur (www.sisemin.gov.ee)

⇒ Sites disponibles

- Ministère des Finances (www.fin.ee)
- Ministère de la Justice (www.just.ee)
- Ministère des affaires sociales (www.sm.ee)
- Ministère de l'Environnement (www.envir.ee)
- Ministère de l'Agriculture (www.agri.ee)
- Ministère de la culture (www.kul.ee)
- Ministère de la Défense (www.mod.gov.ee)

(Source : blog F-Secure)



Club des Vigilants

POUR APPRIVOISER L'AVENIR



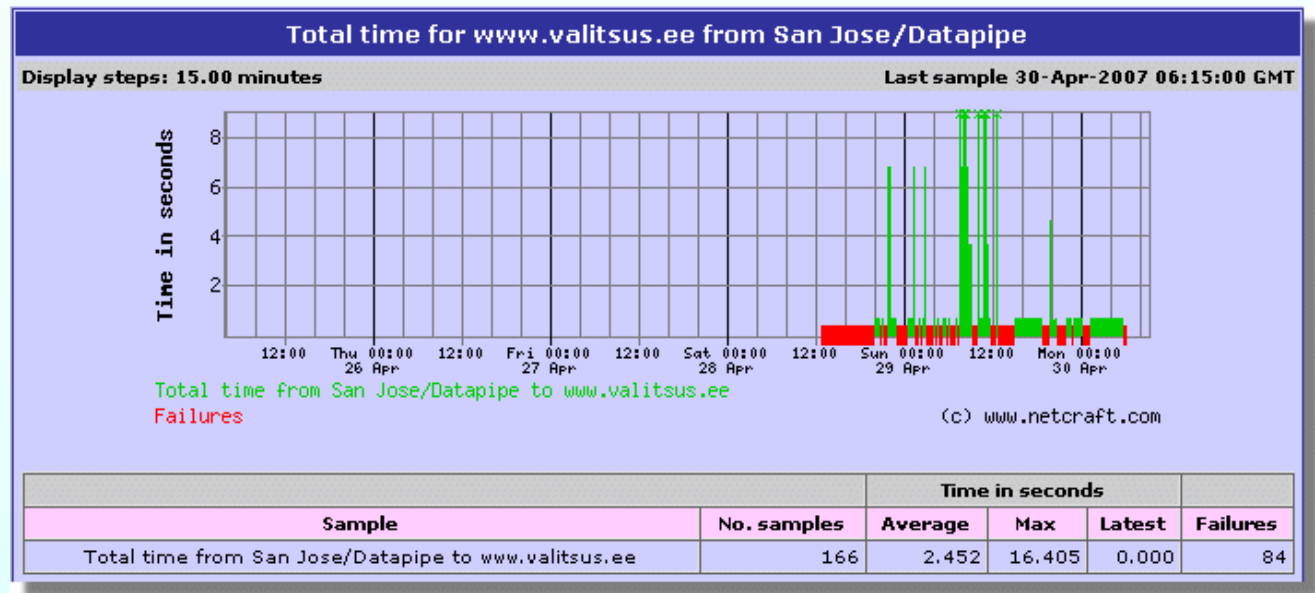
Cyberguerre



30 avril 2007 à 06h00

Le site du gouvernement
est bien mal !

Uptime
(source NetCraft) :



Mode crise :

- Passage en mode allégé des sites principaux,
- Utilisation du mode texte,
- HTML simple, sans images.

(Source : Blog F-Secure)



Club des Vigilants

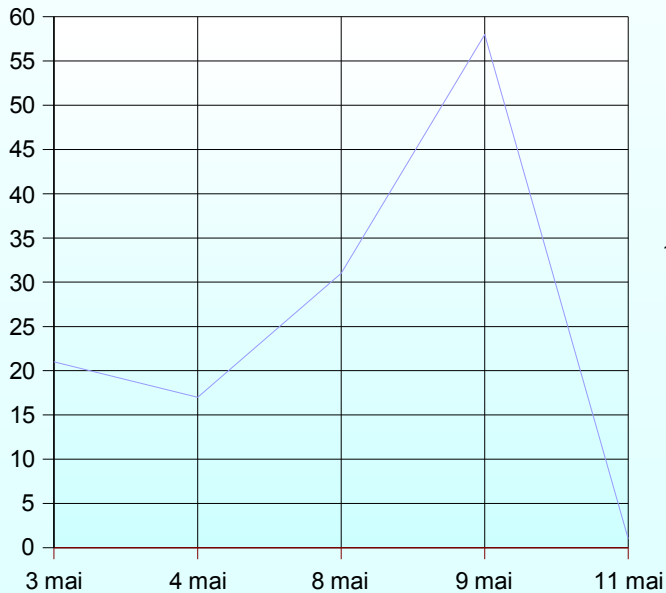
POUR APPRIVOISER L'AVENIR



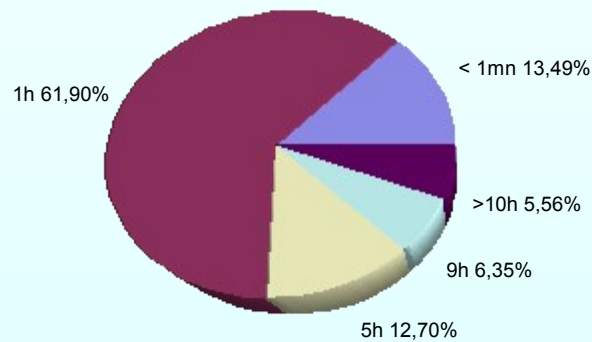
Cyberguerre



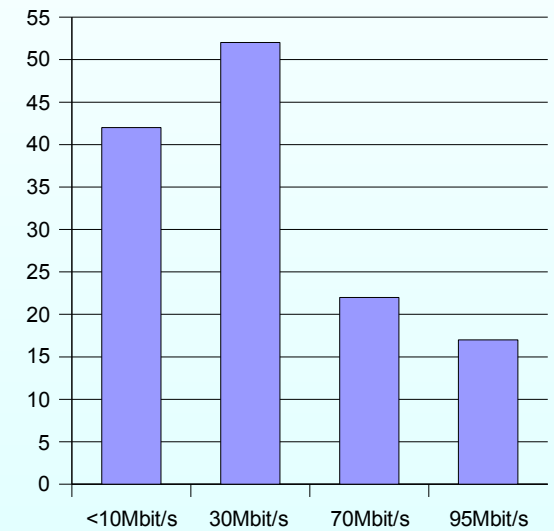
Nombre d'attaques



Durée des attaques



saturation Bande passante



Environ 120 attaques ciblées en 2 semaines,

dont 10 attaques dépassant les 90Mbit/s et d'une durée de près de 10 heures !

(Source : blog Arbor Networks)



Club des Vigilants

POUR APPRIVOISER L'AVENIR



Cyberguerre



9 mai 2007 : Arrestation d'un pirate de 19 ans

10 mai 2007 : Communiqué de TERENA et des TF-CSIRT :

- ➔ « Les CSIRT ont commencé à défendre l'espace internet gouvernemental et public de l'Estonie depuis le 3 mai, à la demande du CERT-EE estonien. »



13 mai 2007 : 13 prix Nobel soutiennent l'Estonie



18 mai 2007 : L'OTAN s'indigne.
Sollicitation par l'Estonie.
L'OTAN fournit son aide technologique
Le service NCSA (Cybercriminalité) enquête.

Plusieurs enquêtes en cours :

- ➔ Union Européenne
- ➔ OTAN
- ➔ Organismes privés, et CERTs

(Sources : terena.org, nato.org, europarl.europa.eu)



Club des Vigilants

POUR APPRIVOISER L'AVENIR



Cyberguerre



Forces offensives gouvernementales dans le monde :

USA : Donald Rumsfeld a admis l'existence d'une force offensive US en 2005
Barksdale Air Force Base, Louisiane : dédié guerre électronique et cyberguerre

Chine : Bataillons dédiés cyberguerre. Attaques vers Taïwan.
Le Pentagone vient de publier un rapport à ce sujet.

Russie : Attaques vers l'Estonie en mai 2007.

OTAN : Ouverture possible d'un centre de cyberdéfense en 2008

Et les autres pays ?

**Certainement en place
ou en cours de déploiement...**



(Sources : Financial Times, TechNews, CNN)



Club des Vigilants

POUR APPRIVOISER L'AVENIR



Club des Vigilants

Pour apprivoiser l'avenir



[http:// bruno . kerouanton . net](http://bruno.kerouanton.net)

Rump Session SSTIC 2007
31 mai - Rennes, France