



CENTRE NATIONAL  
DE LA RECHERCHE  
SCIENTIFIQUE



**8° JOURNEES**  
**« CRYPTOGRAPHIE ET SECURITE DE L'INFORMATION »**  
**LIMOGES – 8 Février 2008 -**

# La Guerre de l'Information

Daniel Ventre

- CNRS -  
- *Chargé de cours à l'ENST Paris* -

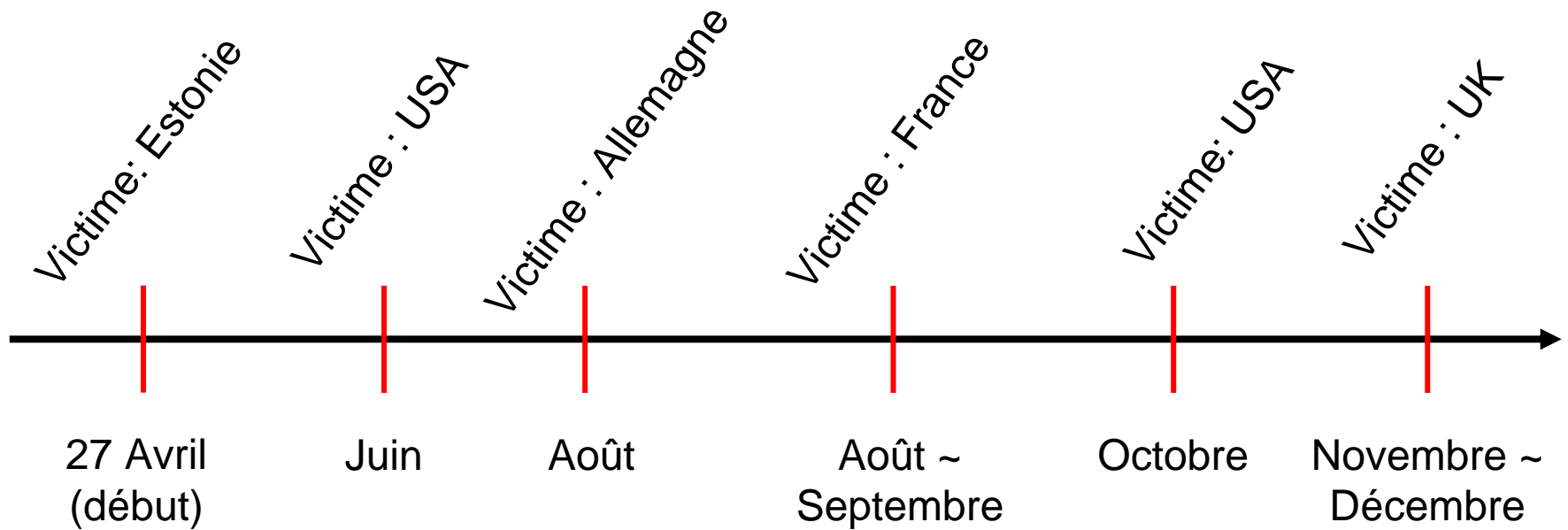
[daniel.ventre@gern-cnrs.com](mailto:daniel.ventre@gern-cnrs.com)

Blog : <http://infowar.romandie.com>

- ❑ 2007: série de cyber attaques
- ❑ Définir la guerre de l'information
- ❑ Cybercriminalité et Guerre de l'Information

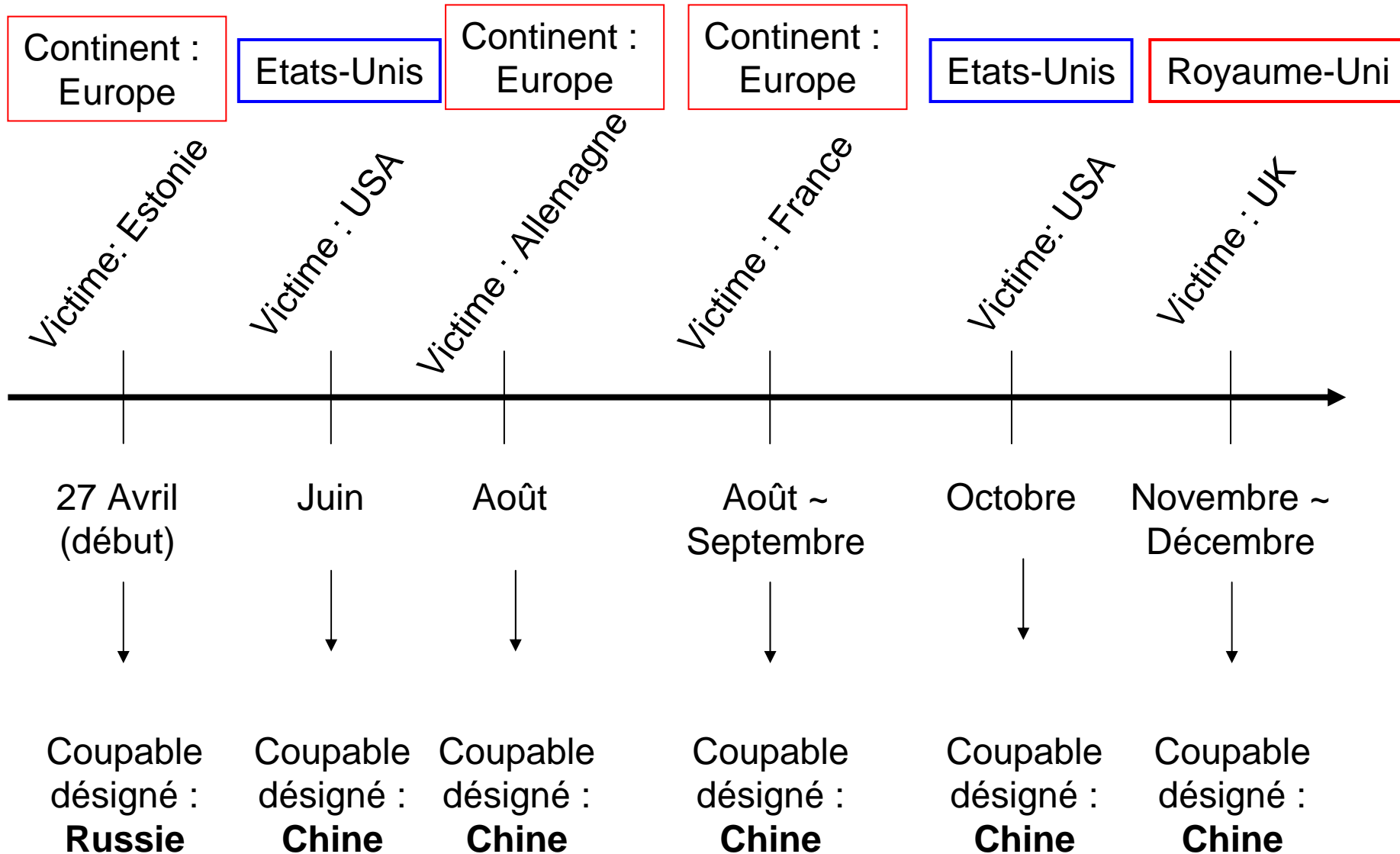
# I – LES EVENEMENTS DE 2007

# Quelques unes des cyber-attaques de 2007



# Les cyber-attaques 2007 : caractéristiques

## Une logique de « blocs » ?



# Les cyber-attaques 2007 : caractéristiques

## 1 - Une logique de « blocs » ?

**Bloc A = Victimes = Etats-Unis, Europe occidentale**

**Bloc B = Agressors désignés par A = Russie, Chine**

# Les CNA de 2007 : caractéristiques – dimension psychologique, réactions

## 2 – La nature des accusations

→ Le Royaume-Uni, la France, les Etats-Unis, l'Allemagne parlent **d'espionnage**

→ L'Estonie parle de **tentative de déstabilisation du pays, de paralysie de ses systèmes, d'acte de guerre...**

**→ Tout autant que les CNA, les accusations sont de nature à tendre les relations diplomatiques**

# Les CNA de 2007 : caractéristiques – dimension psychologique, réactions

## 4 - Image de fébrilité, fragilité, vulnérabilité

- CNA, pas vraiment des surprises : on s'y attend toujours.
- Pourtant les CNA sont toujours présentées comme une surprise!
- Les systèmes de sécurité et les experts apparaissent toujours dépassés, pris au dépourvu, en flagrant délit d'impuissance!
- Sauve qui peut! Face à des agressions « coordonnées », massives (Botnets, DDoS)
- **Aveux d'impuissance, constat de fragilité**
- **Aveux à la face du monde!**
- **Image de désordre, de panique à bord, de sauve qui peut**
- **les vrais agresseurs doivent jubiler!**

# Les CNA de 2007 : caractéristiques – dimension psychologique, réactions

## 5 - Effet de surprise: crédible?

- Avant 2007, des CNA partout dans le monde
- Des CNA sous des formes diverses
- Des CNA d'envergure variable
- Des CNA sur des cibles de nature diverse
- Des CNA avec des motifs multiples
- Des CNA utilisées par des acteurs de nature différente : militaires, hacktivistes, renseignement, etc.

# Des antécédents nombreux: Avant 2007...

Etats-Unis

Etats-Unis

*Moonlight Maze*

*Titan Rain*

1999 :  
série  
d'attaques  
qui dura 2  
ans

Traces  
remontent  
à Moscou

Séries  
d'attaques  
ayant débuté  
en 2003

Enquête en  
cours.  
Pas de  
résultats  
définitifs

**Même si CNA  
de nature  
différente à  
2007, les  
possibilités  
sont connues**

# Les CNA de 2007 : caractéristiques – dimension psychologique, réactions

## 6 – Impression de flou, absence de maîtrise

- Impossibilité de déterminer l'origine exacte des agressions
- Impossibilité d'identifier les coupables
- Impossibilité de faire valoir ses droits et obtenir réparation
- Difficulté à mesurer l'ampleur réelle des dommages
- Absence de maîtrise de la dimension temps : quand les agressions ont-elles réellement commencé? Quand s'arrêteront-elles?
- Seul argument évoqué par les victimes : les attaques sont « coordonnées ». Par qui, comment ...? Aucune précision, aucune certitude
- Flou verbal : uniquement des hypothèses, pas de preuves

# Les CNA de 2007 : caractéristiques – dimension psychologique, réactions

## 6 – Le degré d'expression

- Des hypothèses
- Présentées comme des certitudes
- vocabulaire: attaques, armées, espionnage...
- allégations, accusations

# Les CNA de 2007 : caractéristiques – dimension psychologique, réactions

## Des agressions bénéfiques pour les victimes?

- Apprendre à mieux se connaître
- identifier ses propres failles
- mieux connaître le potentiel des agresseurs
- mieux connaître le domaine des possibles
- utiliser les agressions comme prétextes (politiques, économiques, stratégiques, commerciaux...)
- profiter du désordre ambiant pour mener ses propres opérations d'information?

# II – DEFINIR LA GUERRE DE L'INFORMATION

# Définir la GI

→ Actes de 2007 : GI ?

→ GI = **comment utiliser de manière optimale l'information et les systèmes d'information, pour dominer/vaincre un adversaire (militaire, politique, économique, idéologique...)**

→ GI = **opérations conduites en temps de paix, de crise, de guerre, pour défendre sa propre information et ses propres SI, et/ou attaquer l'information / les SI de l'adversaire.**

→ Objet = lutte pour la dominance de l'espace informationnel

→ Armes : information / systèmes d'information, sans distinction de genre (militaire, civil)

# Les composantes de la GI

Doctrine américaine. 2001. Imbrication des concepts

**Opérations d'information** = actions pour affecter l'information et les systèmes d'information adverses, en tous temps (paix, crise, guerre) à tous les niveaux (stratégique, opérationnel, tactique)

**Guerre de l'information** = opération d'information menées uniquement en temps de crise ou de guerre

## Opérations offensives

- Psyops
- Déception militaire
- Guerre électronique
- Destruction physique
- Cyber attaques, guerre des pirates (CNA)

## Opérations défensives

- OPSEC
- Sécurité physique
- Contre déception
- Contre propagande
- Contre intelligence
- ...

**Chaque composante peut être utilisée à la fois de manière défensive et offensive**

# Objectifs des opérations de GI

- Déstabiliser un adversaire, temporairement ou durablement
- Affaiblir
- Paralyser
- Observer son adversaire
- Modifier le comportement
- Altérer le processus de décision
- Isoler, couper du reste du monde
- Dominer l'espace informationnel
- Prendre l'avantage dans la boucle OODA
- Voir au-delà de l'horizon
- Lever le flou de l'espace du champ de bataille
- Gagner sans combattre
- Combat sans contact

# Les acteurs de la GI

- Les Etats
  - L'armée
  - Groupes structurés
  - Individus isolés
  - Simples « pirates » informatiques
- 
- Motivation politique
  - Motivation idéologique
  - Motivation économique
  - Activistes, partisans, révolutionnaires, terroristes
  - ...etc.

# La dimension temporelle

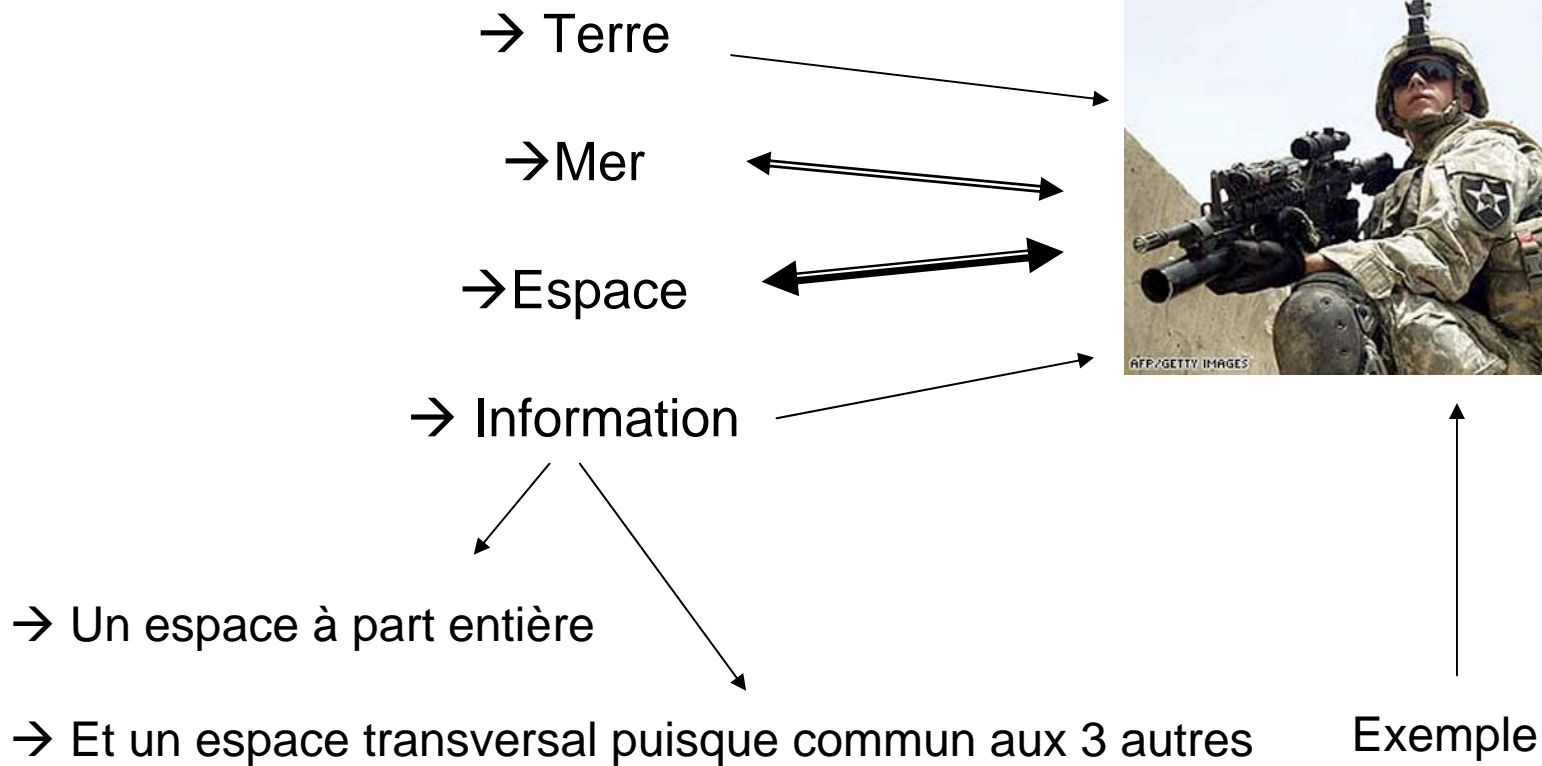
→ En temps de paix (la doctrine américaine parle d'opérations d'information, en temps de paix. La notion de GI s'appliquerait seulement aux opérations menées en temps de crise et conflit)

→ En temps de crise

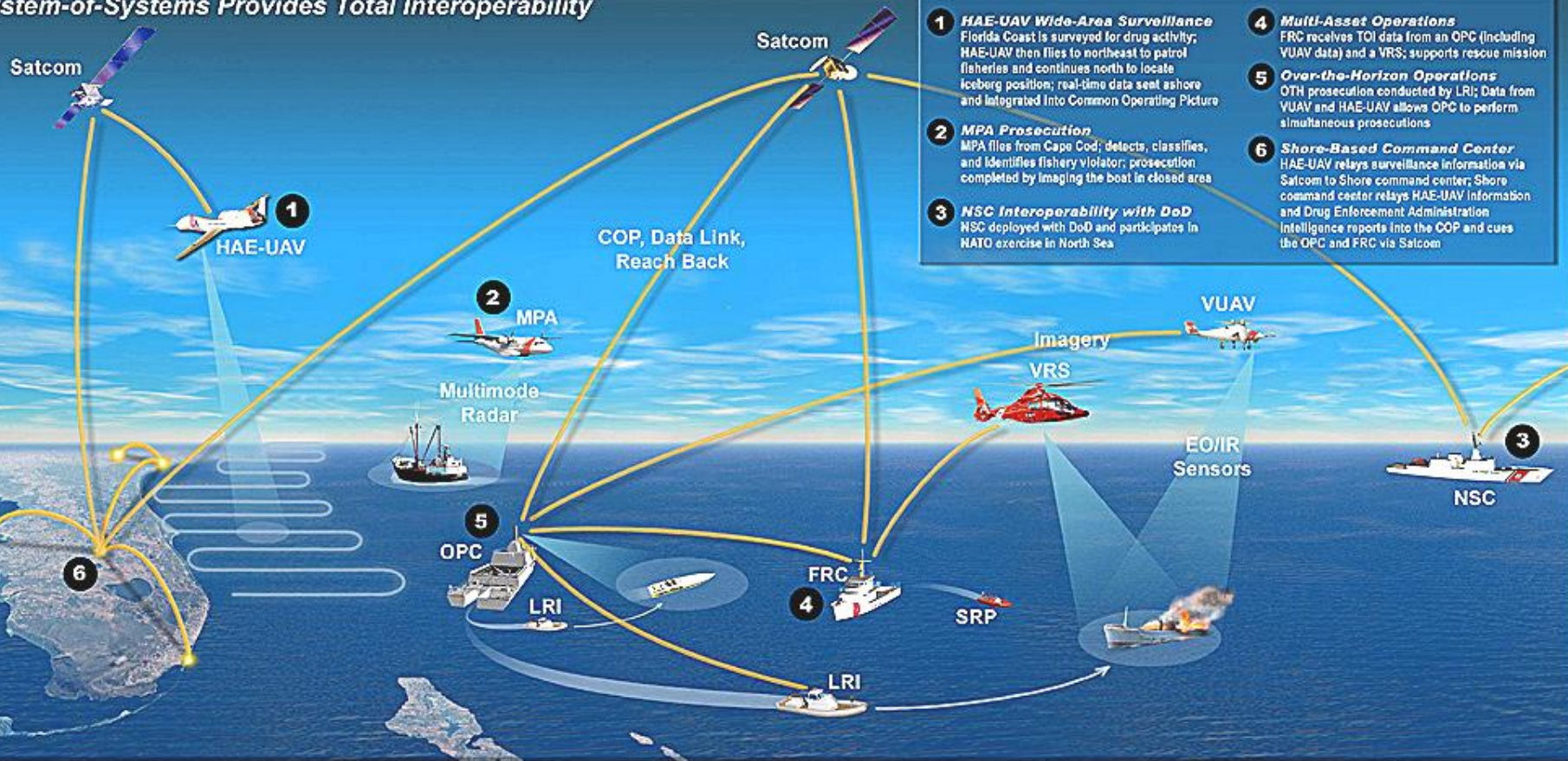
→ En temps de guerre

Plus de frontière temporelle

# La 4° dimension du combat



## System-of-Systems Provides Total Interoperability



Source : [http://www.defesabr.com/Mb/USCG\\_Deepwater\\_C4ISR.jpg](http://www.defesabr.com/Mb/USCG_Deepwater_C4ISR.jpg)

III – VAGUES D'AGRESSION  
2007:

CYBERCRIMINALITE

OU

ACTES DE GUERRE / USAGE DE  
LA FORCE?

## Cyber criminalité =

→ Contrefaçon sur internet

→ Contenus illicites (pédophilie...)

→ « hacking », intrusion dans les SI, intrusion et altération des données, vol de données, défiguration de site, propagation de virus, etc)

→ Fraude (spam, phishing, scam nigérian, usurpation d'identité, ...)

→ Droit pénal, droit civil, convention européenne contre la cyber criminalité, coopération judiciaire européenne/internationale

Mais :

**Quand l'armée d'un Etat A lance une attaque par réseaux d'ordinateur contre les SI d'un Etat B...**

→ Même si l'acte est commis par et contre les SI

→ Même si les techniques et méthodes sont les mêmes (vol de données, DoS, DDoS, défiguration de sites, intrusions...)

**→ on ne peut pas parler simplement de « cyber criminalité »**

## Agression de l'Etat A contre l'Etat B

- Dimension politique
- Dimension diplomatique
- Dimension stratégique
- Dimension juridique
- Dimension militaire

Faire distinction entre « cyber crime » et « acte de guerre / usage de la force »

- Permet d'adapter la réponse, la réaction immédiate
- Permet d'adapter son positionnement international
- Permet d'adapter les modalités de sa propre sécurité

Mais la distinction ne sera pas toujours aisée :

→ Parce que les techniques / technologies sont les mêmes

→ Parce que les cibles peuvent être les mêmes

→ Parce qu'un délit de « cyber criminalité » peut préparer, soutenir, un acte de guerre

→ Parce que le « cyber criminel » peut être le bras armé de la guerre

→ La cybercriminalité peut être mise au service de la GI

- elle peut contribuer à la déstabilisation de la cible (déstabiliser un pays, son économie, le fonctionnement de ses réseaux...)

Distinction importante d'un point de vue juridique

→ Principe fondamental du droit international : interdiction du recours à la force

**Charte des Nations Unies = définit le cadre légal du recours à la force (« jus ad bellum »)**

# Charte des Nations Unies

## Article 2(4)

Principe : Interdit le recours à la force contre l'intégrité territoriale, l'indépendance politique d'un Etat

Exceptions : recours à la force autorisé dans 2 cas :

- Article 42
- article 51

## Article 42

Sur mandat du Conseil de Sécurité, recours à la force peut être autorisé

## Article 51

Droit de légitime défense contre toute attaque armée

## Article 39

Le Conseil de Sécurité a capacité à qualifier un événement de « menace à la paix, rupture de la paix, acte d'agression »

# Droit international : des interrogations complexes

→ Quelle est la définition du « recours à la force »?

→ Quelle est la définition de « attaque armée »? (attaque menée par des forces militaires traditionnelles?)

*\* Note : attaque armée > usage de la force*

→ Quels sont les critères qui permettent de qualifier un événement d'usage de la force ou d'attaque armée?

→ les moyens utilisés?

→ le niveau des dommages causés?

→ le nombre de victimes?

→ la qualité des auteurs (militaires, non militaires)?

→ à quel moment est-on en dessous ou en dessus du seuil « usage de la force »?

→ CNA = ???

→ 7 critères de Michael N. Schmitt : pertinents?

# CONCLUSION

## Revenons aux évènements de 2007

Quelle qualification?

Cybercriminalité?

Acte de guerre?

La qualification déterminera la réponse la mieux adaptée

Code Pénal,  
Convention européenne  
contre la cyber  
criminalité,  
Rôle des polices,  
enquêtes, recherche  
des délinquants,  
procès, sanctions, etc.

Jus ad Bellum, droit  
international, Charte  
des Nations Unies,  
légitime défense, etc.

## Revenons aux évènements de 2007

Quelle attitude adopter?

Répression?  
Réaction agressive?

Anticiper les prochaines agressions?

→ Sur un plan technique

→ Sur un plan juridique:  
comment le droit international peut-il encadrer efficacement ces actes?

Quelles leçons en tirer?

Démonstration faite de la fragilité des SI, de leur vulnérabilité

Démonstration faite de la faiblesse des systèmes de protection des SI

Revoir le concept même de sécurité? La gestion de l'information?  
Organiser le concept de « sécurité collective » (droit international)

# Quelques références bibliographiques

« *La guerre de l'information* ». Daniel Ventre. Edit. Hermès Lavoisier. Octobre 2007. ISBN 978-2-7462-1883-3

*Naissance et historique du concept*

*La GI aux Etats-Unis*

*La GI en Chine*

*La GI en Inde*

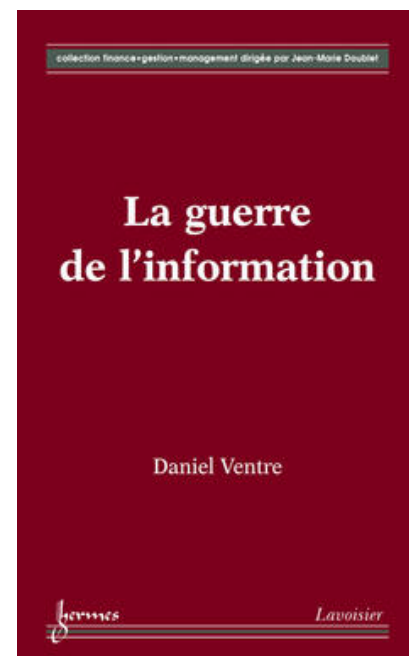
*La GI au Japon*

*La GI en Russie*

*La GI à Singapour*

*Identifier les actes de GI*

*Aspects juridiques de la GI*



Blog de l'auteur sur la guerre de l'information: <http://infowar.romandie.com>

# Quelques références bibliographiques

- *When is a Cyber Attack an « Armed Attack»? Legal Thresholds for Distinguishing Military Activities in Cyberspace.* Thomas C. Wingfield. February 1, 2006.
- *Joint Chiefs of Staff, Joint Pub. 1-02, Department of Defense Dictionary of Military and Related Terms.* April 2001.
- *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework.* Columbia Journal of Transnational Law 885, 900-923. Michael N. Schmitt. 1999.