Les délits informatiques, les lois les punissant et la pratique

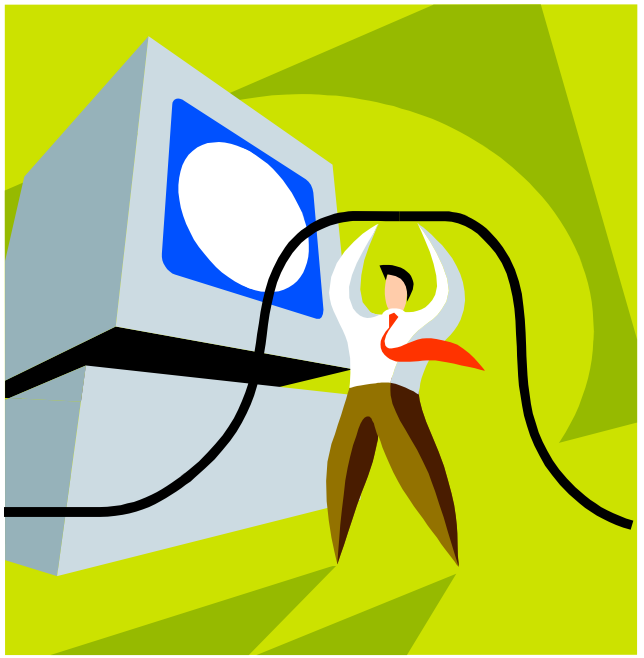
Atelier de l'Afrique de l'ouest sur les cadres politiques et réglementaires pour la cybersécurité et la protection de l'infrastructure de l'information critique (PIIC)

Praia, 27 - 29 novembre 2007

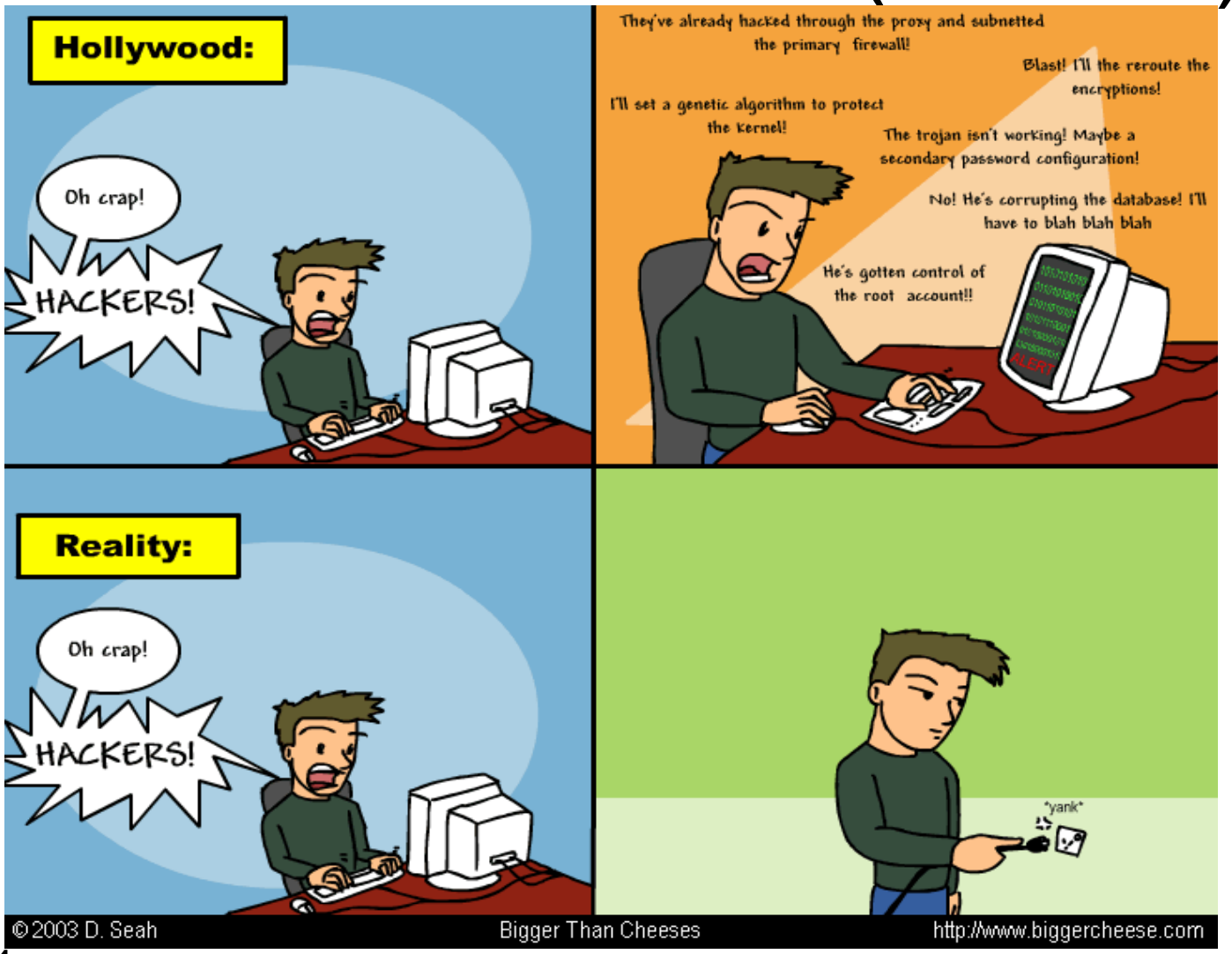
INDEX

I. INTRODUCTION

1. **Antécédents …**
   L'Internet et l'insécurité; la Vulnérabilité technologique (manque de ressources humaines compétentes chez les utilisateurs, les PME, la police, le législateur, les avocats et les juges)



I. INTRODUCTION (Suite…)



I. INTRODUCTION (Suite…)

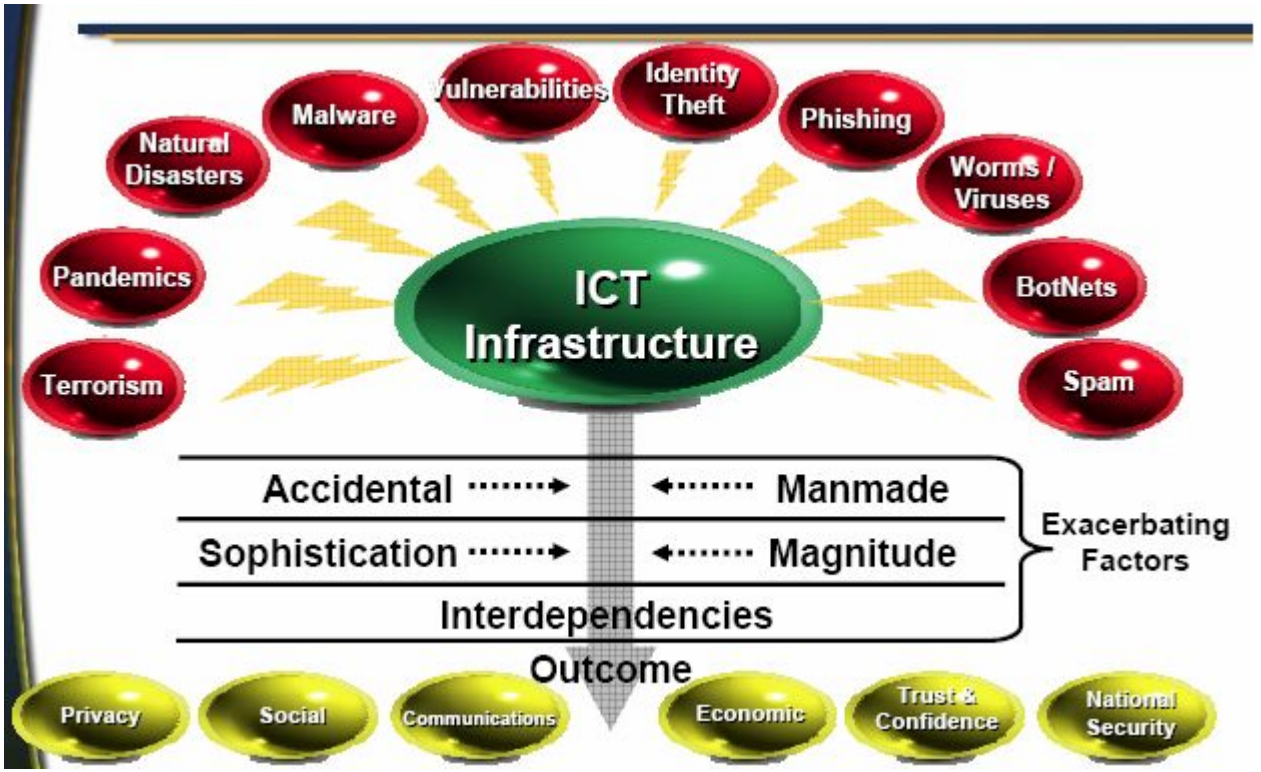
2.Actes criminels non pénalisés !

- Attaque DoS (refus de service)
- Phishing
- Hacking
- Cracking
- Data mining
- Pharming
- Pornographie de mineurs
- Violation du droit d'auteur
- Vol de données informatiques ou d'identité
- Fraude informatique
- Falsification, altération de données
- Sabotage informatique (à l'aide de virus, troyans, botnets, courriels spam, hoax)

I. INTRODUCTION (Suite…)

2.Actes criminels non pénalisés !

Évolution vers un environnement sécurisé:



McCrum, William, Deputy Director General, Telecom Engineering Industry Canada *"Challenges in Developing National Cyber Security Policy Frameworks"*, Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection. 28 August 2007

I. INTRODUCTION (Suite…)

3. Les stratégies privées pour sécuriser les réseaux informatiques.

I. INTRODUCTION (Suite…)

4. La participation de l'État dans la sécurité informatique.

Pouvoir exécutif (Plan d'action, Stratégie nationale),

Pouvoir législatif (La pénalisation des actes criminels, la création des délits informatiques)

Pouvoir judiciaire (création de la police « informatique », application des lois par les juges)

I. INTRODUCTION (Suite…)

5. **L'apport des organisations et de la communauté internationale**

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES

1. Les délits informatiques

1.1. Tentative de définition

1.2. Identification/définition des comportements considérés comme des délits informatiques.

1.3. Conclusions

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES

1. Les délits informatiques

1.1. Tentative de définition

Désaccord doctrinal sur la notion des délits informatiques

Exemple: “Délits commis à travers l’Internet et d’autres réseaux informatiques”

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES

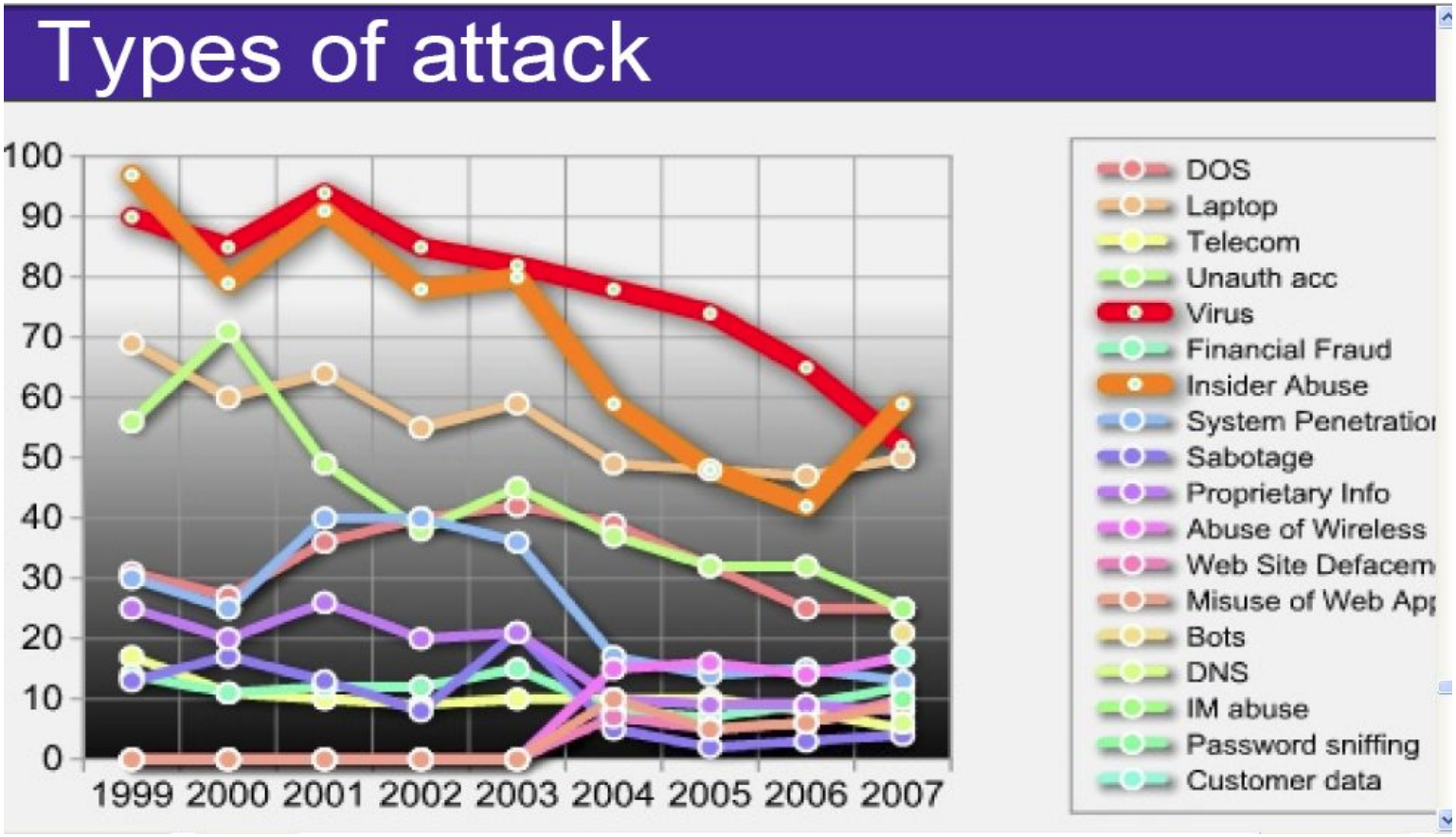
1. Les délits informatiques

1.2. Identification et définition des comportements considérés comme des délits informatiques

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES (Suite…)

1. Les délits informatiques

1.2. Identification et définition des comportements considérés comme des délits informatiques

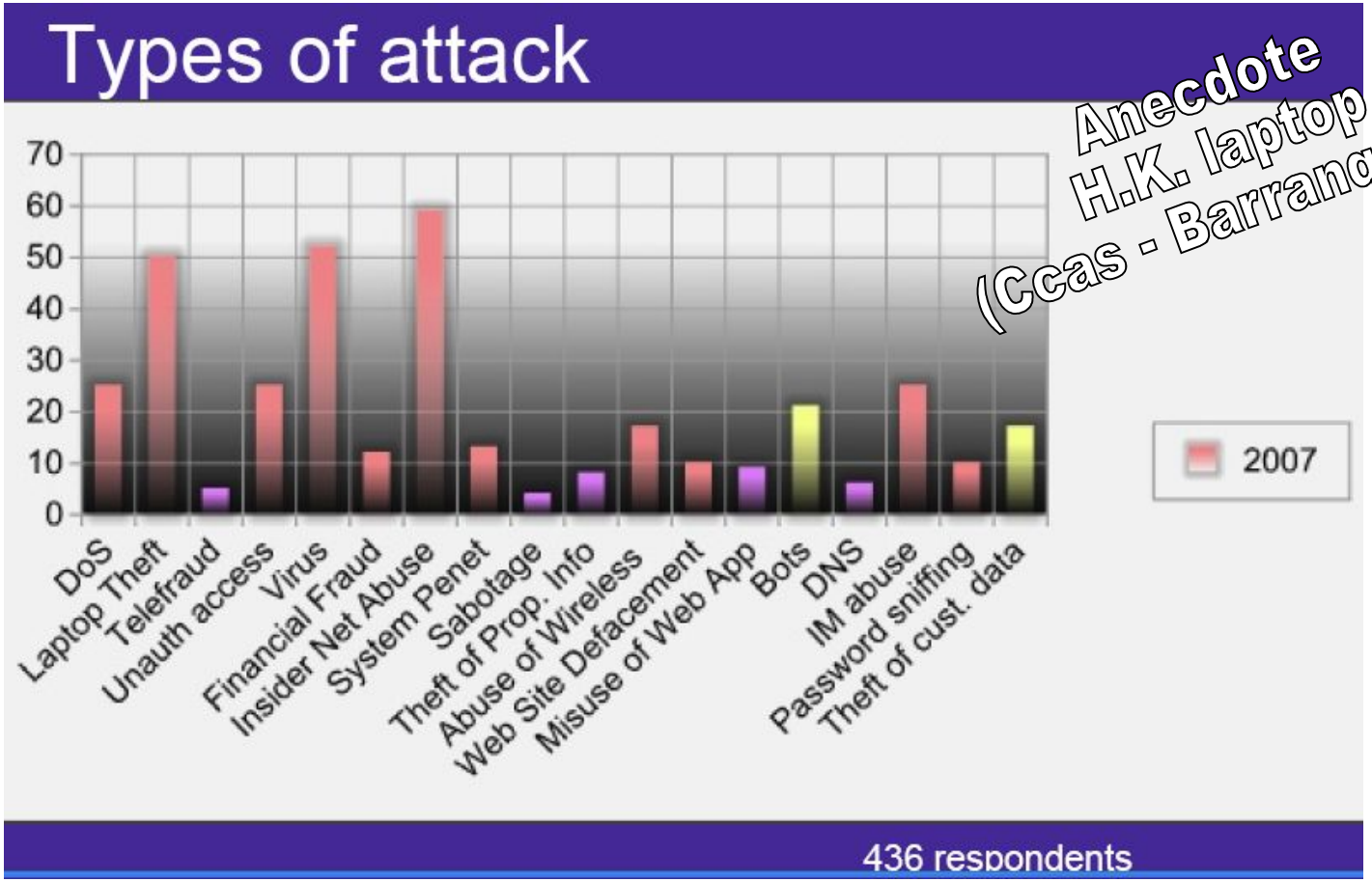


 Richardson, Robert, Director. Computer Crime and Security Survey. CSI.

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES (Suite…)

1. Les délits informatiques

1.2. Identification et définition des comportements considérés comme des délits informatiques



Anecdote
H.K. laptop
(Ccas - Barranquilla)

14 Richardson, Robert, Director. Computer Crime and Security Survey. CSI.

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES (Suite…)

1. Les délits informatiques

1.2. Identification et définition des comportements considérés comme des délits informatiques

Sondage réalisé sur douze mois concernant la nature des attaques ou des abus détectés:

TYPE OF ATTACK	2007
Insider abuse of Net access	59%
Virus	52%
Laptop / mobile device theft	50%
Phishing where your organization was fraudulently represented as sender**	26%
Instant messaging misuse**	25%
Denial of service	25%
Unauthorized access to information	25%
Bots within the organization**	21%
Theft of customer / employee data**	17%
Abuse of wireless network*	17%
System penetration	13%

TYPE OF ATTACK	2007
Financial fraud	12%
Password sniffing**	10%
Web site defacement*	10%
Misuse of public Web application*	9%
Theft of proprietary information (intellectual property)	8%
Exploit of the organization's DNS server**	6%
Telecom fraud	5%
Sabotage	4%

*Added in 2004 survey
**Added in 2007 survey

CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 436 Respondents

CSI Survey 2007. The 12th Annual Computer Crime and Security Survey. COMPUTER CRIME AND SECURITY SURVEY by Robert Richardson, Director, Computer Security Institute

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES (Suite…)
1.3. Conclusions

- Le profil du délinquant a changé;
- Les moyens employés pour commettre un délit ont évolués;
- Un même acte illicite peut comporter plusieurs délits simultanés ou consécutifs; et
- Les délits informatiques causent des dommages plus importants et en moins de temps que ceux causés par un délit traditionnel

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES

2. Normes juridiques de pays qui punissent les délits informatiques

2.1. Dans les Amériques

Le législateur d'au moins 22 pays a discuté un projet de loi visant les délits informatiques (loi spéciale v./ reforme du code pénal).

¾ des pays ont adopté ledits projets de loi.

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES

2. Normes juridiques de pays qui punissent les délits informatiques

2.1. Dans les Amériques (Sondage sur 17 lois nationales sur 22 pays collectés)

- Espionage (1 pays)
- Accès non autorisé (12 pays) =illegal access
- Modification/manipulation/falsif. non autorisée (11 pays)
- Utilisation non autorisée de services et systèmes, info (12 pays) = misuse
- Obstruction de service ou système ou endommagement (7 pays) et DDOS (3 pays) = data & system interference
- Diffusion information non autorisée (12 pays)
- Vol d identité (2 pays)
- Pornographie mineurs (13 pays) = child pornography
- Xénophobie (2 pays)
- Fraude électronique (10 pays) = computer related fraud
- Accès et interception de communications privées (9 pays) et Protection données (2 pays) = illegal interception
- Droits d'auteur (8 pays) = copyright
- Spam (2 pays)
- Investigation préliminaire et la preuve (1 pays) = procedural law

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES

2. Normes juridiques de pays qui punissent les délits informatiques

2.2. en Afrique

Algérie
Afrique du Sud
Botswana
Cape Vert
Côte d'Ivoire
Île Maurice
Nigéria
Sénégal
Zambie

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES
2.3. Pour résumer…

- Lesdits pays ont soit adopté une législation concernant la cybercriminalité, soit ils en ont pris l'initiative.
- Le thème suivant pourrait servir d'appui aux pays sur le point de prendre l'initiative législative.

II. DELITS, NORMES JURIDIC
CAS PRATIQUES
3. La coopération Intern.

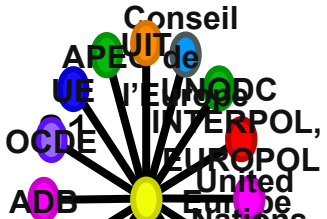
Mai

Oct-Nov.

Juin

Nov. Forum on Internet Governance

Oct.



II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES

4. Les cas pratiques

Jugements et affaires des pays suivants:

Argentine, Australie, Brésil, Chili, Colombie, Etats Unis, Espagne, France, Italie, Mexique, Pays-bas, Pérou, Russie, Vénézuela et Vietnam.

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES

4. Les cas pratiques

Pays	Année	Délit
Argentina	2006; 2003; 2002 1999	Espionage; Virus; website (*to be or not to be…*"une chose"); Interception d'email
Brasil	2007; 2006	Pornographie mineurs; Pharming
Chile	2007	Website hacké/intercepté; sabotage informatique
Colombie	2000	Extorsion
Etats Unies	2007 - 2001	Vol d'identité; fraude; spamming; botnets; vol d'info.; enchères publiques de produits interdits à la vente; viol de confidentialité breach; attaques F.S.I. (ISPs)

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES

4. Les cas pratiques

Pays	Année	Délits
Espagne	2007; 2006	Phishing; fraude; spam; viol du droit d'auteur
France	2008; 2004	Projet de loi; Violation droit d'auteur
Italie	2007	Contenu des Blogs
Méxique	2007; 2004	Vente illicite de biens culturels dans des enchères publiques; s'approprier d'email d'autrui
Pérou	2007; 2004-05	Pornographie mineurs; Phishing; pharming;

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES

4. Les cas pratiques

Pays	Année	Délit
Russie	2007	Botnets
Vénézuela	2007	Pornographie mineurs / pédophilie
Vietnam	Inconnue	Pornographie
Vietnam et Cambodge	inconnue	Abus et pornographie mineurs
Union européenne	2007	Fraude billets-électroniques

III. Étapes suivantes?

- Uniformiser la notion de délit informatique.
- Harmoniser les dispositions légales des délits informatiques (y compris leur description).
- Faciliter les procédures judiciaires, par ex. pour recueillir des éléments de preuve.
- Améliorer la coopération internationale et assistance mutuelle immédiate parmi la police informatique (unités spécialisées), les ministères publics (*prosecutors*) et les juges compétents. Limites: la souveraineté des États, lois nationales, droits de l'homme.
- Publier les initiatives nationales, projets de lois, plans et stratégies nationaux sur le site officiel de chaque État (partage d'info.)

III. Étapes suivantes? (Suite...)

- Au moment de proposer l'adoption d'une telle xx convention ou d'un tel modèle de loi, les organisations internationales devraient prendre en considération les fortes différences culturelles, linguistiques et surtout du système juridique (ex. *common law*, droit civil, droit musulman) de chaque région.

- Coordonner le travail sur la cybercriminalité des organisations internationales et régionales (par ex. UIT…car WSIS ne suffit pas)

- Les avocats doivent S'ABSTENIR de rédiger de lois concernant les TIC s'ils ne comptent pas avec l'étroite coopération du personnel avec un background en ingénierie, *computer science*, technicien informatique, etc.

III. Étapes suivantes? (Suite...)

- Format des lois sur le *cybercrime*: a) soit modifier le code pénal; b) soit créer de lois spéciales sur la criminalité informatique.

- Comment modifier le code pénal: a) soit en créant de tout nouveaux délits; b) soit en indiquant au bout de chaque chapitre (par ex. délits contre les personnes, contre la propriété, etc.) ou au bout de chaque disposition comprenant un délit: « *la peine pour lesdits délits commis avec l'emploi de moyens informatiques sera augmentée d'un tiers* »
  - En tout cas, il faudra vérifier quels délits sont déjà punis par le code pénal et quels actions ne comptent pas encore avec une sanction.

- La confiance ne dépend pas seulement du niveau de sécurité informatique, mais aussi du degré de garanties juridiques et économique qu'un pays peut y apporter.

Lutter contre les délits informatiques est une affaire de nous tous, et non seulement des organes de justice

S.V.P.
Aidez nous
dans le travail de sensibilisation et de capacitation...
train the trainers

"La segurité est basée sur trois piliers fondamentaux: les personnes, les procès et la technologie"
Luc Poulin, ISIQ, Canada

A MON AVIS IL MANQUE UN 4ME PILIER!!!!!

Merci de votre attention

Vous pouvez nous contacter sur:

mg.sarmiento@snconsult.com
http://www.snconsult.com

Les images dont la source n'est pas citée, proviennent du site www.photobucket.com