

Les savoirs criminologiques en matière de cybercriminalité

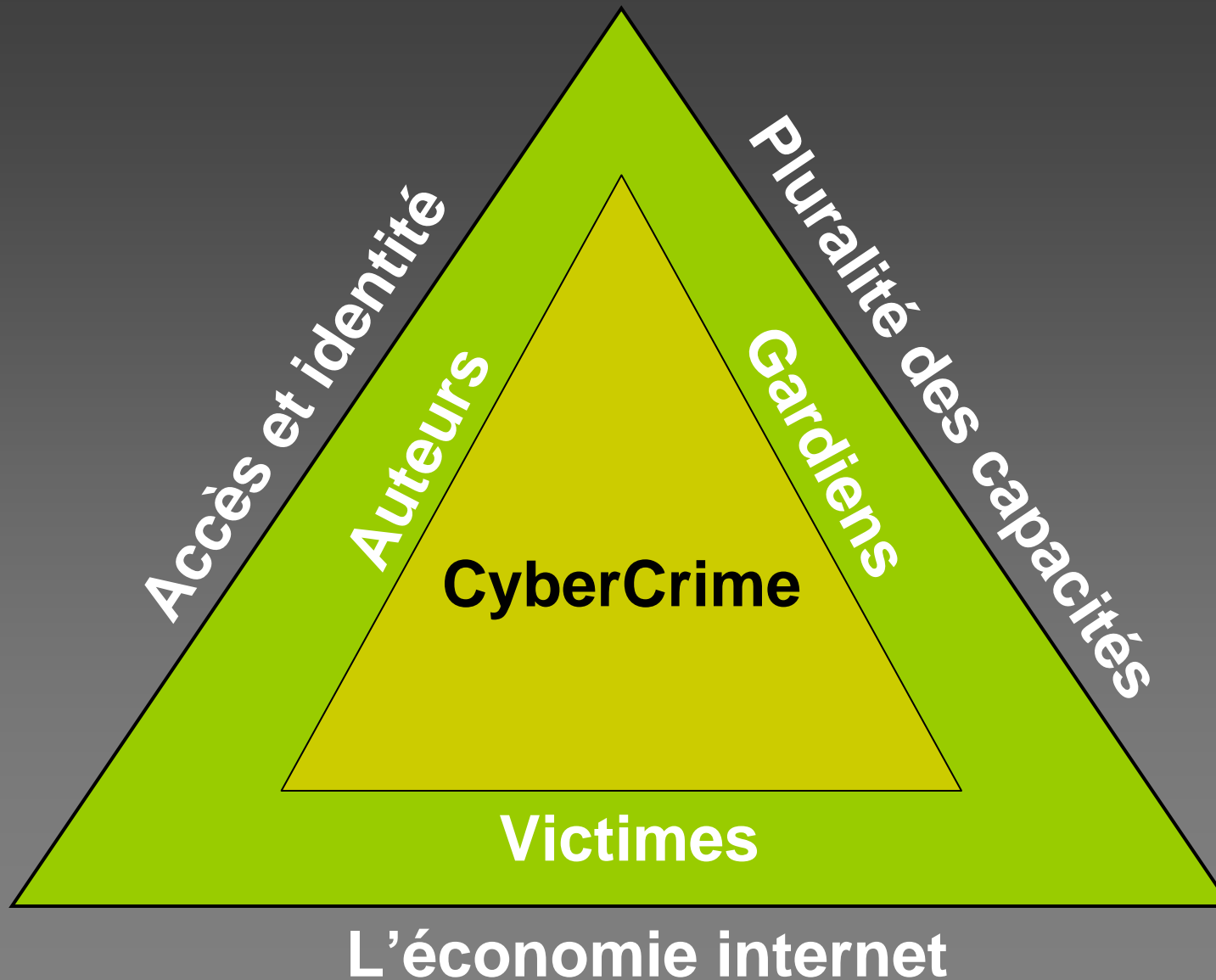
Benoît Dupont



Structure de la présentation

- La complexité du problème
- L'ampleur du problème
- Les victimes
- Les auteurs
- Les gardiens
- Application de la loi vs régulation

Le triangle du CyberCrime

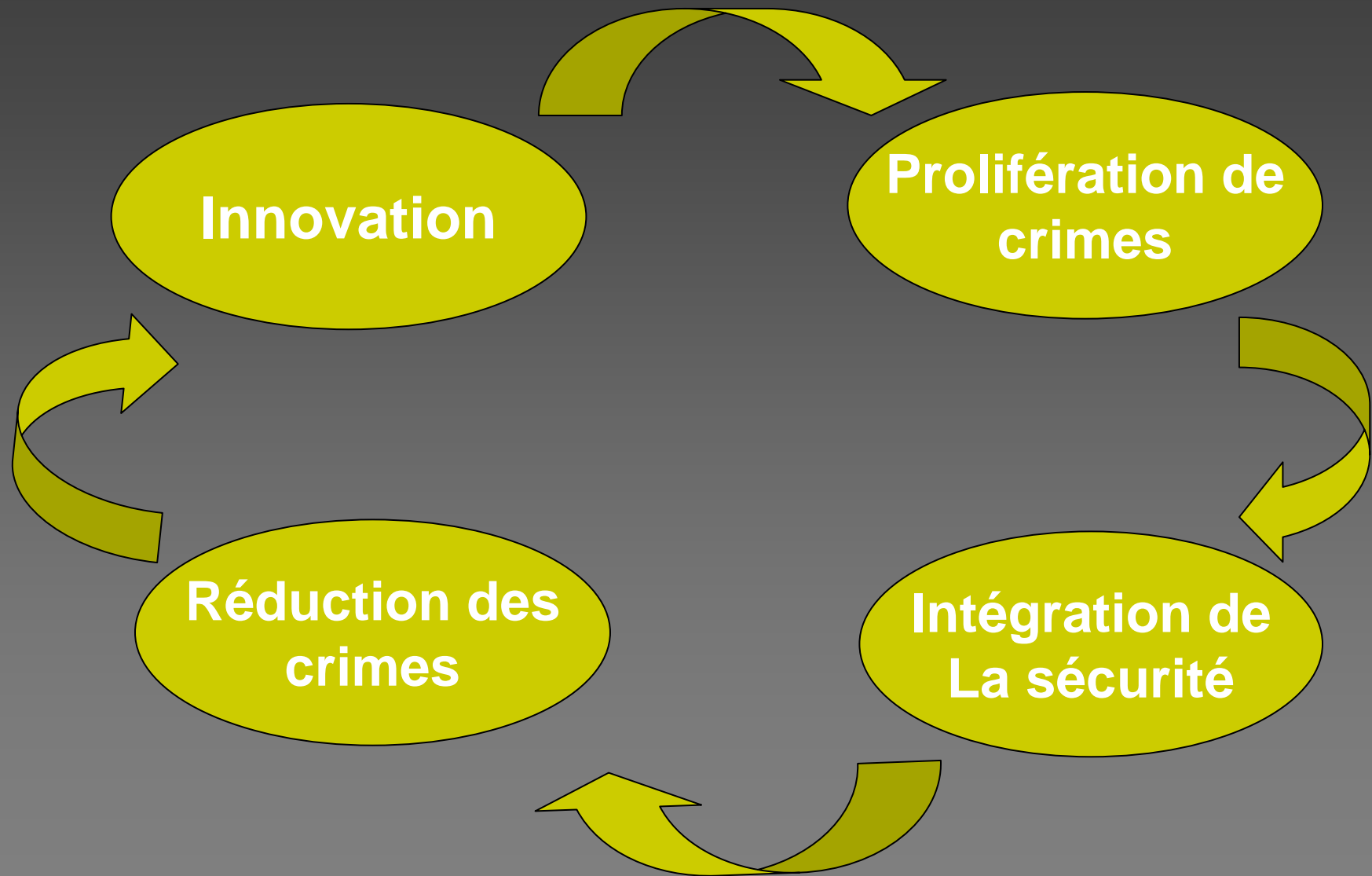


Adapté de Cohen & Felson

Écologie des systèmes d'information

- Globalisation
- Architecture distribuée
- Panoptisme / Synoptisme
- Asymétrie organisationnelle
- Fragmentation de l'identité personnelle
- Structure économique spécifique
 - Commodité d'usage privilégiée
 - "Efficience" des vulnérabilités

Le cycle du CyberCrime: une vélocité accrue



L'Internet criminogène



- Anonymat et désindividualisation
- Défi technique valorisé
- Furtivité
- Repérage
- Fuite
- Reproductabilité

Illustration: 10% d'Internet en 2005

Taxinomie de la cybercriminalité

- **Cyber-intrusion**

Violation de l'intégrité des systèmes d'information, avec ou sans préjudice

- **Cyber-vol**

Acquisition frauduleuse ou par tromperie de biens, de services ou de la propriété intellectuelle d'autrui

- **Cyber-obscénité**

Atteinte aux lois sur la pornographie ou l'ordre public

- **Cyber-violence**

Incitation à la haine, menaces et harcèlement

Un déficit de connaissances scientifiques

- Pas d'interdisciplinarité
- Pas de statistiques criminelles uniformisées
- Dramatisation et surestimation

Exemples d'estimations de pertes attribuées à la cybercriminalité

- Computer Economics : 14 milliards USD (2005)
- Scotland Yard: 220 milliards USD (2006)
- FBI: 400 milliards USD (2004)
- un service de police canadien: 1 600 milliards USD (1.6 trillions - 2005)
- Recours aux sondages de victimisation

Les victimes

- Les individus
 - La fraude et le vol d'identité
 - Profil des victimes
 - Relation avec les auteurs
 - Sous-déclaration à la police
 - Les crimes sexuels contre les mineurs
- Les entreprises
 - Des vulnérabilités systémiques
 - Une confiance excessive
 - Une gestion économique & réputationnelle des risques

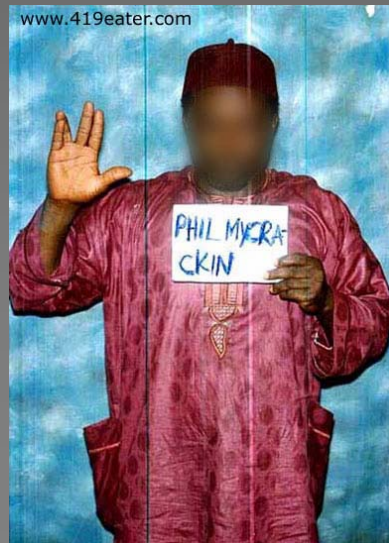
Les auteurs

- Les prédateurs sexuels
- Le mythe du hacker ou “Superutilisateur”
- Crime organisé ou crime organisant ?

**McAFEE VIRTUAL
CRIMINOLOGY REPORT**
ORGANISED CRIME AND THE INTERNET
December 2006



Source: New York Times

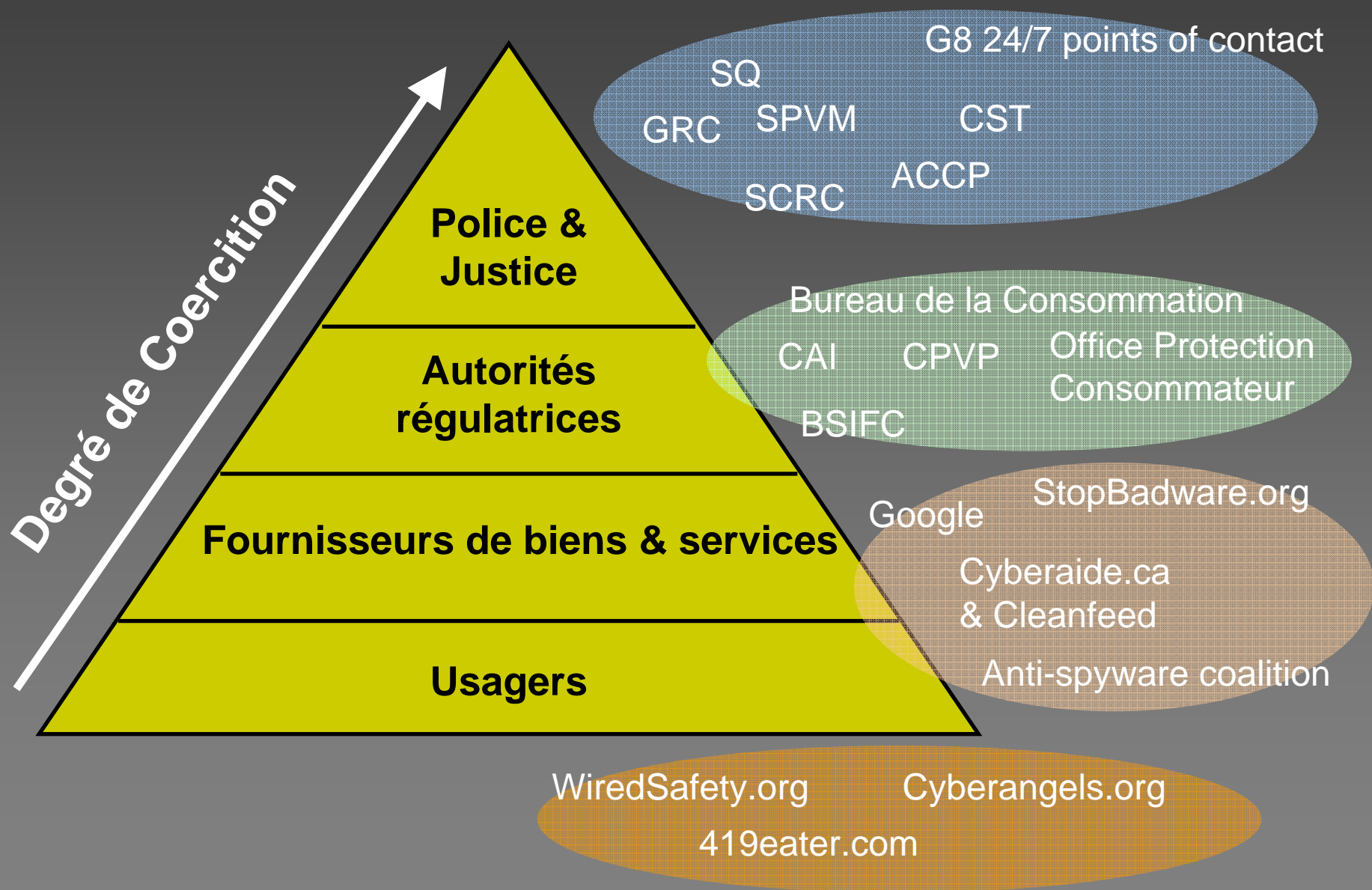


Source: Wired



Source: F-Secure

La pyramide des gardiens



Le modèle de régulation

- Le modèle d'application de la loi est conçu pour une criminalité à faible volume et à fort impact
- Le modèle de régulation se concentre sur l'encadrement des activités légales
- Distribution des responsabilités de prévention et de contrôle: mutualisation de l'expertise
- Pluralité des techniques de prévention et de contrôle utilisées
- Flexibilité procédurale
- Nouveaux modes de coordination requis

16 techniques de prévention

Augmentation des efforts	Augmentation des risques	Réduction des bénéfices attendus	Suppression des justifications
1. Durcissement des cibles	5. Détection des intrusions	9. Suppression des cibles	13. Activité réglementaire
2. Contrôle d'accès	6. Surveillance technique	10. marquage de la propriété	14. Contrôle des «désinhibiteurs»
3. Protection de l'intégrité des données	7. Surveillance par les employés	11. Réduction des tentations	15. Attribution de responsabilité
4. Authentification de l'identité	8. Surveillance par les usagers	12. Déni des bénéfices	16. Incitations au respect des règles

Source: Newman et Clarke 2003

Pour aller plus loin

benoit.dupont@umontreal.ca

www.securisphere.blogspot.com

www.edupont.net