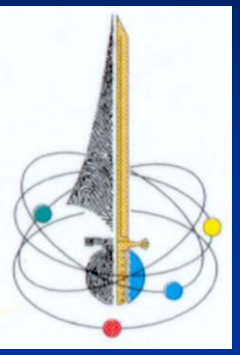
# JSSI 2006



I
R
C
G
N

# La gendarmerie dans la lutte contre la cybercriminalité

Capitaine Nicolas DUVINAGE - IRCGN

# Qu'est-ce que la «cybercriminalité» ?

- **Criminalités qui utilisent de façon accessoire les technologies numériques**
  - Ex.: utilisation d'Internet, de GSM, d'ordinateurs…pour communiquer, créer des documents bureautiques, etc
  - ⇒ Trafics de stupéfiants, délinquance économique et financière, homicide
- **Criminalités qui utilisent de façon principale les technologies numériques**
  - Ex.: diffusion de contenus illicites sur Internet
  - ⇒ Pédophilie, xénophobie…
- **Criminalités dont l'objet est constitué par les technologies numériques**
  - Ex.: atteintes aux STAD, contrefaçon cartes bancaires, infractions CNIL

# L'obligation pour la gendarmerie de s'adapter

- Toutes les cybercriminalités ne nécessitent pas des compétences très élevées
  - ⇒ Plusieurs échelons d'intervention avec des moyens différenciés
- Omniprésence d'objets numériques dans la vie courante (téléphones GSM, ordinateurs, cartes bancaires)
  - ⇒ Nécessité de capacités d'exploitation sommaires et rapides à l'échelon local

⇒ Echelon de base: **enquêteurs N-TECH (à terme 170 répartis sur toute la France)**

⇒ Echelon d'expertise: **Institut de recherche criminelle de la gendarmerie nationale (IRCGN)**

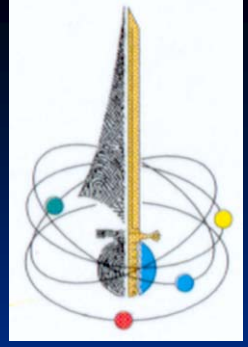
# Les enquêteurs N-TECH

- Formation 6 semaines
- Pack matériel et logiciel complet (environ 5.000 euros / enquêteur)
- Connexion ADSL dédiée
- **Culture générale technique**
  - Réseaux IP, réseaux GSM, carte bancaire
- **Capacité d'analyses sommaires**
  - Systèmes de fichiers (sur disques durs, clés USB, CD/DVD…)
    - Récupération de fichiers « visibles » et effacés
    - « Reconstitution de l'activité Internet » du suspect (index.dat et cache IE…)
  - Téléphones GSM et cartes SIM
    - Récupération de données-utilisateur

# Contraintes liées à la dépendance aux nouvelles technologies

- Consultation de sites web illégaux, utilisation de logiciels non reconnus, téléchargement de fichiers « suspects »
  - Adaptation de la politique SSI interne à la gendarmerie
- Matériels et logiciels très spécifiques
  - Marchés publics inexistants, fournisseurs non référencés
- Nouveautés matérielles (SATA, WiFi, cartes TransFlash…)
  - Mise à jour/renouvellement fréquent des matériels
- Nouveautés logicielles/protocolaires (VoIP, réseaux P2P, évolution des OS…)
  - Mise à jour des connaissances de 170 personnes réparties sur toute la France

…Le tout dans un contexte budgétaire très contraint, et avec la méfiance initiale des chefs !

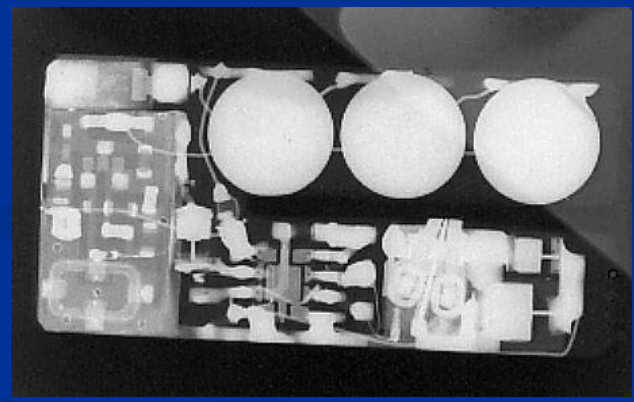


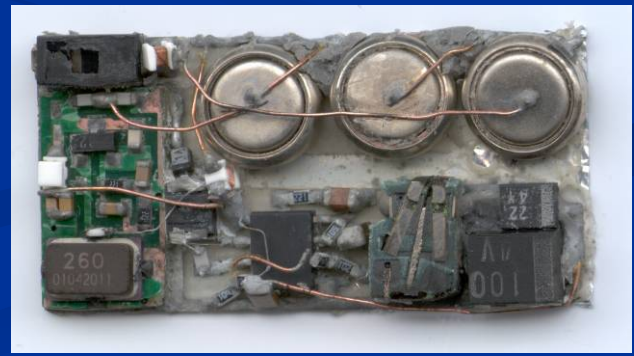
# Institut de Recherche Criminelle de la Gendarmerie Nationale

- L'unique laboratoire de la gendarmerie
  - Environ 200 personnes (ingénieurs, docteurs pharmacie/médecine/biologie, DEA/thèse…)
  - Mission: analyse scientifique des éléments de preuve saisis au cours des enquêtes
  - Domaines: ADN, empreintes digitales, balistique…
- …et en particulier le département informatique-électronique (INL)

# Exemple de compétences du département INL

- Interprétation des traces créées lors de l'utilisation de clients Internet (web, chat, P2P…)
- Réparation physique de disques durs endommagés
- Cartographies GSM
- Analyse du fonctionnement de keyloggers bancaires
- Rétroconception de dispositifs de piégeage de DAB/DAC





# Contraintes liées à la dépendance aux nouvelles technologies

- 12 gendarmes de haut niveau technique
  - ⇒ Difficultés de recrutement et de fidélisation
- Formation continue très spécifique
  - ⇒ N'existe pas toujours « sur étagère »
  - ⇒ Tarifs exorbitants par rapport aux « standards gendarmerie »
- Contacts fréquents indispensables avec les industriels, les universitaires, les opérateurs
  - ⇒ Pendant ce temps la justice patiente pour obtenir ses résultats d'expertise…
- Développement permanent de nouvelles méthodes de travail et processus
  - Ex.: récupération de données dans les téléphones portables (dessoudage de composants)
- Assurance-qualité
  - ⇒ Norme ISO 17025 non adaptée aux « laboratoires numériques »

# Contact


- Capitaine Nicolas Duvinage
- IRCGN – Chef du département informatique électronique
- Tél: 01 58 66 50 62
- Fax: 01 58 66 50 27
- Email: inl.ircgn@gendarmerie.defense.gouv.fr
  n.duvinage@wanadoo.fr