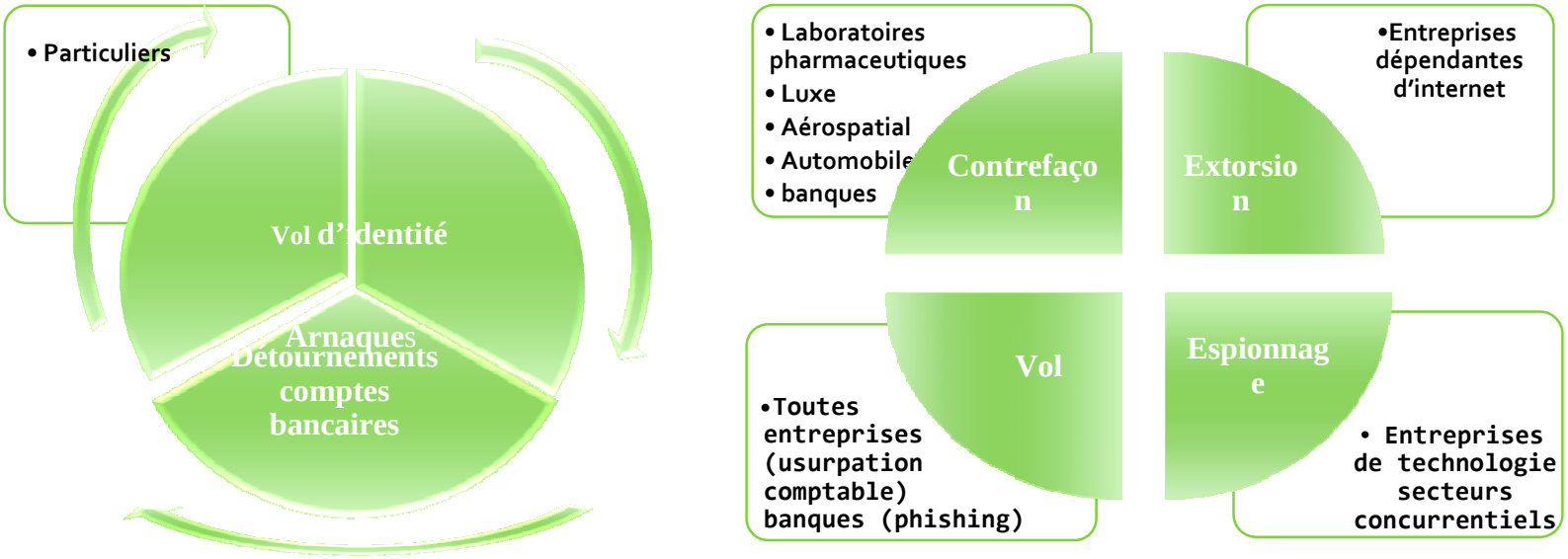
3ème rencontres parlementaires 21/10/15

Réaction face à une atteinte cyber
Preuves numériques & Forces de police

Colonel Philippe BAUDOIN
Coordinateur Cybermenaces
Cabinet DGGN

Cybercriminalité et Cyber-malveillance
Les cibles

La cybercriminalité s'adresse à tous …
porte sur les biens, les données et les flux financiers



Prévention / Traitement …

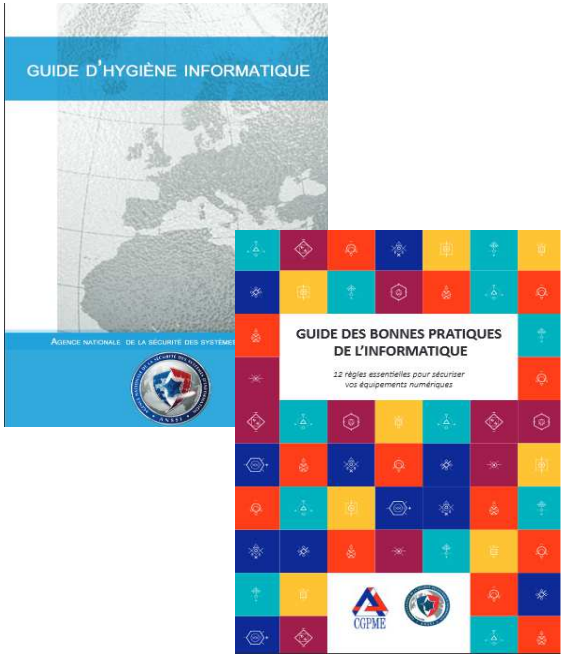
OIV : ANSSI / Grandes entreprises : DGSI / Secteur Défense : DPSD

ETI / PME / PMI & particuliers : GN ou PN

Avant toute attaque

Mettre en œuvre une politique de sécurité des systèmes d'information et des données

- Désignation d'un correspondant/référent SSI
- Cartographie des SI et des *données sensibles*
- Implication des usagers (charte informatique, …)
- Démarche globale (tous lieux, tous supports, pro/perso)
- Organiser la réaction en cas d'incident



✓ Pour les RSSI : guide d'hygiène informatique ANSSI

✓ Pour PME : guide des bonnes pratiques de l'informatique CGPME

✓…

Réaction en cas d'attaque

Les facteurs en faveur d'un dépôt de plainte

Plainte ou signalement ?

Risque de médiatisation et atteinte à l'image de l'entreprise ?

Quelque soit le choix de l'entreprise :

- faire **remonter les faits** (modes opératoires) **aux forces de l'ordre** pour favoriser la **connaissance de l'étendue de la menace**

→ avoir un interlocuteur qualifié et de confiance.

Posture initiale de protection des S.I. et des traces

Mise en œuvre par le RSSI de mesures conservatoires prévues

Preuve numérique

En droit français la preuve est libre

Support immatériel de la preuve numérique

Support matériel de la preuve numérique

- Support sans capacité de stockage, ou avec capacité de stockage
  (volatils ou non)
- Support magnétiques / optiques / électroniques

Moyens de recueil de la preuve numérique

- Constatations et/ou Saisie en perquisition :
  - Sur place
  - A distance

- Sur réquisition judiciaires
- Par constations techniques en milieu ouvert

Traitement de la Preuve numérique

Principes généraux de la criminalistique (Forensique):

- Non modification de la preuve
- Intervention de personnels spécialement formés
- Documentation des actes

La Problématique du stockage distant

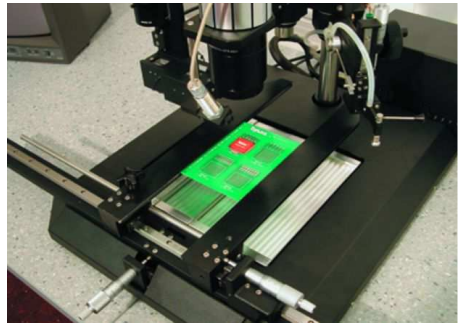
La mise sous scellé

Processus d'examen d'un disque dur

Récupération de données dans les composants électroniques

Traces Internet

Utilisation de moyens de cryptologie



Preuve numérique
L'interprétation et ses limites

On peut tenter de reconstituer un processus chronologique…Mais il faut interpréter avec précaution les dates/heures

On peut déterminer, parmi les traces subsistantes…

Les outils utilisés…
les requêtes entrées…

…Mais l'utilisateur réel n'est pas forcément celui que l'on croit

Les traces ne sont pas forcément issues d'un acte volontaire ou conscient

Lieu de la plainte et de l'enquête

LA PLAINTE (du représentant légal ou une procuration et KBIS)

EST PRISE DANS TOUS SERVICES

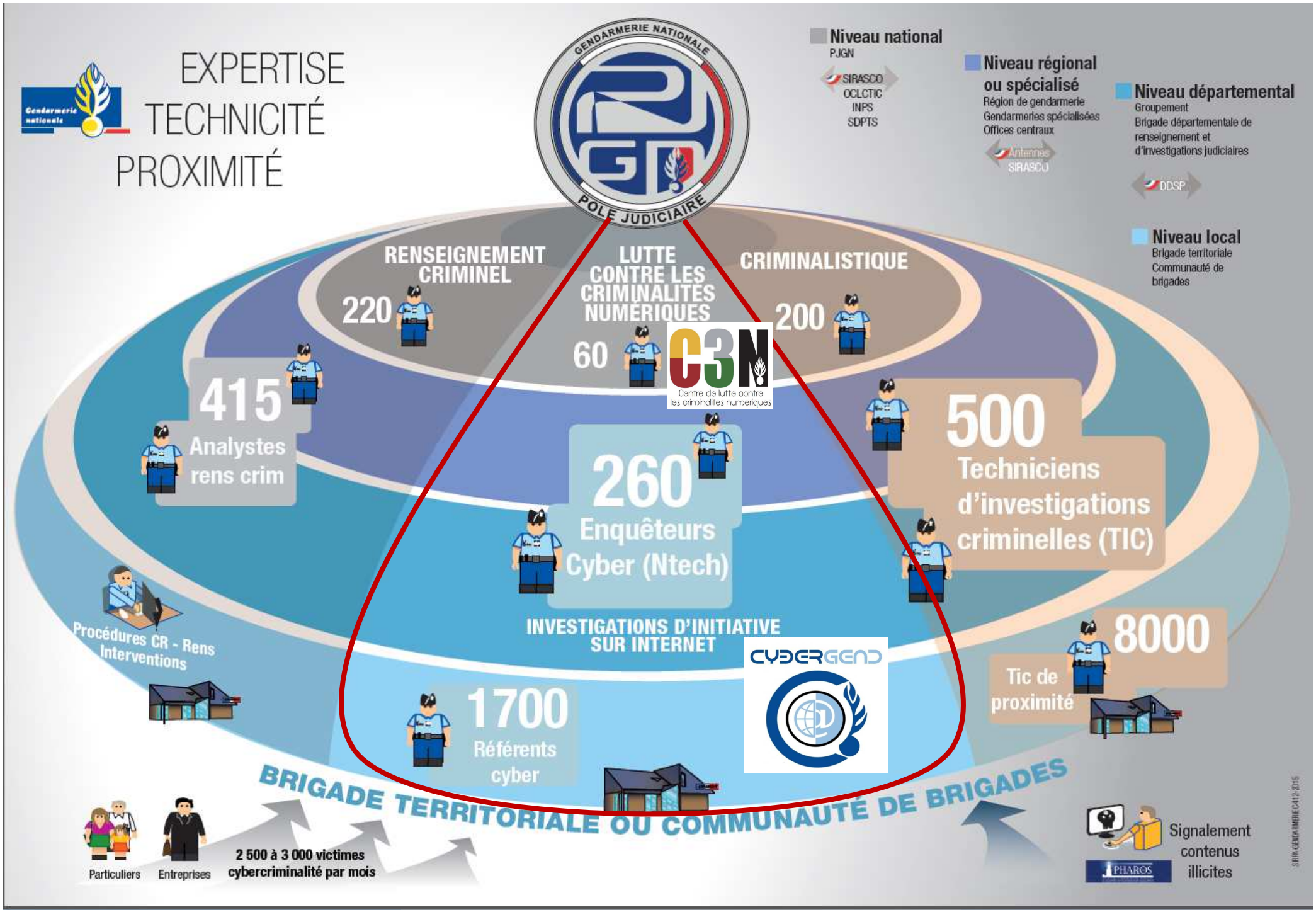
MAIS L'ENQUETE PEUT ETRE DILIGENTEE PAR UN SERVICE DISTINCT

À QUEL SERVICE S'ADRESSER ?

Dépend du lieu de commission des faits et de leur complexité

Cas simple : unité classique

Haute sensibilité ou complexité : services spécialisés


EXPERTISE
TECHNICITÉ
PROXIMITÉ
GENDARMERIE NATIONALE
POLE JUDICIAIRE
Niveau national
PJGN
SIRASCO
OCLCTIC
INPS
SDPTS
Niveau régional ou spécialisé
Région de gendarmerie
Gendarmeries spécialisées
Offices centraux
Antennes SIRASCO
Niveau départemental
Groupement
Brigade départementale de renseignement et d'investigations judiciaires
DDSP
Niveau local
Brigade territoriale
Communauté de brigades
RENSEIGNEMENT CRIMINEL
220
LUTTE CONTRE LES CRIMINALITÉS NUMÉRIQUES
60
C3N
Centre de lutte contre les criminalités numériques
CRIMINALISTIQUE
200
415
Analystes rens crim
260
Enquêteurs Cyber (Ntech)
500
Techniciens d'investigations criminelles (TIC)
INVESTIGATIONS D'INITIATIVE SUR INTERNET
CYBERGEND
Procédures CR - Rens Interventions
1700
Référents cyber
8000
Tic de proximité
BRIGADE TERRITORIALE OU COMMUNAUTÉ DE BRIGADES
Particuliers
Entreprises
2 500 à 3 000 victimes cybercriminalité par mois
PHAROS
Signalement contenus illicites

Adaptation du dispositif

Dans le cadre du plan ministériel de lutte contre les cybermenaces

Les **référents sûreté**[1] et les **référents Intelligence Economique**[1] vont suivre une session de sensibilisation au cyber

Le référent est le lien entre **l'entreprise** et **l'enquêteur**

spécialisé ou assisté d'un NTECH ou d'un ICC

Anticiper, prévenir pour réduire les risques et les menaces.

1. Le réseau des RS et R.IE représente avec leurs correspondants près 1.800 personnels

Défaçage de sites web et déni de service

- ✓ Déclenchement massif après les événements de Charlie
  - 156 affaires dénoncées auprès de la Gendarmerie Nationale
  - les investigations

  ont été menées localement

  par le réseau CyberGend
  - « cibles faciles »

  (sites web peu sécurisés) :

  petites entreprises,

  collectivités locales, écoles,

  associations...

Défaçage de sites web et déni de service

✓Resultats

- Nombreuses équipes de hackers (« hacking teams ») … mais avant tout des « script-kiddies »
  - scan automatique de vulnérabilités
  - challenge du nombre entre « hackers »

- Adresses IP des attaquants n'étaient pas françaises

=> attaques de (très) bas profil


3ème rencontres parlementaires 21/10/15
Colonel Philippe BAUDOIN
Coordinateur Cybermenaces
Cabinet DGGN