Police Judiciaire Fédérale
Federale Gerechtelijke Politie
Föderale Kriminalpolizei

Contexte

PAYS VOISINS

- France
- Allemagne
- Pays-Bas
- Luxembourg

SUPERFICIE

30.528 km²

POPULATION

11.748.716 habitants

DENSITÉ DE POPULATION

383 hab/km²

LANGUES

Une Police intégrée à deux niveaux

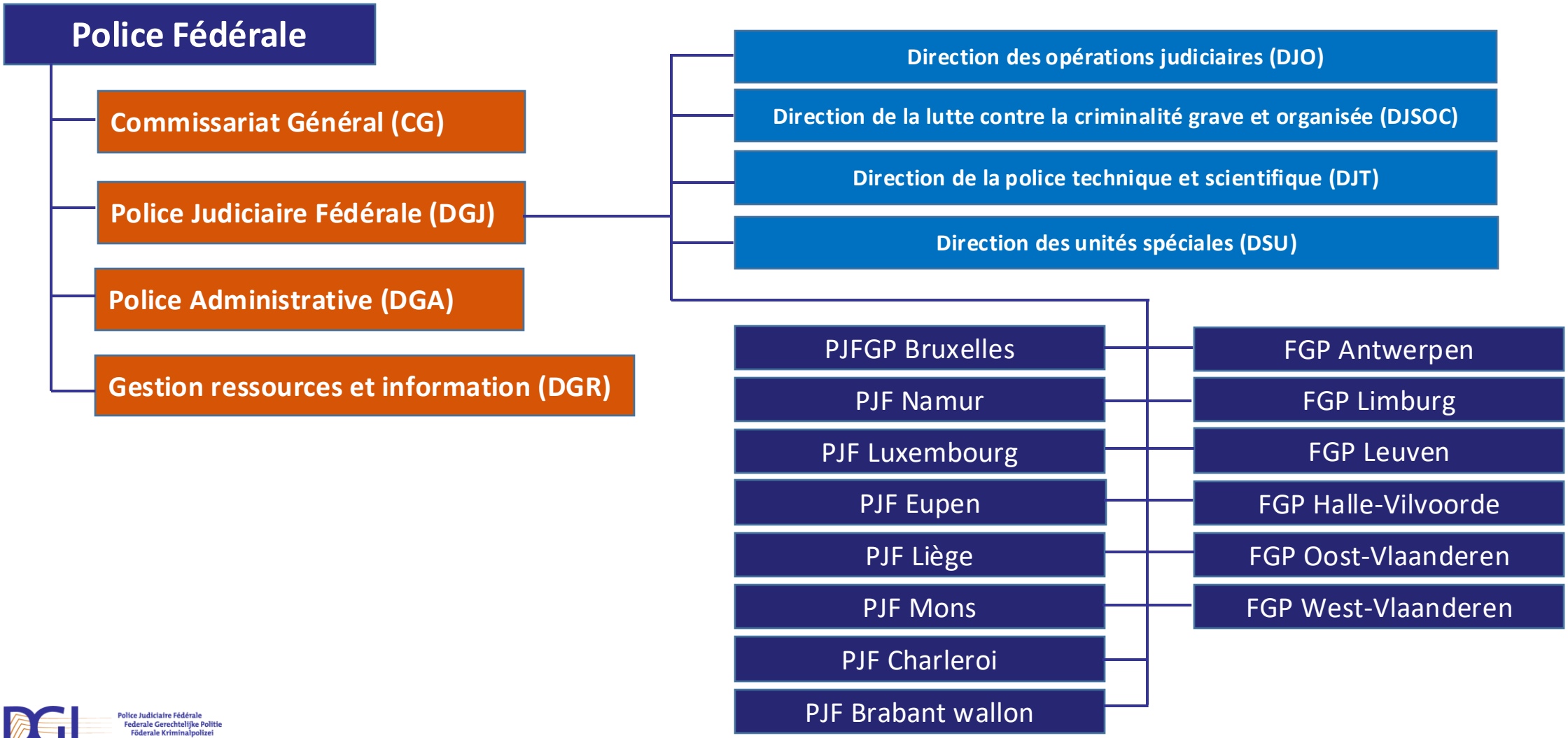
Police Locale
Lokale Politie

- 181 zones de police réparties sur l'ensemble du territoire
- Missions de police de base :
  - ✓ Travail de quartier
  - ✓ Accueil
  - ✓ Intervention
  - ✓ Assistance policière aux victimes
  - ✓ Recherche **locale**
  - ✓ Maintien de l'ordre
  - ✓ Sécurité routière

Police Fédérale
Federale Politie

- Missions de **police judiciaire** et police administrative :
  - ✓ Domaines spécialisés (unités spéciales, police scientifique, …)
  - ✓ Caractère **supralocal**
- Missions d'appui opérationnel, administratif ou logistique
- Représente les services de police belges dans le cadre de la coopération policière internationale

Structure de la Police Fédérale Judiciaire



Directions centrales de la DGJ

DSU
Unités spéciales

- ✓ Intervention
- ✓ Protection
- ✓ Observation
- ✓ Undercover
- ✓ NTSU

DJSOC
Lutte contre la criminalité grave et organisée

- ✓ Stratégie
- ✓ Criminalité organisée
- ✓ Terro (coordination)
- ✓ FCCU (Cyber)
- ✓ OCRC (Corruption)
- ✓ OCDEFO (EcoFin)
- ✓ DJMM (Militaire)
- ✓ FUPHEC (EcoCrim)

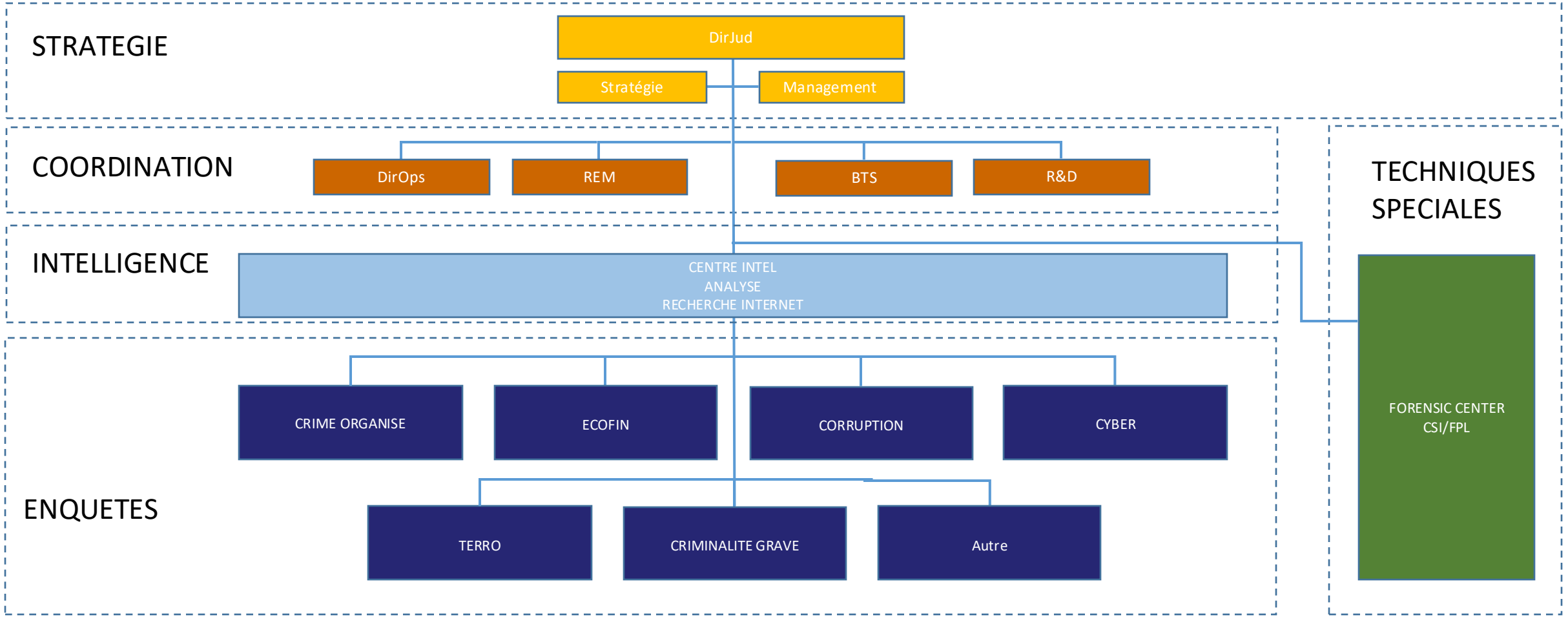
DJO
Opérations judiciaires

- ✓ Permanence nationale 24/7
- ✓ BTS (MPR)
- ✓ Cellule des personnes disparues
- ✓ Avis de recherche FAST (Fugitive Active Search Team)
- ✓ Protection des témoins
- ✓ Saisies et signalements

DJT
Technique et scientifique

- ✓ Coord Labo PTS
- ✓ OCRF (faux documents)
- ✓ DVI (Identification des victimes)
- ✓ Reconnaissance faciale
- ✓ Sciences du comportement
- ✓ Audio/vidéo

14 Directions déconcentrées (PJF) de la DGJ



Principaux défis en matière de sécurité intérieure

1 Criminalité organisée ↗↗

- Drogues (économie, ports (aériens), production propre), trafic d'êtres humains, etc.
- Mafia : mocromafia, Albanie, Italie, etc.
- Blanchiment d'argent, corruption, violence extrême, etc.

2 Cybercrime ↗↗

- Phishing is the new thiefing
- Cybersécurité
- Deep fake
- Conséquences réelles d'une cyberattaque massive

3 Extremisme/radicalisme/terrorisme ↗

- La menace de l'EI et d'Al-Qaïda persiste
- L'extrémisme de droite violent se développe
- Retour de l'extrémisme violent de gauche

4 EcoFin ↗↗

- Fraude sociale - fraude à la TVA, fraude fiscale
- Plus d'argent sale dans les crypto-monnaies

Dans le monde réel … et virtuel

Défis : Approche

AVEC QUI ?

- Autorités judiciaires
- Approche intégrée :
  - ✓ Police locale et fédérale
  - ✓ Partenaires privés et publics
  - ✓ Autorités locales
  - ✓ Monde académique

COMMENT ?

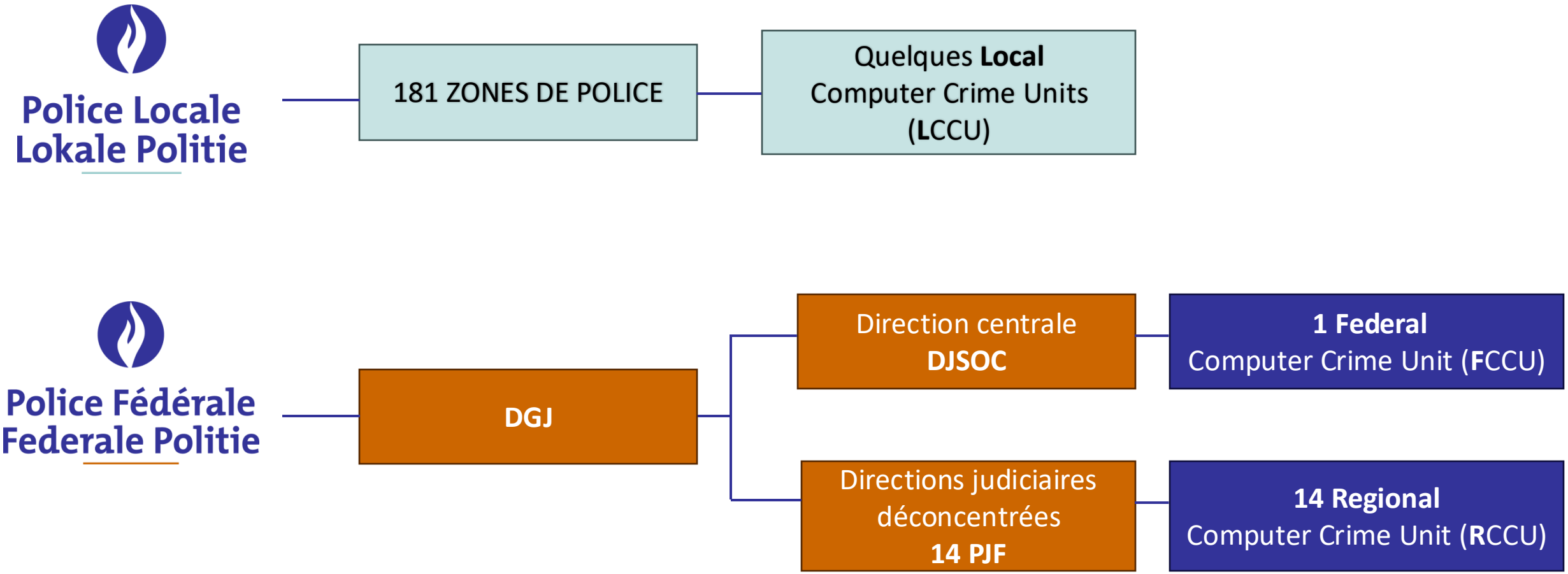
- Enquête judiciaire (réaction)
- Détection/recherche d'informations (monde réel et virtuel)
- Analyse/gestion de l'information
- Image nationale/évaluation des menaces
- Création de projets et innovation

MAIS AUSSI

- Forensics
- Unités spéciales
- Approche administrative

INSPECTEUR PRINCIPAUX
SPECIALISATION PARTICULIERE ICT

Computer Crime Units dans la structure policière



Computer Crime Units dans la structure policière

FCCU	• Point de contact (inter)national 24/7 • Enquêtes attaques sur infrastructures critiques • Formation • Constitution de l'image criminelle
14 RCCU	• Cybercriminalité avec impact sociétal et économique important • Enquêtes Internet • Analyse forensic ICT (Windows, Linux, Mac, Mobile devices, …) • Appui ICT au sens large (Fraude internet et autres)
Police locale	• Première ligne • Gêle la situation • Premières constatations – connaissance technique limitée • Préservation des supports digitaux

FCCU & RCCU : Tâches

FCCU

- **Coordination** de la lutte contre les formes graves et **internationales** de criminalité informatique
- Fournir **un soutien en matière ICT** aux **unités centrales** de la DJSOC + Comité P + AIG
- Assurer la **formation** et **l'échange d'informations** au niveau international
- Donner **un appui spécialisé** au profit de l'ensemble de la **Police Intégrée**

RCCU

- **Traitement complet** des dossiers de **criminalité informatique** grave et/ou organisée
- **Appui** des partenaires dans le traitement des pièces et/ou environnements informatiques, suggestion de suites d'enquêtes, identifications, création d'outils et appui mutuel inter CCU
- **Recherche et développement** - trouver des solutions HighTec opérationnelles au profit des enquêteurs tactiques et/ou CCU

FCCU & RCCU : Organisation

FCCU

- Team **FORENSICS**
- Team **CYBERCRIME**
- Team **INTELLIGENCE**
- Team **R&D**

RCCU

- Chaque RCCU a un **fonctionnement propre** (personnel dédié ou polyvalent, expertise locale, projets)
- Implication dans des **groupes de travail** au niveau **national**
- Participation à des **groupes d'expertise** et **divers projets**
- Policier avant tout = peut être amener à opérer en dehors des RCCU comme **enquêteur classique**

PILIERS CCU

Computer Forensic	• Ordinateurs, réseaux, supports ICT
Mobile Forensic	• GSM, GPS, Automotive, Internet Of Things
Cybercrime	• Hacking, Malware, Ransomware, Quick Reaction Force
Internet investigations	• Open Source Intelligence, DarkWeb, escroqueries, identifications
Image Forensic	

Fonctionnement CCU : Computer Forensics

Recherche sur les réseaux (entreprises, cloudservices, …)

Perquisitions & auditions dans les dossiers avec caractère ICT

Live Forensics

Automotive/Infotainment systems

Analyse et traitement d'images (vidéosurveillance, observations)

Analyse de supports de données

Fonctionnement CCU : Mobile Forensics

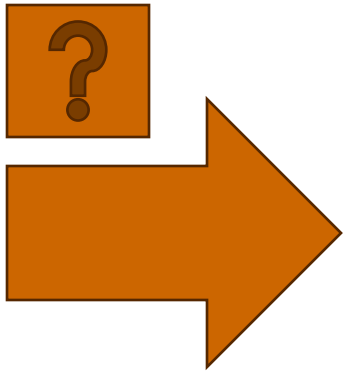
GSMs

SMARTPHONES

DISPOSITIFS GPS

TABLETTES

TRACKERS



Utilisation d'outils spécifiques

- Ufed
- Oxygen
- Axiom Mobile

Crack code accès

- Méthodes propres/Labo

Enquête destructive

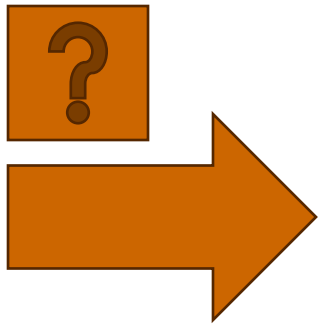
- JTAG & Chip Off

Fonctionnement CCU : Cybercrime

Enquête autonome

Cybercrime

Analyse et assistance technique ICT enquête cybercrime



Coopération nationale

Coopération internationale

Devoir de coopération des opérateurs et prestataires de service

Réclamation de la magistrature – Dispositions de la Loi pénale

Police :

- Accords avec opérateurs étrangers
- Forces de police étrangères comme Europol/Interpol

Traités multilatéraux :

- Convention de Budapest
- Demandes d'aide juridique

CCU : Challenges

DarkWeb

Virual currency & block chain

Malware

Decrypting

IOT

AI

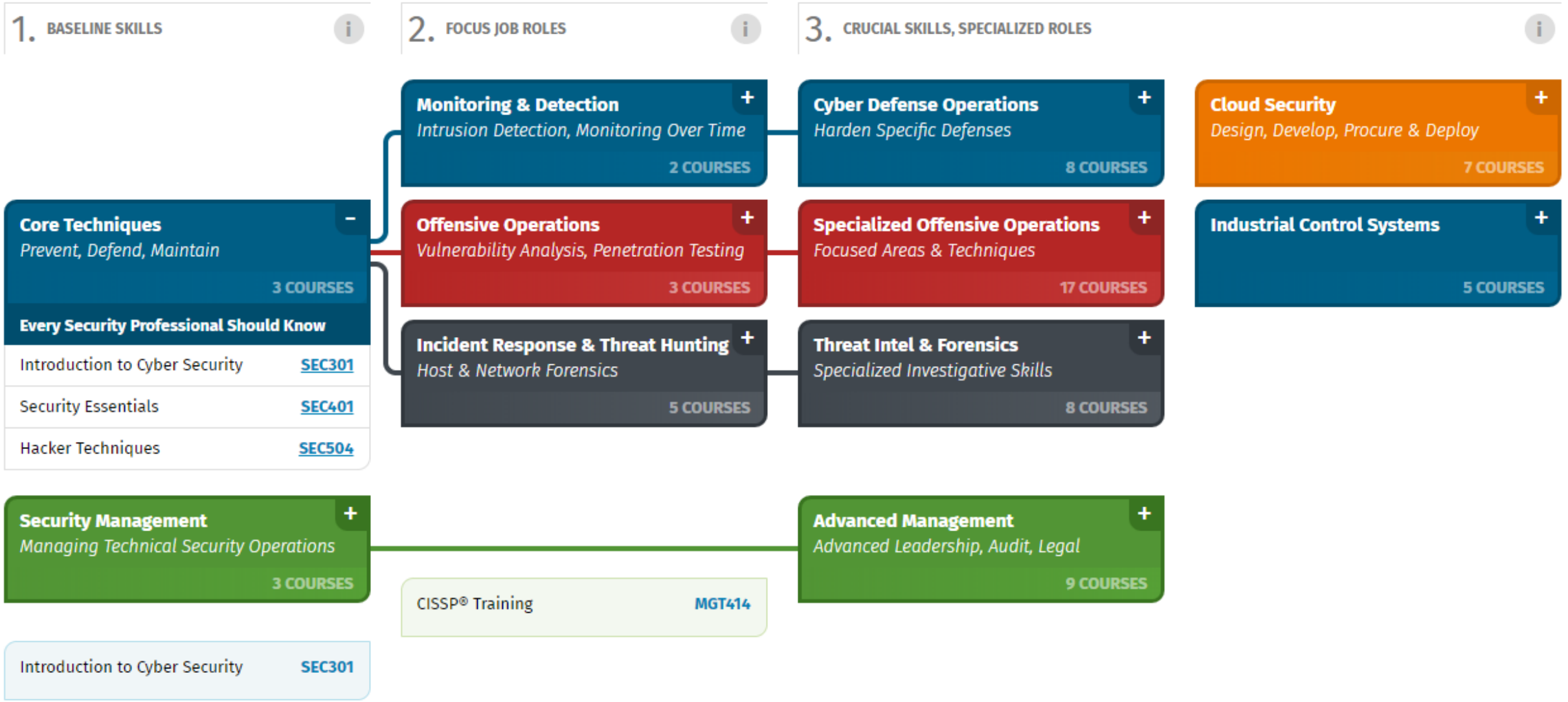
Big Data

Nombreux projets en cours au sein des unités

CCU : Formations

BASIC	• Tous membres CCU • Orienté pour public non IT
INTERMEDIATE	• Tous membres CCU • Brevet CCU (formation fonctionnelle)
EXPERT	• Niches IT – Type Sans Institute ou équivalent • Fréquence annuelle – Budget dédié CCU

SANS INSTITUTE



SANS INSTITUTE

Vulnerability Analysis, Penetration Testing
3 COURSES

Focused Areas & Techniques
17 COURSES

5 COURSES

Core Techniques
Prevent, Defend, Maintain
3 COURSES

Every Security Professional Should Know

Introduction to Cyber Security	SEC301
Security Essentials	SEC401
Hacker Techniques	SEC504

Incident Response & Threat Hunting
Host & Network Forensics
5 COURSES

Forensics Professionals Focused on Endpoints

Windows Forensics	FOR500
Advanced IR & Threat Hunting	FOR508
Enterprise-class IR & Threat Hunting	FOR608

Forensics Professionals Focused on Networks

Ransomware for IR	FOR528
Network Forensics	FOR572

Threat Intel & Forensics
Specialized Investigative Skills
8 COURSES

Essentials

DFIR Essentials	FOR308
Enterprise Cloud Forensics and IR	FOR509

Malware Analysis & Threat Intelligence

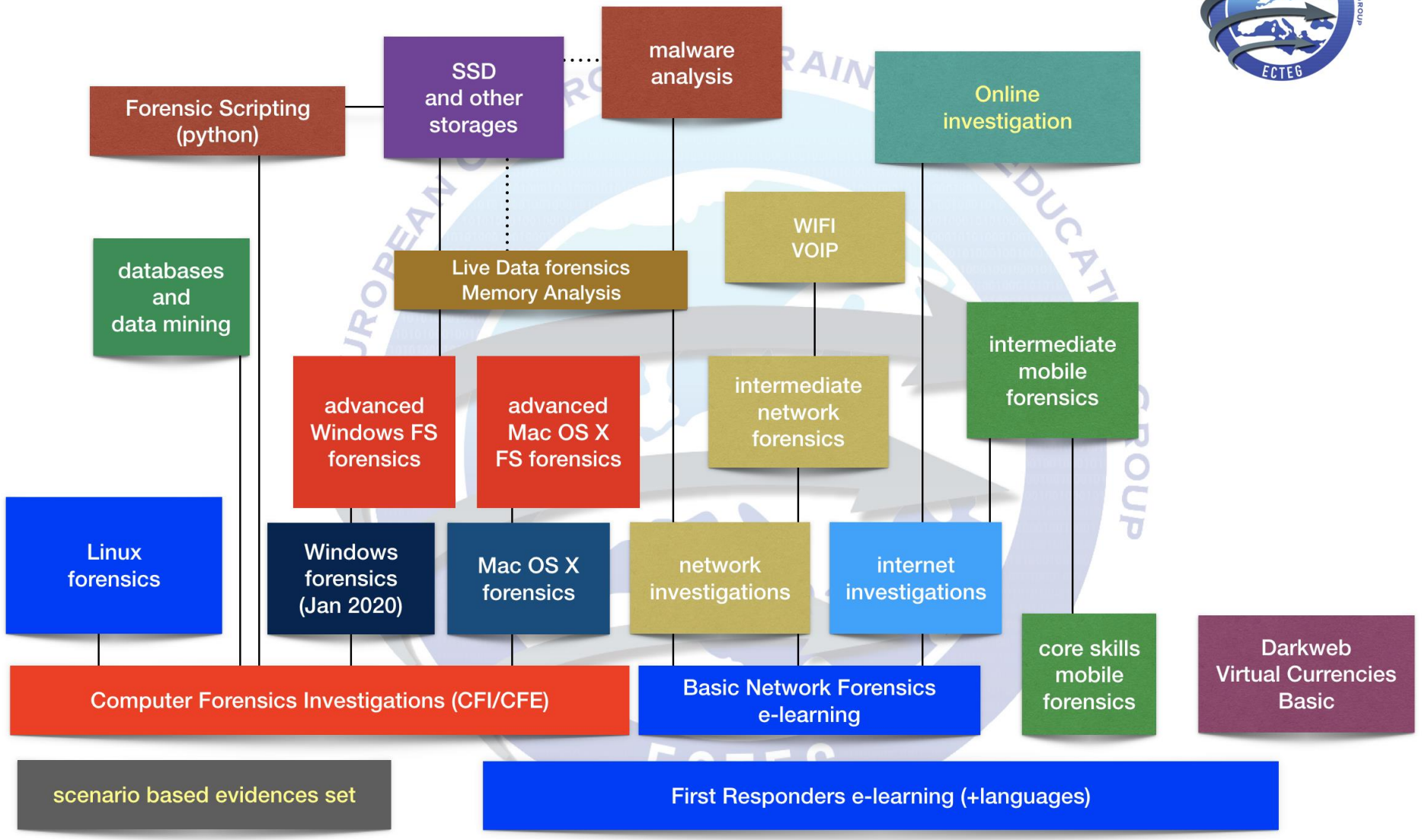
Cyber Threat Intelligence	FOR578
Malware Analysis	FOR610
Malware Advanced Code Analysis	FOR710

Forensics & Media Exploitation

Battlefield Forensics	FOR498
Mac & iOS Forensics	FOR518
Smartphones	FOR585

ECTEG

ECTEG training materials



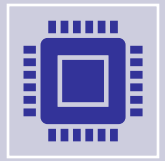
CCU : Partenaires

- Interne police :
  - zones de police, police fédérale, AIG, Comité P, PJF
- Magistrats
- Services publics fédéraux et régionaux avec compétences judiciaires :
  - Armée, lois sociales, impôts, eaux et forêts
- Services internationaux
  - Europol, Interpol, Eurojust, OTAN, services policiers étrangers
- Public : CERT, IBPT
- Monde académique (R&D)
- Privé : FEB, FebelFin, entreprise privée (partenariat)

CCU : Interactions

- La force des CCU réside dans la taille des unités mais aussi dans les interactions et la collaboration entre CCU
- Les CCU disposent d'un panel d'experts dans toutes les matières et répartis sur l'ensemble du territoire
- Toute expertise est bienvenue et trouvera sa place au sein des CCU

CCU : Profils



Collaborateurs avec une formation ICT (Master/Bachelor)

Opérationnels et consultants

Spécialistes réseaux, SCADA, électroniques, Linux, …

Enquêteurs avec compétences ICT – “selfmade”

La complémentarité des différents profils de compétence est nécessaire au bon fonctionnement de même que l’articulation entre compétences opérationelles et techniques

CCU : Qualités recherchées

- Teamspirit
- Autonomie et proactivité
- Curiosité
- Problem solver
- Raisonnement cartésien
- Créativité
- Sociabilité
- Collégialité
- Capacité d'abstraction face aux contenus sensibles
- Résistance au stress
- Capacité à travailler en projet

CCU : Exemple semaine type

Lundi	• Perquisitions avec zone de police en matière de mœurs 5AM – retour au bureau pour réaliser les analyses urgentes
Mardi	• Extraction des données des périphériques mobiles et rendez-vous avec le magistrat
Mercredi	• Réunion du groupe d'expertise Automotive
Jeudi	• Développement de script pour Facebook puis sortie urgente liée à une agression pour vidéo-surveillance
Vendredi	• Rédaction de PV/rapports et dépôt d'objets au Greffe

Epreuve de connaissance profesionnelle

Se déroule en 2 parties avec une difficulté progressive:

- choix multiple
- questions ouvertes

Et 6 grands axes :

- Axe 1 : Hardware
- Axe 2 : Systèmes d'exploitation
- Axe 3 : Réseaux
- Axe 4 : Enquête ICT
- Axe 5 : Criminalité informatique
- Axe 6 : Scripting

Contact

DGJ.Jobs@police.Belgium.eu

Police Judiciaire Fédérale
Federale Gerechtelijke Politie
Föderale Kriminalpolizei

Formulaire de contact :

https://forms.office.com/e/jN1Qap9hjH

Police Judiciaire Fédérale
Federale Gerechtelijke Politie
Föderale Kriminalpolizei

Police Fédérale
Federale Politie