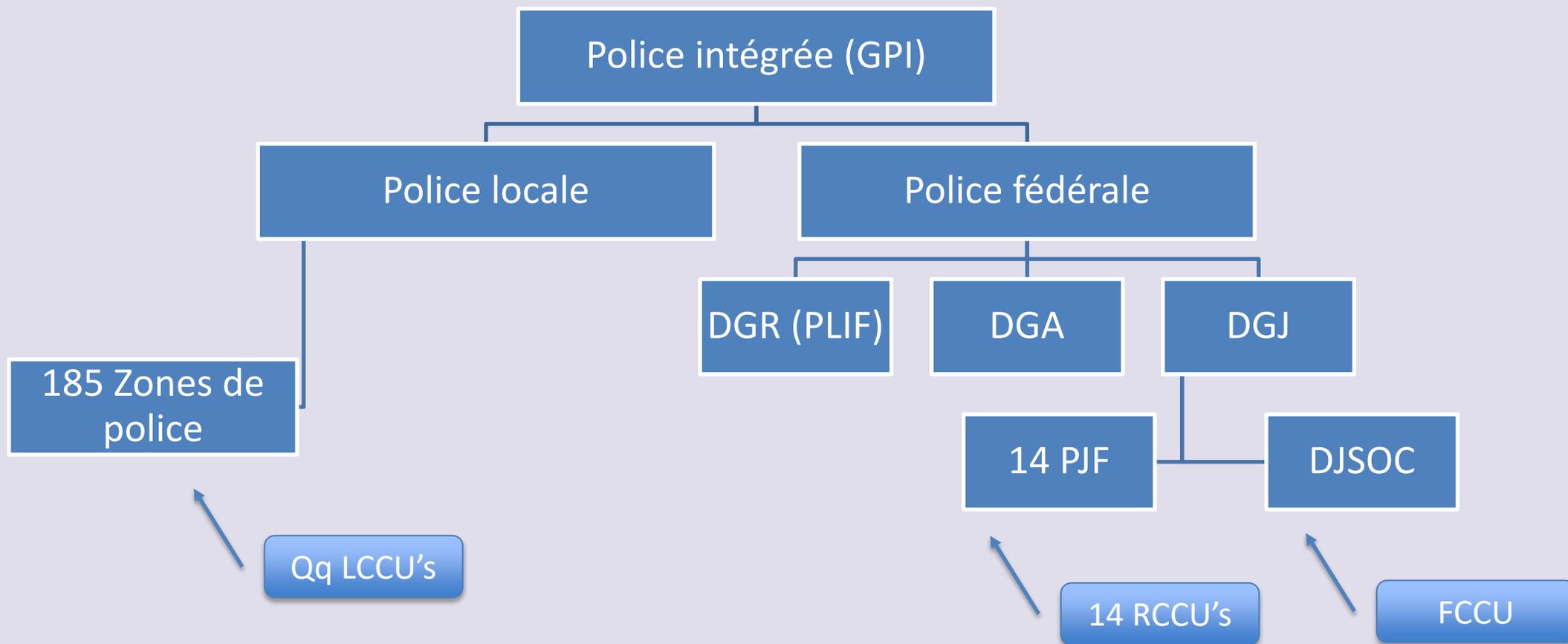




RECRUTEMENT D'INSPECTEURS PRINCIPAUX SPÉCIALISÉS ICT



STRUCTURE POLICIÈRE ET PLACE DES XCCU'S



Pôles d'activité

- 4 (5) piliers :
 - Computer forensic (ordinateurs, réseaux, supports ICT)
 - Mobile forensic (GSM, GPS, Automotive, IoT)
 - Cybercrime (Hacking, Malware, Ransomware, Quick Reaction Force)
 - Internet investigations (OSINT, DarkWeb, escroqueries, identifications)
 - (Image forensic)

FCCU: Federal Computer Crime Unit

- 1 Unité
- Bruxelles
- Au sein de la DJSOC (Direction of serious and organised crime)

FCCU: rôle

- Chargée de coordonner la lutte contre les formes graves et internationales de criminalité informatique.
- Fournit un soutien en matière ICT aux unités centrales de la DJSOC et au Comité P et l'AIG.
- Assure la formation et l'échange d'informations au niveau international.
- Donne un appui spécialisé au profit de l'ensemble de la police intégrée.

FCCU: organisation

- Team "Forensics" fournit un soutien spécialisé aux services centraux d'enquête.
- Team "Cybercrime" mène des enquêtes sur les formes graves et/ou internationales de cybercriminalité.
- Team "Intelligence" s'occupe de la gestion des informations, de l'échange international d'informations et de la création d'une image de la criminalité informatique.
- Team "R&D" développe une expertise dans certains domaines de haute technologie et soutient des recherches spécialisées dans son domaine d'expertise.

RCCU: Regional Computer Crime Unit

- 14 Unités
- 1/Police judiciaire fédérale déconcentrée
 - MONS, CHARLEROI, NAMUR, LIEGE, EUPEN, LUXEMBOURG, NIVELLES, BRUXELLES

Police Judiciaire Fédérale déconcentrée ?

- Missions d'enquête
 - Criminalité grave et organisée déstabilisant la société
 - Enquêtes complexes, supra-locales et/ou internationales

- Missions d'appuis aux autres unités
 - LPTS (laboratoire de Police Technique et Scientifique)
 - RCCU (Regional Computer Crime Unit)
 - Coordination avec les unités spéciales
 - Gestion des indicateurs
 - ACO (Analystes Criminels Opérationnels)

RCCU: rôles

- Traitement complet (jusqu'à la présentation d'un suspect en détention préventive en prison) des dossiers de criminalité informatique grave et/ou organisé (Circulaire du Collège des Procureurs Généraux)
- Appui des partenaires dans le traitement des pièces et/ou environnements informatiques (appui perquisition, audition, analyse de matériel, 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

RCCU: fonctionnement

- Chaque RCCU a un fonctionnement qui lui est propre (personnel cantonné à un pôle/rôle ou polyvalent, expertise locale, gardes, projets...). Il est recommandé de vous renseigner dans les unités susceptibles de vous intéresser.
- Les membres CCU sont impliqués (pilotage, participation) dans des groupes de travail au niveau national. Les membres participent à des groupes d'expertise et des projets.
- L'INPP SP ICT est avant tout un policier et peut ainsi être amené à opérer en dehors du RCCU comme « enquêteur lambda »

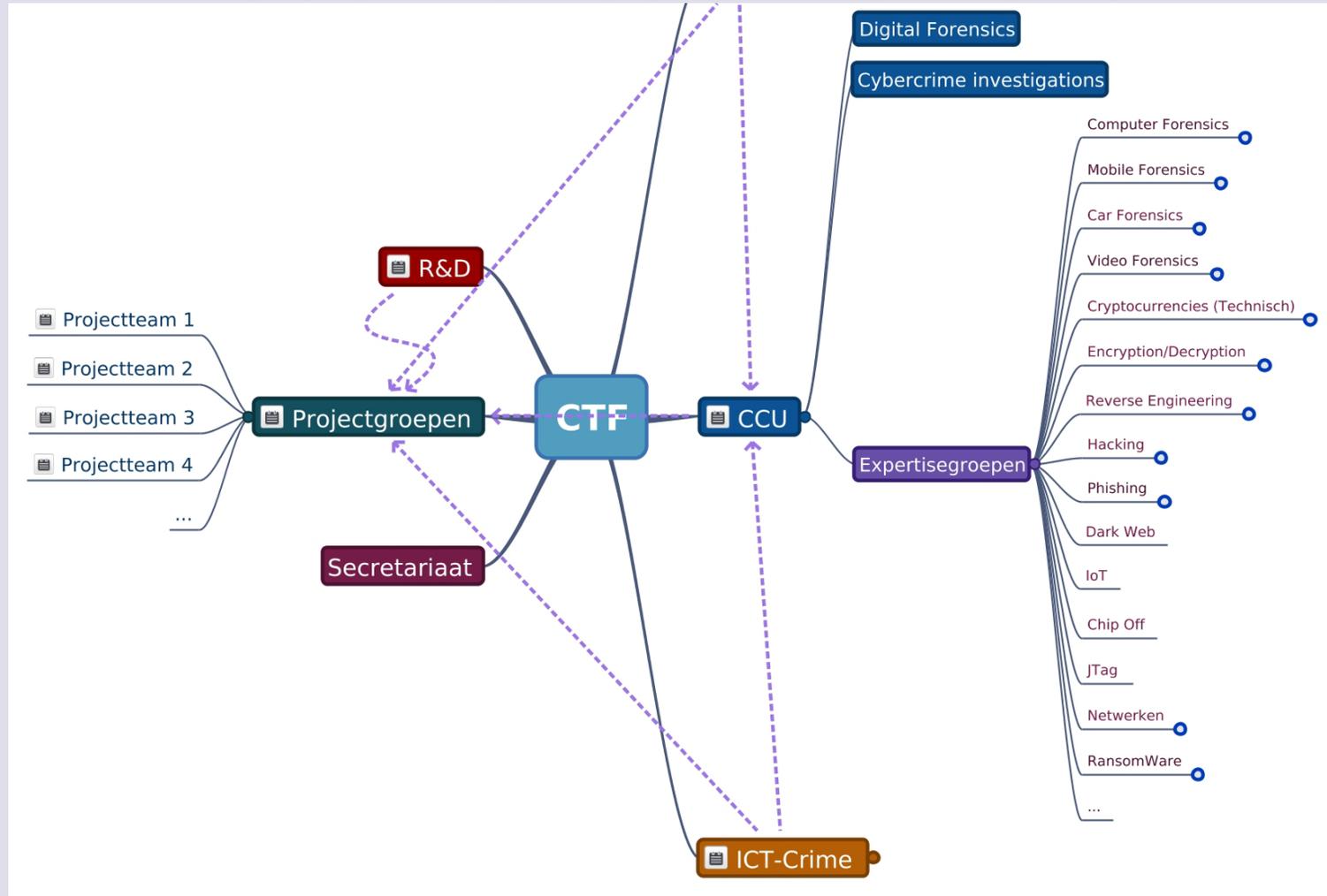
Missions

- Appuis en perquisition
- Descente « digitale » sur scène de crime
- Extractions de données de matériel informatique (Computer et mobile)
- Recherches Internet (OSINT)
- Extractions et exploitation de contenu d'images vidéo-surveillance
- Lutte contre la cybercriminalité
- « Automotive » et « IOT »
- Formations
- Autres appuis techniques

Profil des Enquêteurs

- Compétences techniques
- Compétences policières
- Motivation
- Disponibilité
- Autonomie
- Autodidacte

RCCU: fonctionnement



Challenge

- DarkWeb
- Virtual currency (BitCoin et consorts) & block chain
- Malware
- Decrypting
- IoT
- IA
- BIG DATA

De nombreux projets sont en cours dans les unités

Semaine “type” (dépend de l’organisation du CCU) peut ressembler à :

- Lundi : perqui avec ZP en matière de moeurs à 5hrs AM puis rentre au bureau pour réaliser des analyses urgentes
- Mardi : extraction de données de périphériques mobiles et rdv Magistrat
- Mercredi : réunion groupe d’expertise Automotive
- Jeudi : développement de script pour FACEBOOK puis sortie urgente suite agression pour video-surveillance
- Vendredi : rédaction de PV/rapports et dépôt d’objets au Greffe

Semaine au bureau à développer ou tenter d’arracher des données exploitables d’un PC

RCCU : interactions

- La force des RCCU réside dans la taille des unités mais aussi dans les interactions et la collaboration entre les CCU
- Les RCCU disposent d'un panel d'experts dans toutes les matières et répartis un peu partout sur le territoire
- Chaque expertise est la bienvenue et trouve(ra) sa place dans les RCCU's

CCU: partenaires

- Interne police (ZP, PolFed (navigation, route, port), AIG, Comité P, PJF)
- Magistrats
- Services public fédéraux et régionaux avec compétences « jud » (Armée, Lois Sociales, Impôts, Eaux/Forêts...)
- Services internationaux (Europol, Interpol, Eurojust, OTAN, services policiers étrangers)
- Public : CERT, IBPT,
- Monde académique (R&D)
- Privé : FEB, FebelFin, entreprise privée (partenariat)

LCCU: Local Computer Crime Unit

- Rattaché à une zone de police.
- CCU n'est pas une fonctionnalité systématique d'une ZP
- Rôle souvent plus limité, dépend de l'unité et des directives légales
- Equipe souvent restreinte et sont seuls
- Pas de recrutement actuellement en Wallonie
- Souvent le travail CCU est un travail "part time"

Epreuve professionnelle

- Test écrit en deux parties (choix multiples et questions ouvertes) – 2h30
- Domaine ICT au sens large (DB, réseau, OS, matériel, cybercriminalité, scripting, actualités ICT)

- L'examen de connaissance professionnel se compose de 2 grandes parties : une partie choix multiple et une partie questions ouvertes.
- La matière générale se décompose en 6 grands axes pour ces 2 parties :
 - Axe 1 : Hardware
 - Axe 2 : Systèmes d'exploitation
 - Axe 3 : Réseaux
 - Axe 4 : Enquête ICT
 - Axe 5 : Criminalité informatique
 - Axe 6 : Scripting

- Chaque axe est testé par des questions allant de faciles à difficiles afin d'évaluer au mieux votre niveau.
- Hardware :
Le but est de tester votre connaissance sur le fonctionnement d'un ordinateur, sa structure, ses composants à savoir les composants réseau, les composants matériels ICT dans un cadre général auxquels le personnel des CCU peut être confronté.
Vous devrez, par exemple, sur base d'une photo, reconnaître un composant ou expliquer des options de démarrage, etc.

- Systèmes d'exploitation :

Le but est de tester vos connaissances sur les grands systèmes d'exploitation existants à savoir Windows, Linux et Mac.

Il fait connaître / savoir expliquer le fonctionnement propre de chaque OS, ses particularités et les comparer en termes d'options (comparables).

Certaines commandes (extensions de fichiers) propres vous seront demandées et il vous faudra aussi savoir exprimer leurs pendant dans les autres OS ou bien décrypter certains scripts.

- Réseaux :

Le but est de tester vos connaissances sur le fonctionnement d'un réseau, son architecture, sa sécurisation, etc

Par exemple, l'adressage IP d'un réseau, sous-réseau ou bien la définition de certains termes spécifiques aux réseaux ou les concepts qui régissent le fonctionnement des réseaux.

- Enquête ICT :

Dans cette partie, on va plus toucher à des pratiques liées à des phénomènes de cybercriminalité et la sécurité informatique.

Vous devrez pouvoir connaître et définir des types d'attaques notamment ainsi que les infractions pénales y afférentes.

- Criminalité informatique :
Cela s'approche des questions précédentes mais on vous demandera des tendances actuelles dans le domaine ainsi que certaines définitions afin de déterminer votre capacité à vous tenir à jour dans ce domaine qui évolue très vite.
- Scripting :
Cette partie évalue votre connaissance en scripting / programmation.
Vous devrez expliquer le fonctionnement / résultats de scripts. Ils peuvent être en python, bash ou autre. Seuls les langages courants sont explorés.

Contacts

- RCCU MONS : Christopher DEVOS 065/34.18.25
- RCCU CHARLEROI : Alban GASMANN 071/29.13.22
- RCCU NAMUR : David WARNENT 081/24.22.71
- RCCU LIEGE : Marc SCHAERLAEKEN 04/228.92.35
- RCCU EUPEN (allemand): Danny LOOS 087/63.84.08
- RCCU LUXEMBOURG : Olivier DEGEE 063/67.04.04
- RCCU NIVELLES : Frédéric FRAND 067/28.25.25
- RCCU BRUXELLES : Cédric SMEETS 02/223.95.13

Contacts

- FCCU : Caroline FRERE 02/743.73.32
- DJO : sur demande
- Unités spéciales (DSU) : sur demande

Les adresses mails des personnes reprises ici sont sous la forme
prenom.nom@police.belgium.eu