

RAPPORT ANNUEL 2010

Police judiciaire fédérale
Direction criminalité économique et financière



CONTACTS

DIRECTION

Directeur Johan DENOLF

☎ +32 2 743 74 14

☎ +32 2 743 74 16

✉ djf.direction@skynet.be

OCDEFO

Pieter DE MEY

☎ +32 2 743 72 02 – ☎ +32 2 743 72 04

✉ djf.defo-gefid@skynet.be

Adjoints du directeur

Danièle GOFFINET – ☎ +32 2 743 73 87

Johan DE VOLDER – ☎ +32 2 743 76 87

Jan BUYS – ☎ +32 2 743 76 39

FCCU

Luc BEIRENS

☎ +32 2 743 74 74 – ☎ +32 2 743 74 19

✉ info@fccu.be

OCRC

Alain LUYCKX

☎ +32 2 743 74 48 – ☎ +32 2 743 74 08

✉ djf.ocrc-cdbc@skynet.be

FUSE

Georges CEUPPENS

☎ +32 2 743 72 08 – ☎ +32 2 743 72 33

✉ djf.fuse@skynet.be

OCRF

Alain BOUCAR

☎ +32 2 743 73 03 – ☎ +32 2 743 72 90

✉ ocrf@police.belgium.eu

P&O

Danièle GOFFINET

☎ +32 2 743 73 87 – ☎ +32 2 743 76 69

✉ djf.po@skynet.be

La Police judiciaire fédérale, c'est nous !



Depuis 2006, le pilier judiciaire de la Police fédérale porte le nom de : « Police judiciaire fédérale ». La Direction criminalité économique et financière s'intègre complètement dans le concept plus large de la nouvelle identité. Celle-ci comprend quatre caractéristiques de personnalité et quatre caractéristiques de prestation et est symbolisée par la figure yin-yang représentée ci-dessus. Notre direction participe loyalement à la stratégie de communication correspondante. Ce rapport annuel nous aide à préciser et à souligner auprès de tous les partenaires comment nous contribuons à la sécurité dans notre société.

Ce rapport est aussi disponible (en Français et en Néerlandais) sur le site web de la Police fédérale : www.Poldoc.be

Editeur responsable :

Police judiciaire fédérale, Johan Denolf – Directeur

Rue du Noyer 211, 1000 Bruxelles

Copyright photos couverture : Yves Vandermeer & Yvan Lefever

Une réalisation des Editions Politeia SA

politeia

D / 2011 / 8132 / 121

ISBN: 978-2-509-01005-6

ISBN 978-2-509-01005-6



9 782509 010056 >

LA LUTTE CONTRE LA FRAUDE EN PARTENARIAT !

« Gouverner c'est prévoir », « *Stilstaan is achteruitgaan* », « Reculer pour mieux sauter »...

Voici déjà le neuvième rapport annuel de la Direction criminalité économique et financière de la Police judiciaire fédérale. Comme tout instrument de compte rendu, le rapport annuel est un moment de réflexion sur les options de politique et les missions définies, mais c'est également un instrument de suivi de leur exécution. La communication externe de nos résultats de l'année dernière cadre dans le principe de « transparence administrative » et doit, par un apport de l'extérieur, inciter à la discussion, aux adaptations et à l'enrichissement de la ligne de politique suivie.



Ce rapport annuel s'inscrit ainsi entièrement dans le cycle de la politique. Enfin et surtout, il représente notre façon directe et sincère d'être fidèle à notre désir de rendre compte de nos activités en toute transparence.

Le temps n'est pas venu de baisser les bras. Si « gouverner c'est prévoir » et « stagner équivaut à reculer », il est parfois judicieux, voire nécessaire de « reculer pour mieux sauter ». Lors de la publication du huitième rapport annuel, il nous est revenu, de sources internes et externes, que la présentation, la forme, le volume et même le contenu n'avaient pas résisté à l'usure du temps. Les premières années après la réforme de la police, nous avons bâti sur les services existants, et ce jusqu'à la huitième version. Tout au long de ces années, le rapport annuel gagnait en volume ; nous avons ajouté des chapitres, mais nous avons omis de gommer suffisamment. Nous ne sommes pas restés sourds aux critiques justifiées, et nous avons relevé le défi ; le concept du présent rapport a subi une refonte radicale : nouvelle mise en page, nouvelle répartition du contenu, version réduite, etc. Pour la première fois, nous avons rédigé un rapport annuel propre à la direction DJF : un document expliquant les résultats des divers services dans l'ensemble de la direction DJF. Nous avons tenté de publier un document plus accessible, plus original et plus moderne. Vos commentaires sont les bienvenus !

L'année 2010 a été une année bien remplie. Nous avons cependant réussi à maintenir le cap en nous concentrant sur nos activités principales. Une direction avec notre mission, connaîtra-t-elle jamais une année non remplie, c'est la question à mille euros ! Nous avons fait un choix dans la panoplie des événements clés de 2010 : l'intégration administrative du personnel de la police présent au sein de la Commission des jeux de hasard, la création de la cellule « fraude football », le coup d'envoi de la cellule de soutien et le programme pour la lutte contre la fraude sociale grave et organisée, l'intégration et l'extension des missions du FAST (de « Fugitive Active Search Team » à « Fugitive and Asset Search Team »),... Dans le cadre de l'exécution du Plan national de sécurité, nous avons fait des efforts particuliers pour que les divers services prennent davantage conscience de leurs missions en tant que service central. Pour ce faire, nous avons tenté d'établir un équilibre entre toutes les autres unités de la Police fédérale et les services de la direction DJF. La mission suit son cours.

Comme je l'ai dit ci-avant, il est vrai que stagner équivaut à reculer. Portons donc notre regard sur les années futures. Outre la collaboration avec tous nos partenaires, une lutte efficace contre la fraude s'appuie sur les évolutions législatives, le développement des moyens de contrôle modernes, la conception de mesures spécifiques et la délimitation claire des missions. Il faut en outre faire des choix tant en ce qui concerne les manifestations de fraude, que les moyens déployés. L'organisation doit y être préparée en conséquence. Dès lors, le grand défi à relever pour 2011 sera le renforcement sur le plan de l'organisation de la direction DJF !

Cela fait déjà dix ans que je suis le coach principal d'une équipe d'excellence, de quelques centaines de collaborateurs pourvus de maintes qualités : connaissances et compétences, perspicacité, expertise, faculté de perception intellectuelle, capacité de travail, disponibilité, engagement... C'est avec satisfaction que je passe en revue nos réussites. Je suis donc, avec le recul, un manager satisfait. Je suis parfaitement conscient que je suis un coach principal privilégié ! Hommes et femmes de la direction DJF, merci !

Bruxelles, le 24 juin 2011

Johan Denolf

Directeur de la Direction criminalité économique et financière
Commissaire divisionnaire, Police judiciaire fédérale

TABLE DES MATIÈRES

CONTACTS	2
PRÉFACE	3
CHIFFRES MARQUANTS	6
CHAPITRE 1 — LA DIRECTION DJF	8
1 Organigramme	8
2 Mission et valeurs	9
3 Personnel	10
3.1 Le personnel en chiffres	10
3.2 Membres du personnel et leur statut.....	10
3.3 Personnel en termes de capacité.....	11
3.4 Bien-être au travail	11
3.5 Défis pour l'avenir	12
4 Budget	14
4.1 Généralités	14
4.2 Budget du service FCCU.....	15
5 Les services de la direction DJF	16
5.1 Introduction	16
5.2 Le service OCRC.....	16
5.3 Le service OCRF	18
5.4 Le service OCDEFO	20
5.5 Le service FCCU.....	23
5.6 Le service FUSE.....	26
5.7 Le service P&O	28
6 Suivi Plan National de Sécurité	30
7 Lutte contre la fraude en Belgique	32
8 Projets internationaux	33
8.1 ENFAST.....	33
8.2 International Mass Marketing Fraud Working Group (IMMFWG)	34
8.3 EU cybercrime task force	34
8.4 Présidence EU – Working Party on Frontiers/False documents	35
8.5 Convention UNCAC : engagement international du service OCRC.....	35

CHAPITRE 2 — SUIVI DES PROJETS 2010.....36

1	Introduction.....	37
2	Projet 1 – Un siècle de lutte contre la corruption en Belgique	37
3	Projet 2 – Intégration des officiers de liaison auprès de la Commission des jeux de hasard au sein de DJF/OCRC.	38
4	Projet 3 – Point de contact fraude football	39
5	Projet 4 – FAST financier.....	40
6	Projet 5 – Fraude sociale grave et organisée	41
7	Projet 6 – Botnets.....	42
8	Projet 7 – Infrastructure critique.....	43
9	Projet 8 – Plan de communication et plan de formation.....	44
10	Projet 9 – Locaux d’audition pour majeurs.....	44
11	Projet 10 – Accès à la Banque Carrefour des Entreprises (BCE)	45

CHAPITRE 3 — PHÉNOMÈNES45

1	Phénomène «blanchiment»	45
2	Phénomène «fraude à la TVA»	46
3	Phénomène «corruption».....	47
4	Phénomène «fraudes au préjudice de l’Union européenne».....	48
5	Phénomène «fraude aux cartes de paiement»	49
6	Phénomène «criminalité informatique»	50
7	Phénomène «fraude aux impôts sur les revenus»	52
8	Phénomène «fraude Internet».....	53
9	Phénomène «jeux de hasard».....	55
10	Phénomène «fraude aux marchés publics».....	56
11	Phénomène «escroquerie sans Internet»	57
12	Phénomène «fausse monnaie».....	58
13	Phénomène «faux documents».....	59
14	Phénomène «fraude sociale grave et organisée»	61

CHAPITRE 4 – PROJETS DJF POUR 2011 62

CHIFFRES MARQUANTS

Fraude Internet – préjudice

7.140

Le préjudice moyen causé par la fraude Internet s'élève à 7.140 euros. Dans certains cas, le préjudice prend des proportions énormes. C'est la raison pour laquelle cette moyenne est assez élevée. La médiane, qui donne un aperçu plus correct, est de 725 euros.

p. 54

Transaction – dossier construction d'encaisse

31.000.000

Une affaire de construction d'encaisse frauduleuse par la filiale belge d'un groupe alimentaire américain coté en Bourse, traitée depuis plusieurs années au sein du service OCDEFO et de l'administration des contributions, a été réglée en 2010 par une transaction. La société a consenti à payer 31 millions d'euros.

FAST – dossiers clôturés

263

En 2010, 263 dossiers propres au « Fugitive and Asset Search Team » de la police judiciaire fédérale ont été clôturés avec succès. Il a été procédé à 90 arrestations en Belgique. Parmi les fugitifs localisés à l'étranger, 35 ont été arrêtés en France, 28 aux Pays-Bas et 26 en Espagne. En outre, il y a eu 20 arrestations en Belgique de fugitifs recherchés par un autre pays européen.

p. 23

Préjudice – un dossier de blanchiment

309.388.564

Le préjudice estimé pour le Trésor belge dans un seul dossier de blanchiment, ayant comme phénomène sous-jacent la « fraude fiscale organisée », s'élevait à 309.388.564 €.

Serveurs command & control fermés définitivement

30

En 2010, 30 serveurs command & control (C&C) ont été fermés définitivement par le service FCCU. La plupart provenaient du botnet Koobface, qui faisait déjà l'objet d'investigations en 2009. De tels serveurs C&C sont utilisés pour commander un botnet, qui est un réseau composé de PC infectés d'utilisateurs finaux sous le contrôle d'un hacker.

p. 41

Enquêteurs formés

134

En mai 2010, la formation CCU « Internet Investigations » a été clôturée. Au total, 13 sessions ont été organisées. 134 enquêteurs y ont participé. Il ne reste désormais qu'à former les nouveaux membres du CCU.

p. 31

Investissements dans le matériel ICT

531.000

En 2010, 531.000 € ont été investis dans le matériel ICT pour le bon fonctionnement du service FCCU et des RCCU.

p. 15

Dénonciations exploitables eCops

18.411

18.411 dénonciations exploitables ont été reçues via le point de contact eCops en 2010 : une augmentation de 12 % par rapport à 2009, soulignant à nouveau l'importance de ce point de contact dans la lutte contre les abus sur Internet.

p. 26

CIA

4.217

Dans le cadre de la lutte contre la délinquance financière, fiscale, sociale et économique, les CIA ont transmis 4.217 documents de police à la DJF/FUSE ; le traitement desdits documents s'inscrit dans la gestion de phénomène. En comparaison, 2009 en comptait encore 6.521, ce qui représente une forte diminution de 35 %. En 2008, il s'agissait de 4.594 documents.

p. 27

Réquisitoires bancaires

1.459

1.459 réquisitoires bancaires ont été envoyés et traités par FUSE pour la police intégrée. 102 réquisitoires ont conduit au blocage temporaire ou à une saisie des sommes d'argent présentes sur le compte. En 2009, ce nombre s'élevait encore à 1.690 ; il y a donc eu une diminution de 14 %. En 2008, il y avait eu 1.214 réquisitoires bancaires.

p. 28

La coopération policière internationale

3.940

Dans le cadre de la coopération policière internationale, la DJF a traité 3.940 documents. 2009 en comptait 4.860, ce qui revient dès lors à une diminution de 19 %. En 2008, 4300 documents ont été échangés.

p. 27

Procès-verbaux corruption

5.317

L'OCRC a dressé 5.317 procès-verbaux : en comparaison, 4.538 procès-verbaux ont été dressés en 2009, ce qui représente une augmentation de 17 %.

p. 17

Faux documents – appui technique

14.358

L'OCRF a fourni un appui technique en matière de faux documents dans 14.358 dossiers. Soit une augmentation de 5 % par rapport aux 13.669 dossiers traités en 2009.

p. 19

Faux monnayage – appui technique

2.323

L'OCRF a fourni un appui technique en matière de faux-monnayage dans 2.323 dossiers. Soit une augmentation de 16 % par rapport aux 2.009 dossiers de 2009.

p. 19

Corruption – apostilles reçues

1.335

L'OCRC a reçu, en 2010, 1.335 apostilles, ce qui constitue une diminution de 8 % par rapport à l'année 2009 où 1.452 apostilles avaient été reçues.

p. 17

RIO – pièces traitées

12.000

En ce qui concerne l'année 2010, la première année complète d'utilisation du registre RIO (Registre In Out) des pièces entrantes et sortantes, 12.000 pièces ont été enregistrées, pièces internes non incluses.

Questions parlementaires à la DJF

43

Au cours de l'année 2010, 43 questions parlementaires ont été adressées à la direction DJF.

Appui technique piraterie et contrefaçon

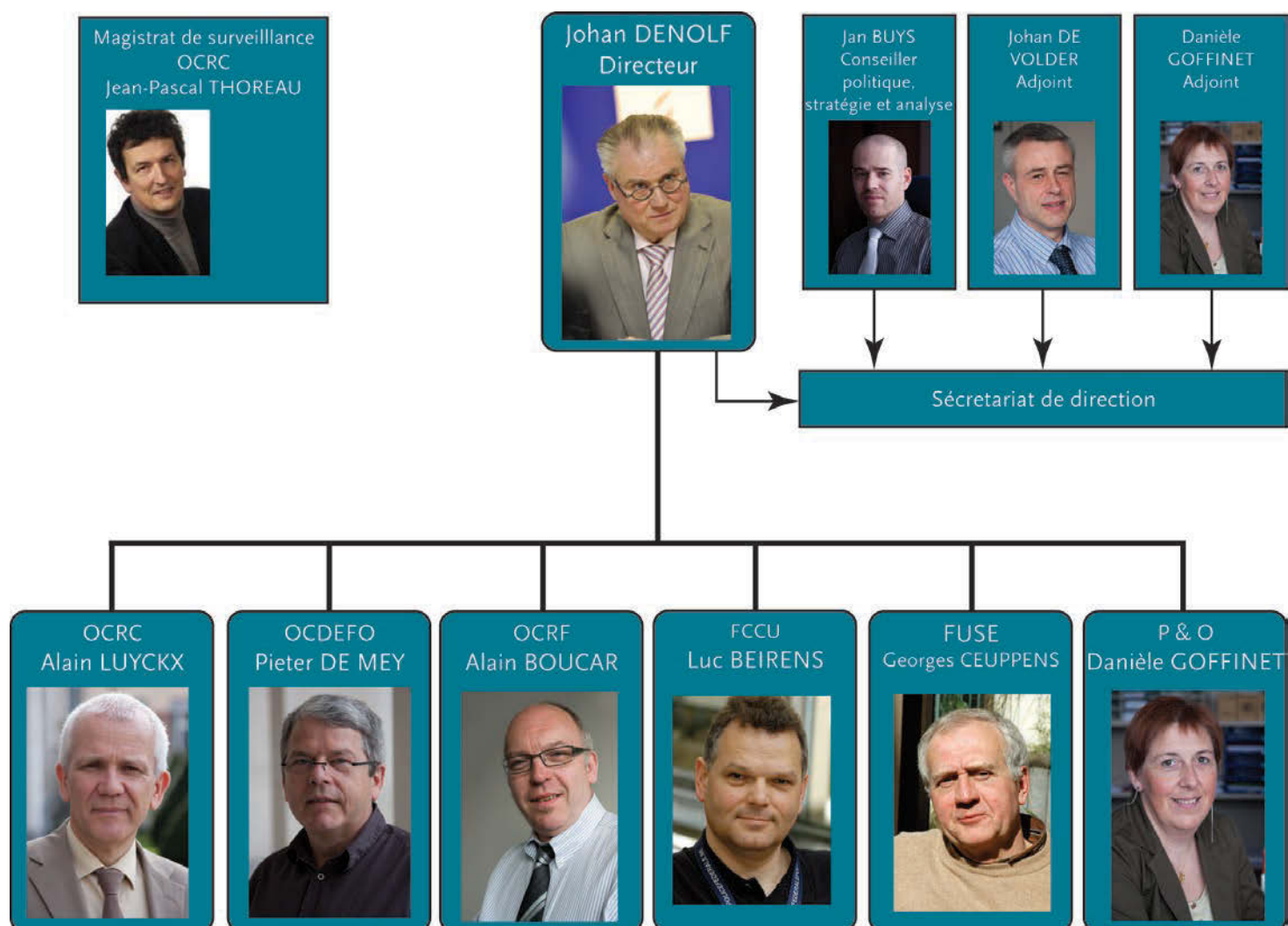
1.013

Il y a eu au total 1.013 dossiers d'appui technique piraterie et contrefaçon pour l'année 2010. En comparaison avec les 1.175 dossiers de 2009, nous constatons donc une diminution.

p. 20

CHAPITRE 1 — LA DIRECTION DJF

1. ORGANIGRAMME



2. MISSION ET VALEURS

La Police fédérale contribue, avec la police locale, à l'accroissement de la sécurité, au maintien et au développement de l'état de droit démocratique, en assurant une fonction de police intégrale et intégrée et en garantissant une prestation de service minimale équivalente sur l'entièreté du territoire. Pour la Direction de la criminalité économique et financière (direction DJF), cela signifie l'exécution des missions de police spécialisées et supralocales, en respectant les principes de spécialité et de subsidiarité, et l'appui aux autorités policières et aux services de police (locaux). Elle contribue avec d'autres acteurs à mieux maîtriser et même réduire les problèmes de sécurité avec professionnalisme, combativité et souci de résoudre les problèmes.

La direction DJF contribue à la maîtrise et à la lutte contre les phénomènes déstabilisant la société sur le plan de la criminalité économique, financière et fiscale organisée, de la fraude sociale grave et organisée, de la corruption (tant publique que privée), de la criminalité informatique, des faux (faux documents et fausses monnaies), des escroqueries organisées (avec ou sans Internet) par le développement et la fourniture :

- d'un appui conceptuel, opérationnel et technique ;
- d'informations, d'expertise et de coordination ;
- d'une capacité de recherche hautement spécialisée.

La Direction de la criminalité économique et financière le fait par :

- une gestion dynamique (recueil, traitement, diffusion et exploitation) des informations spécialisées ;
- une contribution à la réalisation d'une image policière nationale ;
- le développement de modèles conceptuels concernant les formes d'apparition des phénomènes dans la criminalité économique, financière, fiscale et sociale, la corruption, la criminalité informatique ; les faux et les escroqueries organisées et en harmonisant leurs aspects policiers sur une approche intégrale et intégrée ;
- la recherche et le développement de techniques et tactiques spécifiques aux phénomènes et l'élaboration des entraînements et des formations en les initiant ;
- la contribution à une formation générale à partir des compétences centrales ;
- l'initiation et la réalisation d'enquêtes complexes et de grande envergure dans le domaine de la criminalité économique, financière, fiscale et sociale, la corruption, la fraude aux subsides et les délits commis dans le cadre de l'adjudication et de l'exécution des marchés publics ;
- la fourniture – sur demande – de l'appui et de la coordination opérationnels au profit des enquêtes d'information et d'instruction qui sont menées par les directions judiciaires déconcentrées dans les arrondissements ;
- la fourniture d'un appui opérationnel et technique dans le cadre des enquêtes dans un environnement automatisé, de la criminalité informatique, des faux, de la recherche axée sur le butin et la localisation, la recherche et l'arrestation de fugitifs ;
- la coopération avec les partenaires nationaux et internationaux ;
- la prospection des liens de coopération avec les partenaires tant du secteur public que privé.

Lors de l'exécution de ses tâches et de ses missions, la direction DJF respecte les droits et libertés individuels ainsi que la dignité de chaque personne. Son intervention est marquée par l'intégrité et l'impartialité, un grand sens des responsabilités et le respect des normes légales à appliquer. La direction se montre loyale envers les institutions démocratiques. En tant que direction, elle fournit une prestation de service de qualité à l'égard de ses clients et commanditaires et tous les collaborateurs contribuent au bien-être au travail dans un esprit de respect et de valorisation mutuels.

3. PERSONNEL

3.1. Le personnel en chiffres

La Direction de la criminalité économique et financière est la direction centrale la plus importante de la Police judiciaire fédérale en termes de nombre de membres du personnel. Dès son apparition (lors de la réforme des polices en 2001), le tableau organique prévoyait 196 postes, dont 157 destinés à des collaborateurs opérationnels, 39 à des collaborateurs administratifs et logistiques (CAlLog). A l'époque, le cadre était occupé à 75 %. Le nombre de membres du personnel au sein de la direction est toutefois en évolution constante, comme en témoigne le tableau suivant.

L'augmentation du cadre organique (de 223 en 2009 à 251 en 2010) est principalement due à l'ajout d'une nouvelle mission, à savoir la lutte contre la fraude sociale grave et organisée. De plus, les membres du Fugitive Active Search Team (FAST, rebaptisé Fugitive and Asset Search Team) ont été insérés

DJF - Ressources humaines	2007	2008	2009	2010
Tableau organique (TO)	223	223	223	251
Effectifs présents	205	207	196	228
Pourcentage du TO rempli	92 %	93 %	88 %	91 %

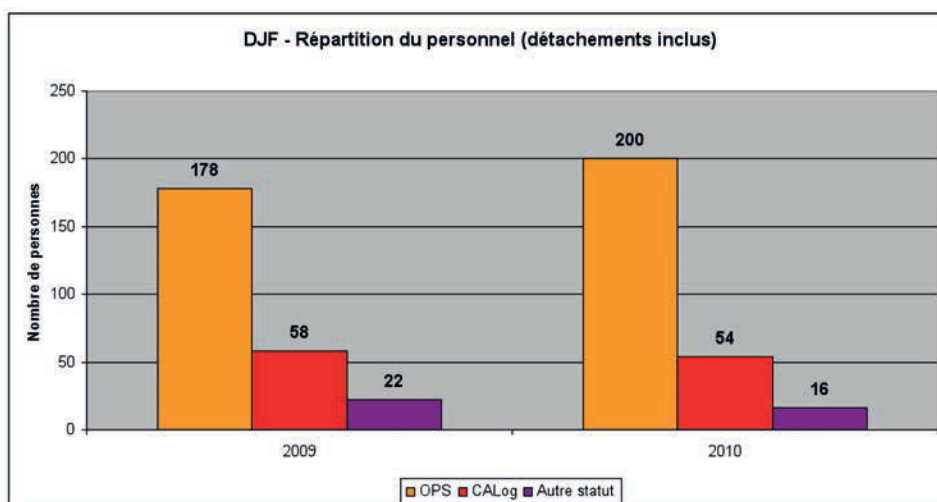
dans l'Office central de lutte contre la délinquance économique et financière organisée (OCDEFO) ; les fonctionnaires de police de la Commission des jeux de hasard ont également été intégrés dans l'Office central de répression de la corruption (OCRC).

Dans le cadre organique précité de 251 collaborateurs, il n'est toutefois pas tenu compte du nombre de collaborateurs détachés à DJF (en 2010, ils étaient une quarantaine). En outre, certains collaborateurs DJF ont été mis à la disposition d'autres services. Un membre du personnel de DJF est officier de liaison de la Police fédérale auprès de la cellule de politique du secrétaire d'Etat à la Coordination de la lutte contre la fraude, Monsieur Carl Devlies. Au total, 270 collaborateurs DJF étaient effectivement présents au 31 décembre 2010.

Au sein du bâtiment « Atrium », dans lequel la direction DJF est installée, les membres du personnel DJF côtoient les fonctionnaires des cellules de soutien (fonctionnaires fiscaux dans la cellule fraude TVA et les fonctionnaires du SIRS dans la cellule de soutien fraude sociale grave et organisée) ainsi que les membres du personnel de la direction de la police technique et scientifique (DJT). La direction DJF assure – avec le partenaire privé – la gestion de l'ensemble du bâtiment.

3.2. Membres du personnel et leur statut

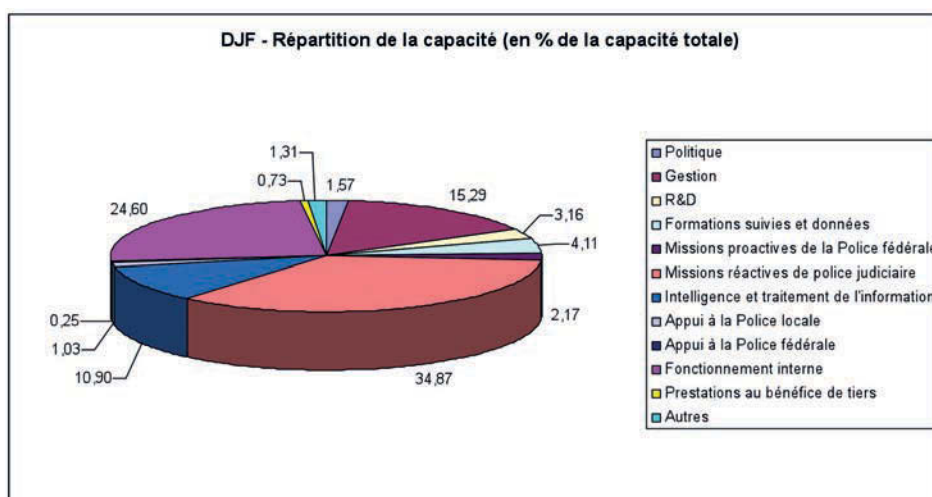
A l'aube de la réforme des polices, les collaborateurs de DJF étaient soumis à divers statuts, dont celui de la police judiciaire près les parquets, la gendarmerie, la police communale, ... Aujourd'hui, les membres du personnel présents (dépendant d'un point de vue fonctionnel de la compétence du directeur DJF) sont répartis en 3 grands groupes : les membres du personnel opérationnel, les collaborateurs CAlLog et les membres du personnel au statut différent, dont les fonctionnaires fiscaux mis à la disposition de la police. Le tableau ci-dessous donne l'aperçu du statut du personnel pour 2009 et 2010.



3.3. Personnel en termes de capacité

En 2010, un total de 507.062 heures a été presté par les membres du personnel de la Direction économique et financière. Le graphique ci-dessous en indique la répartition. Le plus gros pourcentage (34,87 %) consiste en missions réactives de police judiciaire.

Le dénominateur « fonctionnement interne » englobe notamment les jours de vacances et toutes les autres absences (dont absence pour maladie ou accident de travail), soit 24,60 %.



3.4. Bien-être au travail

Les collaborateurs sont la force de la direction DJF. C'est la raison pour laquelle la direction veille particulièrement à leur bien-être, traduit dans différents aspects.

Le directeur opte en toute connaissance de cause pour un management participatif, où les collaborateurs ont voix au chapitre dans le processus décisionnel. A cette fin, il tient des réunions mensuelles avec les chefs de service. Il encourage les responsables à un leadership similaire. Le directeur organise aussi des concertations avec tous les membres du personnel.

Les membres du personnel passant une grande partie de la journée au travail, la direction est très attentive à l'environnement matériel de travail. Des bureaux et du matériel informatique adaptés contribuent à améliorer le bien-être. Les délégations du Comité de concertation de base 197 (CCB 197) ont réagi positivement à l'implication de la Direction économique et financière dans l'exécution de sa tâche de gestion du bâtiment. La police a mis sur pied un

projet de rassemblement de divers services de la Police fédérale, dont la direction DJF, dans un même bâtiment du centre de Bruxelles (sur l'ancien site du Centre administratif). Bien que la réalisation soit prévue en 2014, ce défi génère déjà un gros travail. En effet, la direction estime que nos collaborateurs doivent au minimum conserver les conditions actuelles de travail (voire les améliorer si possible).

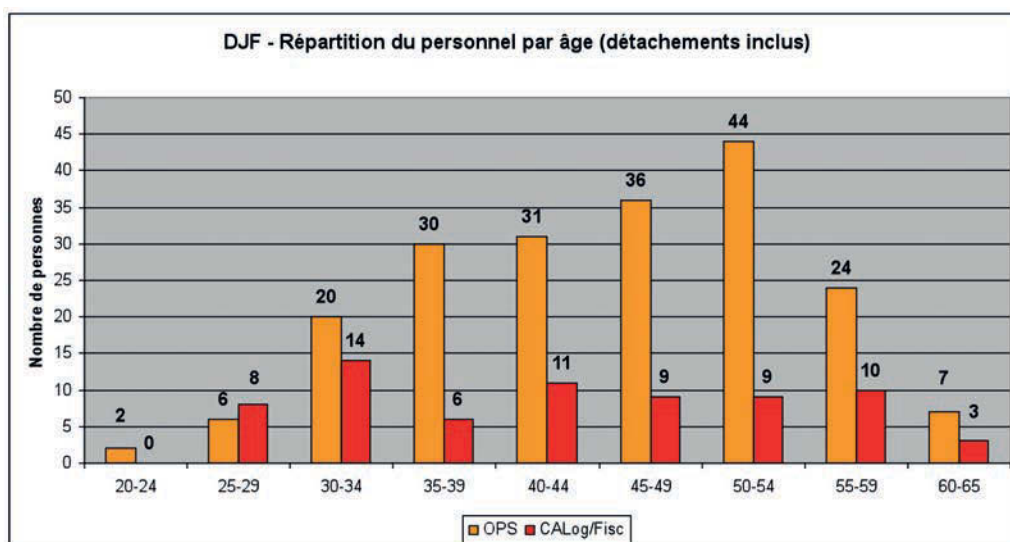
Une amélioration du bien-être et la diminution du stress lié au travail sont possibles si les collaborateurs se sentent soutenus et intégrés dans le groupe, ce qui n'est pas évident pour une grande direction. L'une des clés de la réussite consiste en une journée de teambuilding. Et il va de soi que les problèmes individuels peuvent être résolus discrètement et sur mesure, le stress team et le service médical de la Police fédérale étant ici des partenaires privilégiés.

Au séminaire stratégique de la direction (fin 2010), la décision a été prise d'effectuer un sondage auprès de tous les membres du personnel (une enquête de satisfaction des collaborateurs). Les questions traiteront de thèmes divers : la direction, le fonctionnement du service/team auquel on appartient, la communication interne, l'environnement de travail, l'appui administratif et logistique,... Les informations seront traitées de façon anonyme (par DGJ) et ensuite mises à la disposition de la direction DJF pour permettre au directeur – si possible – de réaliser des améliorations.

3.5. Défis pour l'avenir

Bien que tous les «clients» ne reconnaissent pas en la police un fournisseur de service, c'est pourtant bel et bien le cas. Contrairement à des entreprises de production, où les machines sont le principal capital, la police dispose quasi exclusivement d'un capital «humain». Les connaissances et aptitudes des collaborateurs sont sa force, d'autant plus à la Police judiciaire fédérale.

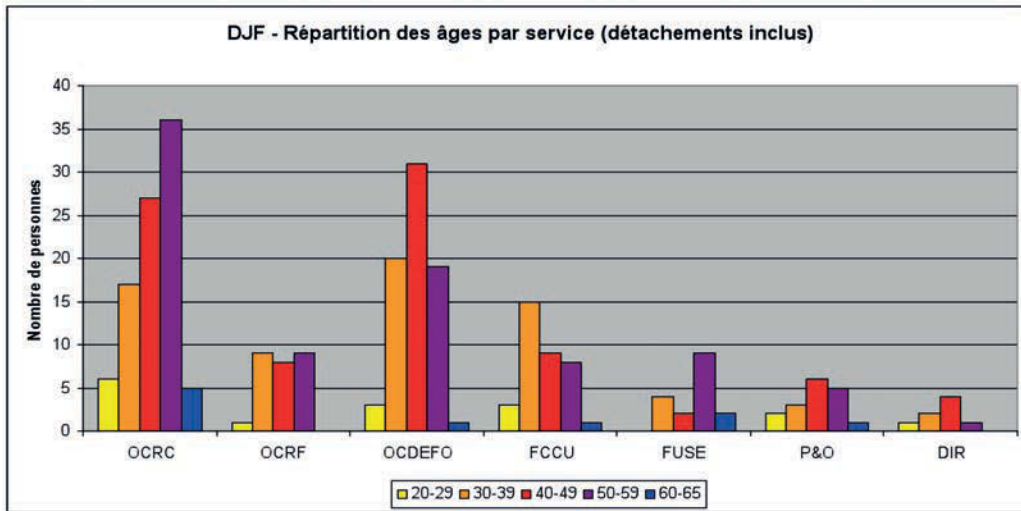
A ce niveau, l'ensemble de la Police fédérale et la direction DJF en particulier seront confrontés à de grands défis à moyen terme. Le vieillissement du corps fait que dans les années à venir, de nombreux collaborateurs auront atteint l'âge de la retraite. Le départ de ces collègues signifie également une perte de savoir-faire et d'expérience. Le graphique ci-dessous démontre le déséquilibre de la pyramide des âges de DJF.



L'âge moyen et médian est de 45 ans à la direction DJF. Dix collaborateurs ont déjà atteint l'âge de 60 ans, et auraient donc déjà pu partir à la retraite. Dans la catégorie des 55-59 ans, l'on trouve 24 collaborateurs opérationnels, dont l'âge légal de la retraite est de 58 ans et 10 CALog et/ou fiscalistes, pour qui l'âge de la retraite est de 60 ans. Ce groupe constitue 13 % du nombre total des membres du personnel de la direction.

Le pourcentage des 50-54 ans est quant à lui plus inquiétant. Avec ses 44 collaborateurs opérationnels et ses 9 CALog ou fiscalistes, ce groupe représente 20 % du nombre total des membres du personnel. Concrètement, cela signifie qu'entre aujourd'hui et dans dix ans, 36 % des collaborateurs auront pris leur retraite ou pourront la demander.

Si l'on examine les âges par service (le staff de la direction est ici indiqué par « DIR »), il apparaît clairement que ce sont surtout le service Federal Unit against Swindling and for Economic and financial documentation (FUSE, avec un âge médian de 51 ans) et le service OCRC (avec un âge médian de 48 ans) qui auront le plus à pâtir de la vague de départs à la retraite. Le service Federal Computer Crime Unit (FCCU) sera le moins touché, avec un âge médian de 40 ans.



Pour contrer ces départs massifs, il faudra à l'avenir investir sérieusement dans le « knowledge management » (pour ne pas perdre tout le savoir faire), mais aussi dans la formation de nouveaux collaborateurs (en effet, une grande partie de l'expérience ne peut être acquise qu'en interne). La formation de nouveaux collaborateurs peut sérieusement grever le budget consacré aux formations, d'autant plus lorsque le gouvernement demande aux autorités et à leurs services de faire preuve de modérations budgétaires.

4. BUDGET

4.1. Généralités

Les dépenses totales de la Direction économique et financière ont augmenté de 1.239.993 € (+7,4 %), pour atteindre 17.986.411 € pour l'exercice 2010. En examinant les chiffres de plus près, l'on constate immédiatement que cette augmentation est due à la hausse du coût total en personnel (qui a augmenté de 1.603.584 € pour atteindre 14.279.506 € en 2010). Rien d'étonnant en soi car le cadre organique a augmenté (à cause de missions complémentaires) et le vieillissement du personnel accroît le coût salarial.

Le second gros poste de dépenses reste évidemment les bâtiments. La location représente 2.131.523 €, hors entretien (qui à lui seul revient à 421.631 €).

Poste	Détail	2007	2008	2009	2010
Personnel	Salaires	12.182.097	12.147.269	12.261.869	13.865.453
	PRE (heures supplémentaires,...)	385.962	423.671	360.937	386.184
	Formation	15.000	15.000	10.500	27.869
	<i>Sous-total personnel</i>	12.583.059	12.585.940	12.633.306	14.279.506
Bâtiment	Loyer du bâtiment Atrium	2.007.373	2.007.373	2.109.658	2.131.523
	Entretien du bâtiment	446.789	648.000	499.000	421.631
	Energie (électricité)	75.426	43.296	47.695	36.980
	<i>Sous-total bâtiment</i>	2.529.588	2.698.669	2.656.353	2.590.134
Parc automobile	Investissement	84.000	275.310	21.984	60.000
	Entretien	14.261	12.241	12.281	12.526
	Carburant	54.620	61.863	55.912	56.114
	<i>Sous-total parc automobile</i>	152.881	349.414	90.177	128.640
Matériel	Achats locaux (investissement)	47.717	50.477	49.841	46.206
	Achats (consommables)	51.000	63.000	62.000	69.030
	Photocopieur (achat & entretien)	7.233	12.400	10.776	3.718
	Informatique (investissement)	77.780	105.210	182.902	46.887
	<i>Sous-total matériel</i>	183.730	231.087	305.519	165.841
Communication	Téléphone et télécopie (lignes fixes)	75.426	43.296	47.695	36.980
	Internet	6.848	7.320	7.338	6.741
	<i>Sous-total communication</i>	82.274	50.616	55.033	43.721
Autres	Frais de voyage	60.155	81.497	19.204	56.131
	Représentation CGPR	1.200	1.200	1.200	1.350
	<i>Sous-total autres</i>	61.355	82.697	20.404	57.481
Au bénéfice des PJF	Investissement ICT RCCU et FCCU	780.350	431.869	813.891	531.000
	Accès données (Euro DB, Cofaces)	94.380	94.380	94.380	94.380
	Bibliothèque EcoFin	38.716	38.853	33.706	39.194
	<i>Sous-total au bénéfice des PJF</i>	913.446	565.102	941.977	664.574
Total		16.507.644	16.635.924	16.746.418	17.986.411

4.2. Budget du service FCCU

4.2.1. Investissements dans la technologie et l'informatique

En 2010, la Police judiciaire fédérale a mis à disposition un budget d'investissement de 531.000 euros pour l'achat de matériel d'enquête ICT spécifique destiné à la Federal Computer Crime Unit (FCCU), aux RCCU et à la Cellule télécommunication et interception (CTI).

La Direction de la criminalité économique et financière, via le Service FCCU et en collaboration avec le Service d'appui technique à la politique de la direction générale de la police judiciaire, a lancé huit adjudications pour l'achat de matériel standardisé pour l'enquête ICT.

L'objectif des investissements pour 2010 était non seulement de remplacer le matériel dépassé (acheté en 2007), mais aussi de mettre à disposition du nouveau matériel tel que :

- un poste de travail comprenant les logiciels et disques durs nécessaires à tous les membres opérationnels CCU ;
- un serveur pour visualiser l'infrastructure ;
- des mises à jour de logiciels pour analyse légale de PC et réseaux (X-ways et FTK).

4.2.2. Moyens matériels en dehors du budget police

En 2010, le SPF Justice a une fois encore libéré un budget (d'environ 200.000 euros) pour l'achat de supports de données (disques durs, CD-ROM et DVD) sur lesquels les RCCU peuvent enregistrer et conserver des copies.

Il n'est pas anormal que ce matériel soit payé par le SPF Justice : cela a déjà été le cas et cela s'explique par le fait qu'il s'agit de frais de justice. La copie légale constitue en effet une preuve en matière répressive. DJF/FCCU, fort de son savoir-faire et de son expertise, donne un avis technique au SPF Justice sur les achats et gère la provision pour le SPF Justice. Cette collaboration est très appréciée des deux parties et constitue une plus-value pour chacune d'elles.

5. LES SERVICES DE LA DIRECTION DJF

5.1. Introduction

La direction DJF est dirigée par le directeur mandataire Johan Denolf. L'année 2010 était la dernière année de son deuxième mandat. Il a obtenu une bonne évaluation pour la période achevée et par ce fait un nouveau mandat. A la fin de l'année 2010, la lettre de mission a été rédigée, avec pour titre : « Un mandat fidèle à la mission de la Direction de la criminalité économique et financière, renforçant l'organisation de la direction et établissant les acquis et réalisations du passé ».

La direction DJF se compose, outre des adjoints, du conseiller en politique, stratégie et analyse et du secrétariat de direction, de six services qui seront décrits ci-après.

5.2. Le service OCRC

5.2.1. Organisation

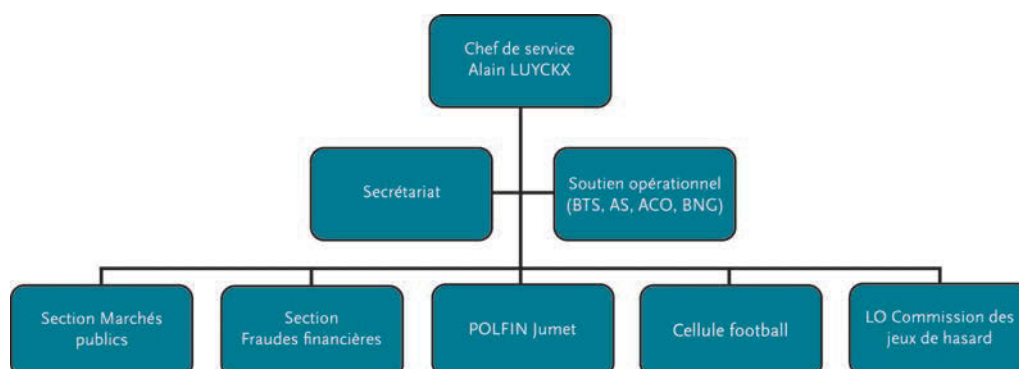
L'Office central pour la répression de la corruption (OCRC) compte deux sections composées d'enquêteurs appartenant aux rôles linguistiques francophone et néerlandophone :

- la section « Marchés publics » s'occupe principalement de dossiers relatifs à des fraudes en matière de marchés publics (par exemple les adjudications publiques lors de travaux sur le réseau routier) ;
- la section « fraudes financières » s'occupe de tous les autres dossiers de fraude confiés au service, notamment les fraudes aux subsides ou en matière de permis (par exemple permis de construire).

Chaque section est divisée en équipes d'enquête plus petites dont la taille varie selon l'importance et l'ampleur du dossier.

En 2010 le service OCRC a intégré deux entités particulières :

- la cellule « Fraude et Football », qui est chargée de la lutte contre la fraude dans cette discipline sportive, a été créée à la demande des ministres de l'Intérieur et de la Justice. Elle enquête sur des matchs truqués qui peuvent être la conséquence de la corruption de joueurs et/ou d'arbitres en vue d'obtenir les gains des paris ;
- Les officiers de liaison auprès de la Commission des jeux de hasard et ce, notamment, en vue d'une meilleure coordination des enquêtes entre la Commission des jeux de hasard et la police.



5.2.2. Domaines d'activité

Le service OCRC est l'un des plus grands services au sein de la direction DJF. La majorité du personnel y est chargée de tâches opérationnelles, judiciaires comme l'exécution de perquisitions, l'audition de témoins et de suspects, l'arrestation de personnes, la saisie de pièces à conviction,... Le service, qui est le successeur du Comité supérieur de contrôle, se différencie toutefois de son prédécesseur du fait qu'il ne dispose plus de la compétence de mener des enquêtes administratives sur, par exemple, le déroulement des adjudications publiques. Il s'agit donc uniquement d'enquêtes d'information et/ou d'enquêtes judiciaires qui sont réalisées soit de manière autonome, soit en appui des unités déconcentrées de l'arrondissement. Le choix de l'une ou l'autre méthode dépend, notamment, de la gravité des faits (qui constituent la base de l'enquête), de la fonction (publique et/ou privée) exercée par un suspect, de la crainte du soupçon de partialité si l'enquête était traitée au niveau de l'arrondissement.

Les compétences du service OCRC sont les suivantes :

- la recherche et l'appui à la recherche des crimes et délits complexes et/ou graves relevant de la corruption publique (au sens large) ;
- la recherche et l'appui à la recherche des crimes et délits complexes et/ou graves relevant de la corruption privée ;
- la recherche et l'appui à la recherche des infractions à la législation sur les marchés publics ;
- la recherche et l'appui à la recherche des infractions à la législation sur les subsides publics ;
- la recherche et l'appui à la recherche des crimes et délits relevant de la corruption publique dans les institutions de la Communauté européenne et des infractions à la législation sur les subsides européens ;
- l'exécution d'enquêtes qui peuvent troubler l'opinion politique de par la personnalité des suspects ;
- l'exécution de missions stratégiques telles que le suivi du PNS, la recherche et le développement pour les phénomènes propres et le suivi de ces phénomènes.

5.2.3. Le service OCRC et quelques résultats

Les délits comme la corruption publique, la concussion et le détournement par des fonctionnaires, le conflit d'intérêt de la part des fonctionnaires ou des mandataires et la fraude aux marchés publics peuvent gravement perturber l'opinion publique. Lors de la réforme de la police, le niveau politique a pris la décision de conserver une capacité d'enquête pour ce genre de dossiers au niveau central. La perception qu'a le grand public de l'intervention de ces fonctionnaires de police est qu'il s'agit d'une intervention plus neutre et plus indépendante que celles que pourraient mener les équipes d'enquête travaillant sur le même territoire que le(s) suspect(s). Les magistrats (membres du ministère public ou juges d'instruction) confient dès lors un grand nombre de missions à DJF/OCRC. En 2010, 1.335 apostilles ont été reçues, ce qui constitue une légère diminution par rapport à l'année 2009 (diminution de 8 %), année où un nombre record de 1.452 apostilles avait été enregistré. Les fonctionnaires de police du service ont rédigé un total de 5.317 procès-verbaux initiaux et subséquents, ce qui représente une augmentation de 17 % par rapport à l'année 2009. Le tableau ci-dessous montre l'évolution de ces quatre dernières années.

DJF/OCRC - Apostilles & procès-verbaux	2007	2008	2009	2010
Nombre d'apostilles reçues	972	1.104	1.452	1.335
(évolution par rapport à l'année x-1)	-16 %	+14 %	+32 %	-8 %
Nombre de procès-verbaux rédigés	3.778	2.994	4.538	5.317
(évolution par rapport à l'année x-1)	+22 %	-21 %	+52 %	+17 %

Des résultats excellents n'ont pas seulement été enregistrés sur le plan opérationnel. 2010 a également été une année chargée en ce qui concerne les missions conceptuelles. Ainsi, l'analyse des phénomènes « corruption publique, concussion et le conflit d'intérêt » a été réalisée pour les exercices 2007 à 2009. Cette analyse est la première entièrement basée sur les chiffres de la BNG.

L'année 2010 est également l'année au cours de laquelle la police intégrée prépare l'Image policière nationale de sécurité 2011. Un effort particulier en matière de formation d'image est pour ce faire demandé à la Police judiciaire fédérale. Le service OCRC a procuré des informations sur les phénomènes suivants dans le cadre de l'Image policière nationale de sécurité (IPNS) :

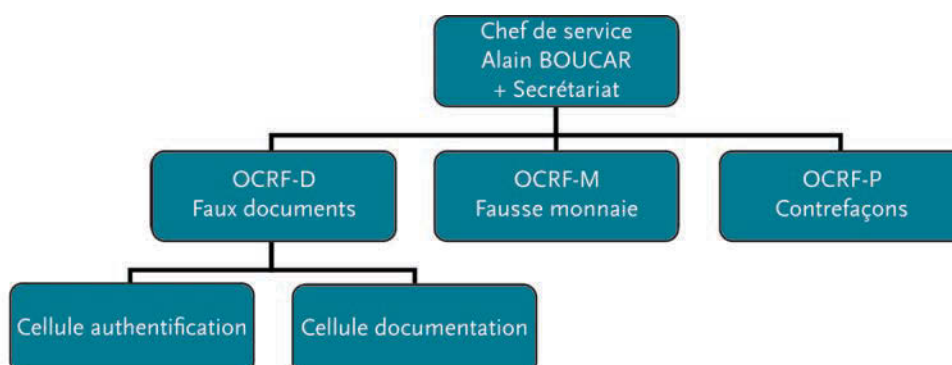
- corruption (corruption publique, corruption privée, concussion, conflit d'intérêt et détournement par un fonctionnaire) ;
- infractions en matière de jeux de hasard et de loterie (en ce inclus la fraude football) ;
- fraude au préjudice des administrations publiques (marchés publics et subsides au niveau européen et belge).

Nous reviendrons dans la partie de ce rapport annuel consacrée aux projets sur la journée d'étude (qui s'est tenue le 27 octobre 2010) consacrée aux 100 ans de lutte contre la corruption en Belgique sous le vocable « persisting the way to integrity, vers une approche plus proactive de la corruption ».

5.3. Le service OCRCF

5.3.1. Organisation

L'Office central pour la répression des faux (OCRF) est composé de trois sections : la section fausse monnaie (située dans les bâtiments de la banque nationale de Belgique), la section faux documents et la section contrefaçon. Cette dernière unité sera supprimée début 2011 suite à l'évaluation réalisée durant le séminaire stratégique de la direction (13 et 14 décembre 2010). Il a en effet fallu constater que l'administration des Douanes et Accises prend en charge 96,5 % de la problématique et qu'un accord de coopération entre police et douane faisait toujours défaut. Le nombre limité de membres du personnel dans cette section et le départ de l'un d'entre eux pour Europol ont donc mené à l'exécution de la décision prise, décision approuvée par le directeur général et qui a été communiquée aux partenaires concernés.



5.3.2. Domaines d'activité

L'Office central pour la répression des faux (OCRF) est un point de contact et d'appui national et international pour la répression :

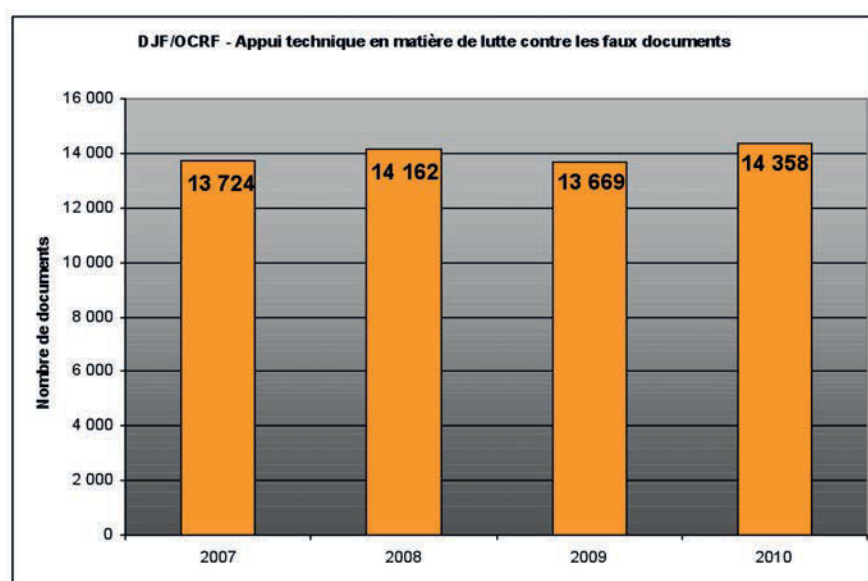
- des falsifications de documents d'identité ;
- de la fausse monnaie ;
- des contrefaçons de produits pouvant compromettre la santé publique, ainsi que la violation des droits d'auteur ou d'autres formes de piraterie (ce dernier domaine d'activité disparaîtra en 2011).

Le service OCRF remplit les missions suivantes :

- soutenir les actions répressives des services de Police fédérale et locale en matière de faux et de falsifications en leur offrant une expertise de qualité et un appui technique ;
- brider la contrefaçon et l'usage de faux documents ;
- aider les services compétents à améliorer la sécurité de leurs documents ;
- et contribuer à améliorer la confiance du public dans la monnaie unique euro et ce par une action efficace contre la fausse monnaie.

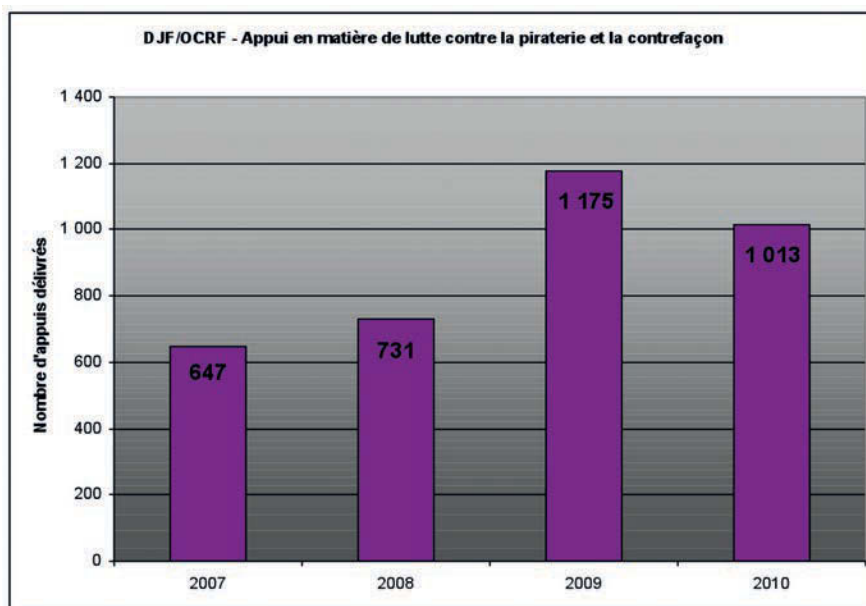
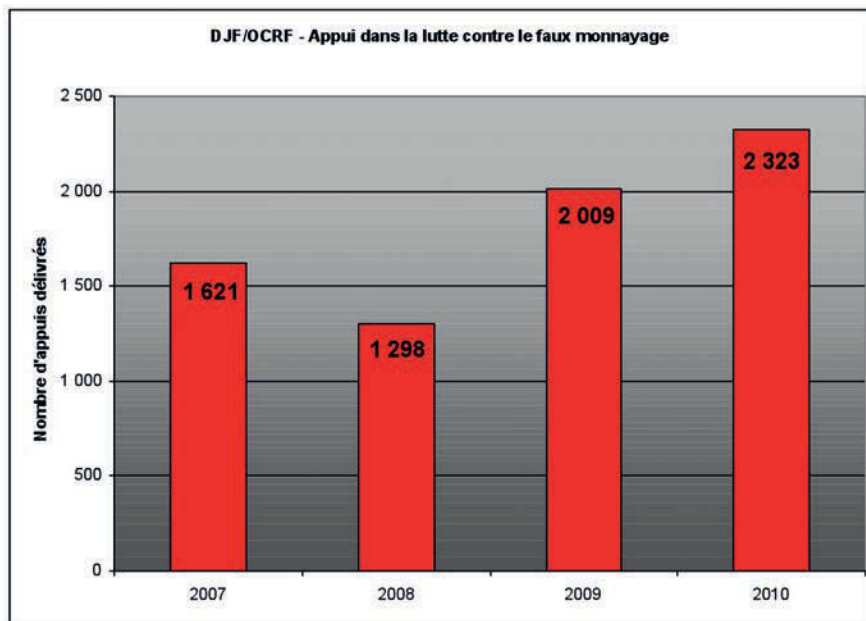
5.3.3. Le service OCRF et quelques résultats

Le « core business » de la section « faux documents » réside dans la fourniture d'un appui spécialisé en matière d'authenticité des documents, tant en ce qui concerne les permis de conduire (en exécution de la circulaire OP17) que les inscriptions des citoyens des états membres de l'Union européenne en Belgique (projet « Europa », en exécution de la circulaire du 31 décembre 1997). Avec les 14.358 documents dont l'authenticité a été contrôlée, la section « faux documents » a établi un nouveau record. Le nombre est le plus élevé de ces quatre dernières années et représente en même temps une augmentation de 5 % par rapport à l'année 2009. Le graphique ci-dessous détaille cette évolution.



Au niveau conceptuel, la section « faux documents » s'occupe principalement du développement de Braingate (une banque de données des documents analysés), et l'appui technique au SPF Intérieur (en matière de délivrance de documents). Le service assure également une grande part de la formation des autres services publics.

La section « fausse monnaie » fournit principalement un appui technique. En 2010, elle a été sollicitée à 2.323 reprises. Pour l'année 2009, l'appui technique s'élevait à 2.009, ce qui signifie une augmentation de 16 %.



L'appui de la section « contrefaçon » est passé de 1.175 en 2009 à 1.013 en 2010, ce qui représente une baisse de presque 14 %. Cet appui demeure toutefois plus élevé que pour les années 2007 et 2008.

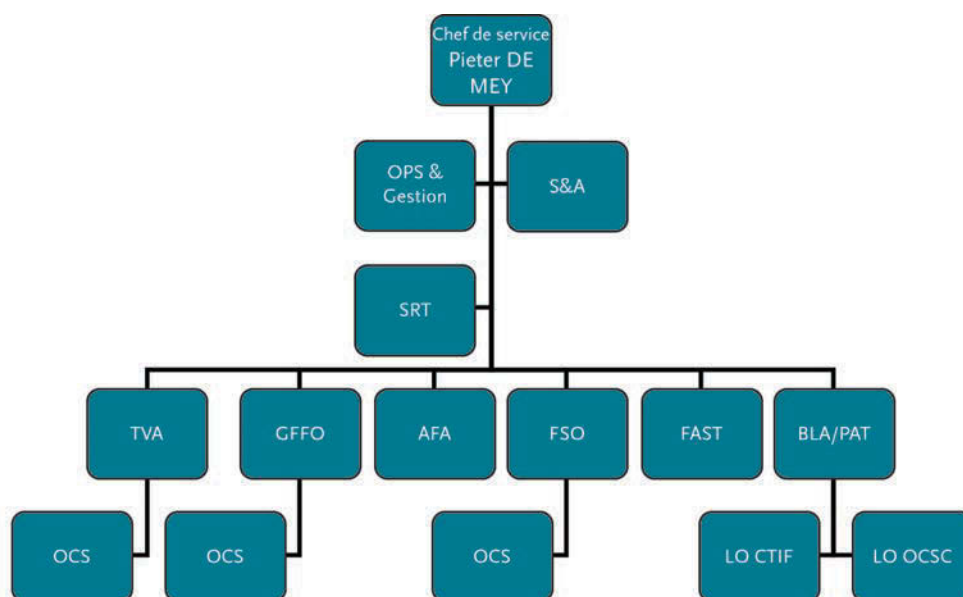
5.4. Le service OCDEFO

5.4.1. Organisation

Pour l'exécution de ses missions, l'Office central de lutte contre la délinquance économique et financière organisée (OCDEFO) dispose de policiers opérationnels et de membres du cadre administratif et logistique, répartis dans 6 sections : blanchiment/patrimoine, TVA, fraude fiscale organisée (GFFO), fraude sociale grave et organisée (FSGO), Fugitive & Asset Search Team (FAST) et enfin la section Analyse financière (AFA).

Ces collaborateurs sont par ailleurs secondés par 16 fiscalistes, qui sont des fonctionnaires mis à disposition par le SPF Finances, pour appuyer la police grâce à leur expertise particulière dans l'exécution des enquêtes (autonomes ou en appui). Après une formation supplémentaire imposée, ils reçoivent tous la qualité d'officier de police judiciaire (OPJ), qui leur permet de poser certains actes d'enquête de manière indépendante. Ces fiscalistes ne doivent toutefois pas être confondus avec les collaborateurs du SPF Finances qui travaillent dans la cellule d'appui Fraude à la TVA (et qui sont détachés du SPF Finances). Ces derniers ne disposent en effet pas de la qualité d'officier de police judiciaire, mais sont chargés de la coopération administrative particulière sur le plan fiscal (avec Eurofisc) et de la diffusion des connaissances sur les modes opératoires en matière de fraude à la TVA auprès des autorités judiciaires et policières (ministère public et police).

Un organe similaire a été mis sur pied pour la fraude sociale. Conséquemment à l'exécution du plan d'action 2009-2010 pour la lutte contre la fraude du secrétaire d'Etat Devlies, un nouvel accord de coopération a été conclu, englobant une section policière opérationnelle (GSF) et une cellule d'appui (OCS). Cette OCS est composée d'inspecteurs sociaux et de personnel policier. Elle joue un rôle important de par son expertise conceptuelle et technique. Ce dispositif multidisciplinaire



a pour but, par une approche intégrale et intégrée, de détecter et démanteler prématurément les structures criminelles qui facilitent ou aident à organiser la fraude sociale grave.

5.4.2. Domaines d'activité

Le service OCDEFO a été fondé en 1993. En 1994, il était hébergé auprès de l'ancien Service général d'appui policier (SGAP), pour ensuite rejoindre en 1998 la police judiciaire près les parquets, où ses missions ont pour la première fois été fixées dans un arrêté royal. Depuis la réforme des polices, ce service constitue une division de la direction DJF. L'histoire du service est caractérisée par un accroissement du personnel. Le service dispose d'un grand nombre d'enquêteurs qui assurent son fonctionnement opérationnel. Ils mènent des enquêtes spécialisées autonomes ou fournissent un appui aux autres unités de la police intégrée et ce, pour les phénomènes de blanchiment d'argent, de fraude à la TVA, de fraude à l'impôt sur le revenu et, depuis 2010, de fraude sociale grave et organisée (voir les chapitres « Suivi des projets 2010 » et « Phénomènes »).

Le service est également requis pour coordonner/exécuter les commissions rogatoires internationales pour lesquelles aucune PJF ne peut être désignée ou pour lesquelles la coopération de plusieurs PJF doit être harmonisée. Dans cette optique, l'alimentation des Analytical Work

Files d'Europol (comme notamment l'AWF Sustrans en matière de blanchiment et l'AWF MTIC en matière de fraude à la TVA) est une mission importante aux dimensions supranationales.

Outre la mission opérationnelle précitée, les missions conceptuelles (comme la formation d'image, l'élaboration de stratégies, la mise à jour des réseaux) font l'objet de beaucoup de soins.

Au sein de DJF/OCDEFO, beaucoup d'attention est traditionnellement consacrée à la recherche sur la recherche orientée vers le butin et/ou les avoirs suspects, qui se traduit par un partenariat avec la Cellule pour le traitement des informations financières (CTIF), où des officiers de liaison sont mis à contribution. Une procédure a spécialement été élaborée pour intervenir rapidement lorsque le blanchiment d'argent est en cours. Dans une telle situation, l'argent en question sera rapidement saisi, via la procédure dite « Répap », pour éviter qu'il ne disparaisse dans le système financier. Qui parle de saisie d'avoirs parle aussi de la gestion de la valeur des biens en attendant un jugement de fond devant le tribunal. Cette gestion de la valeur est confiée à l'Organe central pour la saisie et la confiscation (OCSC), un autre partenaire où le service compte deux officiers de liaison. Et, pour boucler la boucle, une coopération particulière existe avec les Pays-Bas et la France car les auteurs de délits de blanchiment (outre les sujets belges) sont principalement des personnes de nationalité néerlandaise ou française.

Une autre nouveauté depuis 2010 est le rattachement du « FAST », qui recherche les fugitifs et à propos duquel nous parlerons davantage dans la suite de ce rapport annuel (Suivi des projets, page 38).

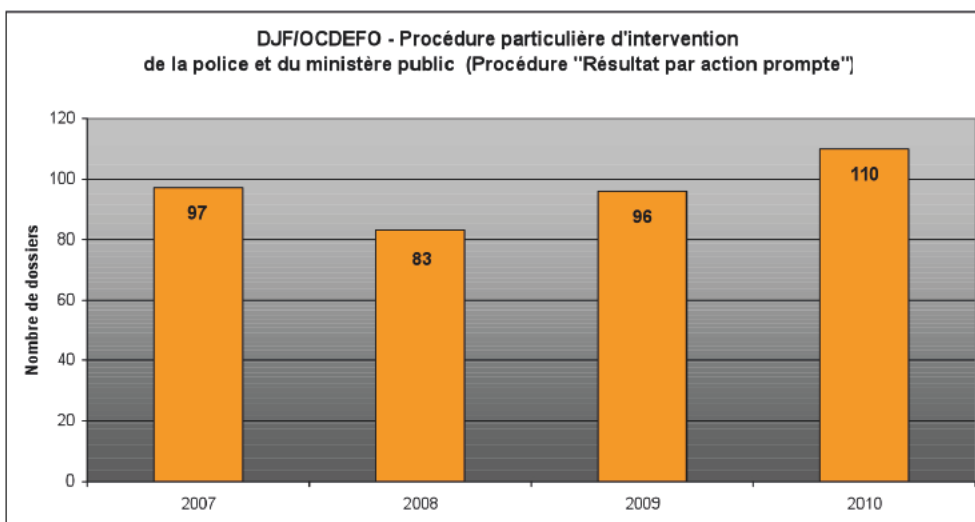
5.4.3. Le service OCDEFO et quelques résultats

Une grande partie du personnel du service OCDEFO est chargée de missions d'enquêtes opérationnelles. Il convient donc d'en rendre compte au moyen de quelques chiffres-clés. Ainsi, le nombre d'apostilles

reçues en 2010 a atteint 571, soit une augmentation de 48 %. Le nombre de procès-verbaux (initiaux et subséquents) a toutefois chuté de 13 % pour atteindre les 1.898 en 2010.

DJF/OCDEFO - Apostilles & procès-verbaux				
	2007	2008	2009	2010
Nombre d'apostilles reçues	693	466	385	571
(évolution par rapport à l'année x-1)	+36 %	-33 %	-17 %	+48 %
Nombre de procès-verbaux rédigés	2.037	1.612	2.182	1.898
(évolution par rapport à l'année x-1)	-2 %	-21 %	+35 %	-13 %

La confiscation des avantages matériels est importante pour la section blanchiment/patrimoine. En ce qui concerne l'intervention rapide de la police et du ministère public sur les



montants détectés par la Cellule de traitement des informations financières (appelée procédure Répap, «résultat par action prompte»), 110 dossiers d'intervention ont été ouverts en 2010 (soit une augmentation de presque 15 % par rapport à 2009). Il s'agit de plus, comme le montre le graphique ci-dessous, du nombre de dossiers le plus élevé sur les quatre dernières années.

Un montant total de 42,14 millions d'euros a été enregistré pour ces 110 dossiers, contre 25,81 millions d'euros pour l'année 2009, ce qui signifie une augmentation de 16,33 millions d'euros. De même, le montant effectivement saisi augmente sensiblement. Dans l'un des dossiers, les services chargés de faire respecter la loi ont pu, outre l'argent apparu dans les signalements « REDSOP », identifier d'autres sommes et les confisquer.

Lieu d'arrestation	Nombre	Pourcentage
Belgique	90	34,22 %
France	35	13,31 %
Pays-Bas	28	10,65 %
Espagne	26	9,89 %
Roumanie	14	5,32 %
Allemagne	12	4,56 %
Grèce	8	3,04 %
Italie	7	2,66 %
Royaume-Uni	6	2,28 %
Autriche	3	1,14 %
Hongrie	3	1,14 %
Slovénie	3	1,14 %
Suisse	3	1,14 %
Autres	25	9,50 %
TOTAL	263	100,00 %

En 2010, 263 dossiers propres à la section FAST de la Police judiciaire fédérale ont pu être clôturés avec succès. Comme le montre le tableau ci-dessous, 90 arrestations ont eu lieu en Belgique. Parmi les fugitifs localisés à l'étranger, 35 ont entre autres été arrêtés en France, 28 aux Pays-Bas et 26 en Espagne. Par ailleurs, le FAST a procédé en Belgique à l'arrestation de 20 fugitifs qui étaient recherchés par un autre pays européen.

5.5. Le service FCCU

5.5.1. Organisation

Les services de police spécialisés dans l'analyse légale des systèmes d'informatique et de télécommunication d'une part et dans la lutte contre la cybercriminalité d'autre part sont développés sur deux niveaux :

- les « Regional Computer Crime Units » (RCCU) au sein de la Police judiciaire déconcentrée (PJF) et
- la « Federal Computer Crime Unit » (FCCU) au niveau national au sein de la direction DJF.

Le service FCCU lui-même comporte trois sections :

- la section recherches Internet ;
- la section opérations ;
- la section « intelligence » et e-payment.



5.5.2. Domaines d'activité

La «Federal Computer Crime Unit» (FCCU) s'attaque, avec les «Regional Computer Crime Units» (RCCU), à la criminalité informatique dans le but de protéger les citoyens dans le monde virtuel contre toute forme de criminalité «traditionnelle» et «nouvelle». Le service FCCU est un point de contact national et international, tant sur le plan stratégique qu'opérationnel. Ainsi, le service FCCU travaille avec les partenaires de BelNIS (Belgian Network Information Security) pour parvenir à une stratégie nationale quant à la sécurisation des systèmes informatiques, en particulier ceux des autorités et des infrastructures critiques.

Le service FCCU fournit un appui spécialisé aux services de recherche centraux tels que les services OCRC et OCDEFO, l'AIG, le Comité P ou aux RCCU et ce, dans le cadre de l'analyse des systèmes ICT pour les formes traditionnelles de criminalité (principalement l'analyse technico-légale des systèmes ICT). Les RCCU reçoivent également un appui lors du traitement des dossiers de criminalité informatique et de fraude à la télécommunication. Cela a donné lieu en 2010 à l'ouverture de 100 dossiers en appui, dans lesquels différentes tâches ont été effectuées. Le service FCCU a copié/analysé 240 supports de données pour un total de 31,39 téraoctets (ou 31.390.000 gigaoctets). Suite à l'évolution technologique, des disques durs d'une grande capacité sont de plus en plus souvent trouvés chez des particuliers, et par ailleurs en larges quantités. Cela a pour conséquence une quantité de données à analyser toujours plus grande dans les enquêtes judiciaires.

Tenant compte de cette évolution, DJF/FCCU se voit obligé d'adapter à la réalité ses méthodes de travail relatives au traitement de ces données. Depuis quelques années, le service FCCU a donc adopté une méthode de travail qui requiert une plus grande contribution des unités requérantes. Cette méthode consiste à fournir aux enquêteurs des données structurées par dossier, qui sont reprises dans un index et leur permet d'effectuer eux-mêmes des recherches. Dans cet esprit, le programme «Forensic Robust Investigation Toolkit» (Frit) a été développé pour une consultation simultanée et automatisée en fonction des besoins des enquêteurs. Grâce à ce programme, un temps précieux est épargné, tant pour les membres du service FCCU que pour les enquêteurs traditionnels qui peuvent effectuer leurs recherches dans un délai plus court et avec une meilleure vue d'ensemble sur toutes les données qui sont reprises dans leur dossier.

Par ailleurs, la recherche et le développement (R&D) ont été mis au point en matière de nouveaux systèmes ICT, de programmes de recherche légale et de nouvelles plates-formes sur Internet comme les sites de réseaux sociaux, les plates-formes de chat, les réseaux d'échange de fichiers, etc.

A côté de cela, de plus en plus de formes classiques de criminalité se retrouvent également sur Internet. Dans ce contexte, DJF/FCCU gère, en collaboration avec le SPF Economie, le point de contact des autorités belges pour la criminalité liée à Internet, eCops, où les internautes peuvent signaler des infractions constatées sur la toile.

Le service FCCU est également le point de référence pour ce qui concerne l'identification des utilisateurs d'Internet auprès des opérateurs internationaux comme, notamment, Microsoft et

Google. Des liens de coopération sont établis dans ce sens avec des partenaires nationaux et internationaux.

Les connaissances engrangées par le service FCCU sont diffusées au cours des nombreuses sessions d'information qui sont organisées lors des formations policières générales ou spécifiques, par les écoles supérieures, les universités, les associations d'entreprises mais également pour le grand public. Ces sessions ont pour but de donner des astuces pour se prémunir contre les délits qui ressortent des phénomènes dont DJF/FCCU est responsable.

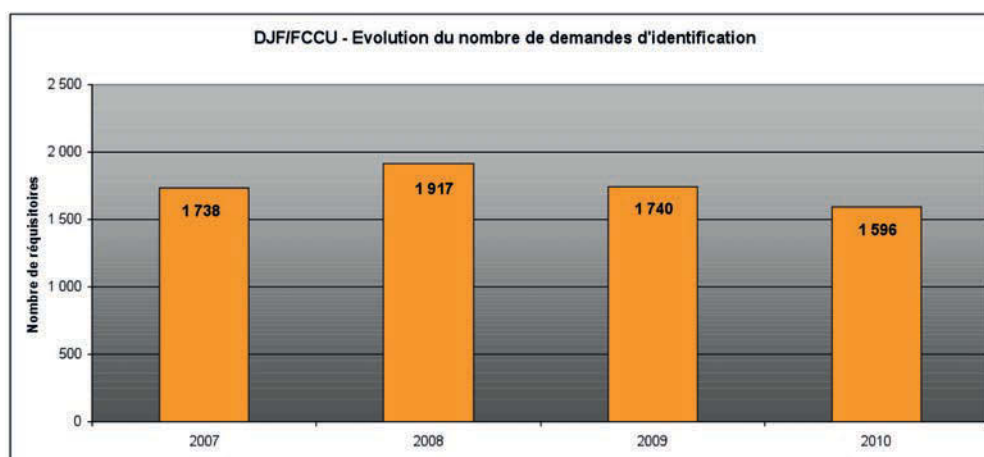
En ce qui concerne l'«intelligence» et la mise à jour des informations, le service FCCU se charge des images des phénomènes de criminalité informatique, de fraude Internet et de fraude à la carte de paiement. Plus spécifiquement pour la fraude Internet, le service tente de cartographier son approche nationale et internationale. Concernant la fraude à la carte de paiement, c'est surtout le «skimming» qui constitue la problématique la plus importante.

5.5.3. Le service FCCU et quelques résultats

Le développement de l'«Internet Information and Investigation System» (I3S), une banque de données dans laquelle les données liées aux domaines d'activité des RCCU et du service FCCU peuvent être encodées, a été achevé en 2010 et lancé dans une phase de test. Ce système peut être utilisé tant par les PJF que par d'autres services comme, par exemple, le service Traite des êtres humains, pour mener des enquêtes liées à Internet, se documenter, échanger des informations pertinentes ainsi que détecter des liens entre différents dossiers.

En 2010, le service FCCU a reçu, en tant que point de référence pour l'identification des utilisateurs d'Internet, 1.596 demandes d'identification, plus précisément pour des utilisateurs d'adresses e-mail, d'adresses IP et de pseudonymes (date d'extraction mars 2011). Le nombre de demandes a légèrement baissé (de 8 %), en raison du fait qu'il y a moins de demandes dans le cadre des dossiers internationaux, à grande échelle. Microsoft MSN demeure le chef de file en ce qui concerne le nombre de réquisitions exécutées. DJF/FCCU est en effet le point de contact national pour cet ISP (Internet Service Provider). Le service est également le point de contact national pour l'identification des utilisateurs de Google et, depuis 2010, également celui de eBay et Facebook. Le graphique ci-dessous montre les évolutions.

Via www.ecops.be, les infractions constatées par le surfeur sur Internet peuvent être signalées aux autorités. Les signalements d'infractions à la législation économique sont directement transmis au SPF Economie. Depuis août 2009, les signalements concernant la pornographie enfantine et les mœurs, ainsi que ceux qui sont parvenus via Child Focus, sont directement



transmis au service central Traite des êtres humains de la Police fédérale. Le tableau ci-dessous donne un aperçu des signalements reçus ainsi que du service en charge.

DJF/FCCU - eCops : nombre de dénonciations reçues et transférées	2008	2009	2010
Nombre total de dénonciations à traiter par le SPF Economie	1.928	1.715	1.582
Nombre de dénonciations à traiter par le service Traite des êtres humains		2.939	3.078
Nombre de dénonciations à traiter par le service FCCU		11.753	13.751
Nombre de dénonciations à traiter par la Police fédérale	12.534	14.692	16.829
Nombre total via eCops	14.462	16.407	18.411

Les signalements traités par le service FCCU ne contiennent pas nécessairement des informations pertinentes sur un délit. Il ressort toutefois du tableau ci-dessous qu'une grande part d'entre eux en contiennent et même qu'un délit peut être constaté. Les signalements reçus via eCops ne peuvent toutefois avoir une valeur juridique de plainte de la part d'une victime. Si celle-ci souhaite déposer plainte, elle est alors dirigée vers la police locale. Dans la majorité des cas, les informations reçues se rapportent à des faits d'escroquerie sur Internet.

DJF/FCCU - eCops : Informations en relation avec les délits	2008	2009	2010
ICT-crime	616	554	839
Escroquerie sur Internet	6.741	8.082	7.669
Autres	1.596	1.255	1.979
Dénonciations contenant des informations pertinentes en matière de délits traitées par le service FCCU	8.953	9.891	10.487
Pourcentage en rapport avec le nombre de dénonciations traitées	71 %	84 %	76 %

5.6. Le service FUSE

5.6.1. Organisation

La Federal Unit Against Swindling and for Economic and Financial documentation (FUSE) est construite autour d'une section documentation EcoFin, qui est donc chargée du traitement du flux d'informations, et d'une section « escroquerie sans Internet » qui fournit principalement des informations relatives à des missions rogatoires internationales en matière d'escroquerie, et réalise également quelques missions conceptuelles, outre l'éventuelle coordination des enquêtes.



5.6.2. Domaines d'activité

Fuse recherche essentiellement l'efficacité dans la récolte, la gestion et la transmission des informations contenues dans la documentation policière en usage et ce, pour tous les phénomènes de la direction DJF. Une mutation s'est opérée en plusieurs étapes depuis 2006, passant d'une comptabilisation des documents policiers à une gestion active des informations qui y sont contenues.

Cette gestion s'effectue comme suit : l'ensemble des documents transmis à FUSE (mieux connu dans le milieu policier comme le flux d'information dans le cadre de la MFO 3 / B 42) est actuellement traité par un système STS REPORT qui permet non seulement d'effectuer des recherches mais aussi de visualiser les documents scannés ou enregistrés sous format électronique (Word, PDF, excel...) grâce à un logiciel « Optical Character Recognize » (OCR).

Cette application engendre :

- une transversalité dans l'exploitation des informations de la direction DJF et en permet une consultation simultanée. Plus de 38.000 documents ont ainsi été traités en 2010 ;
- une rationalisation de la transmission des documents vers les gestionnaires de phénomènes.

Le service FUSE est aussi le point de contact central pour tous les échanges de correspondance internationale de la direction DJF. La gestion des documents internationaux permet une collaboration rapide de notre direction centrale dans le cadre de l'entraide judiciaire européenne et de la collaboration policière internationale tout en veillant au respect de la transmission des renseignements au niveau national.

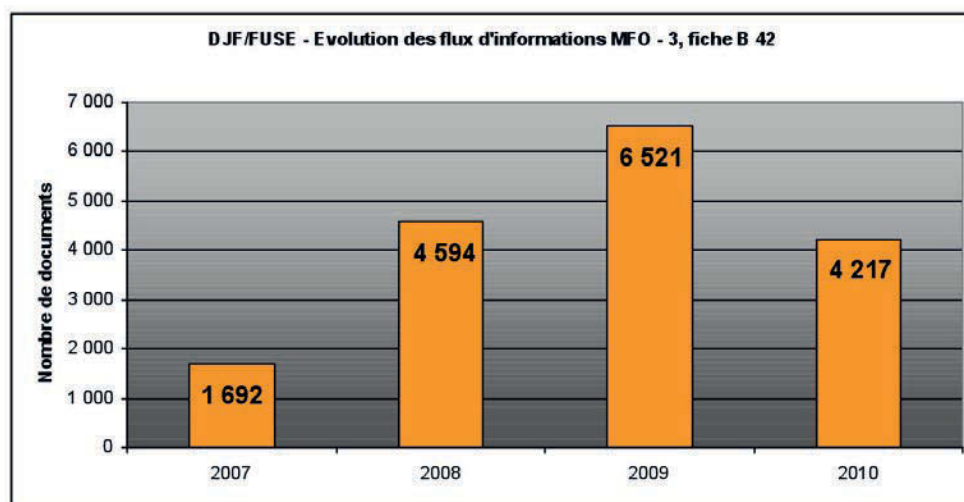
Le service FUSE gère, à l'échelon national, la transmission des réquisitoires judiciaires à destination des organismes financiers lorsque l'institution n'est pas identifiée. Une étude est actuellement en cours visant à automatiser la transmission directe de ces réquisitoires par l'enquêteur via l'ordinateur policier.

DJF/FUSE gère aussi le phénomène escroquerie au niveau central sur plusieurs axes :

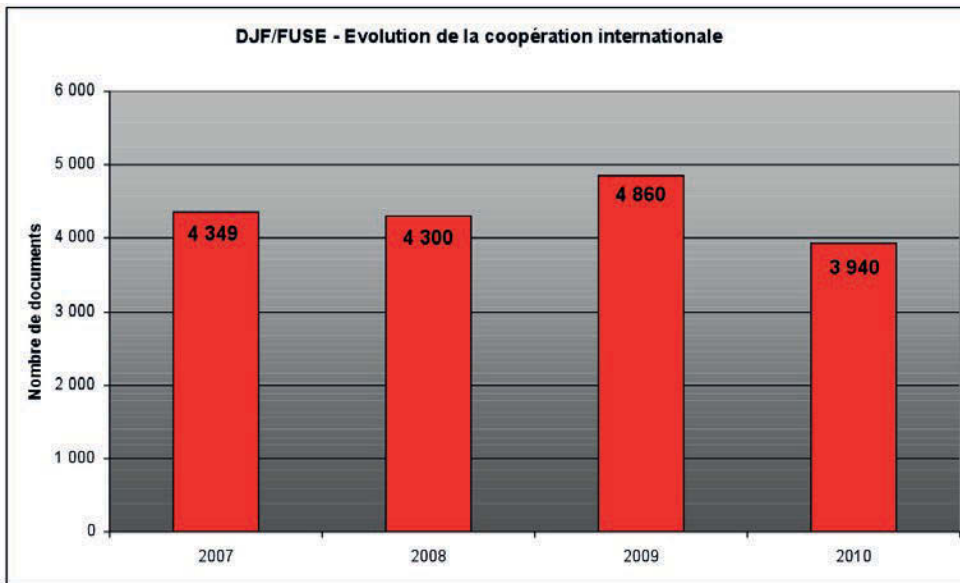
- la détection des nouveaux MO que nous signalons ensuite sur le plan national (tant au sein de la police qu'au public via les médias, en collaboration avec les partenaires externes privés et publics) ;
- l'appui et la coopération policière nationale et internationale ;
- la prévention réalisée par les mises en garde et les conseils aux victimes potentielles ;
- le signalement de failles dans la législation et la formulation de recommandations utiles pour la modification de cette législation.

5.6.3. Le service FUSE et quelques résultats

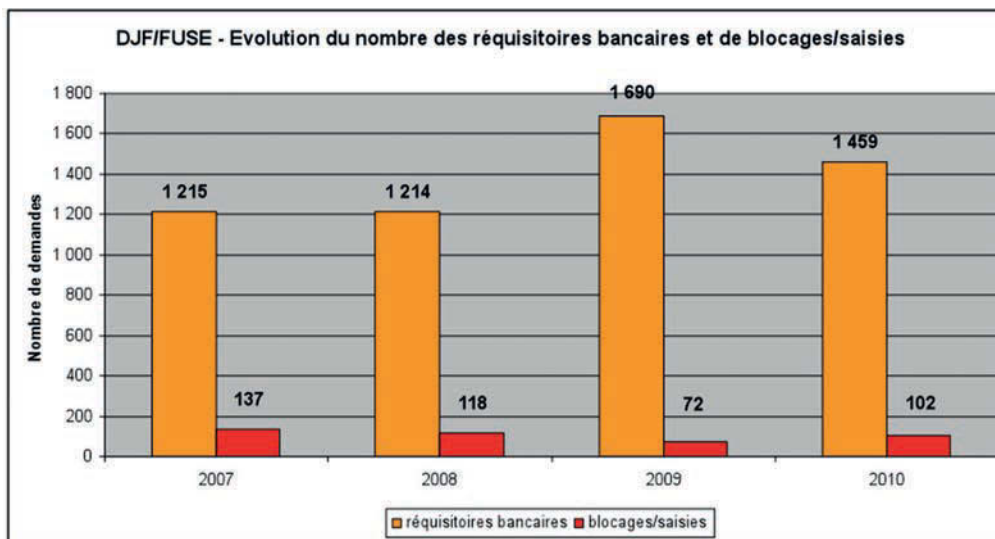
La circulaire ministérielle concernant les missions fédérales (MFO-3) oblige les services de police (police locale et directions d'arrondissement) à transmettre des informations, via leur CIA, à la direction DJF si celles-ci ont trait aux phénomènes EcoFin qui sont repris dans la fiche B-42 (parmi lesquels le blanchiment, la corruption, l'escroquerie,...). Depuis 2008, ce flux d'information semble avoir atteint sa vitesse de croisière, avec un pic de 6.521 documents en 2009. En 2010, ce chiffre chute à 4.217 (une diminution d'au moins 35 %). Une nouvelle campagne de sensibilisation s'impose donc.



Le service FUSE est également un carrefour pour tous les documents relatifs à la coopération policière internationale dans les domaines EcoFin. L'évolution montre que le niveau le plus bas depuis quatre ans a ici été atteint, avec 3.940 documents en 2010 (soit une diminution de 19 % par rapport à 2009).



Lors des enquêtes d'information ou d'instruction, des comptes bancaires de suspects doivent souvent être identifiés (en vue de l'obtention des historiques). En 2010, 1.459 réquisitoires bancaires ont été transmis, pour la police intégrée, par le service FUSE (qui remplit ici un rôle centralisateur) aux institutions bancaires, ce qui signifie une diminution de 14 %. Dans certains cas, le compte bancaire est bloqué et les sommes saisies. Cela s'est passé dans 102 cas, et constitue donc un revirement en 2010 étant donné que ce nombre avait diminué de 2007 à 2009. Le graphique ci-dessous reflète la situation.



5.7. Le service P&O

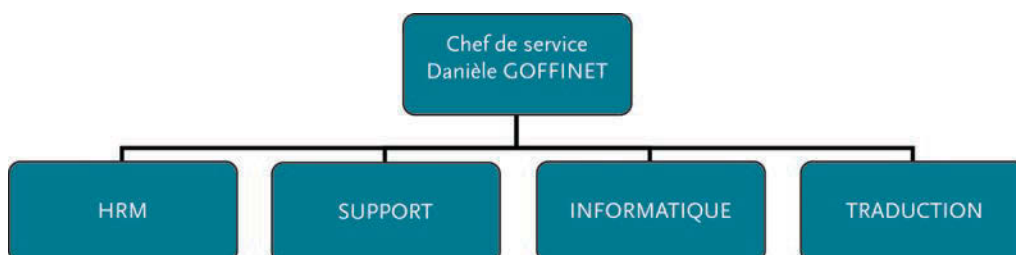
5.7.1. Organisation

Le service Personnel & Organisation (P&O) est le service le plus récent de la direction DJF. Il n'a été créé qu'en 2009, lorsque le besoin d'un tel service est apparu suite à un exercice EFQM.

Fin 2010, le service P&O était constitué d'un chef de service (qui depuis fin 2009 remplit aussi les tâches de directeur adjoint, mais demeure toutefois chef de service de P&O), 2 membres opérationnels et 23 membres CALog (dont 6 détachés de DSL et 3 de DST).

Ces membres du personnel sont répartis au sein de différentes sections :

- HRM : veille à la gestion du personnel pour l'ensemble de la direction ;
- Support : veille à la gestion logistique et à la gestion du bâtiment ; le responsable de cette section s'occupe également de l'aspect communication ;
- Informatique : veille à la mise à jour de l'informatique de la direction DJF ;
- Traduction : réalise les traductions pour toute la direction.



5.7.2. Domaines d'activité

Le service P&O centralise, pour toute la direction, les tâches relatives à la gestion du personnel, au « facility management », au suivi de l'infrastructure informatique, à la communication et aux traductions. Ce service gère par ailleurs le bâtiment « Atrium » pour les directions DJF et DJT.

5.7.3. Le service P&O et quelques résultats

Les résultats du service P&O ne s'expriment pas en chiffres et en graphiques étant donné que le service joue principalement un rôle d'appui ; ce fut notamment le cas pour l'organisation du colloque « persisting the way to integrity, vers une approche plus proactive de la corruption », qui s'est tenu le 27 octobre 2010.

Le teambuilding de la direction DJF a également été entièrement organisé par le service P&O. Le 14 septembre 2010, différents groupes de la direction sillonnaient les rues de Bruxelles. Après la promenade, chacun a pu savourer une paëlla, préparée par un collaborateur du service OCDEFO. Une visite du Parlement européen était prévue l'après-midi.

6. SUIVI DU PLAN NATIONAL DE SÉCURITÉ

Le Plan national de sécurité (PNS) 2008-2011 prévoit deux phénomènes prioritaires pour la direction DJF : d'une part, la lutte contre la criminalité économique et financière grave (le blanchiment, la fraude¹ et la corruption) et d'autre part, la lutte contre la criminalité informatique grave.

Dans les phénomènes prioritaires, la direction DJF se doit d'actualiser les analyses stratégiques (analyses de phénomènes). En 2010, différentes analyses de phénomène ont été réalisées : corruption (exercices 2007-2009), impôts sur les revenus (exercices 2007-2009) et fraude à la TVA (exercices 2007-2009). En raison de la capacité en personnel, aucune analyse du phénomène de criminalité informatique grave n'a pu voir le jour. De plus, la préparation de la rédaction de l'Image policière nationale de sécurité (IPNS) a été entamée en 2010 et la direction DJF y fournit une contribution pour 14 phénomènes différents. Pour chacun de ces phénomènes, sont calculés ou estimés la vulnérabilité (du milieu ou des victimes), la menace des auteurs et l'impact. Les données sont fournies à la direction de l'information policière opérationnelle (CGO), plus précisément au service appui à la politique – analyse stratégique (CGOP/A), chargé de centraliser et de traiter les données.

En 2009 déjà, des analyses portaient sur l'ICT en tant que moyen dans les phénomènes (prioritaires). L'impact des virements électroniques, de l'augmentation de la capacité des PC et d'autres supports (smartphone,...), de la précision des scanners et imprimantes, sur de nombreux phénomènes EcoFin ne souffre aucun doute, tout comme Internet, qui constitue souvent un refuge pour les auteurs d'escroqueries. Le lien entre l'ICT et la criminalité informatique saute aux yeux, mais l'éventuel impact de botnets et des command & control centers sur notre infrastructure critique est cependant fortement sous-estimé.

Concernant l'approche intégrale (de toutes les facettes) et intégrée (impliquant tous les partenaires) de phénomènes sécuritaires, la direction DJF tient le haut du pavé. Concernant la fraude TVA organisée, il existe la cellule mixte de soutien TVA ; pour la fausse monnaie, la collaboration est étroite avec la Banque nationale de Belgique ; pour la criminalité informatique, les réseaux conceptuels (e.a. BelNIS) reçoivent un appui et une contribution ; en matière de blanchiment, des formations sont dispensées à l'administration des Douanes et Accises (sur l'approche des «cash-courriers») et, en matière de blanchiment toujours, le fonctionnement de la Cellule de traitement de l'information financière (CTIF) est soutenu ; et concernant la saisie d'avantages patrimoniaux illégaux, il existe une collaboration étroite avec l'OCSC,...

Dans le domaine du flux d'informations vers la BNG liées aux phénomènes prioritaires, il reste encore beaucoup de travail. De nombreux procès-verbaux, dressés par les services de police locale et les PJF, ne répondent toujours pas aux directives de saisie reprises dans les fiches de saisie. Mais également au sein de la direction DJF, quelques points névralgiques ont été mis en lumière au cours du séminaire stratégique de 2010, e.a. en matière de circulation et de gestion de l'information. D'où la formulation de quelques points à améliorer. Pour chacun de ces domaines, une fiche a été rédigée et un groupe de projet désigné, chargé de rapporter directement au conseil de direction DJF. La rédaction d'une offre de service de la direction DJF en est un exemple. Cette offre de service vise à faire connaître aux partenaires les domaines de compétence de DJF et à leur faire savoir quand ils peuvent y faire appel.

Dans le dossier-programme, en matière conceptuelle, quelques autres objectifs opérationnels très

1 Il faut entendre par « fraude » : la fraude à l'impôt sur les revenus, la fraude TVA (organisée) et la fraude à l'identité.

spécifiques aux phénomènes, ont été postulés. Il convient d'indiquer le fait qu'en 2010, la direction DJF a été invitée dans le groupe de travail d'experts chargé de formuler les recommandations d'application du principe UNA-VIA en matière de lutte contre la fraude fiscale. La direction fournit également une importante contribution, via le service FCCU, à l'élaboration d'une législation en matière de rétention d'informations.

Concernant l'appui, le projet d'établir une offre pour un service équivalent en matière de lutte contre la fraude à la TVA par le biais d'un «service level agreement» (SLA) entre les PJF a provisoirement été suspendu et ce en raison des projets de réforme de la Justice (dont la réduction des 27 arrondissements à 16). En 2010, les polices locale et fédérale n'ont pas été interrogées sur leurs besoins en matière d'appui souhaité dans les phénomènes prioritaires. L'alimentation de l'Intranet, développé en 2008 avec la Direction générale de la police administrative, la Direction des opérations et de l'information administrative, le Service immigration (DGA/DAO-Immi), semble asseoir son succès. Le site a été consulté 150.000 fois, dont 90.000 consultations de la partie du site gérée par DJF/OCRF.

Une part non négligeable de l'appui fourni concerne la formation. Ainsi, 134 enquêteurs CCU ont été formés au thème «Internet investigations». En 2010, les nouvelles moutures des formations EcoFin, adaptées en 2009, ont été dispensées pour la première fois. De tels updates doivent être réguliers car la législation évolue rapidement, et certainement dans les domaines fiscaux (impôts sur le revenu et TVA). Les formations sur la corruption sont moins sujettes à modification, bien que la législation sur les marchés publics ait été modifiée en 2010, ce qui a nécessité d'affiner la formation.

La direction DJF est également chargée de la coordination d'enquêtes et d'opérations impliquant plusieurs arrondissements et de la coordination internationale (par exemple une commission rogatoire à exécuter simultanément dans plusieurs pays). Le Joint Investigation Team (JIT) en matière de corruption, qui a pu voir le jour avec la France sur base de l'instrument réglementaire européen, est l'exemple par excellence d'une telle coordination opérationnelle, et constitue le tout premier team d'enquête international dans cette matière.

Des informations sont également fournies à différents niveaux de politique (dont le secrétariat d'état à la Coordination de la lutte contre la fraude, les réseaux d'expertise «Corruption» et «Ecofinfisc» près le Collège des Procureurs généraux,...). Des réunions de réseaux spécifiques à certains phénomènes sont également organisées, dont la réunion tenue le 17 juin 2010 à Oudenaarde et celle du 21 juin 2010 à Marche-en-Famenne (sur le blanchiment, la fraude TVA et la fraude à l'impôt sur le revenu) ainsi que celle du 27 octobre 2010 à Bruxelles au sujet de la corruption (à l'occasion du centième anniversaire du Comité supérieur de contrôle) ou encore encore les réunions organisées à Bruxelles avec les RCCU (à l'Atrium). En plus des réseaux, de nombreuses informations sont diffusées via le magazine Atrium-news, qui traite notamment des thèmes suivants :

- Alimentation BNG dans le domaine du phénomène de blanchiment ;
- fil conducteur en matière de fraude Internet ;
- (approche de la) fraude sociale grave et organisée ;
- loi relative aux pratiques du marché et à la protection des consommateurs ;
- jeux de hasard ;
- escroquerie nigérienne ;
- l'administrateur (provisoire) de biens ;
- (benchmarking avec les Pays-Bas) dossier auto-apprentissage criminalité financière et économique.

Dans le domaine du contrôle de gestion, l'attention s'est focalisée sur la qualité de la saisie. Pour améliorer celle-ci, le projet de la PJF Dendermonde en matière de fraude a fait l'objet de notre collaboration en 2010. Le service FCCU a également un rôle particulier dans l'utilisation des techniques telles que réglées par les articles 90ter à 90novies inclus du Code d'instruction criminelle.

Enfin, il va de soi que les services OCRC, OCDEFO et FCCU ont mené des enquêtes opérationnelles (de façon autonome ou en appui d'une recherche locale ou PJF).

7. COORDINATION DE LA LUTTE CONTRE LA FRAUDE EN BELGIQUE

La lutte contre la fraude en Belgique n'est pas l'apanage du tandem police – ministère public. Diverses autres autorités sont également actives dans la répression de la fraude. Les efforts de ces services sont d'autant plus fructueux lorsque la collaboration augmente. Une tâche importante est dévolue au secrétaire d'Etat à la Coordination de la lutte contre la fraude, Monsieur Carl Devlies. Ce secrétaire d'Etat, adjoint au Premier ministre, a créé le Collège pour la lutte contre la fraude fiscale et sociale, au sein duquel le directeur DJF représente la Police fédérale.

Le plan d'action 2009-2010 du Collège pour la lutte contre la fraude fiscale et sociale contient une partie «échange d'information» (concentrée e.a. sur le «data matching»), mais aussi une partie sur l'approche intégrale et coordonnée, scindée en quatre chapitres. Le premier, relatif à la prévention et à la détection de la fraude, décrit le projet «meilleures harmonisation et collaboration entre les auditeurs légaux privés et les services publics chargés de la répression de la fraude, plus particulièrement dans le domaine de la fraude horizontale», pour lequel le directeur DJF est «project manager». Pour un contrôle efficient de la lutte contre la fraude, le projet «checkdoc bis» a été proposé. Il s'agit d'un élargissement du champ d'application. Via checkdoc, un système en ligne pour la validité des documents d'identité utilisés, un commerçant peut, avant la transaction, vérifier si le document d'identité présenté n'est pas connu comme volé, perdu, périmé ou nul. A défaut de moyens budgétaires, checkdoc bis reste provisoirement lettre morte. Le troisième chapitre (politique de poursuites et sanction concluante) prévoit une étude de la capacité policière en matière financière, pour augmenter cette capacité si nécessaire. Enfin, le quatrième chapitre du plan d'action précité traite de l'approche internationale.

8. PROJETS INTERNATIONAUX



8.1. ENFAST

En février 2006, les bureaux d'Interpol Lyon ont accueilli une réunion de travail « Interpol fugitive ». Les délégations allemande, néerlandaise et belge ont alors émis l'idée d'une collaboration plus étroite en Europe et de la création d'un réseau : « European Network Fugitive Active Search Teams » (ENFAST). Depuis la création du Mandat d'arrêt européen (MAE), les services de police européens coopèrent beaucoup plus fréquemment : le cadre légal unique permet en effet d'effectuer rapidement des arrestations et des remises à la frontière. Grâce à la création d'un réseau européen visant une collaboration transnationale accrue, la localisation et l'arrestation de fugitifs sont aujourd'hui plus efficaces et plus efficaces.

La Présidence belge de l'Union européenne a proposé à cette plate-forme sans précédent de voir auprès des divers Etats membres si ce rêve du team FAST belge pouvait devenir réalité. La conférence, organisée à Bruxelles dans le cadre de la Présidence belge les 9 et 10 septembre 2010 à Bruxelles, a visé juste : les 27 étaient présents et ont approuvé une résolution permettant la mise en place du réseau « ENFAST ». Une telle collaboration est un signal fort adressé aux fugitifs : au sein de l'Union européenne – grâce à la collaboration unique et aux points de contact opérationnels dans la majorité des Etats membres –, les informations quant à l'endroit où le fugitif signalé (au niveau international) se cache peuvent faire l'objet d'une réaction rapide. Cette énergie, combinée à l'instrument fort qu'est le MAE, renforce l'exécution des peines.

Lors de la conférence, les services de police et les magistrats chargés de rechercher les fugitifs semblaient partager leur passion, leur implication et leur ténacité. Ces caractéristiques prouvent leur utilité dans la localisation et l'arrestation de personnes souhaitant se soustraire à l'exécution de leur peine. Grâce à la création de ce réseau, « ENFAST » répond également dans l'immédiat à l'une des recommandations de la commission chargée d'évaluer les 10 ans de réforme des polices : en effet, l'objectif était d'optimiser la coopération policière internationale. La direction DJF et le service OCDEFO, auquel appartient le FAST depuis le 1er mars 2010, sont donc particulièrement fiers de cette réalisation. Mais le projet n'est évidemment pas terminé : le réseau devra être renforcé ces prochaines années.

La direction DJF espère d'ailleurs que l'idée d'envisager de priver les auteurs fugitifs des avantages patrimoniaux dans la phase de l'exécution de la peine pourra compter sur l'enthousiasme des partenaires européens. Mais avant de soulever ce point au forum international, le service doit poursuivre le développement de la recherche active d'avantages patrimoniaux de criminels confisqués et pas encore découverts en Belgique. Le FAST belge a donc été rebaptisé en 2010 Fugitive and Asset Search Team (FAST), mais pour l'instant uniquement dans un contexte belge.



8.2. International Mass Marketing Fraud Working Group (IMMFWG)

L'IMMFWG est un groupe de travail international créé en 2007 sous l'impulsion du « Department of Justice » américain, pour aborder en mode de coordination internationale le phénomène de la fraude massive. Il faut entendre par fraude massive toute forme de fraude avec utilisation de moyens de communication de masse, tels que le télémarketing, l'Internet, les mailings (courriers) de masse, en vue de contacter les victimes (potentielles) et de communiquer avec elles.

La fraude massive couvre le domaine de compétence tant de la section fraude Internet du service FCCU (membre du groupe de travail depuis début 2008) que du service FUSE (membre depuis fin 2010), qui traite du phénomène d'escroqueries sans Internet. L'autorité belge de protection des consommateurs, le SPF Economie et la CTIF – dans le cadre de la recherche axée sur le butin/follow the money – sont également impliqués dans le groupe de travail afin d'arriver à une meilleure collaboration.

Le groupe de travail vise le développement d'initiatives au niveau international dans l'approche intégrée de ces formes d'escroquerie, en échangeant notamment des informations et des bonnes pratiques, en élaborant des projets de prévention, de dissuasion, d'enquête, etc.

L'International Mass Marketing Fraud Working Group se réunit deux fois par an (printemps et automne). DJF/FCCU et le SPF Economie étaient les hôtes de la dernière réunion de novembre 2010 à Bruges.

8.3. EU cybercrime task force

L'EU Cybercrime Task Force (EUCTF) est un groupe de travail composé, en exécution d'une recommandation européenne de 2008, des chefs des « cybercrime units » nationales des États membres de l'UE, du « hightech crime center » d'Europol, d'un représentant d'Eurojust et d'un représentant de la Commission européenne.

L'objectif de cette « task force » est de rendre des avis aux institutions européennes demanderesse en vue de sécuriser le cyberspace et de lutter contre le cybercrime.

Dans cette stratégie, tous les aspects peuvent être abordés (organisation, législation et opérations).

En sus, cette « task force » sera avec d'autres à la tête d'initiatives en cours ou planifiées au sein d'Europol, comme l'établissement d'une image, la formation, le développement ICROSS (plate-forme à Europol pour l'interconnexion des points de contact nationaux comme eCops.be), et autres.

En octobre 2010, le chef de service FCCU a pris la présidence de cette « task force » pour deux ans. Sa tâche consiste principalement à diriger les travaux et à fournir un appui dans la rédaction de textes de politique durant et entre les réunions de l'EUCTF.

En outre, des contacts fréquents auront lieu avec la Commission européenne et d'autres partenaires en cas d'éventuelles initiatives dans ce domaine.

8.4. Présidence EU – Working Party on Frontiers/False documents

Lors de la présidence de l'Union européenne au second semestre 2010, le chef de service de l'OCRF a présidé le groupe de travail relatif aux faux documents dénommé « Working Party on Frontiers/False Documents ».

Ce groupe a pour but de lutter contre la problématique de l'usage de faux documents au sein de l'UE essentiellement au niveau technique

Toutefois, le domaine du faux document évolue. Nous constatons une baisse significative de l'interception de faux documents notamment aux postes frontières, entre 25 et 50 % selon les pays.

Plusieurs constats peuvent être établis :

- **Au niveau technique :**
 - faible qualité du contrôle de première ligne : usage de contrôles automatisés, formation des contrôleurs,...
 - déplacement du contrôle : la première ligne n'est plus uniquement le contrôle des entrées sur le territoire aux postes frontières. Elle se situe de plus en plus au sein de nos administrations communales et de nos consulats.

- **Au niveau tactique:**
 - détournement des procédures : phénomène de l'obtention induite/faux intellectuel (les faussaires obtiennent de vrais documents dans nos administrations sur base de faux documents présentés) et du « look alike » (usage de documents authentiques d'autrui)

Afin de répondre à la problématique actuelle, la présidence belge a axé sa mission sur la réalité de terrain en souhaitant :

- améliorer la qualité de contrôle de la première ligne par la mise en place de « bonnes pratiques » et la sensibilisation des autorités (policières ou non) ;
- élargir les compétences du groupe au point de vue technique en ce qui concerne les documents non suivis actuellement (ex : cartes d'identité, documents sources) et au point de vue tactique (qu'en est-il des procédures de délivrance ?).

Ce projet a été accueilli très favorablement par les autres Etats membres. La présidence hongroise a d'ailleurs repris ce projet comme sujet central de sa présidence.

8.5. Convention UNCAC : engagement international du service OCRC.

La corruption est un mal qui touche tous les pays du monde. Conscient de ce fait, le service OCRC a désigné trois de ses membres pour participer au cycle de « reviewing » à l'ONU du traité « United Nations Convention Against Corruption » (UNCAC) actuellement en cours et qui a débuté en 2010.

En effet, tous les signataires de ce traité acceptent d'être audités et d'auditer les autres signataires en matière de lutte et de législation anticorruption, ainsi qu'en matière de mise en œuvre des recommandations de l'ONU. Un pays est toujours audité par deux autres pays : en l'occurrence, la Belgique est chargée d'auditer l'Espagne, avec l'aide de la Lituanie. Notre pays a pris en charge l'examen de l'incrimination, des approches pénales et judiciaires de la corruption en Espagne, tandis que la Lituanie se penche sur la qualité de la coopération internationale espagnole en ces matières.

Les membres de la DJF/OCRC concernés étudieront donc plus spécifiquement les différents aspects de la législation espagnole et son application ainsi que la qualité et la complétude des réponses fournies par ce pays au questionnaire d'évaluation. Si nécessaire, ils formuleront des recommandations tant sur le plan législatif que sur son application.

Il s'agit là d'une belle occasion de tisser des liens avec ces deux pays et de renforcer encore l'implication de la Belgique et du service OCRC dans la coopération internationale contre la corruption et ses ravages.

CHAPITRE 2 — SUIVI DES PROJETS 2010

1. Introduction

Dans le rapport annuel 2009 (p. 112-113), la direction DJF avait mis en avant une série de points d'attention prioritaires pour l'année 2010. Cette partie du rapport annuel examine dans quelle mesure les projets proposés ont effectivement été réalisés. Cette justification est effectuée de la manière la plus transparente possible, en gardant à l'esprit le but originel, les moyens nécessaires, le processus et enfin le résultat.

2. Projet 1 – Un siècle de lutte contre la corruption en Belgique

BUT :

L'échange de savoir-faire et d'expertise en matière de lutte contre la corruption pour continuer à optimiser cette lutte en Belgique.

MOYENS :

A l'occasion du centième anniversaire de la lutte contre la corruption en Belgique (d'abord le Comité supérieur de contrôle, ensuite l'Office central de lutte contre la corruption au sein de la direction DJF), une journée d'étude a été organisée avec différents experts nationaux et étrangers. A cette occasion, différents thèmes ont été abordés dont entre autres, l'image du phénomène, le secteur privé en tant que partenaire dans la lutte contre la fraude, l'approche de la corruption par la banque mondiale et la manière de procéder de l'OLAF pour protéger les intérêts financiers de l'UE.

PROCESSUS :

Un groupe de travail, sous la direction du directeur DJF, a été mis sur pied afin de préparer cette journée d'étude. Divers partenaires (SPF Budget, I-Force, le Parquet fédéral, l'Université de Gand, Transparency International, la Banque mondiale, l'OLAF, le Service anti-corruption français et l'OCDE) ont été conviés et ont accepté de faire un exposé.

RÉSULTAT :

La conférence s'est tenue le 27 octobre 2010 dans les locaux prestigieux de la Banque nationale de Belgique. La conférence a été ouverte par le ministre de la Justice Stefaan De Clerck et clôturée par le secrétaire d'Etat pour la coordination de la lutte contre la fraude Carl Devlies en présence de pas moins de 316 personnes venues de 10 pays différents.



3. **Projet 2 – Intégration des officiers de liaison auprès de la Commission des jeux de hasard au sein de DJF/OCRC.**

BUT :

Une meilleure lutte contre la fraude en matière de jeux de hasard et de fraude liée aux paris sportifs par l'optimisation des échanges d'information entre la police et la Commission des jeux de hasard compétente, ainsi que l'enrichissement policier des connaissances sur le phénomène « jeux de hasard ».

MOYENS :

L'intégration des fonctionnaires de police auprès de la Commission des jeux de hasard dans la direction DJF a pour but d'encoder leurs PV en BNG de sorte que les informations soient accessibles à toute la police intégrée. Cette intégration permet également aux membres policiers d'utiliser le réseau et des canaux d'information de la direction (notamment l'« Atrium news ») pour diffuser leurs connaissances dans la problématique des « jeux de hasard ».

PROCESSUS :

1. Evaluation de l'ancienne situation à l'aide d'une analyse SWOT.
2. Réalisation d'un « benchmarking » (comparaison) des fonctionnaires de police qui travaillent pour d'autres organes liés aux autorités judiciaires et policières (e.a. la Cellule pour le traitement des informations financières en matière de lutte contre le blanchiment et l'Organe central pour la saisie et la confiscation).
3. Elaboration d'une proposition d'adaptation (dans ce cas l'intégration auprès de DJF/OCRC) acceptée par le directeur général de la Police judiciaire fédérale et la Commission des jeux de hasard.
4. La mise en œuvre par étapes d'un accord conclu pour arriver à un échange d'information structuré et enrichir les connaissances sur le phénomène auprès de la police.

RÉSULTAT :

Les résultats à long terme ne peuvent pas encore être annoncés car la mise en œuvre est trop récente. Quelques résultats peuvent néanmoins être communiqués :

- le phénomène « jeux de hasard » est repris dans l'IPNS 2011 réalisé au sein de la police et ce, en étroite collaboration avec la Commission des jeux de hasard ;
- les PV des fonctionnaires de police sont encodés en BNG ;
- les fonctionnaires de police qui travaillent au sein de la Commission des jeux de hasard sont maintenant guidés sur le plan administratif à partir de la direction DJF.

4. Projet 3 – Point de contact fraude football

But :

Le but est une lutte plus efficace contre la fraude football par une mise à profit maximale des informations disponibles et des signaux d'alerte. C'est pourquoi, outre les canaux existants (police, magistrature, Commission des jeux de hasard, Union royale belge de football,...), l'on veut parvenir à une canalisation des plaintes et dépositions, un système standardisé de déclarations où toute personne peut à tout moment faire part d'une irrégularité dans le domaine de la corruption et des paris sur les rencontres de football et ce, à une instance spécifiquement désignée à cet effet.

Moyens :

Les moyens suivants ont été mis en place pour créer le point de contact :

- création de ce point au sein du point de contact national existant (PCN) de la Direction des opérations et informations en matière de Police judiciaire fédérale (DJO) ;
- création d'un site web www.fraudefootball.be dans les trois langues nationales et en anglais ;
- création d'un formulaire unique pour les déclarations via Internet ;
- création d'un numéro d'appel téléphonique : 0800/44.44.2 ;
- création par CGPR d'un logo (sifflet d'arbitre avec le logo de la police en dessous) ;
- désignation d'un coordinateur fraude football auprès de DJF/OCRC et du Parquet fédéral ;

Processus :

Le processus comportait les étapes suivantes :

- cette initiative a été prise à la demande des autorités politiques en décembre 2009 ;
- plusieurs réunions ont eu lieu, notamment avec le Parquet fédéral, la Commission des jeux de hasard (compétente pour les jeux de hasard sur Internet) et d'autres services de la Police fédérale ;
- une procédure a été développée en interne à la police sur la façon d'agir en cas de déclaration ;
- le déclarant peut demander que ses données d'identité soient masquées ; cela signifie que celles-ci ne sont connues que de la police et du parquet mais ne sont pas reprises dans le dossier d'information ou d'instruction ;

Résultat :

Le point de contact est opérationnel (24h sur 24h, 7 jours sur 7) depuis le 28 mai 2010. Une première évaluation sera réalisée après un an de fonctionnement.

5. Projet 4 – FAST financier

BUT :

L'optimisation de l'exécution de la peine, du fait que le FAST, outre la recherche de criminels en fuite, consacrera, dans les dossiers qui lui sont confiés, également de l'attention à la récupération des avantages patrimoniaux illégaux pour lesquels la confiscation prononcée peut être exécutée.

MOYENS :

Pour donner à ce projet l'étoffe adéquate, le FAST a été intégré en 2010 au service OCDEFO. Ceci afin d'y trouver les informations, l'expertise et l'appui lors de la recherche d'avantages patrimoniaux illégaux éventuellement encore à récupérer. A cet effet, le FAST travaille en étroite collaboration avec les spécialistes de la section Blanchiment/Patrimoine.

PROCESSUS :

Pour chaque dossier traité par le FAST, on vérifiera si des éléments indiquant des avantages patrimoniaux illégaux éventuellement récupérables peuvent être découverts sur base de données connues (confiscation prononcée qui n'a pu être réalisée) ou sur base de données jusque-là inconnues (qui apparaissent suite à la recherche de fugitifs).

Toutes les sources nationales et étrangères peuvent être découvertes via des réseaux officiels (CARIN, ENFAST, FIU-net et autres canaux d'échanges policiers) ou non et, lors de chaque échange d'information à propos d'un fugitif, on prête désormais attention aux avantages patrimoniaux illégaux connus ou non.

RÉSULTAT :

Cette manière de procéder et la synergie entre les deux spécialités augmentent sensiblement les occasions de rechercher et retrouver des avantages patrimoniaux illégaux dans l'entourage des criminels en fuite.

Dans le cas des dossiers où une confiscation a été prononcée, les règles nationales et internationales d'exécution des décisions judiciaires sont suivies et aboutissent à une récupération maximale des avantages patrimoniaux. Si de nouveaux éléments indiquant des avantages patrimoniaux illégaux jusque-là inconnus sont découverts, une enquête blanchiment complémentaire peut être ouverte.

6. Projet 5 – Fraude sociale grave et organisée

But :

Le but est la lutte intégrale et intégrée contre la fraude sociale grave et organisée pour poursuivre ceux qui organisent effectivement ce genre de fraude, rechercher leurs avantages et les leur retirer (bénéfices et moyens de fonctionnement) par l'installation d'une cellule d'appui mixte. Tenant compte du principe de subsidiarité, les autres informations éventuelles sur les « profiteurs » possibles de la fraude seront envoyées aux services compétents pour suivi ultérieur. Le projet a été entrepris après l'étude de faisabilité réalisée à la demande du secrétaire d'Etat pour la Coordination de la lutte contre la fraude (projet issu du plan d'action 2009-2010).



Moyens :

Le Service d'information et de recherche sociale (SIRS) et la Police judiciaire fédérale détacheront des personnes vers la cellule d'appui mixte fraude sociale. Par ailleurs, le gouvernement a débloqué en 2010 un budget de 768.000 euros pour le fonctionnement de cette cellule fraude sociale et un programme fraude sociale organisée auprès de DJF/OCDEFO (708.000 euros annuellement à partir de 2011).

Processus :

Un protocole de coopération rédigé en 2010 a été approuvé par les comités de gestion de l'ONEM et de l'ONSS, le comité de direction du Bureau fédéral d'orientation du SIRS, le comité de direction de la Police fédérale, le Collège des Procureurs généraux. Avec les signatures des ministres des Affaires Sociales, du Travail, de la Justice, des Indépendants, de l'Intérieur et du secrétaire d'Etat pour la Coordination de la lutte contre la fraude, ce protocole est entré en vigueur le 1^{er} octobre 2010.

Outre la sélection d'une dizaine de membres de la police, la sélection de trois inspecteurs sociaux a par ailleurs été clôturée en 2010. Le recrutement du dernier inspecteur social sera bouclé en 2011.



Résultat :

La cellule d'appui mixte est mise en place. La présentation à la presse aura lieu en février 2011.

7. Project 6 – Botnets

BUT :

Mieux déstabiliser et lutter contre les réseaux criminels qui s'attaquent aux ordinateurs ou pratiquent le hacking via les ordinateurs de personnes ne se doutant de rien. Les ordinateurs de ces personnes sont contaminés par des malwares. Le contrôle de l'ordinateur de l'utilisateur individuel est ainsi repris au moment opportun par les auteurs. Tous les ordinateurs infectés forment un réseau d'ordinateurs (botnet) qui peut être utilisé via quelques PC (Command & Control-servers) pour attaquer d'autres ordinateurs.

MOYENS :

Concevoir et tester une contre-stratégie qui doit permettre de fermer les C&C-servers de sorte que le botnet ne soit plus actif. Cela demande une bonne connaissance des méthodes de travail des criminels, notamment en étudiant la manière dont les auteurs prennent le contrôle des PC des utilisateurs (et via quel malware).

L'utilisation du « Virologic System ». Ce système, développé par le service FCCU, analyse et détecte les malwares sur les stations de travail qui font partie d'un botnet. On vérifie quel malware a été installé et utilisé par les hackers pour contrôler les postes de travail de manière illégale. Une analyse plus approfondie de ce malware peut mener à l'identification des C&C-servers.

Le partage des informations obtenues avec d'autres services de police, notamment par l'alimentation de l'Analytical Workfile « Cyborg » d'Europol, constitue la base pour relier entre eux les différents dossiers botnet au niveau national et international et poursuivre les échanges d'information.

PROCESSUS :

La détection et la localisation des C&C-servers est principalement effectuée par des partenaires externes. Le flux d'information vers DJF/FCCU arrive surtout de « CERT.be » qui est en contact étroit avec ses homologues dans le monde entier. Dès qu'un C&C-server a été localisé en Belgique, le service FCCU entre en action pour mettre ces servers hors service et ce, sous la direction du Parquet fédéral.

Le partage des informations avec d'autres services de police (après alimentation des banques de données visées à cet effet).

RÉSULTAT :

En 2010, le « Virologic system » a détecté 5115 formes et versions différentes de malwares sur les postes de travail. Grâce à l'analyse ultérieure et à la coopération avec les partenaires internationaux, DJF/FCCU a localisé et fermé 30 C&C-servers en Belgique. La majorité de ces C&C-servers faisait partie du Koobface-botnet.

8. Projet 7 – Infrastructure critique

But :

Une meilleure protection de l'infrastructure critique contre les menaces sérieuses et le développement proactif des plans d'action pouvant être déployés en cas d'attaque.

Moyens :

Pour pouvoir réagir de manière adaptée aux menaces sérieuses sur les infrastructures critiques, de bons accords de travail doivent être conclus entre les partenaires, en l'espèce entre le CERT, le Parquet fédéral et DJF/FCCU. Ces accords sont mis par écrit dans un condensé faisant partie d'un texte similaire à un « plan catastrophe » pour l'environnement électronique. Toutefois, ils doivent être non seulement mis au point mais également testés et évalués.

Processus :

Au sein de BELNIS, la plate-forme de concertation fédérale pour la sécurité de l'information, différents sous-groupes de travail ont été créés qui, chacun, travaillent sur les initiatives d'amélioration pour protéger les infrastructures ICT critiques :

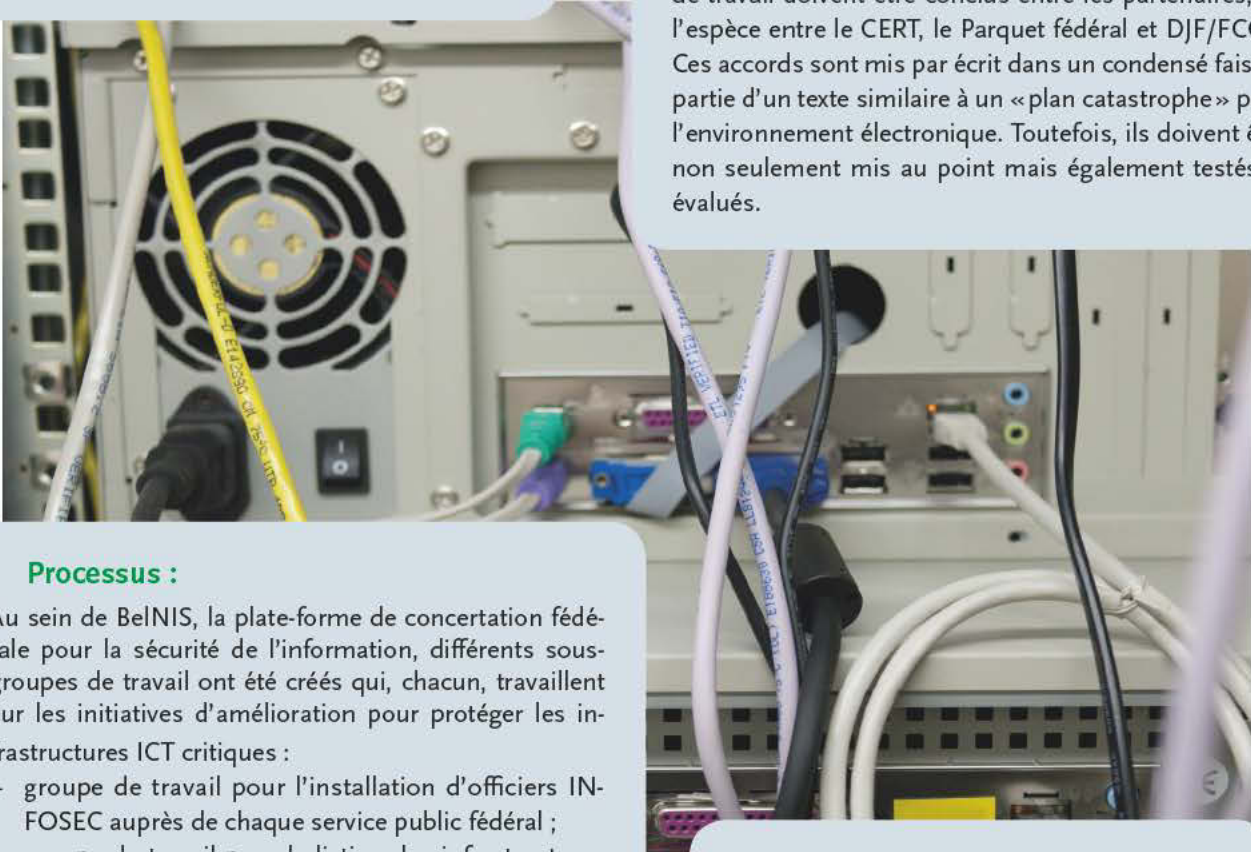
- groupe de travail pour l'installation d'officiers INFOSEC auprès de chaque service public fédéral ;
- groupe de travail pour le listing des infrastructures ICT critiques ;
- groupe de travail pour la détection des incidents sur les infrastructures ICT des autorités ;
- groupe de travail pour le traitement des incidents sur les infrastructures critiques ;

En partant du savoir-faire et de l'expérience engrangés, chaque membre du groupe de travail tente de contribuer au développement d'un plan d'action qui doit être déployé en cas d'attaque.

Résultat :

DJF/FCCU dirige les activités du groupe de travail pour le traitement des incidents sur les infrastructures critiques. La fourniture d'une première version d'un condensé pour le traitement des incidents peut être attendu pour fin 2011.

Le service FCCU a aussi participé au groupe de travail pour la détection des incidents sur les infrastructures ICT des autorités et y a contribué au développement d'une méthode qui détecte les attaques et les infections par malware.



9. Projet 8 – Plan de communication et plan de formation

BUT :

Améliorer la communication interne au sein de la direction DJF par l'introduction d'un plan de communication dans le domaine de la communication non opérationnelle, ce en application d'une recommandation du trajet EFQM.

Les résultats des efforts de formation seront également optimisés pour toute la direction DJF par l'élaboration d'un plan de formation. Ce plan de formation fixe les priorités à suivre par chaque service et chaque membre du personnel. Il tiendra aussi bien compte des besoins de l'organisation que des souhaits des membres du personnel. Ce plan de formation sera également utilisé dans le cadre de la procédure d'évaluation.

MOYENS :

Le service P&O a intégré ces deux missions dans l'ensemble de ses tâches. Dans une première phase, il a été fait appel à deux stagiaires pour analyser la problématique du plan de communication et, ensuite, un groupe de travail a été mis sur pied au sein de la direction DJF. Le plan de formation a été rédigé par le service P&O en collaboration avec les chefs de service. Le service P&O :

- suit l'exécution en déterminant pour chaque offre de formation dans quelle priorité du plan de formation ladite formation s'inscrit. ;
- établira pour chaque membre du personnel une fiche individuelle sur laquelle les formations suivies seront consignées et qui sera enregistrée dans le système GALOP.

PROCESSUS :

Pour le plan de communication, une stagiaire a réalisé une analyse descriptive de la communication (non opérationnelle) existante (au moyen d'un petit questionnaire).

Un deuxième stagiaire a élaboré un questionnaire plus représentatif et une analyse « swot » plus large. Dans le rapport final rédigé, plusieurs recommandations ont été formulées. Ce rapport a été présenté aux participants au séminaire stratégique (tenu en décembre 2010). Ensuite, une équipe a été chargée de la réalisation concrète du plan de communication qui tient compte des constatations de l'analyse et des points prioritaires exprimés au cours du séminaire.

RÉSULTAT :

Plan de communication :

1. L'analyse et les recommandations ont mis en évidence l'importance de la communication.
2. La rédaction et la mise en œuvre du plan de communication sont prévues pour début 2011. Une évaluation de son introduction aura lieu après une année d'entrée en vigueur, après quoi d'éventuelles adaptations y seront apportées. Ce sujet sera suivi de près par le conseil de direction DJF.

Plan de formation :

Le plan de formation a été publié en octobre 2010 mais ici aussi, il est encore trop tôt pour tirer des conclusions.

Par ailleurs, la deuxième phase doit encore être réalisée, à savoir la rédaction des plans de formation par membre du personnel, qui tiendra compte de deux projets récemment proposés par la direction générale : le « knowledge management » et le « survival kit ».

10. Projet 9 – Locaux d'audition pour majeurs

BUT :

Deux locaux d'audition pour majeurs doivent permettre à la Direction criminalité économique et financière de rencontrer les recommandations émises dans le cadre de l'arrêt SALDUZ et les directives des Procureurs généraux qui en ont découlé.

MOYENS :

Trois locaux (2 salles d'audition et un local technique) ont pu être libérés au sein du bâtiment Atrium.

La DGJ a financé l'achat du matériel technique pour une salle d'audition et le local technique.

La DJF a financé l'achat du mobilier pour ces locaux.

Une personne a pu suivre la formation (principe du « train the trainer »).

PROCESSUS :

Suite aux évolutions en matière judiciaire (arrêt SALDUZ), la DGJ a pris la décision d'équiper les PJF de locaux d'audition pour majeurs. La direction DJF, étant composée de services opérationnels, a pu bénéficier de cette décision.

Un local a été mis en place et une personne a été formée.

Deux personnes (OCDEFO et FUSE) sont chargées de la gestion quotidienne de ces locaux.

Une note de service sera publiée en 2011 afin de définir clairement les principes d'utilisation.

RÉSULTAT :

Un local d'audition pour majeurs a été installé en 2010 et est opérationnel. Nous attendons pour le second de voir l'évolution du dossier « Salduz ».

11. Projet 10 – Accès à la Banque Carrefour des Entreprises (BCE)

BUT :

Le projet (qui avait été inscrit dans le plan d'action 2009-2010 du secrétaire d'État pour la Coordination de la lutte contre la fraude) avait pour but de donner accès à la police intégrée, structurée à deux niveaux, à la Banque Carrefour des Entreprises (BCE) et de consacrer ainsi l'argent épargné (94,380 €, qui ont été dépensés pour l'accès à la banque de données d'une entreprise privée) à l'accès à une banque de données internationale contenant des données économiques.

MOYENS :

L'accès serait assuré via la plate-forme informatique de la police, à savoir Portal.

PROCESSUS :

La Police doit d'abord obtenir l'autorisation pour accéder aux données de la Banque Carrefour des Entreprises.

Dans le cadre des enquêtes en cours, les services de police doivent pouvoir disposer des données personnelles et de certaines données historiques. Pour ces raisons, un module supplémentaire (software) devra également être développé par la police.

RÉSULTAT :

A ce jour, la police n'a pas encore accès à la BCE.

CHAPITRE 3 — PHÉNOMÈNES

1. Phénomène « blanchiment »

La majorité des infractions sont commises dans le but de s'enrichir. A la Police judiciaire fédérale, l'accent est mis sur la recherche et la récupération, c'est-à-dire la saisie et la confiscation, de ces avantages patrimoniaux illégalement perçus. Cette approche financière de la criminalité peut s'opérer par la voie d'une enquête de blanchiment (approche inductive) ou par la voie d'une enquête de patrimoine (approche déductive).

L'infraction de blanchiment vise la gestion, la conversion, le transfert, la dissimulation, le déguisement et la modification des revenus d'activités criminelles et/ou le camouflage de l'origine illégale d'avantages patrimoniaux. L'enquête de patrimoine vise l'évaluation, le dépistage, la saisie et in fine la confiscation des avantages patrimoniaux générés par une infraction par ailleurs connue.



Relativement à l'image de ce phénomène, on retiendra que depuis 2006, la police intégrée enregistre annuellement entre 600 et 700 procès-verbaux initiaux (ou considérés comme tels dans la BNG) visant une infraction de blanchiment. L'essentiel de ces procès-verbaux dénonce des transactions ordonnées depuis les grandes agglomérations, principalement Bruxelles et Anvers. Chaque année, plus du tiers des infractions de blanchiment commises en Belgique sont localisées dans ces deux arrondissements.

Le Fonds monétaire international estime que les gains cumulés de manière illicite couvrent 2 à 5 % du produit intérieur brut

mondial. Rapportée au PIB de la Belgique, cette fourchette représente 6,6 à 16,5 milliards d'euros circulant dans notre pays et dont l'origine serait criminelle.

L'approche intégrale des avoirs patrimoniaux illégalement perçus est notamment sous-tendue par le fonctionnement de la CTIF qui s'intègre dans le volet préventif de l'arsenal législatif belge en matière de blanchiment. Ce système de dénonciation des transactions suspectes par les prestataires de services financiers (comme les banques) a pour but d'éviter et de prévenir l'utilisation du système bancaire et financier par les blanchisseurs d'argent sale.

Ce système préventif de dénonciation des transactions suspectes à la CTIF ayant montré suffisamment son efficacité et étant ressenti comme tel par de plus en plus de criminels, ces derniers sont tentés d'utiliser davantage la contre-stratégie consistant à transférer physiquement leurs avoirs criminels en espèces. Par ailleurs un Arrêté royal du 05 octobre 2006 portant certaines mesures relatives au contrôle du transport transfrontalier d'argent liquide touche également cette problématique du transport d'argent cash. Face à cette tendance, la Police fédérale poursuit le développement de son projet «Cash Watch». En partenariat avec les douanes, la Police fédérale porte une attention particulière à la détection et à la répression des mouvements d'avoirs criminels en espèces. Le niveau international de cette problématique n'est pas oublié. A titre d'exemple, la Police fédérale a reçu 47 informations concernant le transfert d'argent liquide en

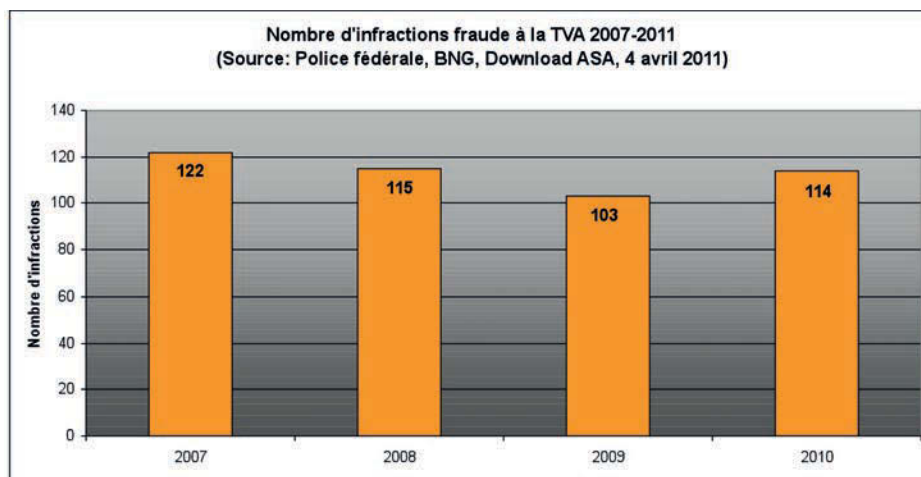
France par des Belges. Au total, 12 personnes étaient connues dans la base de données BNG et 40 rapports d'information ont été rédigés et envoyés aux arrondissements compétents. Deux de ces dossiers avaient un lien avec le phénomène du terrorisme.

La Police fédérale dispose d'officiers de liaison auprès de la CTIF et auprès de l'Organe central pour la saisie et la confiscation (OCSC). Les deux officiers de liaison de l'OCSC contribuent au développement du nouveau réseau informel des ARO (« asset recovery offices ») et s'investissent dans la coopération internationale via le réseau CARIN. L'OCSC, avec le soutien des officiers de liaison de la Police fédérale, est par ailleurs point de contact belge pour ces deux réseaux. Au niveau de la problématique du transport d'argent en espèces, la Police fédérale entretient un partenariat privilégié avec les services de la Douane qui est compétente en cette matière.

2. Phénomène « fraude à la TVA »

La fraude TVA organisée correspond à l'obtention d'avantages patrimoniaux illégaux par une organisation (criminelle), composée de personnes physiques et d'entreprises qui se concertent pour éluder la taxe sur la valeur ajoutée due à l'Etat et/ou récupérer un remboursement indu de la TVA par le biais de falsifications et/ou du non-respect des prescriptions relatives à cette taxe et ce, dans le cadre du commerce international de biens et/ou de services (pour autant que la fraude ne soit pas exclusivement basée sur des documents).

La fraude TVA organisée fait partie du phénomène sécuritaire prioritaire « criminalité économique et financière grave » (PNS 2008-2011), pour lequel la direction DJF a élaboré un dossier-programme. La section fraude TVA de DJF/OCDEFO développe l'image nationale du phénomène. En 2010, une analyse du phénomène portant sur les années 2007 à 2009 a été réalisée. La plupart des dossiers sont reliés au territoire de Bruxelles-Capitale. Le graphique ci-dessous indique le nombre d'infractions pour la période 2007-2010¹.



Au-delà de cette analyse annuelle du phénomène, l'approche policière axée sur l'information fait appel au savoir-faire et à l'expertise de la cellule de soutien fraude TVA (OCS fraude TVA), où siègent également des membres du SPF Finances. Ses membres étudient les modi operandi et tentent de chiffrer le préjudice annuel. Pour 2007, le préjudice s'élevait à 44,23 millions € et à 29,8 millions € pour 2008. En 2009, le préjudice s'élevait à 93,6 millions €, dont 79 millions € dus à la fraude à l'émission de CO². Pour 2010, le préjudice est de 29 millions €. En raison de l'introduction du « reverse charge » dans certains pays, on assiste à de nouveaux glissements territoriaux, vers la Belgique notamment.

¹ Les infractions sont imputées à une année sur base de l'année du PV, telle que reprise dans le numéro de notice.

Ce phénomène est abordé de manière intégrale et intégrée. Intégrée signifie que diverses autorités harmonisent mutuellement leurs activités. L'application du « data mining » aux déclarations TVA (mensuelles ou trimestrielles) par la cellule OCS permet de détecter et d'arrêter la fraude à un stade précoce. La police et le ministère public garantissent une ouverture rapide des enquêtes à mener sur les groupes d'auteurs. La clé du succès réside dans la recherche axée sur la saisie des avantages patrimoniaux illégaux en vue de les faire confisquer par le juge qui se prononcera sur la cause.

La fraude s'étendant généralement à plusieurs Etats membres de l'UE (ou même à des pays tiers), la collaboration entre plusieurs pays est nécessaire, et ce dans le domaine de l'échange administratif dans le réseau Eurocanet et de l'échange de données alimentant les banques de données VIES I (livraisons intracommunautaires de biens) et VIES II (livraisons intracommunautaires de services). Mais il faut également collaborer au niveau policier, et là, EUROPOL joue un rôle important avec son AWF MTIC (Analytical Work File, Missing Trader Intra Community), une banque de données indispensable à la lutte contre la fraude à la TVA. Il est clair que les commissions rogatoires internationales classiques jouent un rôle important dans la collecte de la preuve contre les groupes d'auteurs transnationaux.

Le service OCDEFO est également pilote du réseau réunissant diverses directions arrondissementales (PJF) en vue d'échanger de nouveaux modi operandi et tendances. Ainsi, un glissement de la fraude visant les biens (voitures de luxe, ordinateurs) vers la fraude visant les services (téléphonie) et les biens immatériels (droits d'émission de CO²) a pu être constaté.

Malgré l'exemple que montre la police belge (et le SPF Finances) au niveau européen et les bons résultats engrangés (en effet, le préjudice pour le Trésor belge s'élevait encore en 2001 à 1,1 milliard €), la prudence reste de mise, d'autant plus que la fraude à la TVA engendre une concurrence déloyale préjudiciable aux entreprises de bonne foi. En matière d'enregistrement policier dans la banque de données de la police intégrée, structurée à deux niveaux, il reste encore une bonne marge d'amélioration, malgré la fiche de saisie créée à cette fin. En effet, les informations essentielles sur le caractère organisé ou non sont trop peu encodées, ce qui hypothèque la qualité de l'image.

3. Phénomène « corruption »

Le phénomène « corruption » doit être compris au sens étendu, qui recouvre également les infractions de concussion, de prise d'intérêt et de détournement commis par un fonctionnaire, soit les infractions reprises dans la loi du 10 février 1999 relative à la répression de la corruption et cela en raison des liens étroits qui unissent ces diverses infractions.

La corruption est abordée d'un point de vue essentiellement répressif par la Police intégrée. Les dossiers nécessitant un savoir-faire plus spécialisé et une plus grande expertise dans ce domaine particulier sont confiés à l'Office central pour la répression de la corruption. La lutte contre la corruption regroupe de nombreux partenaires, parmi lesquels il convient de faire la distinction entre les partenaires internes et externes. Parmi les partenaires internes, on compte les PJF des 27 arrondissements judiciaires, pour lesquelles le service OCRC fournit un appui lors d'enquêtes complexes, différents offices centraux, qui selon le cas, appuient ou se font appuyer par le service OCRC, tels que les services OCDEFO ou FCCU. Les partenaires externes comprennent le Collège des Procureurs généraux et son réseau anticorruption, Transparency International, ainsi que les services de police de nombreux pays lorsque des faits de corruption s'avèrent impliquer des auteurs vivant dans d'autres pays que la Belgique.

Afin de mieux protéger la société belge contre ce genre de méfait, il est nécessaire de développer une connaissance fine de ses tenants et aboutissants : parallèlement à ses enquêtes, le service OCRC étudie donc ce phénomène dans le but de permettre à la Police intégrée de faire les meilleurs choix stratégiques possibles dans cette lutte.

La prévention en matière de corruption n'est pas absente des préoccupations de la Police intégrée. Cependant, pour être efficace, cette prévention passe par la formation de fonctionnaires ou de personnes risquant d'être confrontés à de tels abus. Il arrive donc au service OCRC de partager ses connaissances avec divers partenaires du monde civil ou policier, en ce compris dans des pays étrangers : l'internationalisation de la corruption est une réalité, elle est donc prise en compte.

La corruption est un phénomène dont les dégâts les plus importants sont indirects, voire difficilement mesurables. En effet, les flux financiers liés à la corruption ne sont pas les aspects les plus dangereux : c'est le coup porté au système démocratique et à ses lois, ainsi, par voie de conséquence, qu'à la confiance du citoyen dans les institutions de son pays qui représente les dégâts les plus insidieux et les plus menaçants.

Par ailleurs, les surcoûts imposés à la communauté par les résultats de la corruption pour le corrupteur sont tout aussi difficiles à évaluer : l'obtention d'un visa ou d'un permis de séjour de façon illégale peut entraîner des dégâts si ce visa ou permis est obtenu d'une manière illégale par une personne de mauvaise foi (intention de commettre un attentat). Autre exemple : la non signalisation d'un fraudeur par un contrôleur fiscal aura un coût à plusieurs étages. L'Etat ne récupérera pas les sommes dues. En conséquence, les possibilités d'investissement de l'Etat dans des domaines comme l'emploi, les soins de santé, l'éducation,... seront réduites.

La corruption est un délit dont les conséquences sont grave, mais difficile à chiffrer : il est donc important de garder ces éléments en tête afin de ne pas sous-estimer la menace qu'elle représente. Ce phénomène est difficile à prévenir en raison de profils de corrupteurs et de corrompus très variables parmi le peu d'entre eux qui soient connus. La corruption peut se produire à tous niveaux de pouvoir, dans le chef de fonctionnaires de tous niveaux, pour peu qu'ils soient en position de fournir le service illégal désiré.

Dans le cadre de l'Image policière nationale de sécurité, certains groupes d'auteurs ont été identifiés comme plus menaçants, de même que certains secteurs ont été perçus comme particulièrement vulnérables. Il est donc possible que le futur Plan national de sécurité apporte une attention particulière au secteur des travaux publics (comme secteur vulnérable) et à la menace que représenteraient certaines personnes morales et certains profils de fonctionnaires ou de mandataires (en tant qu'auteurs).

4. Phénomène « fraudes au préjudice de l'Union européenne »

Ce phénomène repose sur les mêmes bases que la corruption et la fraude aux marchés publics, à un considérable point près : le milieu dans lequel il se produit. En effet, l'Union européenne est d'une part grande pourvoyeuse de marchés publics à travers toute l'Europe, et grande productrice de règlements et de directives. Dès lors, ces fraudes se déroulent dans un contexte international, dans des pays et des juridictions multiples, ayant des lois parfois fort différentes, et en se référant à des législations européennes spécifiques, ce qui complexifie d'autant plus les enquêtes à mener.

Par ailleurs, la fraude au préjudice de l'Union européenne n'est considérée comme un phénomène et étudiée comme telle par la direction DJF que depuis 2010. L'expertise stratégique policière dans ce domaine en est encore à ses débuts.

L'Union européenne dispose d'un outil propre pour gérer la prévention et effectuer des enquêtes administratives : l'Office européen de lutte anti fraude, l'OLAF. Lorsqu'une fraude est découverte et fait l'objet d'une plainte, le Parquet fédéral confie l'enquête au service OCRC (suite aux accords conclus). Ce partage des tâches attribue donc la seule responsabilité du volet répressif de ce phénomène à la police, plus particulièrement au service OCRC et au service OCDEFO pour certains appuis, ainsi qu'au service FCCU pour l'appui technique fréquemment nécessaire.

L'impact de la fraude au préjudice de l'Union européenne est sensiblement identique à celui de la corruption et de la fraude aux marchés publics, mais nuit également gravement à la crédibilité de l'Union européenne et à la confiance dans ses institutions et son engagement envers les peuples européens. En période de crise de l'Union et de marasme économique, ces nuisances prennent une importance plus grande encore.

La vigilance est d'autant plus de mise que la mafia semble être très active dans ce domaine, et que son niveau d'organisation et de capacité de pénétration dans les milieux officiels est bien connu, d'autant plus que les sommes en jeu sont extrêmement élevées.

5. Phénomène « fraude aux cartes de paiement »

La législation ou la littérature ne donne pas de définition littérale de la « fraude à la carte de paiement ». La disposition pénale utilisée pour lutter contre le phénomène est reprise dans la loi du 28 novembre 2000 en matière de criminalité informatique. Le phénomène peut être défini comme suit : « la fraude à la carte de paiement est un délit patrimonial consistant à utiliser réellement ou virtuellement les données d'une carte dérobée ou copiée (carte de banque, de crédit, de débit, carte carburant, carte privative,...), et à utiliser frauduleusement d'autres applications financières. »

La fraude à la carte de paiement est liée à d'autres phénomènes tels que la criminalité informatique, l'escroquerie avec Internet, le blanchiment et d'autres formes de criminalité. Ainsi, les criminels piratent par exemple des banques de données relatives aux cartes de paiement, ils effectuent des achats sur Internet avec les données volées et ils utilisent des « money mules » pour blanchir les bénéfices.

Le phénomène a un fort impact sur notre société car la confiance accordée aux moyens financiers est mise en doute. Le « skimming » consiste à copier les données de la bande magnétique d'une carte de paiement et à filmer/enregistrer le code PIN. Ce modus operandi constitue une menace internationale pour les systèmes de paiement, et le secteur bancaire en est la victime finale.

Un autre modus operandi pour obtenir les données indispensables est le « shouldersurfing » consistant à voler la carte de banque et à regarder lorsque le code PIN est introduit. Ce délit est commis principalement au niveau local, plutôt dans des grandes villes et les victimes sont souvent des personnes âgées. Le préjudice issu de l'utilisation frauduleuse de ces cartes est totalement ou partiellement à charge des victimes.

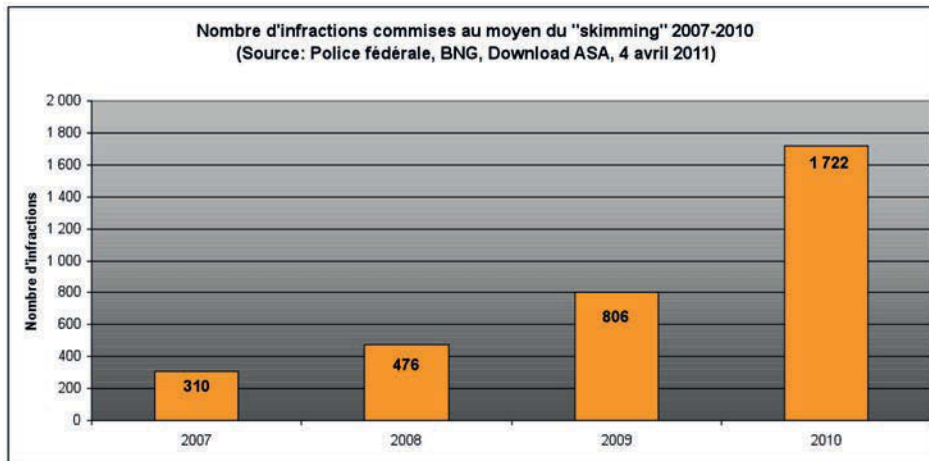
Le phénomène est abordé de façon intégrée. Les dossiers sont souvent traités au niveau local. Dans les différentes directions arrondissementales (PJF), des teams assurent le suivi de dossiers relatifs à ce phénomène et essaient de cartographier les groupes d'auteurs organisés.

La fraude est commise dans plusieurs Etats membres de l'UE, mais aussi dans des pays tiers, d'où la nécessité de collaborer au niveau international. Au niveau policier, Europol joue un rôle important avec l'Analytical Work File « Terminal ». Le groupe de travail européen chargé de ce phénomène utilise les « nouvelles technologies », telles que les vidéoconférences, permettant d'échanger des informations par des canaux officiels avec d'autres Etats membres. Cela facilite la collaboration, optimise le flux d'infos et accélère les demandes d'assistance judiciaire. Exemple : en 2010, la police belge a pu collaborer avec la Bulgarie et la Tchèque (dans un dossier de la PJF Anvers).

Dans le cadre de l'approche intégrale, la prévention est aussi abordée. En 2010, des campagnes médiatiques ont sensibilisé le « citoyen » aux dangers du « skimming » et du « shouldersurfing ». Des conseils utiles de prévention pour éviter la fraude ont été diffusés (cf. PJF Bruxelles et Anvers). En collaboration avec le service « sécurité et prévention » du ministère de l'Intérieur,

un flyer « fraude à la carte de paiement » a été diffusé au niveau national.

Depuis 2007, on constate que le nombre d'infractions (tentatives et faits) au modus skimming augmente fortement chaque année, ce que confirment les partenaires privés.



Une variante du skimming en forte progression récemment est le skimming aux terminaux de paiement de stations-service.

Les criminels placent un dispositif modèle « all-in-one » de skimming sur : le terminal, qui combine deux fonctions : d'une part la copie de la bande magnétique et d'autre part, l'enregistrement de l'image du code lorsque la victime l'introduit. Souvent fabriqués sur mesure selon la marque du terminal, il devient compliqué de voir immédiatement ces dispositifs.



De nombreuses nouvelles technologies peuvent constituer une menace pour l'avenir. Les derniers développements tels que les paiements par GSM, les « prepaid credit cards », les systèmes de paiement virtuels sur Internet, la « near field communication » (NFC), n'ont pas encore d'impact mesurable sur la fraude.

6. Phénomène « criminalité informatique »

Le terme criminalité informatique ne porte que sur l'atteinte à la sécurité d'un système ou à l'intégrité de données stockées dans un système informatique et non sur l'utilisation de l'informatique comme moyen pour commettre d'autres délits.

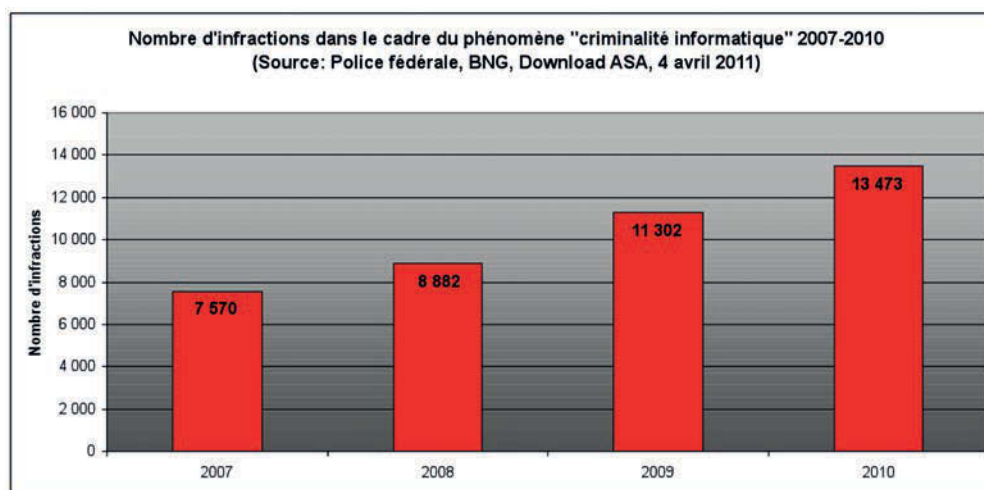
Sont comprises toutes les formes de criminalité informatique telles que le hacking, l'espionnage et l'atteinte aux infrastructures critiques, réseaux d'entreprise et PC individuels.

La criminalité informatique est souvent une composante (modus) d'autres formes de criminalité patrimoniale et est liée à d'autres phénomènes tels que la fraude Internet, le blanchiment, l'extorsion sous la menace de « ransomware » (cryptage de fichiers) et l'escroquerie.

Le nombre de faits dans le cadre du phénomène de criminalité informatique en BNG est en augmentation continue depuis des années : de 2007 à 2010, une hausse de 78 % a été

constatée. Une grande partie des infractions (tentatives et faits) concerne de la fraude aux cartes de paiement, qui d'ailleurs ont la même qualification judiciaire.

L'impact politique et économique de la criminalité informatique sur la société peut s'avérer



très important si la cible est une infrastructure critique, comme l'ont vécu quelques pays européens.

En 2010, l'affaire WikiLeaks a démontré que c'était surtout la fiabilité des informations qui était menacée et que le cyberenvironnement est utilisé pour collecter mais aussi pour transmettre des informations. Pendant l'affaire WikiLeaks, force a également été de constater que les cyberactivistes sont capables de s'organiser très rapidement en passant par des réseaux sociaux pour procéder à des cyberattaques de systèmes ICT critiques, qui ne fonctionnent alors plus.

La plupart des cybercriminels utilisant des malwares et botnets, DJF/FCCU se concentre sur la déstabilisation de ces réseaux en démantelant les botnet servers. Ainsi, d'autres infections aux malwares sont évitées et commander les ordinateurs infectés se complique. Ces actions sont menées sous la direction du Parquet fédéral.

Lorsqu'un logiciel malveillant est un élément important dans le dossier, il est analysé par le « Virologic System », et ainsi, des preuves à charge ou à décharge peuvent être récoltées. En 2010, 5115 formes différentes de malwares ont été détectées.

Vu le caractère international du cybercrime, ce phénomène requiert une approche intégrée de différents partenaires nationaux et internationaux, dont CERT.be, en contact étroit avec leurs homologues partout dans le monde et qui envoient directement les données des botnets au service FCCU. En 2010, DJF/FCCU a fermé 30 command & control-servers (C&C), la majorité en provenance du botnet Koobface.

Au niveau international, la coopération avec Europol est étroite grâce à l'Analytical Work File « Cyborg », base internationale de jonction de différents dossiers et d'échange d'informations.

Grâce aux efforts intensifs de l'officier de liaison de la Police fédérale aux Etats-Unis, la collaboration avec les services de recherche américains et les fournisseurs d'accès à Internet est excellente.

7. Phénomène « fraude aux impôts sur les revenus »

Dans la lutte contre la fraude fiscale grave et organisée, la Police judiciaire fédérale se consacre principalement au traitement qualitatif de dossiers. Le service OCDEFO gère des dossiers autonomes. Tout comme pour les années précédentes, ceux-ci ont constitué en 2010 la majeure partie du travail (les dossiers autonomes représentent en effet 44 % de la charge, les dossiers d'appui 38 % et les dossiers pour avis et analyse, 18 %). DJF/OCDEFO organise également, de la manière la plus efficiente possible, une transmission de l'information et assure également un appui aux PJF.

Au sein du phénomène fraude à l'impôt sur les revenus, certaines tendances se font jour, notamment l'essoufflement des dossiers de fraude impliquant des sociétés d'encaisse. Dans ces dossiers, les tribunaux rendent les jugements les plus divers : condamnations, dépassements du délai légal, acquittements. En outre, de nombreuses transactions sont acceptées, permettant au Trésor public de récupérer des montants dus.

Une deuxième tendance concerne l'afflux de nouveaux dossiers subséquents à une coopération policière internationale accrue. Ils contiennent des données client de détenteurs (belges) de comptes au Liechtenstein et en Suisse. Cette typologie a été abordée en long et en large dans la presse financière. En cas de fraude à l'impôt sur les revenus, il n'est d'ailleurs pas exceptionnel de retrouver des constructions de sociétés écran dont le siège social est établi dans un paradis fiscal ou un centre offshore. C'est la raison pour laquelle la police a coopéré au projet n° 34 du plan d'action 2009-2010 du secrétaire d'Etat Carl Devlies, intitulé « Abus de paradis fiscaux à des fins frauduleuses ». Le responsable de projet est le SPF Finances, qui doit rendre compte au Collège pour la lutte contre la fraude sociale et fiscale.

La troisième tendance se situe dans l'approche du phénomène de fraude fiscale grave et organisée. Ce phénomène n'est pas l'apanage de la police judiciaire et du ministère public. Les contrôles, enquêtes administratives et autres actions visant les mécanismes de la grande fraude fiscale organisée incombent à la première ligne de l'Administration de l'inspection spéciale des impôts (ISI) et subsidiairement de l'Administration de la fiscalité des entreprises et des revenus (AFER) du Service public fédéral Finances. En cas de constat de fraude, deux formes d'intervention sont possibles : un trajet administratif ou judiciaire. A l'heure actuelle, il n'est pas exclu que les deux trajets soient suivis simultanément. L'appel à UNA VIA, soit le règlement d'un cas de fraude par une seule voie (soit administrative, soit judiciaire), s'est traduit en un groupe de travail où siégeait la police. Ce groupe de travail a formulé quelques recommandations, susceptibles d'être reprises dans un projet ou une proposition de loi. Les services de police et le ministère public pourraient voir augmenter leur charge de travail. D'autre part, une proposition de loi donnant plus de liberté de manœuvre au ministère public pourrait également être mise sur la table. La transaction n'étant actuellement possible que dans les informations, la proposition de loi visée² – introduite à la Chambre le 8 février 2011 – pourrait déjà avoir un impact en 2011. Le ministère public peut alors proposer une transaction dans la phase d'instruction, voire dans la phase devant la juridiction de jugement. Bien que les revenus puissent en être augmentés par la transaction, il y a un revers à la médaille : le nombre de confiscations peut diminuer. Une bonne gestion de la recherche, en concertation avec le ministère public, est donc indispensable dans ce phénomène.

Enfin, l'évolution dans l'arrêt *Salduz* (de la Cour européenne des droits de l'Homme) pourrait influencer fortement sur les processus de travail, dans la mesure où le suspect disposera du droit de se faire assister d'un avocat durant l'audition (ce que vise la proposition de loi introduite à la Chambre³).

2 Doc. Parl., La Chambre, 2010-2011 (législature 53), Doc 1185/001.

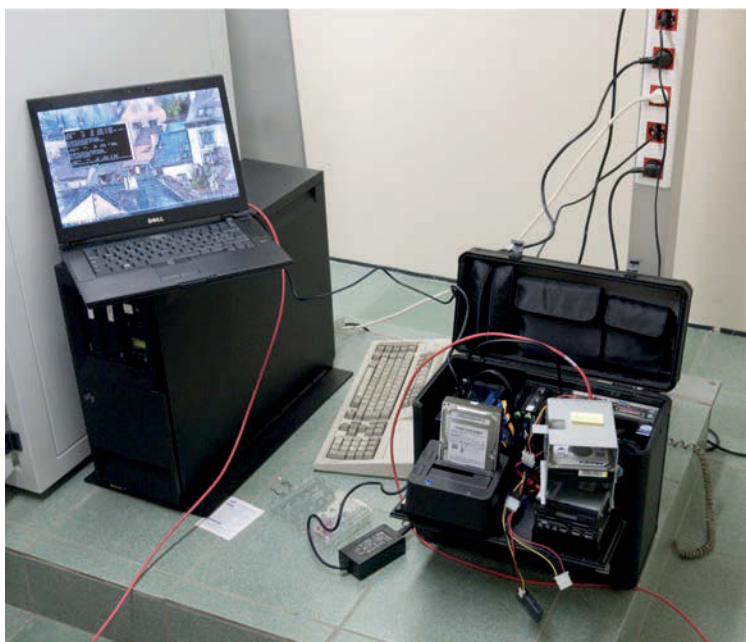
3 Doc. Parl., la Chambre, 2010-2011 (législation 53), Doc 0422/001.

8. Phénomène « fraude Internet »

La notion de « fraude Internet » n'est pas définie juridiquement. Elle tombe en fait sous le coup de la qualification courante d' « escroquerie » (art. 496 du Code Pénal⁴). La fraude Internet comprend toutes les formes d'escroquerie et de fraude commises via Internet ou par le biais d'un moyen électronique. La distinction entre la fraude Internet et la « simple » escroquerie réside dans le type de communication entre l'auteur et la victime.

Les escrocs sont très imaginatifs et recherchent toujours de nouvelles façons d'extorquer de l'argent. Nous pouvons même affirmer qu'il existe autant de scénarii que d'escrocs, bien que l'on retrouve toujours les mêmes formes de base, qui sont :

- la fraude au commerce en ligne ;
- l'« advanced fee fraud » (fausses loteries, faux héritages,...) ;
- la fraude à l'émotion (fraude à l'amitié, fausse histoire d'amour,...) ;
- la fraude à l'identité (vol et usage criminel d'identité, dont fait partie le phishing).

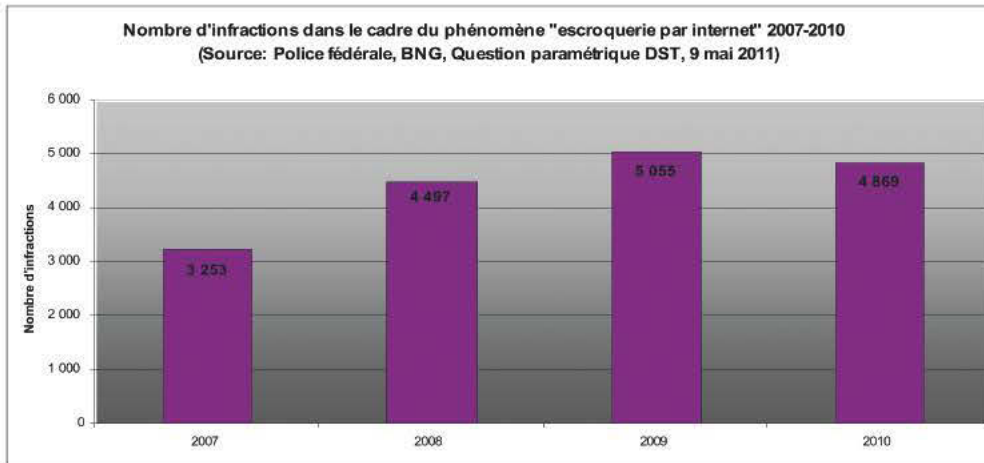


La fraude Internet est liée à d'autres phénomènes tels que le blanchiment (recrutement de « money mules ») ou la criminalité informatique (utilisation du hacking et vol d'identité pour créer des sites web de phishing).

Concernant la fraude Internet, la Belgique est plutôt un pays de victimes. Les victimes de la fraude Internet se situent partout en Belgique et sont dupées par des auteurs opérant presque toujours depuis l'étranger et profitant du caractère transfrontalier des technologies Internet pour rester impunis. Parfois, les victimes portent plainte depuis l'étranger contre des escrocs agissant depuis la Belgique. Ces groupes d'escrocs opèrent principalement depuis Anvers, Bruxelles et leurs environs.

Selon les chiffres de la BNG, le phénomène de fraude Internet a connu une forte hausse entre 2007 et 2009, pour compter plus de 5.000 infractions. Pour 2010, le nombre semble retomber à 4.869 infractions. Si l'on tient compte d'un chiffre noir de 80 % (ce qui ressort d'une étude néerlandaise), l'on peut estimer à 24.345 le nombre d'infractions réellement commises en Belgique en 2010. Le Moniteur belge de sécurité (version 2008-2009) n'aborde pas encore la question du chiffre noir pour ce phénomène.

⁴ Se faire remettre des biens/moyens par la victime en faisant usage de moyens frauduleux (faux nom, fausse qualité, lui faire croire certaines choses,...).



Dans l'image ainsi formée, le service remarque également une forte hausse du nombre de cas de fraude à l'identité, souvent combinée au phénomène « phishing ».

L'impact de la fraude Internet sur la société est souvent minimisé. Il est vrai qu'une grande partie des victimes ne perd que des sommes plutôt limitées. Toutefois, des montants de dizaines, voire de centaines de milliers d'euros sont régulièrement cités. Les cas de fraude à l'amitié par exemple sont très éprouvants pour les victimes. Outre le préjudice financier, elles souffrent de graves préjudices émotionnels car elle se sentent coupables de s'être fait avoir et ne parviennent pas surmonter cette culpabilité.

En outre, le préjudice issu d'escroqueries ne peut être répercuté sur un tiers (banque ou assurance) : la perte est individuelle et entièrement supportée par la victime. Il n'est pas rare que des victimes s'endettent pour payer l'escroc (en empruntant de l'argent à des amis, de la famille ou des institutions financières).

Préjudice causé par la fraude Internet	2007	2008	2009	2010
Préjudice moyen en euro	4.472	2.572	6.031	7.140
Médiane du préjudice en euro	750	400	945	725
(Source : Police fédérale, IMS+, extraction du 3 janvier 2011)				

Pour 2010, le préjudice moyen par victime augmente, pour atteindre 7.140 euros. La médiane, qui donne un aperçu plus correct, diminue légèrement pour arriver à 725 euros par cas. Le cas le plus grave pour 2010 est celui d'une fraude à l'investissement où la victime a perdu 310.000 euros dans une entreprise fictive d'investissement. Le dossier complet de cette fraude portait sur deux millions d'euros rien que pour la Belgique.

Si l'on tient compte d'un chiffre noir de 80 %, la perte totale issue de toutes les escroqueries Internet en Belgique pour 2010 avoisine les 146 millions d'euros.

En l'état actuel des choses et au vu du nombre peu élevé de poursuites, la prévention, par la conscientisation et la stimulation de la prudence des citoyens et des consommateurs, constitue un premier remède. Le service FCCU, avec certains partenaires, tente de mettre le plus possible le phénomène dans la presse afin de générer l'attention qu'il mérite. La principale collaboration dans ce domaine a pour partenaire le SPF Economie (participation au « Fraud Prevention Month »). De même, une dizaine de communiqués de presse sur les nouvelles formes d'apparition sont diffusés chaque année.

Une autre approche consiste à éliminer les « facilitateurs » de la fraude Internet. Les criminels utilisent en effet des services d'entreprises légitimes afin de pouvoir commettre leur fraude. Lorsqu'on intervient à ce niveau, l'escroc ne peut accomplir son délit. Le blocage temporaire

de comptes mail, le blocage et l'élimination de sites de phishing et de faux sites « escrow⁵ », l'annulation de petites annonces frauduleuses, l'interruption de la communication en annulant des numéros de téléphone ou de fax, etc., sont autant de moyens adaptés à la stratégie consistant à frustrer et à stopper les criminels.

Au niveau national, le service FCCU et le SPF Economie collaborent également à la « Plateforme de concertation sites de petites annonces » afin de développer des modes de prévention et de réduire le nombre de petites annonces frauduleuses en concertation avec les entreprises concernées.

Une autre forme importante de collaboration se situe dans l'intervention réactive contre les sites de phishing. Une procédure de règlement a été élaborée en 2010 avec le CERT belge afin de retirer lesdits sites le plus rapidement possible du net (dès leur détection), tant en Belgique qu'à l'étranger.

Au niveau international, la Belgique collabore étroitement avec les membres du « International Mass marketing Fraud Working Group » (IMMFWG), qui se penche sur des modèles pratico-opérationnels de collaboration afin d'améliorer l'effet préventif et répressif de la lutte contre la fraude Internet.

Dans le cadre des dossiers traités par les services de police belges, le service FCCU développe des liens nationaux et internationaux afin de pouvoir compulser des dossiers. Dans ce cadre, un échange d'informations plus approfondi entre les partenaires nationaux et internationaux est d'une importance capitale.

9. Phénomène « jeux de hasard »

Les infractions à la législation sur les jeux de hasard peuvent être de deux types. Le premier est fondé sur le non-respect de règles encadrant l'exploitation licite de jeux de hasard : un mauvais étalonnage des appareils de jeu, du laxisme dans le contrôle d'identité des joueurs dans les salles de jeu (joueurs exclus pouvant quand même jouer, souvent au détriment de leurs proches). Le second type d'infraction est basé sur la pratique et/ou l'exploitation de

jeux illégaux (par exemple via Internet). Dans cette catégorie, citons les tournois de poker, les agences de paris ou les loteries illégales. Les officiers de liaison du service OCRC (en collaboration avec la Commission des jeux de hasard), sont principalement actifs dans la lutte contre ce deuxième type d'infraction.

La prévention et le contrôle administratif des jeux de hasard sont pris en charge par la Commission, qui a d'ailleurs produit un DVD et un fascicule utilisés dans le cadre d'une campagne ciblant les jeunes, visant à les sensibiliser quant aux dangers du jeu. Les aspects répressifs sont pris en charge par la Commission, appuyée par la police locale, une PJF, ou un Office central (suivant les cas de figure) et le Ministère public.



⁵ Ainsi, l'escroc peut par exemple introduire un escrow ou une caution. Il s'agit d'un service indépendant servant d'intermédiaire et garantissant le déroulement correct d'une transaction, au profit du vendeur mais aussi de l'acheteur. L'acheteur envoie l'argent à l'intermédiaire qui le conserve temporairement et fait savoir au vendeur que l'acheteur a respecté sa part du contrat. Le vendeur envoie à son tour l'objet à l'acheteur qui, dès réception de l'article, contacte l'intermédiaire et donne son feu vert pour payer le vendeur. La caution règle le vendeur.

Les jeux de hasard sont considérés comme un phénomène et étudiés de cette manière par la direction DJF depuis 2010. L'expertise stratégique policière dans ce domaine en est donc encore à ses débuts.

L'impact du phénomène « jeux de hasard » sur la société est assez protéiforme. Une mauvaise protection des personnes ayant un problème d'addiction au jeu, comme par exemple en enregistrant mal ou pas du tout les joueurs dans une salle de jeux, et donc en n'excluant pas les personnes interdites de jeux, a de multiples conséquences indirectes, tant du point de vue financier que social, professionnel et familial. Violences domestiques, faillites, chômage, voire criminalité pour obtenir de quoi jouer encore, la liste est longue. Le jeu chez les mineurs est également un problème existant et connu, dont les conséquences sont tout aussi dramatiques.

Autre type d'impact existant, la création de réseaux criminels exploitant des salles de jeux ou des tournois illégaux amène son cortège de règlements de compte et de crimes violents, ainsi que la pratique de l'usure envers les joueurs, bien souvent par les mêmes personnes qui organisent ces jeux illégaux.

Du point de vue financier, les gains illégaux réalisés par les organisateurs de jeux clandestins entrent dans l'économie parallèle, appauvrissant l'économie officielle, entraînant des difficultés notamment en matière de financement de l'Etat (ces sommes ne sont pas taxées) et potentiellement injectées dans d'autres activités criminelles.

10. Phénomène « fraude aux marchés publics »

Sous cette appellation sont regroupées toutes les manœuvres visant à obtenir frauduleusement l'attribution d'un marché public ou à en tirer un bénéfice indu, notamment en surfacturant matériaux et services. Les ententes préalables entre fournisseurs, la manipulation du cahier des charges et le fractionnement de marchés publics dans le but d'éviter les contrôles (également appelé « saucissonnage ») sont autant de manœuvres illicites que l'on retrouve dans la fraude aux marchés publics.

La fraude aux marchés publics n'est abordée que d'un point de vue répressif par la police intégrée. Eu égard aux spécificités nombreuses et complexes de cette matière, ces dossiers sont pratiquement tous confiés au service OCRC. Dans ce phénomène également, le service continue de développer ses connaissances, au travers d'études et d'analyses stratégiques (par exemple pour l'IPNS en 2010).

Les PJJ des 27 arrondissements judiciaires peuvent selon le cas être appuyées ou appuyer le service OCRC lors d'enquêtes pour fraude aux marchés publics, ainsi que différents offices centraux, tels que le service OCDEFO (pour le volet fraude fiscale) ou le service FCCU (pour l'analyse technico-légale de données digitales).

La fraude aux marchés publics n'est considérée comme un phénomène que depuis peu : aucune analyse de risque complète n'avait été effectuée avant 2011. Les premiers résultats indiquent un nombre de faits connus très faible (56 incidents entre 2006 et 2009) mais pointent du doigt un chiffre noir très élevé (de plus de 99 %).

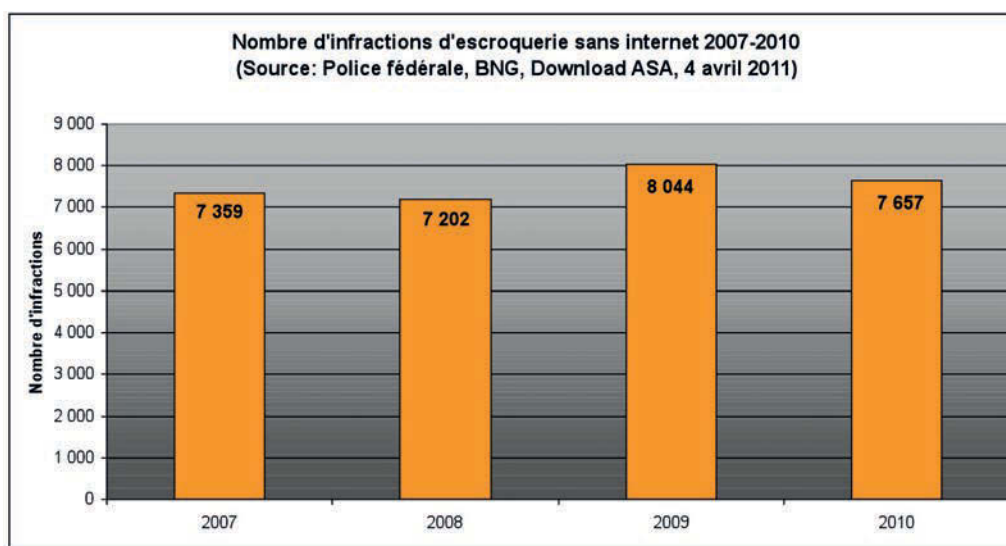
Les marchés publics sont très nombreux chaque année en Belgique. Par ailleurs, il n'existe aucun registre permettant d'en connaître le nombre exact ni d'en suivre le déroulement. Ceci illustre bien les difficultés de contrôler la validité et le bon déroulement des marchés publics. Les vulnérabilités de ces marchés se situent donc dans la procédure et dans le cadre dans lequel se déroule cette procédure. La méthode du saucissonnage, évoquée plus haut, contourne la procédure régulière en utilisant l'un de ses points particuliers : en dessous d'une certaine somme – variable selon le type de bien ou de service à acquérir –, il n'est pas requis de faire un appel d'offre et d'ainsi faire jouer la concurrence pour obtenir un meilleur prix.

Le marché sera donc scindé pour correspondre artificiellement aux conditions permettant de passer par une procédure négociée. Autre point de vulnérabilité possible, le cahier des charges. Ce document énumère l'ensemble des exigences de l'émetteur du marché public. Le cahier des charges peut être rendu si précis qu'une seule entreprise serait en mesure d'y répondre. Dans ce cas, la corruption d'un fonctionnaire chargé de réaliser ce cahier peut permettre à cette entreprise d'obtenir le marché en orientant les exigences de l'entité émettrice de ce marché. Les services d'audit au sein des différents départements de l'Etat (tant fédéral que communautaire et régional) sont donc confrontés à des défis majeurs pour découvrir les fraudes et en informer le ministère public, ce qui explique le chiffre noir.

Les fraudes aux marchés publics ont un impact très direct sur la bonne marche de la société et de l'Etat, mais difficile à estimer. En effet, les surcoûts entraînés par ces délits peuvent être extrêmement importants, tant en raison de la taille des moyens engagés qu'en raison de l'ampleur des surcoûts : lors de fraudes de ce type dans différents pays d'Europe, certains travaux publics se sont révélés avoir coûté jusqu'à 65 % de plus que le prix normal. Si l'on songe aux dizaines voire centaines de milliers de marchés publics passés chaque année en Belgique, l'on réalise vite que les pertes financières totales causées par ces fraudes représentent une somme aux dimensions considérables.

11. Phénomène «escroquerie sans Internet»

L'infraction pénale est inscrite dans l'article 496 du Code pénal, qui prévoit une peine d'emprisonnement d'un mois à cinq ans et une amende de 26 à 3.000 €, augmentée de décimes additionnels. Le graphique ci-dessus restitue le nombre d'infractions (faits et tentatives) pour la période 2007-2010.



Etant donné le nombre élevé de faits, chaque service de police locale (assurément l'accueil et la recherche) est confronté à ce phénomène, tant en ce qui concerne le phénomène avec que sans Internet. La division actuelle des «faits» permet de voir comment l'impact d'Internet sur le phénomène évolue. Les escroqueries sans Internet ont augmenté de 4 % pour la période 2007-2010, là où les escroqueries avec Internet ont connu une croissance explosive pour la même période, à savoir une augmentation de 78 %.

Cela signifie également que la Police judiciaire fédérale doit engager de facto plus de capacité pour ce phénomène. Un grand nombre d'auteurs commettent plusieurs tentatives et faits d'escroquerie avec des victimes dans plusieurs zones de police, entraînant donc une reprise des affaires par la PJF. Il faut par ailleurs faire remarquer que l'augmentation du nombre de faits avec Internet a aussi un impact sur le fonctionnement des RCCU.

DJF/FUSE a engagé un nombre limité de membres du personnel (trois personnes) sur le phénomène escroquerie sans Internet. De ce fait, seules quelques tâches principales sont exécutées. Le service traite les documents reçus en exécution de la MFO-3, B42 (il s'agit du flux d'information provenant de la PJF et des services de police locaux). Le service adapte par ailleurs les tableaux BNG pour faciliter l'encodage par les nombreux services qui sont quotidiennement confrontés à ce phénomène. Il a également élaboré une fiche d'encodage utile lors de la saisie. Le service met en outre, via l'intranet de la police, un vade-mecum à la disposition de la police intégrée. Étant donné que l'escroquerie est également un phénomène étendu dans les pays limitrophes, il existe beaucoup de demandes des services de police étrangers (documents appelés « INI » et « INO ») ainsi que des demandes d'entraide judiciaire qui parviennent au service via le Parquet fédéral. Les informations sur les modes opératoires sont diffusées via les articles dans l'Atrium News de la direction DJF. Le service FUSE tente également de susciter la vigilance de la population par rapport aux nouveaux modes opératoires conformément à la devise « mieux vaut prévenir que guérir ». Le service presse de la Police fédérale est partenaire dans cette diffusion.

Malgré l'effectif restreint de la section « swindling », la police tente de construire un réseau de partenaires. Ainsi, le SPF Economie est un partenaire important, tout comme l'Institut belge des services postaux et télécommunications (IBPT) et Bpost. Une participation est mise en œuvre avec le SPF Economie comme avec divers autres services de police étrangers, notamment dans le cadre du projet Europol en matière de Mass Marketing Fraud. Étant donné que les malfaiteurs approchent leurs victimes via Internet, téléphone, fax ou brochures, le but de ce projet est d'entraver le plus rapidement possible les lignes de communication entre l'auteur et la victime et donc de limiter au maximum le nombre de victimes. Le flux d'argent est ensuite surveillé afin d'identifier les commanditaires.

Le service FUSE a aussi créé un groupe de travail pour informer la banque et la poste sur la vulnérabilité de processus aux escrocs ou à leurs complices. Ils sont ainsi plus aptes à augmenter leur capacité à se défendre et à réduire l'impact des actions des escrocs.

Il n'est pas illogique de penser que le nombre d'infractions va également continuer à augmenter à l'avenir (le nombre de personnes qui déposent plainte en cas de tentative d'escroquerie diminue fortement, rendant ainsi l'augmentation statistique imputable uniquement à des faits accomplis). Étant donné que les auteurs ne seront souvent poursuivis que pour une série limitée de faits (ceci vaut également pour d'autres tromperies), la peine effective ne dépasse souvent pas les trois années, limitant ainsi les suites de l'exécution de la peine pour les auteurs. Par ailleurs, seules quelques victimes des auteurs enregistrés peuvent être identifiées, rendant ainsi très difficile les mesures de réparation envers les victimes. Comme beaucoup de victimes sont confrontées à ce phénomène, il est bien possible que ce fait nourrisse le sentiment d'insécurité du citoyen (pour l'année 2008, 8 % de la population se sentait souvent ou toujours menacée⁶).

12. Phénomène « fausse monnaie »

Ce sont les services de police locale qui sont les plus actifs dans la lutte contre le phénomène de la fausse monnaie, bien que la plupart des arrondissements appliquent la règle selon laquelle, en cas d'émission de faux billets sur plusieurs zones de police, le dossier est confié à la Police judiciaire fédérale. Les services de la Direction générale de la police administrative (par exemple la police de la route et la police des chemins de fer) sont bien évidemment confrontés eux aussi au phénomène. Au niveau PJF, c'est l'OCRF, section fausse monnaie, qui joue un rôle spécifique pour la police intégrée. Ce service est le point de contact unique pour les faux billets et les fausses pièces. Ainsi, l'OCRF connaît bien les tendances pour 2010,

⁶ Source : moniteur de la sécurité 2008-2009.

qui peuvent se résumer comme suit :

- Tout comme pour les années précédentes, le nombre de faux billets en devises étrangères détectés en Belgique semble continuer à baisser. Cela est dû au fait que de moins en moins de billets étrangers sont changés/utilisés en Belgique.
- L'augmentation du nombre de faux billets d'origine italienne continuera probablement à augmenter en 2011. Mais nous nous attendons à ce que la hausse soit bien moindre que celle constatée en 2010.
- Le nombre de fausses pièces de monnaie stagne depuis quelques temps et n'augmentera probablement pas en 2011. Toutefois, rien n'indique non plus que ce chiffre subisse une forte évolution à la baisse.
- Pendant et subséquemment à la crise économique, nous avons constaté une nette augmentation des falsifications « d'amateurs », fabriquées à l'aide de toners ou d'imprimantes à jet d'encre. Nous présumons que ce type de faux billet va régresser jusqu'au niveau antérieur à 2008.

En outre, la section fausse monnaie a été désignée bureau central national de lutte contre la fausse monnaie dans la convention internationale du 20 avril 1929 « portant répression de la fausse monnaie (avec protocole) ». De surcroît, les pays ayant adopté l'euro affichent une grande uniformité en matière d'action policière. Les dispositions pénales en vigueur dans ces pays pour ce phénomène font d'ailleurs également l'objet d'une uniformisation poussée.

13. Phénomène « faux documents »

Depuis 1997, la section « documents » du service OCRF gère le « Projet Europa ». Ce projet consiste à contrôler l'établissement des ressortissants européens sur le territoire belge. Par ce contrôle, la section s'assure que les documents présentés pour inscription dans les administrations communales sont authentiques. Ce contrôle n'est toutefois pas aisé et nécessite une très grande expérience car selon la législation européenne, seule une copie du document prise par les administrations communales peut être envoyée pour analyse technique.

Outre le fait que sont présentés des documents étrangers obtenus indûment (faux intellectuels) ou en la possession d'une personne ressemblante (« look-alike »), l'objectif du demandeur n'est plus seulement l'inscription comme européen en Belgique (afin de pouvoir bénéficier de tous les bénéfices liés à ce statut : accès au marché du travail, libre circulation dans l'espace Schengen, accès à la sécurité sociale, facilité lors de l'inscription,...). Lors des auditions menées

par les services de police, il appert que les demandeurs utilisent leur statut d'europpéen pour installer un climat de confiance avec autrui et ensuite commettre des escroqueries ou se tourner vers d'autres phénomènes (TEH,...). Bien que ces constatations soient assez récentes et qu'une image du phénomène n'ait pas encore pu être établie, ces tendances sont confirmées par celles de l'escroquerie où l'on voit des personnes qui achètent des produits à crédit par le biais de documents obtenus illégalement (parfois accompagnés de fausses fiches de salaire).



Les partenaires du service sont tant les unités policières de terrain que les services administratifs (communes, Office des étrangers). Force est de constater que ces services administratifs (communes et consulats) représentent de plus en plus la première ligne de contrôle. Nos frontières se déplacent. Les aéroports ne sont plus uniquement les points stratégiques de contrôle. Un investissement futur (prise de conscience, formation) doit être fait au niveau de ces services.

Le service a constaté les tendances suivantes :

- Les documents d'identité et de voyage intègrent de plus en plus de mesures de sécurité faisant la part belle aux nouvelles technologies. Couplée à une professionnalisation des faussaires, cette multiplication de sécurités a un effet négatif sur la qualité de contrôle de la première ligne (administrations communales, policiers de terrain, CPAS, compagnies de location de véhicules, etc.). Le contrôle de documents devient l'apanage de spécialistes.
- Documents d'identité roumains et bulgares. Dès qu'un nouveau pays intègre l'UE et n'est donc plus soumis à visa, on constate une augmentation des faux originaires desdits pays (par exemple : Roumanie, Bulgarie, Pologne). Pour ces trois pays, les utilisateurs de faux documents sont souvent moldaves. Tout ressortissant européen désirant s'installer en Belgique doit présenter un document d'identité valable auprès de l'administration communale de résidence. Vu le point soulevé ci-dessus et la mauvaise qualité du contrôle effectué par les fonctionnaires communaux, il a été décidé en son temps de faire pratiquer le contrôle par les spécialistes de l'OCRF, section documents. Ce contrôle se base uniquement sur des photocopies noir et blanc (la législation européenne nous interdit le contrôle du document original). Même si les spécialistes sont plus performants, la qualité grandissante des faux a comme conséquence que la détection de faux sur base de photocopies devient de plus en plus aléatoire.
- De moins en moins de faux en circulation : les statistiques des contrôles frontaliers européens montrent une diminution qui peut aller jusqu'à 50 % pour certains. Si une vision optimiste pourrait conclure à une diminution des faux en circulation, les experts s'accordent pour dire que cette diminution n'est pas proportionnelle au nombre de faux en circulation mais serait plutôt due à une diminution des interceptions. Il a déjà été fait mention de la perte de qualité de contrôle de la première ligne, mais le mode opératoire « faux intellectuel » est également à l'origine de ce constat.
- Augmentation des faux intellectuels : de plus en plus de documents étrangers présentés à l'appui d'une procédure en Belgique sont douteux quant à leur délivrance légale. D'un point de vue technique, ces documents sont bons. De plus en plus de documents annexes (attestations de naissance, de mariage, certificats médicaux,...) sont présentés dans les procédures. Outre la délivrance légale, les experts ne peuvent se prononcer sur ce genre de documents faute de spécimens de comparaison ou de documentation fiable.
- Déclarations répétées de perte de documents d'identité. Elles émanent de personnes qui sont souvent d'origine congolaise ou maghrébine (sur 45 cartes d'identité électroniques belges saisies par les services espagnols, 44 montraient des noms d'origine de cette région et 36 étaient connus des services de police). Certaines familles se sont spécialisées dans les « pertes » répétitives.
- Implémentation de la biométrie et des contrôles automatisés. Si la biométrie est une solution contre le mode opératoire de « look-alike », elle a également un effet pervers. Elle va déplacer nos frontières vers nos postes à l'étranger. En effet, ce sont nos agents en poste qui auront la responsabilité de la phase d'identification du demandeur. Comme dit plus haut, ces fonctionnaires n'ont pas l'expérience suffisante pour détecter un faux qui leur sera présenté. Ils encoderont donc les empreintes du demandeur mais sous une autre identité. Ce porteur illégal n'aura aucune difficulté pour entrer sur le territoire européen par un « e-gate ».

14. Phénomène « fraude sociale grave et organisée »

Le fonctionnement du programme et de la cellule de soutien n'a été lancé que fin 2010. Il est donc impossible de déjà délivrer une image du phénomène. Le phénomène a été défini comme suit dans le protocole : « Par fraude sociale grave et organisée, on entend toute forme d'acte délibéré, comportant le non paiement de cotisations dues (fraude aux cotisations) ou la perception indue d'allocations (fraude aux allocations), qui résulte de l'action d'une organisation structurée composée de deux ou plusieurs personnes et/ou de (d'une) personne(s) morale(s) qui, de manière concertée, commettent (commettront) des infractions ou des délits dans le but d'obtenir des avantages patrimoniaux directs ou indirects et :

- font usage de structures commerciales ou autres pour commettre, dissimuler ou faciliter la commission des infractions ou
- ont recours aux menaces, à la violence ou à la corruption ou
- déploient des contre-stratégies qui mettent en danger l'intégrité physique des membres du personnel des services d'inspection (par exemple des membres du personnel de l'inspection sociale du SPF Sécurité sociale, du contrôle des lois sociales du SPF Emploi, Travail et Concertation sociale, de l'inspection de l'ONSS ou de la Direction sauvegarde du régime de l'ONEM) ou
- abusent de personnes qui se trouvent en situation précaire (article 2 du protocole de coopération en matière de lutte contre la fraude sociale grave et organisée).

Le domaine de travail est donc particulièrement vaste. C'est pourquoi priorité sera donnée à l'approche d'un secteur plus restreint encore à définir et ce, sur base du savoir-faire du SIRS et des services d'inspection. La direction DJF espère pouvoir proposer les premiers résultats dans ce domaine dans le rapport annuel de l'exercice 2011.

CHAPITRE 4 – PROJETS DJF POUR 2011

Projet 1 – Le Business Process Reengineering (BPR) visant à optimiser la structure d'entreprise de la DJF

Non seulement les processus doivent être constamment évalués – et au besoin redéfinis ou redirigés – mais le leadership audacieux implique que la structure de la direction DJF puisse être mise en question. Il est probable que 10 ans après la réforme de la police, une nouvelle structure de la direction DJF soit plus adaptée pour faire face aux besoins modifiés de la police intégrée.

Projet 2 – Le recensement et la communication de l'offre de service

L'offre de service de la direction DJF a changé fondamentalement ces dernières années. De nouvelles tâches se sont ajoutées, d'autres ont été modifiées ou supprimées. De plus, les dernières années ont vu l'arrivée de nouveaux partenaires grâce à l'approche intégrée et intégrale des phénomènes. Par conséquent, il semble approprié de refaire l'inventaire de l'offre de service et de communiquer celui-ci à tous nos partenaires sous la devise : de bons accords font de bons amis.

Projet 3 – L'enquête de satisfaction des collaborateurs

Les policiers et policières sur le terrain et beaucoup de nos collaborateurs DJF ont été confrontés ces dernières années à un changement dans leur façon de travailler : de nouveaux processus de travail, de nouveaux outils informatiques, et ce, dans un climat de grande incertitude (le débat sur les tâches essentielles, les économies, la crise économique,...). Tous ces aspects peuvent avoir des retombées sur le travail et ses acteurs. Pour une grande direction, il est moins évident d'être attentif à ce qui se passe quant au bien-être et à la satisfaction des collaborateurs. Une enquête de satisfaction auprès de tous nos collaborateurs devrait parer à ceci. Les conclusions tirées de cette enquête pourront donner naissance à des adaptations sur le plan de la gestion (du personnel).

Projet 4 – La journée d'étude sur les recherches Internet

La police est une organisation en quête d'apprentissage. En matière de criminalité économique et financière, il y a toujours du nouveau sous le soleil. La direction DJF s'est donc fixée le but de mettre chaque année un thème en avant qui apporte une plus-value pour la police intégrée. Malgré la mondialisation, l'Internet est un moyen toujours méconnu de certains. La journée d'étude « L'utilisation de Google dans l'enquête policière » vise à combler ce vide.

Projet 5 – L'élaboration et la mise en œuvre d'un plan de communication et de formation

Etant donné que l'élaboration du plan de communication connaît quelques retards, le projet est reconduit dans le planning de 2011. En ce qui concerne le plan de formation, le deuxième volet, à savoir la fiche individuelle par collaborateur, sera entamé et mise en œuvre.

Projet 6 – L'analyse stratégique, une première analyse complète du phénomène « escroquerie sans Internet »

La direction DJF ne dispose pas d'un analyste stratégique pour tous les phénomènes. Il n'est pas rare qu'un analyste étudie deux, voire trois phénomènes. Pour l'année 2011, il a été envisagé d'élaborer une première analyse complète du phénomène « escroquerie sans Internet » dans le but de lever le voile sur une zone d'ombre de plus dans l'image.

Projet 7 – Le projet latéral DGJ, saisie et confiscation

La direction DJF s'inscrira complètement dans les projets latéraux énoncés par le directeur général de la Direction générale de la police judiciaire (DGJ). Pour ce qui est du projet « saisie et confiscation », la direction DJF sera pilote pour élaborer un projet en collaboration avec les divers partenaires.

Projet 8 – Approche systématique : l'approche intégrée au niveau micro


Le cycle d'évaluation de la police intégrée s'étend sur deux ans. Il consiste en des entretiens préparatoires, des entretiens de fonctionnement et des entretiens d'évaluation. Pour mieux aligner les objectifs de l'organisation sur les objectifs personnels, un modèle spécifique DJF sera développé afin de mieux vérifier si tous les domaines de travail ont été intégrés dans le cycle d'évaluation.

Projet 9 – La désignation d'un officier gestionnaire de l'information

La DGJ a imposé à toutes les directions d'arrondissement de désigner un « officier gestionnaire de l'information ». La direction DJF, ayant quelques services opérationnels, désignera également un officier gestionnaire de l'information qui élaborera un premier plan d'action en la matière.

Projet 10 – La gestion des connaissances (en anglais « knowledge management »)

Les départs de collaborateurs (principalement dus à la retraite) équivalent à une perte de connaissance et d'expérience. Dès lors, une première phase de la gestion des connaissances sera élaborée visant principalement à inventorier toute l'information juridique et à la rendre accessible. Une plus grande mise à disposition de l'image concernant les phénomènes sera également visée.



Les collaborateurs de la DJF participent activement chaque année à la réalisation des objectifs. Ce sont eux qui font la DJF et qui, grâce à leur motivation et leurs initiatives, nous permettent d'évoluer.

Ce rapport est aussi et surtout le leur.