



Les E.S.C.I.

**(Enquêteurs Spécialisés en
Criminalité Informatique)**

de la Police Judiciaire de Toulouse



Que sont les ESCI ?

Que font-ils ?

Comment le font-ils ?

C'est comme à la télé ?



Que sont les ESCI ?

Enquêteurs ?

Policiers !

Spécialisés ?

Formés !

Criminalité ?

Infractions !

Informatique ?

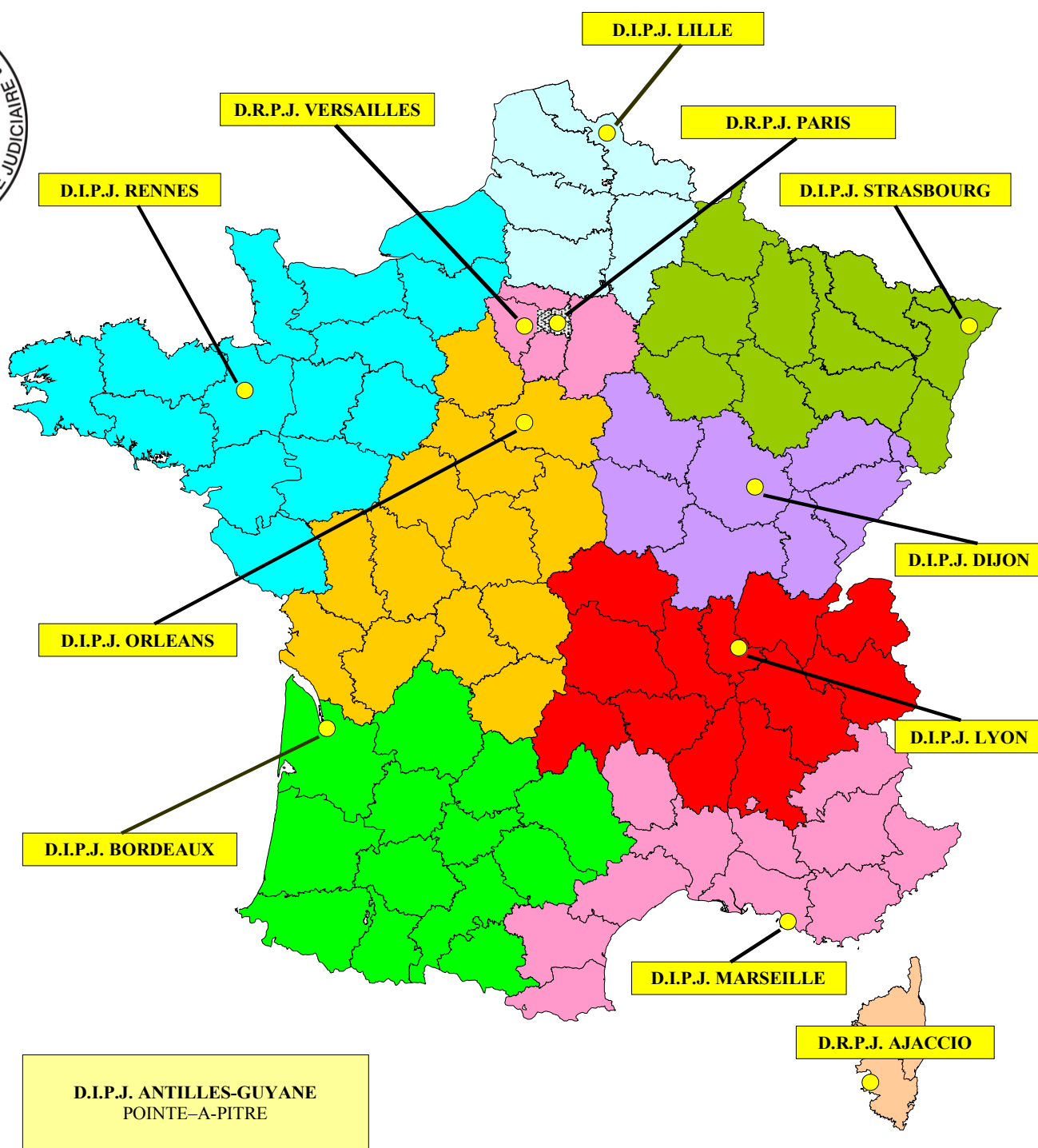
T.I.C. !



Les ESCI sont des policiers.

Ils sont affectés dans les différentes Divisions Interrégionales de Police Judiciaire de la Direction Centrale de la Police Judiciaire, ils sont au moins un par S.R.P.J.

Ces fonctionnaires sont chargés en priorité des enquêtes informatiques de leur secteur géographique, qu'ils effectuent d'initiative ou sur demande des autorités judiciaires





Les ESCI ne sont :

Ni « NCIS » ni « Les Experts », ni des experts judiciaires.



Ce sont des « personnes qualifiées » dans leur domaine.



Les ESCI sont des enquêteurs :

Sans être des experts judiciaires, ils disposent des connaissances nécessaires pour :

- comprendre les plaignants et les situations informatiques
- opérer à minima les investigations techniques indispensables (recherche des traces ou indices technologiques ; copies des disques durs et autres objets informatiques ; etc.)
- être les interfaces entre le monde technique (plaignants, intervenants divers) et le monde judiciaire (procureurs, juges)



Comment sont formés les ESCI ?

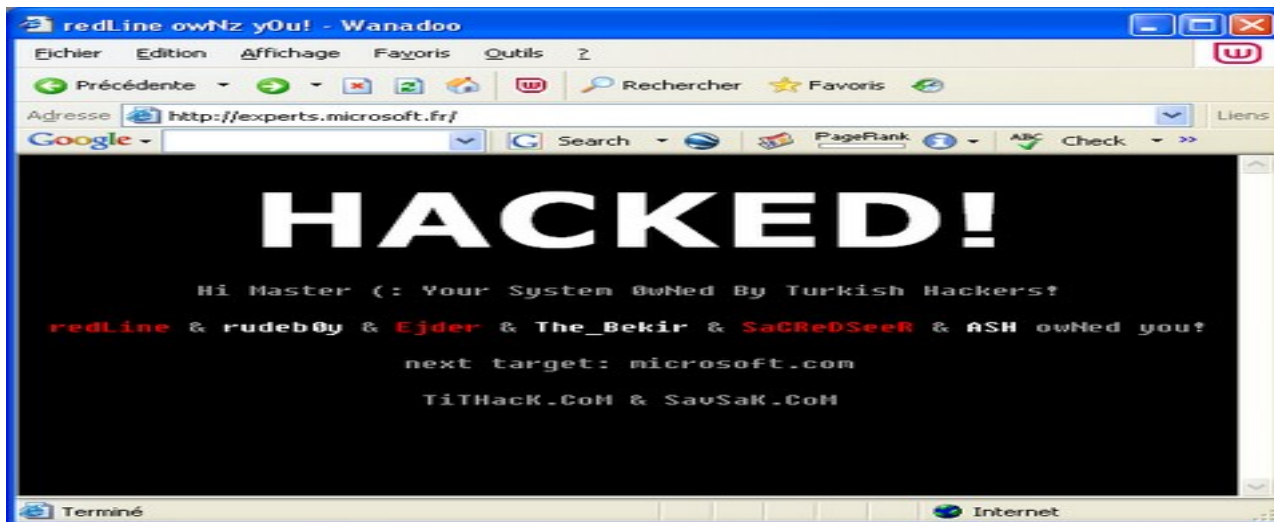
Les ESCI suivent une formation de quatre semaines dispensée par l'O.C.L.C.T.I.C. (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Informatique et de la Communication).

L'ordinateur - La sequence de démarrage - Notion de bit et d'octet - Le disque dur - Windows - La base de registre - Réseau - Téléphonie - Aspects Juridiques - Outils - Linux - Macintosh - Le fonctionnement d'Internet - Cybercriminalité et Internet - L'enquête cyber - Menaces et protections sur Internet - Anonymisation sur Internet



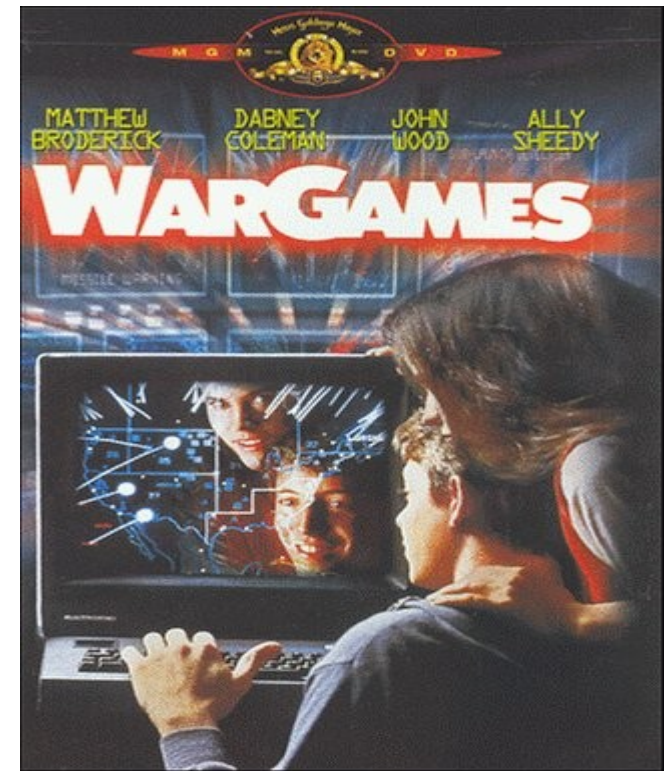
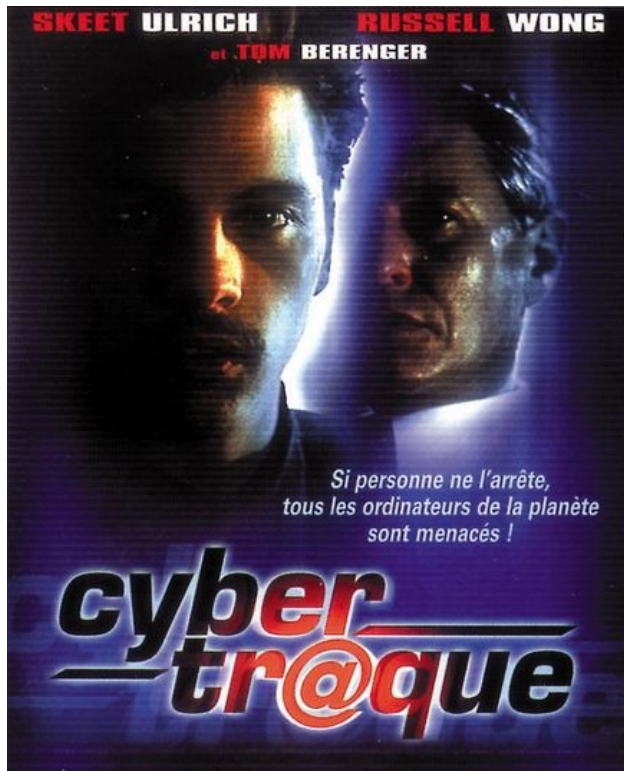
Qu'est-ce que la « cybercriminalité » ?

L'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunications en général et plus particulièrement sur le réseau Internet.





Le mythe de la « cybercriminalité »





La réalité de la « cybercriminalité »

Très peu d'affaires judiciaires relatives à des intrusions / compromissions

... car attaques provenant de l'étranger ou de faible importance
(deface, stockage illicite)

... ou choix du traitement du problème en interne
(image de marque, réticences de la hiérarchie)

... ou même intrusion / compromission non détectée
(confondue avec un virus)

A tort ou à raison, très peu de victimes déposent plainte



La réalité de la « cybercriminalité »

La « cybercriminalité » est pour les policiers répartie en trois familles :

- crimes et délits où l'objet numérique est utilisé de façon « accessoire » : échanges de SMS, envoi de mails, fausse comptabilité, contrefaçon...
- crimes et délits où l'objet numérique est utilisé de façon principale : diffusion de contenu illicite sur internet
- crimes et délits où l'objet numérique est l'objet de l'infraction : atteintes aux systèmes de traitement automatisés de données



Le travail des ESCI

Les ESCI matérialisent l'infraction informatique ou la « traduisent » :

- par l'audition de la victime ou des techniciens,
- par la collecte des éléments sur place (sauvegardes, logs, etc.),
- par la constatation directe des faits.

infractions « informatiques » :

Les ESCI dirigent l'enquête (qualification de l'infraction, information des magistrats)

infractions « non-informatiques » :

Les ESCI assistent leurs collègues enquêteurs



Le travail des ESCI

Les ESCI collectent et analysent les indices et autres éléments d'enquête

- recueillis chez la victime ou le mis en cause, par examen des supports informatiques

(preuve directe)

- recueillis chez les fournisseurs d'accès internet et prestataires informatiques

(preuve indirecte, par la voie des réquisitions judiciaires)

- en analysant les supports remis par les enquêteurs

(analyse forensique informatique)



Avec quoi travaillent les ESCI ?

Une bonne formation initiale puis l'expérience accumulée.

Quelques logiciels spécifiques : Encase, WinHex, des softs spécialisés

Quelques matériels spécifiques : FastBlock (lecture sans altération), ...

Beaucoup de matériels et logiciels « du commerce ».





Alors, c'est comme à la télé ?

Vous avez compris que non.



Mais il existe de nombreux autres services de l'état qui interviennent dans leurs domaines particuliers, avec leurs propres outils et personnels.



Quelques conseils ?

Agir, oui, mais avec prudence et discrétion

Signaler ce que vous pensez être une infraction, oui.

Mais sans alerter toute l'entreprise :

- pour éviter tout risque de déperdition de preuve
- parce que vous n'avez peut-être pas encore tout découvert
- parce que des accusations peuvent se révéler fausses



Quelques conseils ?

Eviter tout risque de déperdition des preuve :

- extraire / graver les fichiers d'historiques (logs serveur ou internet)
- remplacer l'objet informatique suspect par un autre
- faire une copie bit à bit des supports qui ne peuvent être remplacés
- conserver les supports ou objets informatiques dans un endroit sûr

Parce que vous n'avez peut-être pas encore tout découvert :

- l'intrusion découverte est-elle la seule ?
- l'incident est-il une cause ou une conséquence de l'infraction ?
- savez-vous si l'infraction a une origine interne ou externe ?
- s'agit-il d'une malveillance consciente ou d'une erreur involontaire ?



Quelques conseils ?

Eviter toute action pouvant être préjudiciable :

- chacun a droit au respect absolu de sa vie privée : sauf en cas d'extrême urgence ou d'extrême gravité, vous ne pouvez pas analyser les fichiers personnels privés du suspect ni fouiller son vestiaire et ses dossiers en son absence.

- chacun est présumé innocent tant qu'il n'est pas jugé coupable : des accusations même énoncées de bonne foi peuvent avoir de lourdes conséquences. « Il n'y a pas de fumée sans feu » peut détruire une réputation pour toujours.



Quelques conseils ?

Comment déposer plainte ?

- directement auprès du service de Police ou de Gendarmerie local
- par lettre-plainte auprès du Procureur de la République du TGI local
- par l'intermédiaire d'un avocat



Des questions ?



Coordonnées utiles :

**Service Régional de Police Judiciaire de Toulouse
23 bd de l'Embouchure 31066 TOULOUSE**

05 61 12 77 22 ou 05 61 12 77 23

yves.le-hir@interieur.gouv.fr

Merci.