HONEYPOT,
UN « POT-POURRI »… JURIDIQUE

Panorama des risques juridiques à envisager pour un déploiement légalement maîtrisé de systèmes « pot de miel »

Conférencière :
Marie BAREL,
Juriste spécialiste TIC et
Sécurité de l'information

Séquencement

1. *Honeypots*, le « piège à pirates » (Misc 8)
   - ► De la provocation aux crimes et aux délits
   - ► Le fait justificatif du consentement de la victime
   - ►Obligation de sécurisation des systèmes d'information
2. « *Honeypots, tracking hackers* » (L.Spitzner)
   - ► Traçabilité et protection des données à caractère personnel
   - ► Moyens avancés de capture de données et légalité de la preuve
3. *Honeypots*, entre contrôle et réponse
   - ► Responsabilité
     - ► Rebond
     - ► Capacité de réponse : option *Port scan* et technique des « *markers* », le cas de Specter

Conclusion : ► Nouvel article 323-3-1 (art. 34 LCEN)

1. *Honeypots*, « piège à pirates » ?

Source image : site web de Ryan BARNETT « *Honeypots: Monitoring and Forensics* ».
<http://honeypots.sourceforge.net>

Mythes et réalité

Honeypot, une dénomination bien ou mal à propos ?

- **Honeypot ou « pot de miel », une terminologie à la suggestivité forte…**
  - Thésaurus : leurre – fausse information – attraction – incitation – piégeage – provocation
  - Presse spécialisée :

    « Honeypots, le piège à pirates ! » (MISC 8)
    « On n'attrape pas les pirates avec du vinaigre, mais avec du miel » (JDNet)
    « Honeypots, l'art de la désinformation et de l'information » (Blocus-zone)
  - Un taux d'utilisation encore faible (dans son mode « production »)

- **…mais peut-être trompeuse ?**

Source image : http://www.realisateur.qc.net/Rentree_2002.htm

Principe de fonctionnement

- Valeur de production = zéro
- Activité/trafic attendus = zéro

+

Toute l'activité (flux entrants et sortants) enregistrée sur un *honeypot* est déjà SUSPECTE PAR NATURE.

- « Effet microscope » produisant une réduction drastique du niveau de bruit : meilleure gestion des faux positifs et faux négatifs

- Une capture d'informations *a priori* pertinentes, exempte de problèmes de limitation ou d'épuisement de ressources

- Le honeypot agit généralement comme une **boîte noire** : enregistrement *passif* de l'ensemble du trafic et de l'activité passant par lui

Concept de honeypot et risques juridiques associés

1. De la **provocation** aux crimes et aux délits (art.23 L. 29 juillet 1881) ?
2. Des systèmes *volontairement* vulnérables,
   - **consentement** implicite de la victime ?
   - une négligence coupable : de l'existence d'une **obligation de sécurité** ?

FAQs : *honeypot* et incitation

Re: Les « pots de miel » sont-ils légaux ?

> Thème 1 : l'incitation au crime

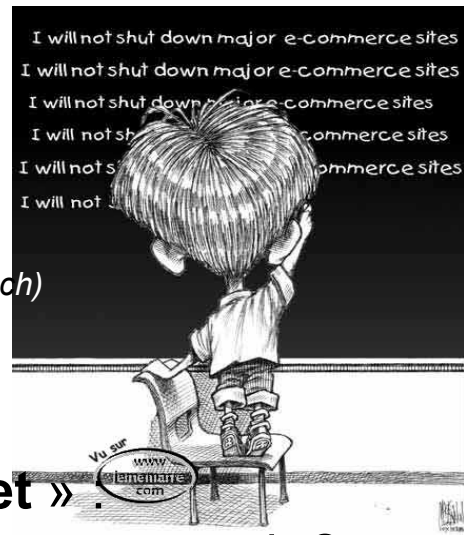
- « Le problème, c'est que ton pot de miel va simuler des failles évidentes sinon ce ne serait pas attirant. Donc, de par cette simulation de failles, tu incites les pirates à passer à l'action (…). »
  - « Je trouve ça vraiment dégueulasse de pousser les personnes à la faute… »
- « Sauf qu'un pot de miel n'incite pas. Si une personne attaque après s'être fait avoir par un pot de miel, alors c'est que l'intention était déjà là. C'est de l'invitation, pas de l'incitation. »
- « Il ne s'agit pas franchement d'incitation à mon sens ; le pot de miel est passif, il ne fait qu'attendre ! »

Source dessins : http://w3.uqah.uquebec.ca/poohs/page_a_winnie.html

De la provocation aux crimes et aux délits (art.23 L. 29 juillet 1881) ?

- Absence de l'élément constitutif essentiel : la **publicité**

  - Une conception vulnérable : un acte de *publicité* en soi ?
  - Le besoin de furtivité, contre-pied de la provocation directe
  - Indépendance de la *résolution criminelle* de l'attaquant par rapport à la vulnérabilité apparente du système
    - Des attaques par cible d'opportunité (*easy kill, shotgun approach*)
    - Des attaques « auto exécutables »



- Nécessité d'une **provocation « suivie d'effet »** : le consentement de la victime comme fin de non-recevoir ?

Source dessins : http://www.jememarre.com

Système *volontairement* vulnérable = consentement implicite de la victime ?

- Une équation trop évidente ?
- Distinction entre *honeypots* de recherche et *honeypots* de production (M. Roechst) : pour une approche pragmatique

- Entre recherche fondamentale… : **observer mieux et plus**

  VA(HR) ↗ ☮(☠,  , ⌖, 💣)

- … et sécurité appliquée : **mieux défendre et protéger**
  - Prévention (ex. *Bait and Switch*)
  - Détection et performances des NIDS (ex. *dtscp*)
  - Réponse (ex. *Specter* : options *Port Scan* et *markers*)

Système *volontairement* vulnérable : une négligence coupable ?

- Exigence de protection du système : une condition de l'incrimination d'atteinte à un STAD (articles 323-1 et suivants du Code pénal) ?
  - Travaux parlementaires français : loi Godfrain_1988
    - Sénat : « *le droit pénal ne doit pas compenser l'insuffisance ou la défaillance des mesures de sécurité* »
    - AN : la protection du système n'est pas une condition de l'incrimination
  - Jurisprudence :

➢ CA Paris, 5 avril 1994 : « *il n'est pas nécessaire, pour que l'infraction existe, que l'accès soit limité par un dispositif de protection* »

➢ affaire Tati/Kitetoa (2002) : un cas d'espèce à l'issue atypique >>>

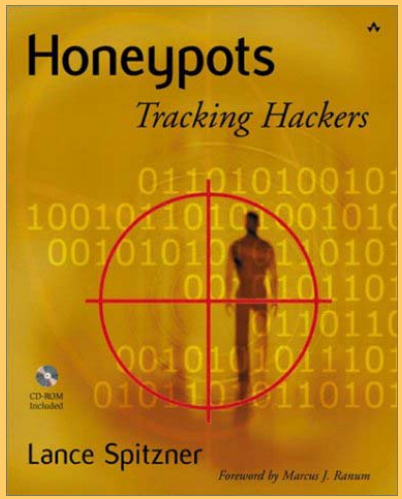
  - Travaux de la Commission européenne : proposition de décision-cadre relative aux attaques visant des systèmes d'information_JOCE 27/8/2002

- « (…). Le fait est néanmoins est qu'une grande partie des utilisateurs s'exposent malheureusement à des attaques faute d'une protection technique adéquate (voire même de toute protection). En vue de prévenir les attaques contre ces utilisateurs, le droit pénal doit couvrir l'accès non autorisé à leurs systèmes, *même si ces systèmes ne bénéficient pas d'une protection technique appropriée. C'est pour cela qu'il n'est pas nécessaire que des mesures de sécurité aient dû être déjouées.* »

Source image : http://www.milanpresse.com

- Des risques connexes à anticiper
  - Recours de tiers victimes ('victimes par rebond' ; article 29 L.6 janvier 1978 « Informatique et libertés »)
  - Exclusion de garantie en matière d'assurance des risques IT

2. Honeypots, « *tracking hackers* »



Quelles limites à la capture de données et la surveillance des activités de l'attaquant ?

Honeypots, « *tracking hackers* »

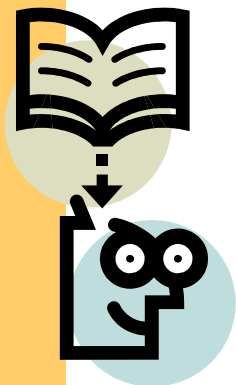
2.1 Limites … au regard de la réglementation sur la protection des données personnelles

2.2 Limites … au regard du principe de légalité de la preuve

Capture de données et « *privacy* » (1/2)

- Types d'informations collectées
  - Architecture et ressources (*fingerprinting* passif) : type d'OS, etc.
  - Méthodes de l'attaquant (ports scannés, vulnérabilités recherchées, *exploits*, etc.)
  - Provenance de l'attaque : nom de domaine (.fr, .nl, …), adresse IP, « signature » (« Iranian Hackers » v. Odebi e.g.)
  - Identification de l'attaquant : e-mail, site web personnel, données Whois, …

- Nature juridique des données collectées
  - Exemple de l'adresse IP, une donnée à caractère personnel ? : une qualification implicite
    - L'attaquant, une personne *identifiable indirectement,* selon des *« moyens susceptibles d'être raisonnablement mis en œuvre »* (Directive 95-46)
    - « *Données relatives au trafic* » (Directive 2002-58) : effacement ou anonymisation
    - CNIL, *Rapport sur la cybersurveillance des salariés sur leur lieu de travail : « données de connexion »*



« Honeypots : observer les pirates dans un tube à essai » - JDNet Solutions, 25/10/02

FAQs : *Honeypots* et *privacy*

Re: Les « pots de miel » sont-ils légaux ?

> Thème 2 : vie privée

- « Est-ce que je suis censé déclarer à la CNIL tout ce que je loggue au niveau iptables ? »
  - « Si tu stockes les IP alors tu dois les déclarer à la CNIL et mettre en place un système de sécurité adéquat. *Vieux souvenir de droits informatiques*. »
    - « Non, tu ne dois déclarer à la CNIL que les fichiers qui contiennent des informations personnelles sur des personnes. »
- « Je pense que les pots de miel sont parfaitement légaux, dans la mesure où on ne divulgue pas les informations *privées* concernant les pirates. Et vous qu'en pensez-vous ? »

Capture de données et « *privacy* » (2/2)

- Conséquences de l'application du régime de la protection des données personnelles
  - « Attaquants internes » et *honeypots* de production : conditions de la cybersurveillance
    - Sur la forme : respect du principe de loyauté et de transparence
      - Obligation d'information *préalable* des salariés
      - Consultation des instances représentatives du personnel (CE)
      - Notification à la CNIL
        - De la nécessité de déclarer les fichiers de journalisation ou « fichiers de *logs* » ?
        - Portée de l'anonymisation des données : condition de l'irréversibilité

  - Exigence du consentement des personnes concernées (article 7 Dir. 95-46) et « attaquants externes »
    - L'exception de nécessité « à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement » (alinéa f)

Capture de données et principe de légalité de la preuve (1/4)

Source image : http://www.socomenin.com.tn/ client25.htm

- Moyens avancés de collecte d'informations
  - Interception de frappes clavier (*keystrokes)*
  - Interception de messages instantanés ou *chat* (IRC, MSN Messenger, etc.)
- Des modes de preuve acceptables ?
  - « Les infractions peuvent être établies par tout mode de preuve » (art. 427 C.Proc.pén.) : principe de liberté de la preuve, sous réserve d'une administration loyale de la preuve
  - Problème de la légalité de la preuve :
    - article 226-1 du code pénal : atteinte à l'intimité de la vie privée

« Est puni d'un an d'emprisonnement et de 300.000 F d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° (…) »

- article 226-15 alinéa 2 du code pénal : interception des correspondances

« Est puni des mêmes peines, le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions. »

Source image : http://www.amazon.fr

Capture de données et principe de légalité de la preuve (2/4)

- Modes de communication protégés
  - Notion de « correspondance »
    - Trib.corr. Paris, 2 novembre 2000, affaire « CNRS » (au sujet du courrier électronique) : un message exclusivement destiné à une ou plusieurs personnes physiques ou morales individualisées (adresse nominative) ou déterminées (adresse fonctionnelle)
  - « Paroles », «images »

Source image : http:// www.eas.asu.edu/ elearn/images/

- Une qualification adéquate ?
  - Interception *chat* : messages instantanés entre une ou plusieurs personnes physiques
  - Interception *keystrokes* : *sniff* des pseudo frappes clavier à destination de la machine cible
    - Dialogue homme>machine

- Vers un « droit au respect des données transmises »
  - article 3 (« interception illégale »), Convention sur la cybercriminalité (Conseil de l'Europe, 8/11/01)
    - Protection des « transmissions non publiques de données » informatiques
      - Rapport explicatif, paragraphe 55 : la communication sous forme de transmission de données informatiques peut se dérouler
        - À l'intérieur d'un même système informatique (UC > écran ou imprimante)
        - Entre deux systèmes informatiques appartenant à la même personne
        - Entre deux ordinateurs communiquant entre eux
        - Entre une personne et un ordinateur (« par le biais du clavier par exemple »).

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Capture de données et principe de légalité de la preuve (3/4)

- Nature protégeable des échanges
  - Caractère privé des données
    - Article 9 du Code civil
    - Art. 226-1 C.pénal > section I « de l'atteinte à la vie privée » ; « Atteinte à l'intimité de la vie privée » / « (paroles) prononcées à titre privé (…) » ;
  - Caractère confidentiel du mode de transmission

- Le principe de secret des correspondances issu de la loi n°91-646 du 10 juillet 1991 est indépendant du fondement de la protection de la vie privée
- Article 226-15 : Chap.2, section IV du Code pénal, *« De l'atteinte au secret »*
- Article 3, Convention sur la Cybercriminalité : protection des « transmissions non publiques de données »
  - Le terme « non publiques » caractérise le mode de transmission et non la nature des données transmises.

Source dessins : http://www.auracan.com/

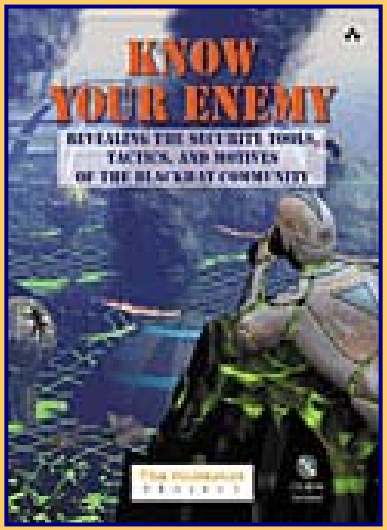
Capture de données et principe de légalité de la preuve (4/4)

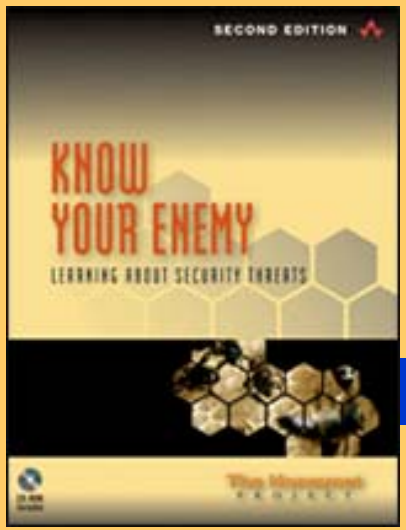
- Méthode du faisceau d'indices : du concept de l' «expectative raisonnable de vie privée » au concept d' « expectative raisonnable de confidentialité »

– **Exemple du « bavardage-clavier » (Mémoire de François Blanchette, *l'expectative raisonnable de vie privée et les principaux contextes de communication dans Internet,* 2001 - Montréal)**

Facteurs qui accroissent l'expectative raisonnable de vie privée/confidentialité	Facteurs qui diminuent l'expectative raisonnable de vie privée/confidentialité
☑ Accès restreint (cercle relationnel uniquement) ☑ Connexion d'ordinateur à ordinateur (communication un à un sans recourir au réseau IRC) ☑ Ouverture d'une fenêtre confidentielle (chiffrement SSL)	☑ Forum IRC (canal IRC accessible à tous) ☑ Connexion via un serveur IRC ☑ Ouverture d'une fenêtre confidentielle (*a contrario*) ☐ (…) ☐ La possibilité d'obtenir des informations sur les personnes correspondant à un pseudo

3. Honeypots, entre contrôle et réponse





Le « bras armé » de la sécurité

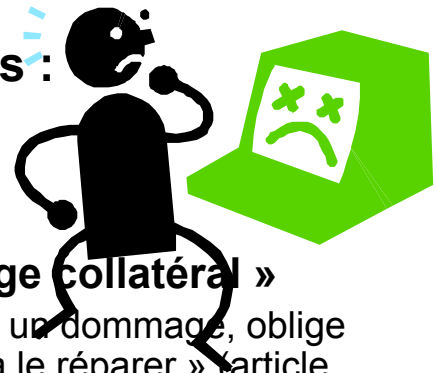
Source images : http://www.honeynet.org/book/index.html

Honeypots, entre contrôle et réponse

3.1 Responsabilité … du fait d'une attaque par rebond

3.2 Responsabilité … du fait de la réponse aux attaques

3.1 Rebond : maîtriser les risques



- **Des risques techniques différenciés : entre forte et faible interaction**
- **Risques juridiques :**
  - **Recours de la victime de « dommage collatéral »**
    « Tout fait de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer » (article 1382 C.Civ.)
  - **Risque assurantiel**
- **Capacité de contrôle : solutions techniques**
  1. L'interdiction !? 

  2. La limitation de bande passante (ex. Netfilter) ou du nombre de connexions sortantes dans le temps (Cf GenI)
  3. L'analyse des connexions sortantes et la neutralisation des paquets malveillants (cf GenII, Snort_inline)

 Source image : http://perso.wanadoo.fr/yann.wehrling/jeannette.html

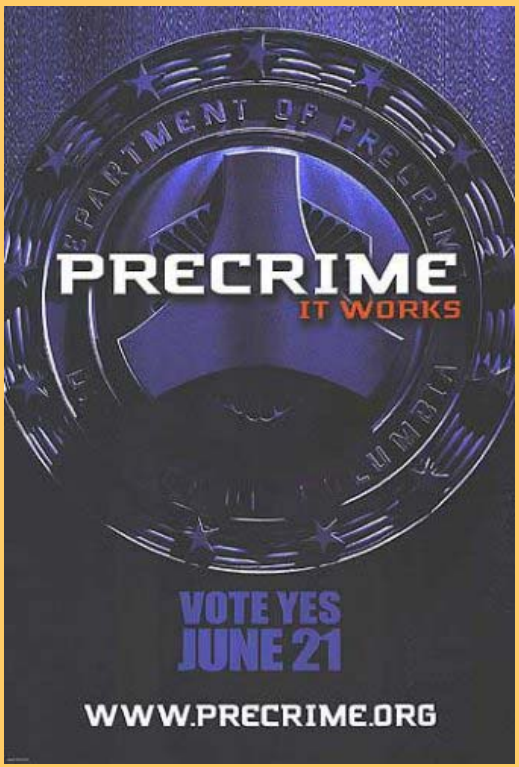
3.2 Capacité de réponse

- Le cas de SPECTER

Source image : http://www.specter.com

  - L'option *Port Scan* : une forme de « contre-attaque » ?
    - Un potentiel de malveillance : dérive d'un usage normal du système
    - Nécessité d'un commencement d'exécution
  - Les fichiers traces ou « *markers* » : le « mouchard virtuel »
    - Contrecarrer les nouvelles stratégies de défense des pirates (*Trojan defence*) : Cf affaire Aaron Caffrey et Julian Green (UK, 2003)
    - Article 323-3 C.Pén.: délit d'introduction frauduleuse de données
      - Un acte de légitime défense « pour interrompre l'exécution d'un crime ou d'un délit » ?
      - Etat de nécessité : un acte de défense « nécessaire à la sauvegarde (…) du bien » ?

CONCLUSION : quel avenir pour les *honeypots* ?



Source image : http://adorocinema.cidadeinternet.com.br/filmes/minority-report/minority-report-poster02.jpg

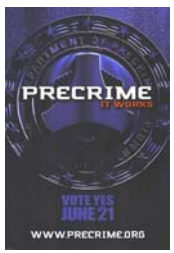
Date : printemps 2004

Auteur : Parlement français, vote de la LCEN

Chef d'inculpation : nouvel article 323-3-1 du Code Pénal

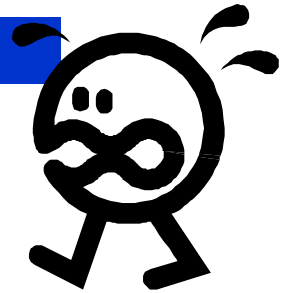
Nouvel article 323-3-1 du code pénal

- « Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée *conçus ou spécialement adaptés pour* commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 (du code pénal) est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »



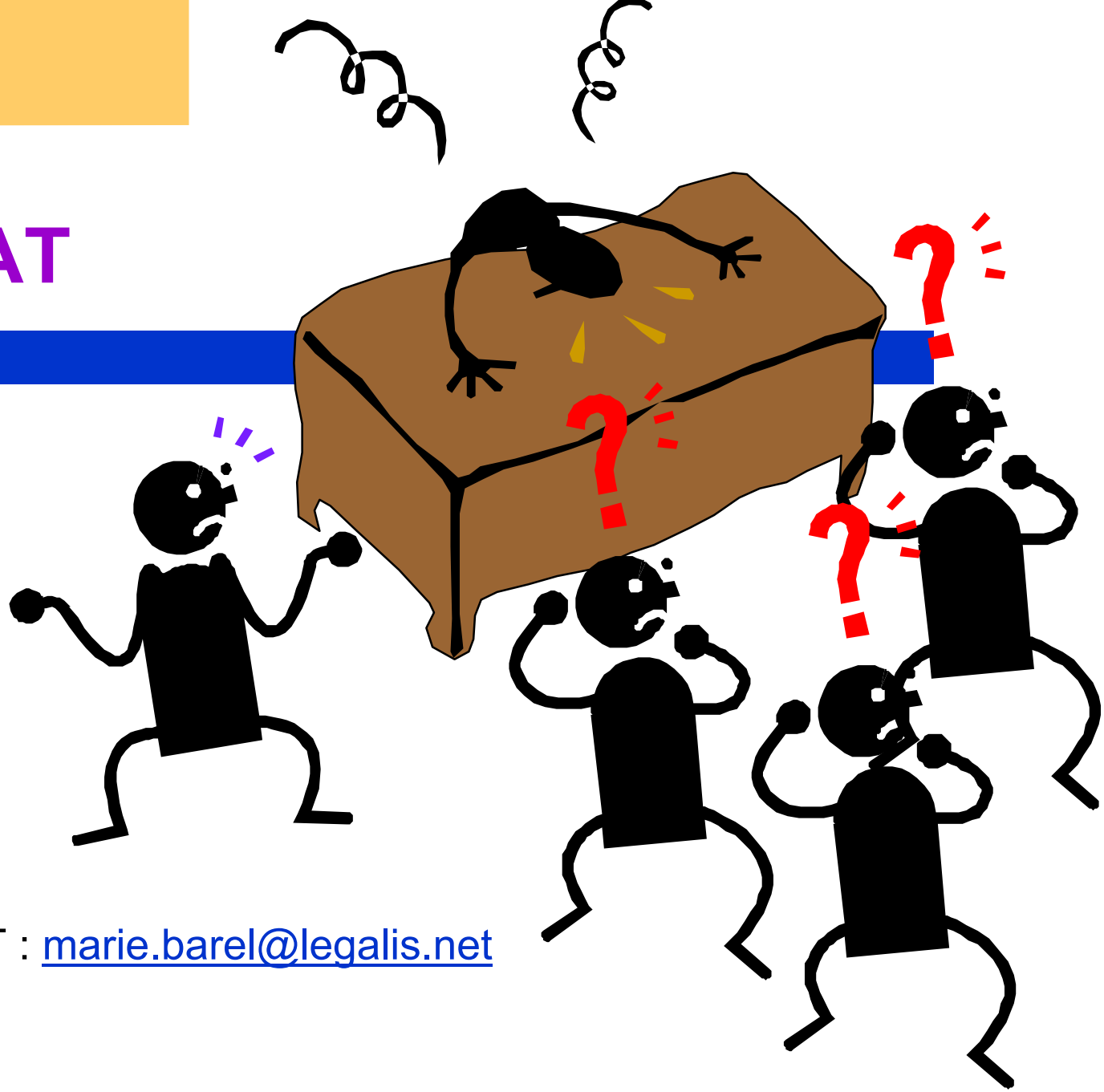
- Répression autonome des « attitudes d'amont »
- Logique d'anticipation des infractions principales de fraude informatique, sous l'impulsion de la Convention sur la cybercriminalité

Nouvel article 323-3-1 du code pénal



- Un champ d'application très vaste
  - La détention, un élément isolé
    - Un délit volontaire, mais sans intention spécifique
- Des dispositifs « *conçus ou spécialement adaptés* pour commettre » une infraction de fraude informatique
  - Article L 163-4-1 du Code monétaire et financier
  - Problème des dispositifs à double usage : du principal et de l'accessoire
- L'absence de « motif légitime »
  - Suppression de l'alinéa 2 : exception des « besoins de la recherche scientifique et technique ou de la protection et de la sécurité des réseaux de communication électronique et des systèmes d'information »
  - Appréciation souveraine des juges
    - Problème des publications : pour une divulgation responsable

DEBAT



CONTACT : marie.barel@legalis.net