**Zeitschrift:** Reihe Kriminologie / Schweizerische Arbeitsgruppe für Kriminologie = Collection criminologie / Groupe suisse de travail de criminologie

**Herausgeber:** Schweizerische Arbeitsgruppe für Kriminologie

**Band:** 24 (2006)

**Artikel:** Technologies de l'information et limites des moyens de preuve

**Autor:** Lathoud, Bertrand

**DOI:** https://doi.org/10.5169/seals-1051078

BERTRAND LATHOUD[1]

# TECHNOLOGIES DE L'INFORMATION ET LIMITES DES MOYENS DE PREUVE

**Résumé**

La nature particulière des technologies de l'Information et de la Communication influence la production, la collecte et l'interprétation des éléments de preuve. Le problème est de savoir de quelle manière. Il est donc nécessaire de restituer l'enjeu de cette réflexion. Il s'agit en fait de faire un bilan des limites que peuvent connaître les moyens de preuve dans le domaine des technologies de l'information. Cela impose de répondre à trois questions afin de proposer des éléments de réflexion pertinents.

Tout d'abord, on doit se demander dans quel contexte se situe-t-on? Il ne s'agit pas de se restreindre à une perspective uniquement juridique, ou purement technique. Le crime réalisé au moyen des Technologies de l'Information et de la Communication (TIC) pose problème sur ces deux plans simultanément, et la problématique relative aux moyens de preuve qui s'ensuit est elle aussi multi-disciplinaire.

Deuxièmement, la question de la méthode est posée de par le simple fait que le domaine est particulièrement récent, et, pour les sous domaines datant déjà d'un nombre suffisant d'années, en constante évolution (exemple = téléphonie). Les avancées en matière de criminalistique, dans ce domaine, sont réelles, mais il subsiste un certain nombre d'inconnues majeures, notamment en ce qui concerne l'évaluation scientifique du raisonnement d'inférence qui peut être construit à partir des éléments de preuve découverts sur une scène de crime informatique.

Enfin, il paraît préférable de s'en tenir à une approche empirique dont le but est d'illustrer ces limites, telles qu'elles ont été observées dans des cas réels. Il faut en particulier souligner la sensibilité de cette problématique pour les marchands. Les questions de théorie criminalistique sont importantes car ce sont elles qui permettront à l'avenir de construire les outils conceptuels et pratiques à partir desquels on pourra, devant une Cour, évaluer avec un risque minimal et maîtrisé, les indices rassemblés lors des investigations. Mais avant de proposer des réponses de pure théorie, il paraît essentiel de présenter le problème sous tous ses aspects, dont la dimension économique fait partie.

C'est pourquoi, les limites seront exposées à partir de cas rapportés par la presse suite à une procédure judiciaire publique, ou à partir de cas vécus dans la pratique.

---

1 bertrand.lathoud@laposte.net

**Informatik und Grenzen der Beweismittel**

Der besondere Charakter der Informations- und Kommunikationstechnologien beeinflusst die Erzeugung, die Sammlung und die Interpretation der Beweiselemente. Nur wie genau geschieht dies. Um eine Antwort geben zu können, erscheint notwendig, die Grenzen der Beweiskraft der Informationstechnologien zu ermitteln. Dies wiederum setzt die Beantwortung dreier Fragen voraus. Zum einem ist nach dem jeweiligen Kontext zu fragen. Dabei geht es darum, sich nicht ausschliesslich auf eine rechtliche oder technische Perspektive zu beschränken. Eine mittels Informations- und Kommunikationstechnologien (IKT) begangene Straftat bereitet Probleme in beiden Bereichen gleichzeitig und die Beweisproblematik ist ebenfalls multidisziplinär.

Weiter stellt sich die Frage nach der zu verwendenden Methode einfach schon deshalb, weil diese Technologien erst in jüngster Zeit aufgekommen sind, während die Technologien, die schon seit geraumer Zeit bekannt sind, eine ständige Evolution feststellbar ist (z.B. im Bereich der Telephonie). Die Fortschritte der Kriminalistik in diesem Bereich sind zwar erheblich, aber es bestehen doch grössere Unsicherheiten, namentlich hinsichtlich der wissenschaftlichen Evaluation der Schlussfolgerungen, die überhaupt Gültigkeit beanspruchen können auf der Basis der erhobenen Daten und Beweise.

Schliesslich scheint eine empirische Vorgehensweise angezeigt, deren Ziel es ist die Grenzen dieser Beweismittel anhand von realen Fällen zu illustrieren. Insbesondere ist auf die hohe Sensibilität der Händler hinzuweisen. Diese Fragen der kriminalistischen Theorien sind bedeutsam, weil sie erlauben werden, zukünftig begriffliche und praktische Werkzeuge zu entwickeln, mit welchen mit einem minimalen und kalkulierbaren Risiko die erhobenen Indikatoren vor einem Gericht bewertet werden können. Aber bevor Antworten der reinen Theorie vorgeschlagen werden, scheint es unerlässlich, alle Aspekte des Problems zu analysieren, und damit auch den wirtschaftlichen. Aus diesem Grund werden im Folgenden die Grenzen dieser Beweismittel anhand von praktischen Fällen diskutiert, namentlich auch Fällen, über welche die Medien als Folge eines öffentlichen Strafverfahrens berichtet haben.

Dans un monde qui se «virtualise» par l'usage croissant des technologies de l'information et de la communication, tant au niveau professionnel que personnel, la capacité de la justice pénale à poursuivre des comportements délictueux ou criminels commis dans cet univers technologue, devient un enjeu de première importance. *Que peut-on dire alors de l'influence que peut avoir la nature particulière des technologies de l'Information et de la Communication sur la production, la collecte et l'interprétation des éléments de preuve?*

## Introduction

En premier lieu, je souhaiterais restituer l'enjeu de cette réflexion. Il s'agit de faire un bilan des limites que peuvent connaître les moyens de preuve dans le domaine des technologies de l'information. Il me paraît donc nécessaire de poser trois questions afin de proposer des éléments de réponse pertinents.

*Tout d'abord,* on doit se demander dans quel *contexte* se situe-t-on? Il ne s'agit pas de se restreindre à une perspective uniquement juridique, ou purement technique. Le crime réalisé au moyen des Technologies de l'Information et de la Communication (TIC) pose problème sur ces deux plans simultanément, et la problématique relative aux moyens de preuve qui s'ensuit est elle aussi multi-disciplinaire.

*Deuxièmement,* la question de la *méthode* est posée de par le simple fait que le domaine est particulièrement récent, et, pour les sous domaines datant déjà d'un nombre suffisant d'années, en constante évolution (exemple = téléphonie). Les avancées en matière de criminalistique, dans ce domaine, sont réelles, mais il subsiste un certain nombre d'inconnues majeures, notamment en ce qui concerne l'évaluation scientifique du raisonnement d'inférence qui peut être construit à partir des éléments de preuve découverts sur une scène de crime informatique.

*Enfin,* il paraît préférable de s'en tenir à une approche empirique dont le but est d'*illustrer* ces limites, telles qu'elles ont été observées dans des cas réels. Je souhaite en particulier souligner la sensibilité de cette problématique pour les marchands. Les questions de théorie criminalistique sont importantes car ce sont elles qui permettront à l'avenir de construire les outils conceptuels et pratiques à partir desquels on pourra, devant une Cour, évaluer avec un risque minimal et maîtrisé, les indices rassemblés lors des investigations. Mais avant de proposer des réponses de pure théorie, il paraît essentiel de présen-

ter le problème sous tous ses aspects, dont la dimension économique fait partie.

C'est pourquoi, les limites seront exposées à partir de cas rapportés par la presse suite à une procédure judiciaire publique, ou à partir de cas vécus dans la pratique.

## 1 Un contexte favorable au développement de nouveaux comportements criminels

### 1.1 Pourquoi ces comportements sont-ils réellement nouveaux?

Si la victime, in fine, est la même que lors de la commission de n'importe quelle activité délictueuse ou criminelle, à savoir une personne physique ou une organisation, la nature et l'usage des systèmes vont induire des comportements nouveaux soit par leur qualité, soit en raison de leur volume.

En effet, l'omniprésence des systèmes numériques de traitement et de communication de l'information, en fait des cibles privilégiées tant pour des actions de dégradation de biens ou services, que pour des vols. Par exemple, la presse spécialisée rapporte chaque semaine des cas de DDOS (Déni de Service Réparti) ou de piratage de page d'accueil. Quel que soit l'usage délictueux, le même système va contenir les éléments de preuve. Une des difficultés majeures sera alors de circonscrire la scène de crime pour autant que cela soit possible. La mise en réseau des systèmes et les modes de gestion de l'infrastructure rendent parfois extrêmement difficile la recherche des lieux physiques ou logiques recelant des traces créées par la commission de l'infraction.

De plus, en raison de l'abstraction que représente la numérisation des informations traitées, on ne trouvera a priori que des éléments

physiques reliant des machines ayant interagi au moment supposé de l'activité délictueuse ou criminelle. L'identification en tant qu'individualisation d'un auteur potentiel ne pourra être réalisée sur la base de ces éléments, que si l'on dispose au préalable d'un lien solide entre la machine d'extrémité et l'identité de son utilisateur.

L'étape de l'enrôlement d'un utilisateur est alors aussi sensible que dans des domaines plus traditionnels tels que les services financiers. C'est le moment où l'on peut demander à connaître l'identité réelle d'un utilisateur, afin de la lier à une machine, ou à un moyen de paiement dont l'utilisation subséquente n'impliquera pas de contrôles d'identité contraignants.

## 1.2 Valeur de la preuve et renforcement de la confiance dans la nouvelle économie

Un point lié au contexte me paraît également important à souligner. La problématique liée à la valeur des éléments de preuve est un des arguments certainement critiques dans le processus de construction et de renforcement de la confiance dans l'économie «en-ligne».

L'impact économique non-négligeable de la fraude en ligne par exemple, peut entraîner la disparition «silencieuse» d'une partie de l'offre (entreprises menées à la banqueroute, associations de producteurs de Cartes de Crédit), ou la fuite des consommateurs, comme le montre le sondage réalisé récemment par IBM (Figure 1).

**Figure 1:** Extrait des résultats d'un sondage effectué à la demande de IBM Corp. auprès d'un échantillon représentatif d'utilisateurs américains (Déc. 2005)

*[...]*
** 50 percent don't use shared wireless networks such as in a coffee shop or airport*
** 38 percent don't bank online*
** 37 percent don't use credit card information online*

*In the last 12 months, survey respondents have taken certain actions to protect themselves against the growing cybercrime threat:*

** 29% have stopped reading credit or debit card information over the phone*
** 27% have stopped buying from unfamiliar retailers*
** 18% have stopped paying bills online*
*[...]*

Une somme d'incidents considérés individuellement comme mineurs, peut provoquer un retrait des acteurs du e-commerce, ou du moins une diminution importante des ressources affectées aux processus producteurs de valeur-ajoutée, et une redirection des budgets vers les dépenses liées à la sécurité. En 2004, par exemple, 32% des affaires informatiques rapportées au FBI correspondaient à un dommage inférieur à 100 $.

Il me semble également clair que le sentiment d'impunité (peut-être infondé mais néammoins réel) des pirates informatiques, facilite le passage à l'acte. Nous fondons cette remarque sur les interactions que nous avons pu avoir avec certains d'entre eux au travers de nos activités professionnelles. Certains n'hésitent pas à contacter le service de support à la clientèle pour se plaindre des restrictions qu'ils subissent dans l'usage du service à la suite de tentatives de fraude qu'ils admettront bien volontiers avoir commises lorsqu'ils se sentiront hors d'atteinte d'une éventuelle poursuite pénale.

La demande de résultats lors des investigations menées par les autorités de police et justice s'en verra accrue. Comme il n'est nullement question d'affaiblir les garanties offertes par la procédure pénale en matière notamment de présomption d'innocence; la qualité et l'effi-

cacité des enquêtes, particulièrement de leur volet technique, seront des facteurs-clé de réussite.

Cette nécessité d'obtenir des résultats en matière de poursuites ne vient pas uniquement de la visibilité donnée par les médias à ces cas. La presse a souvent rapporté les affaires les plus «visibles». Il s'agissait de déni de service, de propagation de virus à grande échelle, ou encore de vandalisme à l'encontre de la «vitrine» Internet d'une institution. D'autres cas ont moins attiré les reporters. Ils illustrent le phénomène que l'on pourrait qualifier de criminalité dite «à bas bruit». Cette dernière est représentée par les actions qui ne sont pas médiatisées, soit parce qu'individuellement elles ne sont d'aucun intérêt pour les médias, soit parce qu'elles ne sont pas ébruitées par les victimes. Cela ne signifie en rien qu'elles sont de faible importance, en particulier pour ces dernières. Les avertissements publics du NHTCU[2] en Angleterre sont néammoins le signe que ces dernières existent bien, en particulier toutes les agressions de type racket ou chantage.

Pour les actions peu médiatiques, le vol d'identité est caractéristique. Il se pratique de diverses manières, dont certaines très «traditionnelles». Mais dans le contexte des technologies de l'information, la méthode la plus couramment employée est le Phishing. Il consiste en l'envoi massif de mails rédigés de telle sorte que l'utilisateur croit avoir à faire à sa banque ou à toute autre institution détenant des éléments d'information permettant d'authentifier son identité. Les criminels accumulent ainsi des données personnelles avec lesquelles ils peuvent réaliser des transactions financières ou commerciales frauduleuses sous une autre identité que la leur. Comme l'a montré l'étude empirique de CHRISTOPHER ABAD sur l'économie du Phishing,[3] un véritable marché existe pour la revente de ces éléments d'identité.

2 National High Tech Crime Unit – now part of the Serious Organized Crime Agency – Les avertissements en question ont été diffusées dans les années 2002 et 2004.

3 http://www.cloudmark.com/releases/docs/the_economy_of_phishing.pdf

Lorsqu'il s'agit de découvrir ces cas, et d'enquêter à leur sujet, on ne peut utiliser que les éléments techniques, car les données relatives à l'identification de l'utilisateur sont valides. On peut donc rechercher en priorité des indices au niveau des informations systèmes telles que les logs de connexion. Il sera parfois possible de trouver quelques indications lorsque la transaction permet d'accéder à un service basé sur l'usage des Technologies de l'Information et de la Communication. La corrélation entre ces deux niveaux d'indices fournit une base plus solide pour l'individualisation des machines des auteurs, voire pour leur identification personnelle.

Concrètement, cette criminalité est au moins autant «globalisée» que l'est l'économie. Notamment, sur les cinq dernières années, le rapport de Symantec, qui s'essaie à diverses prévisions à court-terme, a surtout été un moyen de constater la répartition géographique apparente des pirates informatiques. Asie, Europe et Amériques: il y a au moins un pays de chacun de ces trois continents au sommet du classement.

Si l'on prend un exemple issu de la pratique, il a été possible de constater que des ventes de comptes frauduleux pour un service web particulier, se faisaient depuis 4 continents, au travers de revendeurs ne se connaissant pas nécessairement. Ce réseau de distribution ad hoc s'est constitué par le biais du «bouche-à-oreille» électronique: sites web régionaux, IRC, mailing lists, et contacts personnels. Il n'ya aucune cohérence particulière dans les traces relevées dans les logs de connexion au service. Ce sont les aveux de l'un des revendeurs qui permettront de reconstruire la structure.

Cette investigation a confirmé la très faible valeur individuelle des adresses IP lorsque l'on doit faire face à une structure criminelle ad hoc, et capable de s'auto-organiser sur plusieurs continents. De plus, pour arriver à identifier un des membres du réseau, puis l'amener à confesser les faits, et enfin contrôler ses dires, les besoins en ressources techniques et humaines sont très importants.

## 1.3 Caractéristiques particulières des actions criminelles commises en ligne

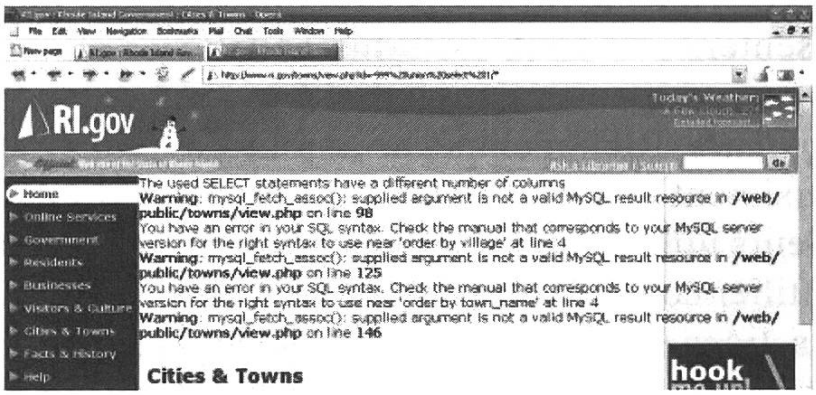
On ne peut pas se préoccupper de l'impact possible des crimes et délits commis au moyen des technologies de l'information, sans insister sur trois des caractéristiques particulières de ce type d'action criminelle. Nous les détaillerons au moyen d'exemples. Mais il faut dès maintenant les présenter.

Elle peut être *ubiquitaire*. Rien n'empêche aujourd'hui un pirate de commettre simultanément plusieurs délits à différents endroits de la planète. Il est d'ailleurs utile de signaler que cette ubiquité est un des moyens de les identifier comme suspects lorsqu'il est possible de relier plusieurs transactions entre elles, et que l'on constate qu'elles se suivent à quelques minutes d'intervalle tout en ayant été commises pour l'une au centre des USA, pour la seconde en Asie du Sud-Est, et enfin pour la dernière d'entre elles dans un pays du Moyen-Orient. Ce sont bien sûr les adresses IP qui permettent cette géolocalisation. Comme les technologies de télétransportation sont encore balbutiantes, on préfère penser à l'hypothèse que ces actions correspondent à une tentative de fraude. Statistiquement, cela s'avère encore l'hypothèse la plus vraisemblable. En tout cas, le pirate est lui physiquement présent à un seul endroit. Un premier défi va donc être de le localiser. Cela reste souvent hors de portée de la victime lorsqu'il s'agit d'une entreprise. Elle ne peut que fournir aux enquêteurs de police, les éléments issus de l'interaction directe avec l'agresseur (fichiers de journalisation et rapports internes des spécialistes concernés).

**Figure 2:** Exemple de mode d'emploi très détaillé extrait d'un site de hackers russes spécialisé dans l'attaque de sites américains

Возможно читателю непонятна цифра "1" следующая после команды "SELECT", но тут нет ничего принципиального. Мы просто возвращаем "1" вместо значения первой таблицы базы.

Вернемся к нашим баранам. Я как и следовало прибавлял значения к запросу. Ход этого можешь увидеть на соответствующем скрине.




Так я тыкался пока не дошел до верного количества столбцов в запросе. Этим запросом оказалось:"http://www.ri.gov/towns/view.php?id=-999+union+select+1,2,3,4,5,6,7,8,9,0,1,2,3,4,5,6,7,8,9,0,1,2,3,4,5,6,7,8,9,0, 1,2,3,4,5,6,7,8,9,0,1,2". Если не поленишься и посчитаешь - узнаешь, что выполнение этого запроса означало, что в таблице 42 столбца :) Так как подбирать названия таблиц и баз было несколько напряжно - у меня сразу появилась одна идея. Я вспомнил, что у mysql есть такая возможность - читать файлы при определенных правах, я решил попробовать. Для этого всего то требовалось выполнить такой запрос:

http://www.ri.gov/towns/view.php?id=-999+union+select+1,2,4,4,5,6,
7,8,9,0,1,2,3,4,5,7,7,8,9,0,1,2,LOAD_FILE('путь_к_файлу'),
4,5,7,7,8,9,0,1,2,3,4,5,6,7,8,9,0,1,2

La deuxième dimension de l'action simultanée est le *volume,* ou encore la capacité à réaliser une grande quantité de délits en un temps réduit, voire instantanément. Cela permet de réaliser de substantiels bénéfices tout en ayant un délit dont la valeur du dommage correspondant est en dessous du seuil de l'insupportable dans le contexte social présent. Le risque de voir une plainte déposée, et une instruction s'ensuivre est alors réduit. Un effet collatéral de la commission d'un grand volume de délits est que le volume de données à analyser par l'enquêteur sera proportionnel. On accroît ainsi le risque de passer à côté d'un indice déterminant.

Enfin, grâce à l'*automatisation,* réaliser l'action criminelle ne nécessite plus d'avoir fini sa Maîtrise à Champ-Dollon ou dans la plaine de l'Orbe. De nombreux logiciels de piratage incorporent des savoir-faire jusque là hors de portée du citoyen moyen. Si l'on prend un outil comme Cain, il permet de réaliser en quelques clics des attaques qui auraient nécessité les connaissances d'un administrateur système Unix quelques années auparavant.

A cette capacité à disposer de savoir-faires intégrés dans les outils, on doit ajouter la possibilité de se former dans des domaines très précis, au travers de sites web personnels où sont décrites et expliquées les procédures de piratage.

On pourrait illustrer la dernière des caractéristiques avec le cas suivant, issu de la réalité. Il a concerné au début de l'année 2006 un portail associant un opérateur de téléphonie mobile et un fournisseur d'accès internet, dans un pays d'Europe centrale. Le portail concerné permet d'accéder à différents service payants.

Après avoir découvert qu'un «nombre magique» permettait de rejouer indéfiniment la même transaction effectuée par SMS, des fraudeurs mettent en place un système de rechargement automatique des comptes de leurs clients.

C'est le système de prévention des fraudes qui va limiter les pertes: il n'autorise qu'un nombre restreint de transactions pour un utilisateur donné pendant une période déterminée. Les fraudeurs s'alignent donc sur ce «rythme» de manière automatique. Mais cela permet de confirmer leur détection en raison du volume soudain de transactions nouvelles similaires que leur automatisation a engendré.

Il faut tout de même reprendre manuellement les fichiers de journalisation afin de caractériser le mode opératoire de cette fraude et faire le tri pour éviter de bloquer les clients honnêtes.

L'identification des outils des auteurs est réalisée en deux temps: une fois le mode opératoire bien défini, grâce à l'utilisation conjuguée du système de détection de fraudes, et de l'analyse manuelle des logs, on recherche les machines ayant généré un volume important de transactions, alors qu'elles n'apparaissaient pas auparavant. Il reste maintenant à la Police à identifier les auteurs et à les lier à ces machines, si cela est faisable.

## 2 Méthodologie d'investigation: quelles contraintes pour les enquêteurs?

### 2.1 Hétérogénéité et imprévisibilité de la population d'auteurs potentiels

Comme on l'a évoqué précédemment, un problème majeur posé par la lutte contre la criminalité des TIC est la capacité à intégrer des savoir-faire techniques dans les logiciels. En effet, cela permet d'accroître artificiellement la population potentiellement criminelle. Plus besoin de longs séjours en «Centrale» pour acquérir de nouvelles spécialités criminelles. Le logiciel compense le manque de connaissances techniques.

Ceci a un impact sur la capacité à apporter des éléments de preuve. En effet, certaines phases préparatoires de l'action criminelle vont se trouver escamotées. Il sera alors plus difficile d'apporter la preuve de l'intention criminelle.

Par exemple, lors de campagnes marketing pour lesquelles l'effet de surprise devait servir à inciter les internautes à consulter certaines pages web, il a été découvert qu'un utilisateur avancé avait créé un «robot» chargé de surveiller ces pages et d'envoyer un message à une liste d'adresses mails en cas de «surprise» disponible. Pour être inscrit, il suffisait de noter son adresse email dans un simple formulaire en ligne. Mis à part l'auteur du robot, aucun des autres inter-

nautes n'avait à interagir avec le site web de l'entreprise concernée. Ils auraient donc pu ne pas apparaître du tout dans les fichiers journaux de connection du site web. Il devient difficile de les suspecter, à moins d'accéder à la liste de mails enregistrés (et là encore, des techniques simples peuvent faciliter la dissimulation des éléments d'identification).

L'anonymisation est aussi beaucoup plus facile en raison de cette capapcité à intégrer les savoirs-faire. En effet, un outil comme TOR[4] va permettre à ses utilisateurs d'être intraçables, tout en évitant la difficulté technique représentée par la recherche, l'identification et la configuration de multiples relais anonymisateurs (appelés communément proxies). On obtient une anonymisation presque parfaite, et utilisable d'un clic de souris.

Avec de telles techniques, les listes de proxies, utilisées pour identifier les tentatives de fraude, deviennent obsolètes.

Enfin, le marché noir de la criminalité sur Internet permet de louer pour de opérations ponctuelles, des groupes d'ordinateurs piratés, appelés communément zombies, sans avoir besoin de connaître soi-même les techniques de prise de contrôle et de gestion à distance. Le lien entre un auteur potentiel et la machine utilisée pour effectuer l'action devient ici aussi très ténu. C'est un tiers qui a réalisé le piratage, souvent dans une fenêtre temporelle éloignée, et ni cet individu, ni l'auteur d'un délit réalisé depuis la machine, n'ont de lien réel avec la machine incriminée.

Afin de mieux comprendre les hypothèses que nous faisons sur les contraintes en matière de méthode, il convient de rappeler brièvement dans quelle perspective nous nous situons, et quel est le contexte dans lequel ont été effectuées nos observations: l'entreprise est un cybermarchand global, c'est à dire qu'il n'y a pas de marché géo-

4 Site officiel: tor.eff.org

graphiquement délimité. Comme le produit est le même quel que soit le continent où il est vendu, les fraudeurs peuvent envisager de l'écouler ailleurs que là où ils ont commis la fraude. Cela peut créer un obstacle insurmontable à leur identification.

La valeur des biens vendus est faible, de l'ordre de quelques Euros, et la marge bénéficiaire est petite. Il faut donc un grand volume de transactions pour espérer obtenir un résultat financier conséquent. Cela a un impact direct sur la fraude. En effet, les fraudeurs vont devoir vendre à un prix inférieur au prix originel, pour espérer attirer des clients. Cela implique pour eux de reproduire le modèle de ventes à fort volume de transactions quotidiennes.

Comme on l'a évoqué, un tel volume rend difficile voire impossible une exploitation exhaustive des éléments de preuve. Mais il permet aussi d'envisager une approche statistique des caractéristiques des transactions incriminées. Des filtres semi-automatisés sont réalisables et peuvent, grâce à l'utilisation de technologies telles que les réseaux de neurones, obtenir des taux de détection très élevés.

Les tentatives sont très nombreuses, mais peu aboutissent. Une partie des fraudeurs fait alors porter son effort sur les systèmes de concurrents. Toutefois, ces accalmies ne sont que provisoires, et de nouvelles techniques sont régulièrement testées, imposant une mise à jour permanente des outils de détection.

Il y a un aspect presque darwinien dans cette lutte: l'accessibilité des services par Internet et l'anonymat des utilisateurs permettent aux fraudeurs d'essayer des variations de leurs attaques jusqu'à trouver la combinaison qui provoque le moins de détection ... Toutefois, les combinaisons ne sont pas infinies, et la mise en place de défenses combinées neutralise la plupart des agressions, y compris nouvelles dans leur mode opératoire.

## 2.2 Excès de données, ubiquité, et faisabilité de l'enquête

Lors de la réponse aux incidents d'origine criminelle, on se heurte très rapidement à des questions qui ne sont pas nécessairement issues de la nature des éléments de preuve, mais qui proviennent plutôt de la manière dont se font les échanges électroniques.

L'identification de l'auteur est une problématique dont les dimensions sont technique, économique, et enfin juridique.

On parle souvent des obstacles techniques, de l'anonymisation, et des outils tels que TOR illustrent la réalité de l'existence d'outils ou procédures qui permettent de masquer le lien entre l'auteur des faits, et le systèmes repéré comme origine de l'action criminelle.

Mais au-delà de la stricte faisabilité technique de l'identification, il y a la question économique posée par le coût des investigations. Lorsque l'on doit rechercher les auteurs d'un délit dont la valeur estimée du dommage est de quelques milliers d'Euros, et que l'enquête doit se dérouler sur plusieurs continents, on peut avoir la tentation d'affecter ses moyens à des affaires locales dont le retentissement est plus grand. Il ne s'agit pas ici de faire la critique des administrations concernées. Il paraît simplement essentiel de rappeler cette question alors que par ailleurs, on sera en mesure de disposer des savoir-faire nécessaires à ce type d'enquêtes. La barrière technique n'est pas la seule sur laquelle il faille se pencher. La question des ressources, et donc de la contrainte économique, se pose également lorsque le volume de données à analyser est trop important.

On n'insistera pas non plus sur les contraintes de procédures, liées à la dimension souvent internationale des affaires, et pour l'évocation desquelles les juristes et praticiens seront certainement les experts compétents à interroger.

La pratique nous a amené à constater que les éléments de base de l'identification d'un suspect, sont les fichiers de journalisation des infrastructures de télécommunications. On parle souvent des «fichiers logs». Ceux-ci apportent l'indication de l'interaction entre les systèmes, et la fenêtre temporelle de cette interaction. Mais il faut rappeler que leur fiabilité et leur validité peuvent être sujettes à caution. Si une machine est contrôlée, localement ou à distance, par l'auteur des faits, il y a fort à parier que la sincérité de ses logs sera difficile à établir.

Avant même de parler du lien entre une machine et un suspect, qui relève en général de la criminalistique classique, l'objectif principal de l'investigation électronique est finalement d'obtenir l'identification de la machine qui a réellement servi à diriger ou déclencher une attaque. Cela va généralement impliquer de travailler sur deux types de données: les données techniques et les données commerciales. Les premières sont souvent difficiles à analyser, en raison de leur technicité justement. Les secondes sont bien souvent des documents, et donc dans une forme plus adaptée aux méthode classiques d'investigation. Dans l'univers de l'Internet, il peut s'agir des formulaires en ligne servant à l'inscription à un service. Il ne faut donc pas nécessairement penser au support papier lorsque l'on évoque le concept de document. Le point positif de cette dématérialisation est la possiblité qui s'ouvre d'automatiser partiellement les recherches au moyen d'outils tels que des robots logiciels spécialisés dans l'analyse de chaînes de caractères alphanumériques. Toutefois, la faiblesse commune à ces informations numérisées est que, dans les deux cas (données techniques et documents commerciaux), l'abstraction que représente le codage numérique affaiblit le lien créé entre l'auteur, la victime et leur environnement au moment de la commission des faits.

## 3 Conséquences pratiques: la mise à mal des éléments de preuve lors d'affaires récentes

### 3.1 Décrédibilisation des éléments de preuve technique: la stratégie du doute

Une première approche privilégiée pour neutraliser les hypothèses de l'accusation est de porter atteinte à la crédibilité des éléments techniques servant à étayer l'hypothèse de l'accusation. Pour ce faire, on peut se baser sur la présence dans la machine du suspect, d'applications capables de réaliser les actions incriminées à l'insu de l'auteur présumé. C'est le cas des «troyens» ou chevaux de Troie, comme le célèbre SubSeven. On peut également souligner la présence d'une vulnérabilité majeure du système d'exploitation, permettant elle aussi le pilotage à distance de la machine, et donc la réalisation des infractions depuis un lieu éloigné, ainsi que la modification des fichiers systèmes en vue de supprimer les traces de ces interactions.

La première stratégie a été utilisée avec succès en Grande Bretagne, lors de deux affaires[5] relatives à la détention d'images à caractère pédopornographique. Dans le cas Schofield, l'accusation a même abandonné les poursuites entre deux audiences du procès. Dans les deux cas, la présence de multiples chevaux de Troie ne permettait pas d'assurer que le téléchargement des images était du fait des possesseurs des machines. En particulier, la Défense avait pu montrer que l'installation de plusieurs de ces troyens était antérieure au téléchargement.

Pour le cas mettant en cause le dénommé AARON CAFFREY[6] dans une tentative d'attaque des installations informatiques de l'autorité de gestion d'un port américain, la Défense s'est basée sur le fait que dans les semaines précédent le piratage reproché à son client, une

5 Cas Schofield – GB – avril 2003 / Cas Green – GB – oct. 2003
6 GB – oct. 2003

vulnérabilité majeure du système d'exploitation avait été découverte et exploitée discrètement par de nombreux groupes criminels informatiques. Le caractère plus incertain de ce système de défense, allié à des éléments convergents issus de l'enquête de police classique, n'a pas mené au même succès que dans les deux cas précédemment cités.

Une autre approche, si l'on ne souhaite pas être incriminé, est de faire en sorte que la trace laissée par l'interaction avec la victime mène à une autre machine que la sienne. Ainsi, il devient aisé de combattre une hypothèse construite par l'accusation sur la base d'éléments d'enquête (tels que des témoignages indirects) incompatibles en apparence avec les traces techniques disponibles. C'est ce que font par exemple les personnes qui profitent de la machine ou de la connexion Internet d'un tiers pour commettre leur forfait. A cet égard, l'affaire NOWAKOSKI[7] a été une première. L'individu a été interpellé par hasard, en raison de son comportement étrange, alors qu'il visitait des sites pédopornographiques à l'aide de son ordinateur portable, accédant au Net par l'intermédiaire de la borne sans-fil (WiFi) d'un particulier. Si l'enquête avait été menée depuis le site incriminé, elle n'aurait abouti qu'au domicile où était installé le point d'accès sans fil. Les traces matérielles auraient été cohérentes entre elles, mais n'auraient permis aucune identification de suspect.

### 3.2 Décrédibilisation des éléments de preuve technique: le manque de fiabilité des technologies utilisées

La stratégie du doute s'exerce aussi en attaquant directement la crédibilité des technologies servant à assurer la garantie des éléments de preuve. Pour l'essentiel, il s'agit de montrer que rien ne permet de prouver l'absence de contamination ou de manipulation de ces éléments de preuve.

7 Canada – nov. 2003

S'il est possible de mettre en cause la fiabilitié ou la validité scientifique des technologies qui garantissent que l'image logique du support original des éléments de preuve, est un clone exact de l'original, alors il sera aisé pour la Défense de bâtir une stratégie sur le doute raisonnable.

En résumé, cela revient à montrer que l'on peut avoir la même empreinte numérique pour deux fichiers différents auxquels on fait subir la même fonction de hachage. Cette fonction est supposée produire un résultat absolument unique pour un ensemble de bits donné. C'est ainsi que l'on garantit la qualité du clônage. Toutefois, l'existence de collisions, c'est à dire d'un résultat identitque pour des fichiers qui ne le sont pas, doit avoir une probabilité d'occurrence infinitésimale.

Si l'on ne peut prouver une inexistence absolue de collisions, on peut au moins considérer ces algorithmes comme sûrs lorsqu'il n'y a pas de méthode permettant de générer des collisions. A partir du moment où ce type de méthode devient théoriquement possible, la confiance dans l'algotrithme diminue, bien que le fait de démontrer que l'on pourrait obtenir une collision ne dit rien de la faisabilité de cette éventuelle méthode.

En pratique, il existe maintenant plusieurs scénarios d'attaque contre MD5[8], qui se sont avérés faisables. Cela a permis à l'avocat d'un suspect, lors d'un procés relatif à un excès de vitesse, de mettre en cause la validité de la photographie prise par le radar. En effet, lorsqu'il a demandé à l'accusation de prouver que la fonction MD5 utilisée par le radar pour signer électroniquement la photo, ne pouvait être manipulée, il n'a reçu aucune réponse. Le juge a donc rejeté la

8 MD5 a été pendant de nombreuses années le standard «de facto» en matière de fonction de «hash». Il a été remplacé par SHA-1 lorsque le NIST américain a décidé de promouvoir un standard officiel en matière de fonctions de «hash».
Cf. www.nist.gov pour les documents officiels
Cf. http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html pour l'analyse des faiblesses de ces algorithmes par BRUCE SCHNEIER.

plainte de l'Administration à l'encontre du conducteur, en l'absence d'expert capable de certifier que les empreintes électroniques n'étaient pas falsifiables.

La fonction de hachage proposée en remplacement de MD5 a depuis été mise en cause elle aussi, mais seulement de manière très théorique. Toutefois, cela signifie qu'il faut, pour les enquêteurs et magistrats, être en mesure d'évaluer en permanence la validité et la fiabilité des technologies utilisées en matière de criminalistique informatique.

S'ils ne peuvent pas tous suivre les formations qu'une telle posture exige, il serait au moins utile de disposer d'un annuaire, ou d'une liste, de professionnels reconnus, afin de faire face à ce type de stratégie de défense.

## 4 Conclusion

Rapidité: une de nos principales conclusions est que la suppression de la valeur du bien volé est au moins aussi importante que la dissuasion par la mise en oeuvre des moyens de la justice pénale. Cette dernière est souvent trop lente pour des délinquants qui agissent sur des périodes de temps extrêmement courtes, et qui utilisent des infrastructures «d'opportunité».

Une préparation des organisations (entreprises etc.) à traiter ces requêtes judiciaires, organisée dans le cadre de la fonction compliance par exemple, devrait faciliter la collecte des éléments de preuve lors d'enquêtes pénales, en permettant un accès plus aisé aux données réellement significatives, ainsi que valides et fiables d'un point de vue criminalistique. De plus, cela éviterait aussi d'avoir à exposer des volumes de données inutiles à l'enquête, mais néammoins reliées à des personnes privées, et donc devant bénéficier d'une protection adéquate de la part de leur détenteur.

Protéger la vie privée des utilisateurs, tout en étant en mesure d'assister efficacement la justice dans la recherche d'éléments de preuve technique n'est qu'un des défis que pose la différence entre les besoins des entreprises et organisations d'un côté, et des administrations judiciaires de l'autre. Le point essentiel est lié à la contrainte temporelle: les premières veulent obtenir rapidement une diminution de la pression criminelle, que ce soit par la prévention (sécurité) ou la répression. Les secondes ont pour mission de juger sereinement l'auteur des faits, dans les conditions prévues par la loi.

Du point de vue des entreprises victimes, il est donc nécessaire de mettre en place par avance les structures organisationnelles et matérielles qui permettront de faciliter la reconstitution des événements d'origine criminelle. Cela implique une capacité à appréhender la valeur criminalistique des données qu'elles produisent à l'occasion de leurs activités quotidiennes. Le bénéfice en sera aussi, pour les organisations concernées, une meilleure aptitude à gérer les incidents survenus dans leur système d'information, quelle qu'en soit l'origine.

Toutefois, travailler ainsi sur la validité et la fiabilité des éléments techniques pouvant potentiellement servir de moyens de preuve, ne sera pas suffisant pour résoudre les questions d'individualisation des auteurs. Le dernier lien à établir, entre la machine et la personne, devrait encore nécessiter à l'avenir l'intervention des moyens de l'enquête classique.