FIGHTING CYBERCRIME: TECHNICAL, JURIDICAL AND ETHICAL CHALLENGES

Guillaume Lovet
Fortinet, France

Email glovet@fortinet.com

ABSTRACT

Since the massive rise of cybercrime in 2005, which now steadily drains several billions (if not hundreds of billions) of dollars per year, a variety of challenges in efficiently fighting cybercriminals have been clearly identified. Clearly? Perhaps not. While it is widely recognized that the big struggle against cybercrime is severely hampered by the combination of the 'no cyber-borders between countries' factor and the 'heterogeneous laws among them' factor, in-depth examinations of the issue are scarce, and often overlook key aspects of the problem. Beyond the juridical issues, the technical challenges involved in fighting cybercrime may not be understood by political deciders, and the ethical aspects often set aside – as shown by the action various governments have taken lately to address the cybercrime issue.

This paper, reviewed by parties with technical, legal, or law-enforcement backgrounds, will shed light on those aspects, and attempt to answer the numerous questions subsequently raised: do we need more international cooperation processes? Would an 'Inter(net)pol' be the solution, or is everything we need already there at a juridical level, as we're only lacking will, knowledge, and concrete collaboration between deciders and experts? Could we end up endangering liberties in the process of addressing cybercrime?

INTRODUCTION

Cybercrime is an umbrella term covering all forms of crime perpetrated with the help of computer networks (regardless of whether the nature of the final target is a computer resource itself or not); its economic impact and the volume of funds passing through the big cyber-laundering machine every year is subject to controversy [1], ranging from USD 100 billion per year [2] to as much as USD 1 trillion [3]. The latter seems exaggerated, but either way, it is considerable. At this point, it is worth pointing out that these big numbers are very much consistent with two facts: the business models of cybercriminals are tremendously profitable [4], and they involve very low risks, be it from law enforcement or other gangs, as compared with traditional crime.

As such, cybercrime may be one of the next big issues governments will face in the medium to short term. Given the borderless nature of cybercrime, it is desirable, of course, that they decide to face it together, and that decisions be taken with a solid knowledge of all the challenges involved. As this paper will attempt to demonstrate, such challenges are broad and complex, and cover technical, juridical and ethical aspects. Some overlap across these three aspects, and some interleave. Which stresses, if this is necessary, that in order to achieve a meaningful comprehension of the cybercrime issue, the three aforementioned aspects need to be considered together, rather than in separate papers. This requires the gathering and digesting of inputs from experts with very different backgrounds, which is what the author has attempted to achieve; the pertinence of the result, as a matter of course, must be examined in the light of restrictions due to the conference paper format (this is not a master's thesis), and of the author's single-edged engineering background.

As a final note, of course, some challenges have been known for some time; others have been barely evoked or plainly ignored in the past, some needed updating, some needed simplification and vulgarization, and some had to be put in perspective with what had been done to address them. We tried to address them all, and we hope the result constitutes valuable food for further thought, appealing to a wide range of backgrounds. In any case, it is widely open to discussion.

CYBERCRIME 101: BRACE FOR IMPACT

Perhaps the very first challenge standing in the way of efficient anti-cybercrime action is that cybercrime itself, and above all its consequences, are generally poorly understood. While in-depth descriptions of the cybercriminal scene, its processes, models and profiles of actors is out of the scope of this document (see for that previous papers by the author [4, 5]), this section aims at proposing a simple, tree-shaped taxonomy, starting from the point of view of a (potential) victim, where the complexity of concepts increases from root to leaves. The goal is to provide a concise and explicit outlook of the cybercrime range of impact, and delimit logical categories of cybercrime components, for technical and non-technical people alike (depending on how far one goes toward the leaves).

On awareness and political action (Pt. 1)

At this point, it is worth noting that none of the challenges described in the following sections cannot be overcome. However, to be addressed efficiently, a strong political will is certainly almost always needed. Now, a strong political will often stems from a strong public opinion. Is there such a thing as a public opinion on cybercrime? Likely not. Most people actually do not know that viruses, trojans and other malware in general are (almost) solely aimed at making money, and view them as more or less mean geek jokes, which in the best case would open one's CD-ROM player and in the worst case burn one's hard-drive. As a matter of fact, most infected people ignore the fact that they are infected, and thereby part of a botnet, the infamous zombie computer networks at the core of cybercriminal activity. This poor awareness is further blurred by laws against illegal downloading, which designate average, tremendously common users as cybercriminals. Salt the whole with a lack of consensus on cybercrime numbers and suspicion of FUD spreading from anti-malware companies for business purposes, and one obtains a very fragile base for political action.

Taxonomy for victims

Yet, there are myriads of more or less academic reports, addressing various aspects of the phenomenon; but their disparity can leave an average user confused when trying to understand the phenomenon as a whole.

The author has detailed a wide range of cybercrime business models in the aforementioned previous publications, yet those did not offer a view 'from the potential victims' eyes', nor did they propose a global taxonomy of cybercrime-related events.

Here is one proposal, with each node having a causality relationship with its parent node (not a type-subtype relationship as traditional alpha-taxonomy implies), such that an event described in a node is 'caused by' a child node:

Individual users can suffer:

- Loss of money
    - Theft of credentials (online banking account, *PayPal* account, MMORPG account, CC number etc.)
        - Phishing
        - Trojans
        - Customer database hack (in the SaaS and Web 2.0 era, a lot of sensitive data sits 'in the cloud', which is cool, because it's always available... for cybercriminals too)
    - Scams
        - *eBay* bogus auctions
        - Fake online shops (pharmacy, watches, etc.)
        - Letters (Nigerian, Russian brides, etc.)
    - Extortion
        - Ransomware (viruses that encrypt the victim's data and ask for a ransom in return for the decryption key)
        - Personal data theft
            - Trojans
            - Online storage space hijacking (email, *Picasa*, *Flickr*, etc.)
- Loss of reputation
    - Impersonation
        - Hijacking of victim's account (email, *Facebook*, *MySpace*, *Twitter*, etc.)
        - Creation of account under victim's name (email, *Facebook*, *MySpace*, *Twitter*, etc.)
- Loss of temper
    - Nuisances
        - Bulk messages (email spam, social networking site spam)
        - Adware pop-up windows
        - Slow computer
- Loss of data (rare, due to the form of cybercriminality)
    - Failed extortion scheme leading to destruction of data held as 'hostage'
- Loss of freedom
    - Victim's IP address hijacked and used for criminal actions, leading to victim's conviction
- Loss of physical integrity
    - Online predators

Reading a path from the root to a leaf gives a scenario. For example, a user can suffer loss of money, caused by theft of their *PayPal* credentials, itself caused by a phishing scheme.

For the sake of clarity, the number of ramifications was kept to a minimum, but some leaves could be developed further. For instance, the presence of a trojan on the victim's system could have been caused by the prior presence of a bot (which was instructed by the botmaster to download and drop the said trojan). And the bot infection itself could have been caused by a drive-by install attack as the user visited a malicious site. This unlucky visit may have been caused by a malicious iframe on a legitimate site that silently redirected the user to the malicious drive-by site. And of course, the presence of the malicious iframe on the legitimate site may have been caused by an SQL injection attack, conducted from an Asprox botnet, etc. The possibilities are virtually endless.

A similar tree can be constructed for companies, corporations and organizations. While organizations may be 'non-profit', the goal of all companies is to generate money, and ultimately the only blow they can suffer is loss of money. But this can happen more or less directly, and be caused by the 'upper' nodes of the following tree:

Companies and organizations can suffer:

- Theft of critical data (intellectual property, customer base: see cases such as *SalesForce* and *Heartland*)
    - Theft of credentials
        - Phishing/social engineering
        - Trojans
        - IT system hack
- Paralysis of production tools
    - Botnet DDoS (external attack)
    - Aggressive virus (internal attack, often not even on purpose)
    - Compromise of SCADA systems (Supervisory Control And Data Acquisition, the systems that control industrial processes in factories, power plants, etc.)
        - Software vulnerability exploitation
        - Trojan horse
- Direct loss of money
    - Online extortion (DDoS blackmail)
- Loss of reputation (top risk identified by UK companies [6])
    - Any of the above incidents becoming public
    - Defacement of the company's website
    - Denigratory posting campaigns (partially automated negative posts on forums, blogs and web-boards)

The crippling of production tools (which the local area network can almost always be considered one of) caused by a virus aggressively spreading inside the enterprise network is more frequent than one may think, even when the goal of the virus itself has nothing to do with denial of (network) service. For instance, the infamous Conficker worm, with its *Windows* shares brute force features, caused numerous problems in infected internal networks, the impact going as far as grounding fighter planes [7].

Cybercrime, laundering and terrorism

Interestingly (and unfortunately), the corporation tree above could be applied to nations almost as it is. With posting campaigns used for guiding public opinion (a method reported to be used in China, albeit with minor automation [8]), rather than for mere denigration. And above all, with a new branch: possible loss of market (and in certain cases, economic) stability, due to important money laundering operations via cybercrime. This effect is documented in traditional money laundering [9], and so is cyber-laundering: cybercrime and traditional crime proceeds alike can be laundered via digital cash transfers as well as via more complex schemes involving botnets and automation (online casinos, VoIP payment systems, adware companies etc.). By translation, it is therefore reasonable to think that cybercrime may become an issue for markets and small economies, if it isn't already.

Quantifying the effects of cyber-laundering is beyond the scope of this paper; however, a case discussed with Mr X, working for a private intelligence company, is edifying. In this cyber-laundering scheme, stolen payment credentials (credit card number, *PayPal* account, etc.) are purchased on the underground by a cybercriminal gang, and used to fund VoIP for end-users' (à la *Skype*) accounts. These VoIP accounts are then used to call premium numbers belonging to the cybercriminal gang, and registered offshore. In order to evade the fraud detection mechanisms, of course, calls are performed from zombie computers (infected machines belonging to a botnet), and therefore appear to have been initiated by regular users. The money laundered so far reaches about 80 million euros. 'And that's only what we're aware of, that is to say, the mere tip of the iceberg, really,' says Mr X.

To conclude this section on the nature and impact of cybercrime, let's address a statement that has probably hampered the fight against cybercrime for a long time:

Unlike traditional crime, cybercrime does not kill people.

No lengthy developments are needed to pick this statement apart: it suffices to say that at the time of writing, cases of terrorist cells (or even organizations) funded by cybercrime are documented. In particular, in a written statement for the US House Committee on Homeland Security [10], counterterrorism expert Andrew R. Cochran recalls that 'The terrorists who executed the devastating 2004 Madrid train bombings, which killed almost 200 people, and who carried out the deadly July 7, 2005, attacks on the transportation system in London were self-financed, in part through credit card fraud.'

The collusion between traditional crime syndicates and cybercrime, on the other hand, is poorly documented, albeit probable. During an interview with the author, a cybercriminal involved in advanced *eBay* scams (including pay-on-delivery scams [5]) reckoned he had been introduced to the business of trojan seeding by his drug dealer.

TECHNICAL CHALLENGES

Convicting cybercriminals is therefore necessary, as they pose a direct threat to potential victims' finances, reputation, data and physical integrity; and also because cybercrime has economic consequences and indirectly promotes 'traditional' violent crime and terrorism, by funding them.

Now, convicting cybercriminals raises various challenges, with, in the first line, a purely technical hurdle to overcome: tracking them down over the network.

Untraceable?

The Hollywood movie *Untraceable* has its imperfections, but if anything, it is crystal clear on one thing (besides the fact that it is always raining in Portland, OR): the actual IP address of a cybercriminal is extremely difficult to locate. The following will be anything but a big revelation for our technical-oriented readers, thus they may hop over the next paragraph.

To put it simply, when a stateful Internet connection (a.k.a. a TCP connection) is established between Alice and Bob, Alice sees Bob's IP address. Thus if Bob does bad things to Alice via this connection, his IP address can be reported. Now, if Cain connects to Bob, and from there, connects to Alice with bad intentions, Alice will still only see Bob's IP address. In other words, Cain has masked his IP address with Bob's. The component which allows Cain to use Bob as a relay is called a proxy (there are various types of proxies, though in cybercriminal schemes socks4 and socks5 proxies are mostly used). Such a component, of course, may have been installed on Bob's computer without his knowledge, by Cain. Or by Daniel, and Cain just rented or purchased access to it. As a matter of fact, most trojans and bots embed a proxy, and in any case, have the capability of loading one after prime infection. Given the prevalence of bot-infected machines (a.k.a. zombie computers), that makes a virtually endless resource of proxies for cybercriminals, all sitting on machines of innocent, unaware users. This is something cybercriminals understand perfectly and exploit ruthlessly, sometimes on a large scale.

Fast-flux networks are one example of such a large scale use of zombie machines as proxies. Fast-flux is a technology used by cybercriminals to make a malicious website resistant, both to firewall website filtering (when it is IP-address-based) and to trace and 'take down' attempts by law enforcement and malware fighters. In its simplest form (called 'single-flux'), the IP address of a fast-flux-hosted website changes constantly. This is so because the name of the website (e.g. www.malicious.com) points to the IP address of a random zombie machine that changes every couple of minutes. Thus each time a user attempts to connect to www.malicious.com, it is pointed to an arbitrary zombie machine, which relays the

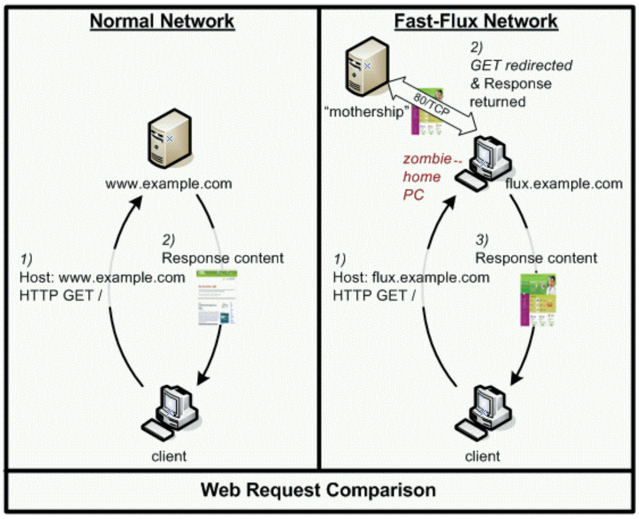

Figure 1: Single-flux hosting. Picture courtesy of The Honeynet Project (honeynet.org).

connection towards the actual (and hidden) location of the malicious content (a.k.a. the 'mothership'). Figure 1 gives a visual feeling of the technology described above.

Now, in the scenario involving Alice, Bob and Cain above, one may object that tracing the connection from Alice to Bob, then from Bob to Cain could be possible, either by obtaining Bob's connection logs (from him or his ISP), or by 'live' spying on Bob one way or another (Bob could be a sleeper agent of law enforcement). Unfortunately, proxies can be chained, and with the emergence of public tools to achieve 'onion routing', it is possible for a cybercriminal to go through a dozen relays before reaching their target. Onion routing, popularized by the surge of Tor, is an extremely powerful means of anonymization over the Internet. In an onion routing scheme, information transmitted between two relay nodes (including the client and the first relay) is encrypted, and from origin to destination each relay only has knowledge of the previous and the next relay. In other words, when the nodes relay information, they don't know what it is, where it is coming from, and where it is going to (see Figures 2 and 3, courtesy of the Tor Project at torproject.org).

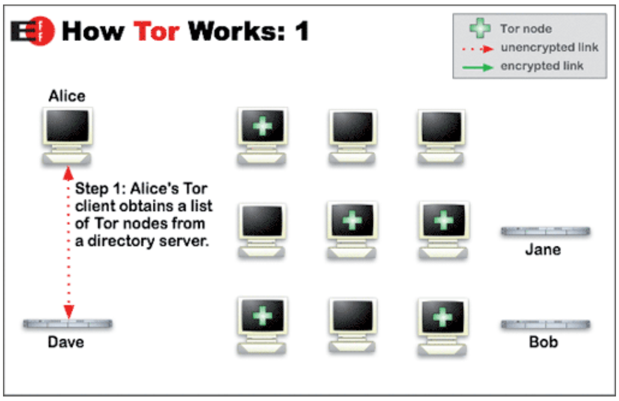
How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob

Figure 2: Grab an onion.

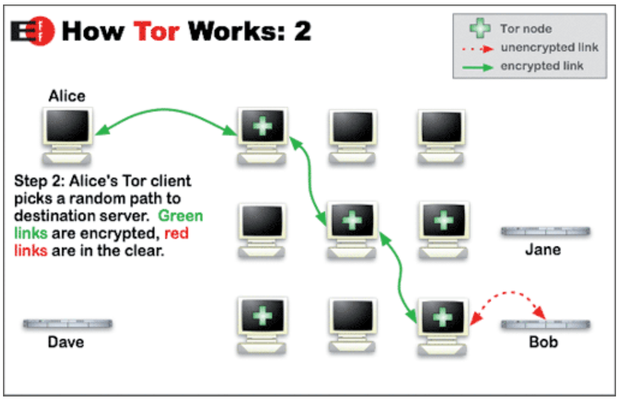
How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Figure 3: Peel it.

Ironically (or not), the Tor project was originally sponsored by the US Navy; the goal was to allow people in potentially hostile territories to use the Internet with the guarantee that local eavesdroppers would be unable to see what sites they were connecting to (e.g. the Navy mail server).

It must be noted that we have no intention of naming Tor as a cybercriminal tool: Tor's developers point out that the goal is to make strong anonymity available to average users easily, which was previously reserved for cybercriminals (through the use of botnets, for instance) – and they are probably right. Simply, the popularity of Tor is a sign that powerful anonymizing technologies on the Internet are commonly available, and make backtracking the network trace of cybercriminals a tremendously difficult task.

This, in large parts, is a direct consequence of the architecture of the Internet and its core protocols. These were devised in the late 1960s, with the intention of creating a robust and survivable network between US military bases (thereby justifying the choice of a packet-switching technology, rather than circuit-switching), likely to keep functioning in case of nuclear attacks. Certainly, neither the global expansion of what today has become the Internet, nor all the issues that would come with it were foreseen. Ensuring indisputable traceability of communications on the Internet would therefore most certainly require it to be rebuilt from scratch; this is not doable and arguably not desirable, for its structure, while hampering some aspects of the struggle against cybercrime, guarantees freedom of speech.

Internet content control

Indeed, events occurring at the time of writing show that countries with a strong tradition in Internet censorship are failing spectacularly in controlling information. In Iran [11], for example, in the stir of the June 2009 events following the presidential elections, all foreign media were banned. Nonetheless, images and reports of the protests kept flooding the Internet [12].

The People's Republic of China, a renowned champion of Internet censorship [13], has such a hard time preventing people from bypassing its 'Golden Shield Project' (a national Internet control and censorship project [14], sometimes referred to as 'The Great Firewall of China'), that it has announced a new directive: as of 1 July 2009, all personal computers sold in mainland China, including those imported from abroad, must feature the *Green Dam* software (either installed/pre-installed, or on CDs). *Green Dam* restricts access to a secret list of sites, and monitors users' activity [15].

Such a move highlights the fact that in much the same way as it is difficult to trace connections, it is extremely challenging to prevent access to information online in a definitive way. While this is bliss for freedom of speech, it has symmetric consequences in the struggle against cybercrime: for instance, access to terrorist-oriented websites (bomb manuals, boot camps, recruitment, communication hubs...) and child-pornography hubs cannot be blocked for tech-savvy users. A non-exhaustive list of tools and processes that may be used by the latter to bypass content filtering include:

- Using a (private or public) proxy
- Using a Virtual Private Network and browsing from there
- Onion routing (see Tor above)
- Using open proxy programs such as *Freegate* or *Ultrasurf*

Computer forensics, encryption and plausible deniability

Another common tendency among reasonably tech-savvy users is the use of cryptography to mask sensible data. Assuming that a cybercriminal has been located (not necessarily by following his network tracks), convicting him will in many cases require collection of evidence from his computer systems. It is the role of computer forensics experts to do so, and their task can prove to be tremendously complicated if the evidence is encrypted.

Many pieces of software allow for file or hard-drive partition ciphering, using encryption methods that cannot currently be broken. But even worse for investigators, some of them, like the very popular TrueCrypt, implement deniable encryption: the same ciphered text, C, can be decrypted with two different keys, one (K1) resulting in a benign clear text M1, and the other (K2) in the sensible clear text M2. Of course, examination of C cannot reveal how many clear texts were encrypted. This empowers users with the option of plausible deniability: if compelled to give out its encryption key, a suspect can provide K1, leading to innocuous clear text data. And the very existence of K2 (and therefore, M2) cannot be proven.

Robust botnets

Aside from convicting cybercriminals, another strategy to limit the impact of cybercrime is to address its epicentre: botnets. As stated above, a significant part of cybercrime revolves around these networks of zombie computers, enslaved to the 'botmaster'. A botmaster can indeed use bots to send spam, propagate new worms, plant trojans, conduct deadly distributed-denial-of-service (DDoS) attacks, perform click fraud, launder money (see the VoIP fraud described above), proxy connections, implement a fast-flux network... The list is virtually endless. Literature on this topic is abundant, and renders in-depth details on botnets far beyond the scope of this paper.

It is relevant to point out, however, that while bots used to receive commands from their master via a single channel (e.g. an IRC chat room, a website or an instant messaging account), modern botnets tend to implement tremendously more robust structures, hence eliminating issue of there being a single point of failure. Indeed, shutting down a traditional botnet would be as simple as shutting down its unique control channel, by the means of public or law enforcement pressure over the company enabling it (knowingly or not), such as a web-hosting company, a name registrar, an IM provider, etc. This is not possible with robust botnets. An example of such is the infamous 'Storm worm' botnet. Functioning as a peer-to-peer network (through the implementation of a Distributed Hash Table system, similar to *eMule* and *BitTorrent* distributed trackers), 'Storm' has no single command and control channel that can be shut down. First identified in January 2007, studies report that as of March 2008, the Storm botnet was responsible for nearly 20% of the world's spam [16]. The gang controlling it has not been identified at the time of writing, and various botnets used peer to peer in the wake of Storm's success (among which was Conficker [17]).

JURIDICAL CHALLENGES AND BEYOND

Its utterly transnational nature is perhaps the most widely accepted characteristic of cybercrime. While opinions on its very definition may vary, everybody agrees on the fact that cybercrime is transnational, and every single white paper on cybercrime, in its introduction (or/and conclusion), highlights the legal challenges implied by cybercrime's 'borderlessness' (even when not elaborating on it in the paper itself). Less known is the fact that several governments have acknowledged it since at least 1997, and that some progress has been made on the long road to solve those legal challenges at an international level. Papers and books providing in-depth analysis from a purely juridical point of view do exist, therefore this part will give a straightforward overview of the situation in terms of national and international legal frameworks, then will attempt to go beyond the sole juridical frame, notably by expressing some points felt by malware fighters.

The theoretical problem: solved centuries ago?

The transnational nature of cybercrime raises an issue because legal and repressive systems in the world are currently based on sovereign jurisdictions with borders. Frequently, in a cybercrime scenario, the attacker sits in country A, and without moving an inch, engages in cybercriminal action targeting a victim in country B. The theoretical problem is therefore: knowing the crime occurs in country B, while the criminal is in country A, how can the criminal be prosecuted and under which jurisdiction?

A very radical and direct way to solve the question would be giving an entity supra-national powers on cybercrime matters, thereby abolishing borders and creating a single, global, cyber-jurisdiction. This seems highly unrealistic (and probably undesirable, but since it is often heard, it is worth discussing here), as it would require countries to give up a significant part of their sovereignty. As of now, it is indeed difficult to imagine the USA letting a cyber-police force possibly including Chinese, Russian, Iranian and North-Korean agents seize computer data on American soil for the purpose of prosecuting an American citizen. And vice versa.

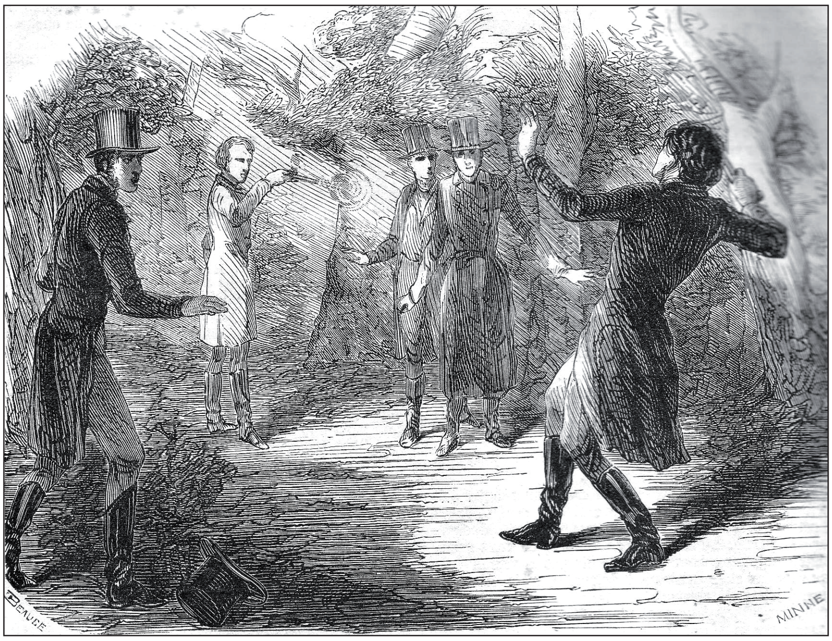

Figure 4: 'Duel au Pistolet' (1857).

That being said, Italian lawyer Andrea Monti once pointed out in a discussion with the author that as a matter of fact, the problem defined above had been studied in law and solved for over 200 years. The paradigm of it was then: a man on the Italian side of the Italo-Swiss border fires with a gun at a man on the Swiss side. The criminal is in Italy, while the victim is in Switzerland. Solving the case involves multilateral treaties, establishing which jurisdiction to apply and defining the ensuing legal procedure. The issues raised by transnational crime are therefore (at least theoretically) juridically soluble without the need of supra-national organizations.

The slow arm of justice

An astute reader would, however, note that the characteristics of cybercrime are somewhat different from those of nineteenth century gunfights: instant offences of a new kind can be perpetrated at very long range, crossing not one but several borders, leaving no material trace, and shielded by routing 'relays'. Specific provisions thus need to be made in order to achieve the following through the boundaries of juridical and administrative borders:

- Investigation of cybercrimes
- Prosecution of cybercriminals
- Execution of sentence for convicted cybercriminals

All the points above require an adapted local legislation to outlaw cyber-attacks (in both the attacker's and the victim's countries) and efficient international cooperation procedures. Contrary to popular belief, this has been acknowledged and understood for a long time, with the Organization for Economic Co-operation and Development (OECD) first studying the legal issues raised by cybercrime in 1983. Recommendations were made in an attempt to harmonize qualification of the same cybercrimes amongst the varied national legal systems [18]. Later, in 1997, the G8 instigated the creation of a Contact Points Network, meant to become the reference directory for international cooperation actions on cybercrime. The goal was really to provide a phonebook that all parties could use to reach a competent point of contact in another jurisdiction, for immediate assistance.

But the most complete attempt to address the juridical issue globally is, at the time of writing, November 2001's Convention on Cybercrime of the Council of Europe.

Current tools and frameworks: the Convention on Cybercrime of the Council of Europe

The Convention on Cybercrime is an international treaty initially drafted by the Council of Europe (CoE), with the addition of the USA, Canada and Japan; however signature and ratification are by no means limited to member states of the CoE, and are open to all countries.

It aims at providing the basis of an effective legal framework for fighting cybercrime, through:

- Harmonization of cybercriminal offences qualification amongst the legal systems of member states.
- Provision for laws empowering law enforcement or/and prosecutors with cybercrime investigation capabilities in each member state.
- Provisions for laws and procedures enabling international cooperation amongst member states during investigation and prosecution of transborder cybercrimes.

Countries ratifying it must implement the provisions made by the Convention within their local legal system and designate points of contact for the cooperation procedures, so as to initiate them expediently upon request from another member state.

The full text of the convention [19] is interesting, and fairly readable. Let us nonetheless have a quick overview of the main provisions it defines:

- Harmonization of cybercriminal offences in domestic legislation is taken care of by Art. 2 to 11. They are: illegal access, illegal interception (ex: sniffing), data interference (i.e. alteration or destruction of data), system interference (ex: DoS or DDoS attacks), misuse of devices (production, distribution and use of hacking tools – explicitly does not apply to security auditing tools, the notion of 'intent' prevailing), computer-related forgery, computer-related fraud, child pornography (producing, distributing, procuring, possessing), infringements of copyright 'on a commercial scale', and aiding/abetting thereof.
- Empowering domestic authorities with cybercrime investigative abilities is addressed in Art. 16 to 21. They concern: expedited preservation of stored computer data (seemingly meant to preserve volatile data such as connection logs at Internet Service Providers – as a side note, the latter are not compelled to store traffic data under this directive, but simply to preserve data that is already stored but would rapidly be deleted otherwise), expedited partial disclosure of traffic data (means ISPs have to immediately disclose the fact that the data to be preserved shows that connection is routed to or from another provider – obviously a directive to address proxy chaining...), production order (to compel ISPs to give out subscriber information upon request from authorities, most likely based on an IP address), search and seizure of stored computer data, real-time collection of traffic data ('traffic data' has to be understood as connection logs), interception of content data (sniffing at ISP level, provided the latter has the technical capacities to).
- Enabling international cooperation during investigation and prosecution of transnational cybercrime is taken care of by Art. 23 to 34. Essentially, they seek to allow authorities of any member state to quickly and efficiently request another member state to make use of its investigative abilities as defined above (Art. 16 to 21) for the purpose of a transborder investigation or prosecution. It must be noted that 'dual criminality' (i.e. action considered as a crime in both countries) shall not be required for a request of expedited preservation of stored computer data, while it may be required for accessing preserved data (pertaining to the aforementioned preservation or not).
- Designation of a permanent point of contact for the '24/7 Network' is ruled by Art. 35

Safeguards are mentioned, so as not to endanger civil liberties (Art. 15 – although the actual implementation of such is, like the rest of the provisions, left to each party), and to preserve a form of sovereignty. International cooperation, for instance, may be refused if:

a 'the request concerns an offence which the requested party considers a political offence or an offence connected with a political offence,' or b 'the requested party considers that execution of the request is likely to prejudice its sovereignty, security, public order or other essential interests.' (Art. 29, 30, 31)

Some exceptions are also possible due to 'established principles of [the party] domestic legal system', so that the constitutional principles of potential member states are not put at stake. Overall the text appears to be well balanced and addresses the relevant issues. Notably, the cybercriminal offences it defines are sufficiently abstract to still be relevant in 2009, albeit the convention was drafted in 2001.

In addition to the Convention itself, Myriam Quemener, general attorney substitute at the Court of Versailles and author of Cybercriminalité (2007), cites an important tool: the European Arrest Warrant (EAW). Introduced by the European law of 9 March 2004, it empowers countries within the EU to obtain the extradition of criminals without the need for dual criminality (i.e. the motive for the prosecution does not need to be a crime in the criminal's country of residence) for a block of 32 'serious' infractions. Cybercrime is one of those. Mrs Quemener adds that the EAW is the only domain of European Laws where cybercrime is specifically mentioned [20].

Issues and challenges

The Convention is therefore a pertinent legal and operational framework; moreover backed up by a wide international coalition (the Council of Europe and the USA, Japan, and Canada) and open to everyone, it is therefore likely to be the 'way to go' in the struggle against transnational cybercrime. However, the current prevalence of cybercrime, the outstanding profitability of its business models [4], and the tremendously low risks they incur [21] indicate that the Convention still has a long way to go, and that way is paved with obstacles, challenges and issues. A brief overview of these follows:

- **Current state of implementation**: at the time of writing, 46 countries have signed the Convention, of which 26 countries have ratified it and effectively put it into force (though half of them with reservations [22]). All the members of the Council of Europe (which, as a side note, spans way beyond the European Union) have signed it, with the exception of Andorra, San Marino, Monaco, Russia and Turkey. Countries outside the Council of Europe that have signed it are Canada, Japan, South Africa and the USA. Of these, only the USA has ratified it at the time of writing. Due to the number of provisions that have to be implemented in the domestic legal systems of signing parties, the ratification process is long, but with two new countries ratifying in 2008 (Italy and Slovakia) and three in the first half of 2009 (Germany, Moldavia and Serbia), momentum does exist. Gaining more signing parties may actually be the biggest challenge.
- **Scarce use of implemented tools**: it seems that up to now, countries that have ratified the Convention and implemented its provisions have rather rarely resorted to the tools it provides. For instance, a country like Romania, although at the edge of cybercrime fighting with about 900 cases processed per year by a specific prosecution service and all provisions fully implemented, only receives a dozen international requests per year via its 24/7 network contact point (as defined by Art. 35). Estonia has received none to this day and France from 10 to 20 per year [18]. As a matter of fact, over the 26 countries that ratified the Convention, only four of them have designated a cybercrime-specific unit (whether a police unit or a Dept of Justice service) as the 24/7 network point of contact of Art. 35 (France, Romania, USA, Norway). Furthermore, three of them have no designated a point of contact at all (Armenia, Bosnia, Ukraine).
- **Operational issues**: in line with the previous point, one cannot but observe that in the ranks of private malware fighters, a form of operational inefficiency from the authorities is also felt. Paul Ferguson, Senior Threat Researcher at *Trend Micro* and member of the Anti-Phishing Working Group, declares on the subject of the take-down operations of malicious websites: 'My experience is that US authorities are completely unable to deal with the situation, and the fact that I (along with other e-crime investigators) pass along information to them, and work with them on a daily basis, is not very encouraging' [23]. When suggested that the authorities may prefer to leave a site 'alive' to spy on it and trace the cybercriminals behind it, he continues: 'Perhaps. But letting people continue to be victimized for, say, three years is way too long for an investigation'. As for Mr X, who investigates the case of massive money-laundering via botnet-powered VoIP calls, he reckons 'we know of eight independent government agencies investigating this fraud space. Nobody is working together' [24]. On a more general note, he continues: 'I know a German law enforcement agency that always complains. They get requests from the US feds that demand responses and action in days/hours. But if in turn they send something out, it takes months.' Finally, he reveals that the often cited public/private cooperation has a long way to go before reaching a state of panacea when it comes to fighting cybercrime: 'when we talk to law enforcement things get messy if you know stuff they don't or give them direction. For some reason they also think they are smarter and/or better informed.'
- **Domestic hurdles**: provisions made by the Convention tend to leave a certain degree of liberty in the implementation thereof, probably in order to avoid head-on clashes with the laws and constitutional principles of potential signing parties. Indeed, articles include locutions such as 'provided for by its domestic law' (Art. 16 and 33), 'to be determined by domestic law' (Art. 21), 'in accordance with its domestic law' (Art. 22 and 29), 'within the limits of its domestic law' (Art. 26), 'to the extent permitted under their domestic laws' (Art. 34) and 'if permitted by its domestic law' (Art. 35). In effect, this affects actual data accessibility, throughout borders and within a jurisdiction alike.
- **Low report rate of offences**: as a matter of course, the fact that cybercriminal offences are still scarcely reported does not foster their investigation. The 2008 Computer Crime and Security survey of the Computer Security Institute reports that when they were victims of cybercriminal offences, only 27% of organizations (both from the private and public sector) reported them to a law enforcement agency. A statement made by John Kane, manager of the IC3 (the US platform for reporting cybercriminal offences online) about the number of

reports processed by the IC3 in 2008 seems to indicate that the situation may not be any better when it comes to individual users: 'It's our belief that these numbers, both the complaints filed and the dollars, represent just a small tip of the iceberg' [25]. He estimates that 'only about 15% of Internet fraud cases ever get reported'.

- **Multiple redundant points of contact**: in an effort to foster cooperation of law enforcement agencies around the world against cybercrime, Interpol created a contact point network, currently featuring 111 'National Central Reference Point' (NCRP). This adds up to the G8 24/7 network evoked above, and the Convention's own 'Art. 35' 24/7 network. To further complicate things, some contact points are the same for two of the three networks, but not always [18]. The efficiency of 24/7 networking may be dissolved by the multiplication of networks, much like the multiplication of standards is deleterious for the public acceptance of a new technology.

Beyond this (non exhaustive) list of pitfalls and challenges, it is remarkable that the Convention mainly cites provisions aimed at tracking cybercriminals by following their network trace. Yet, we have seen in the 'Technical challenges' section above that this can prove to be extremely difficult. This apparent paradox may stem from the fact that back when the Convention was drafted, in 2001, the face of cybercrime and the technical state of the art were different. Indeed, the malware landscape only became fully monetized in 2004, with the massive rise of botnets running on infected *Windows* personal computers. Tor, the software that made onion routing popular, was presented at the 13th USENIX Security Symposium, in 2004. That was also the year when deniable encryption became widely available, with the release of TrueCrypt. Let us be clear: we have no intention here of questioning the utility of the Convention – expedient preservation of data, search and seizure of stored data, real-time collection and interception of data can very much play a critical role in a cybercrime prosecution case. As a matter of fact, due to its very nature, the Convention could hardly have considered any other aspects than the purely computer- and network-related ones. However, it should not mask the fact that now that a significant part of cybercrime is solely aimed at making profit, following the financial trace of cybercriminals can turn out to be as relevant, and perhaps easier, than following their network trace.

Cybercrime and money laundering: one agency to rule them all?

The latter point is all the more valuable considering that cybercrime and money laundering have much in common today. Let us consider the following quote:

> 'In the absence of real authority in global governance, some form of anomie reigns over a part of international activities. It was then inevitable that organized crime slipped through the interstices of a legal order built on the principle of territoriality. The new transnational nature of criminal activity gives it a certain impunity because anti-crime government agencies are formed according to national schemas, and international cooperation is still very difficult. The result is great prosperity of transnational criminal organizations.' [26]

This description would fit remarkably well with cybercrime, yet it was written about money laundering. From a legal and operational point of view, the two therefore share many common characteristics. As a matter of fact, they often interleave. For instance, online casinos operated by offshore shell companies are frequently cited in literature on money laundering [26], as an effective means of transforming dirty financial assets into legit money. The botnet-powered VoIP laundering scheme described by Mr X above is another very recent example. The number of money laundering scenarios involving botnets is actually virtually endless. Some are more or less documented, such as click-fraud laundering [25], where an organization sets up a website with advertising banners and pays botnet owners so they generate automated clicks on the banners from the bots (a.k.a. zombie computers). The organization thus cashes in 'clean' money from advertisers through respected 'pay-per-click' syndication programs, while the botnet herders are paid with dirty assets.

Another worrying vector of money laundering may be Massive Multiplayer Online Role Playing Games (MMORPG), where the purchase and sale of in-game assets with 'real' money (outside of the game) is a common practice; changing in-game money for 'real' money is also typically possible.

Finally, the probable arrival of botnets on mobile platforms (i.e. Smartphones) will certainly sharpen the issue, as those have all the characteristics of a personal computer, plus an integrated billing system (calls or SMS messages to premium numbers).

The big picture

The common point of all the schemes described above is that transactions are hardly traceable, especially when the model involves making a large amount of micro-transactions. This is a typical challenge law enforcement agencies face when struggling with 'traditional' money laundering, and known as 'smurfing' (note: nothing to do with the smurf computer attack, which is a denial-of-service attack). Indeed, smurfing consists of laundering a large amount of money through multiple fractioned deposits, possibly done by many different people (acting as money mules). Each deposit is inferior to the amount above which banks are compelled to fill in a transaction report, which authorities rely on to detect and investigate laundering activity ($10,000 in the USA, for instance, under the Bank Secrecy Act).

The structure of the Internet and the multiplication of online payment systems are such that cyberspace is particularly well adapted to smurfing. This hurdle has been documented to be perceived by the authorities in cybercrime prosecution cases. For instance, the Council of Europe's discussion paper 'The effectiveness of international cooperation against cybercrime: examples of good practice' [18] mentions that 'In some countries, for example, some kinds of offences are prosecuted only if there is a certain amount of damage. If the damage is lower than that, cooperation is refused.' It also mentions that this was referred to as 'difficulties with international requests' by the French and Romanian authorities.

Therefore, the biggest challenge in fighting cybercrime may actually be to 'see the big picture' at an operational and financial level, rather than investigate individual cases which are likely to be abandoned either due to the smurfing effect, or to the technical difficulties in backtracking and convicting cybercriminals via the network (or both). This may be achieved through long term infiltration operations, correlation of data stemming from all the reported individual cases worldwide, and active involvement of anti-money-laundering agencies and organizations.

INTER(NET)POL

Now, correlation of international criminal data thanks to a global database is exactly the type of service Interpol has always been providing to law enforcement agencies; historically, that is precisely its main raison d'être (rather than being an actual investigation force – let alone a supra-national one – as taught by popular belief). Interpol's website gives scarce (and somewhat outdated) information about cybercrime and its involvement in tracking it, but it does have a 'Financial and High Tech Crime Sub-Directorate'. Officials of the aforementioned sub-directorate did show some interest in the author's questions, but at the time of writing, their answers are still pending. Whether or not Interpol's databases are adapted and used in the fight against transnational organized cybercrime is therefore speculative. Either way, increasing the level of involvement of Interpol in the global fight against cybercrime may be a path worth considering. Not only would it provide a well-proven database-tool to help 'see the big picture' and highlight the bridges between cybercrime and money laundering, but it also has the advantage of being a well established inter-governmental organization, comprising 187 member countries. Only the United Nations has more members.

Beyond the juridical framework: geopolitical and socio-economic considerations

Another important characteristic shared between cybercrime and traditional money laundering is that both involve numerous intermediate actors. As developed in [4], the people who create cybercriminal tools (trojans, viruses, worms, exploit packs, phishing kits, etc.) are not the people who enable the use of them on a large scale ('bullet proof' hosting companies, rogue ISPs, bad registrars etc.), who, in turn, are not the ones who use them (after purchase); and of course those who use them are generally not the ones who convert the gathered fruits (banking credentials, credit card numbers, auction site credentials, MMORPG credentials, etc.) into actual money. There are various reasons for that, among which is the fact that each step involves a different set of skills and a different degree of risk. But the point is, upon each step in the chain of intermediaries, monetary added value is created, which indirectly profits the local economy.

In the domain of money laundering, literature cites this 'chain of richness creation' as a phenomenon that undermines the will of local political powers to repress the issue, especially in emerging countries [9]. Developed and emerging countries therefore have a different perception of the problem from one another. This raises an issue because the instruments to address it are adapted to countries with a structured state and a developed justice system, where the problem is viewed under a purely juridical aspect, not under a sociological one (therefore making it a law problem rather than a governance problem). And international treaties and conventions are based on the 'developed countries' vision of the problem. The limits of this vision are rapidly highlighted in emerging countries. On that theme, in *Finance Criminelle* Marie-Christine Dupuis-Danon notes that 'for the sociologist and the criminologist alike, it is not because there is a law against corruption that corruption disappears' [9].

The same reasoning could be applied to cybercrime. Joep Gommers, Director of Operations Europe at *iSight Partners*, corroborates this view: 'There will always be places of lesser law enforcement pressure, and we see many big enabling actors (rogue hosting providers, money movers) physically move around in the world to those places. Unless we plan on fighting global poverty, war and the like – we won't ever eradicate that problem completely'.

In other words, the thought that once all the countries have ratified the Convention on Cybercrime (if it ever happens), there will be no 'cyber-havens' any more is an illusion. To be efficient, ratification and implementation must be accompanied by a strong political and governance will. And since the presence of cybercrime enablers indirectly profits the local economy (much like with money laundering, as described above), it is mainly external factors that can give rise to this political evolution, and catalyse it.

One such factor, largely used by the Financial Action Task Force on Money Laundering (a.k.a. GAFI, by its French acronym) in the domain of money laundering, is pressure from the international community: in 2000 and 2001, the GAFI issued its famous list of 'Non-Cooperative Countries or Territories' (commonly referred to as the GAFI Blacklist) featuring 23 countries. It has proved to be effective, since at the time of writing all but one of the 23 original blacklisted countries have implemented legal and institutional changes (such as creating Financial Intelligence Units) in order to be de-listed [27]. As a consequence, 21 countries have been cleared off the blacklist, and only eight countries have been added since the initial lists [28]. At some point, it could be a path worth exploring in the domain of cybercrime fighting, perhaps with support from the GAFI, which also has an interest in addressing the cybercrime issue due to its ties with money laundering and financing of terrorism.

On a similar note, the rather peculiar case of Romania may be cited as an example. With a nominal GDP of $7,773 per capita, Romania is listed by the IMF as an emerging country [29]. Yet, as mentioned earlier, with nearly 900 cybercrime cases prosecuted per year, a very extensive legal framework, a cybercrime-specific police unit and a cybercrime-specific prosecution service attached to the High Court of Cassation and Justice, Romania seems to be a leading party in the fight against cybercrime. Romania became an 'acceding' country to the European Union in 2004, which is the year it ratified the Convention on Cybercrime. It became an actual member of the EU in 2007. Numerous reforms of the Romanian society stemmed from the will to gain access to the EU [30], and it is not senseless to speculate that addressing the cybercrime issue was one of those, and that amongst other considerations, Romanian officials felt that gaining access to the EU would yield a greater benefit for the local economy than a flourishing cybercriminal scene.

Beyond such international incentives, the idea may be translated at the individual level. Mr Gommers evoked the idea of fighting cybercrime by enabling more profitable legal alternatives for its actors: 'If the business model of operating in the "black" space online is easier then in the "white space", the first will win. However, if we make earning money legitimately easier and making money fraudulently more difficult, e-crime will go down. So instead of fighting incidents, work together with intelligence, industry, communities to attack business models – provide alternatives

– target important enablers of business models and not the actors behind it. There are many actors, but a limited number of business models.'

ETHICAL CHALLENGES

The complex technical and juridical issues arising in the struggle against cybercrime sometimes seem insurmountable. So much so that authorities and governments may legitimately feel helpless, and as a reaction, may be tempted to consider radical directives, in the process endangering human rights in general, and individual liberties in particular. This is a real danger, and must by no means be underestimated; especially in a high-tech domain, the intricacies of which are opaque to the masses.

From protection to censorship

Since 2006, Reporters without Borders has been maintaining a list of countries it calls 'enemies of the Internet' [31] (at the time of writing: Burma, China, Cuba, Egypt, Iran, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan and Vietnam) based on their use of censorship and Internet users' repression. As a matter of course, in those countries, censorship is in large parts used as a means of policing and controlling political opinion, but not only that: pornography and any other theme that may be considered licentious or threatening to civil order is subject to censorship. This is perhaps an indicator that the border between protecting moral values and exercising oppressive censorship and mind control is thinner than one may think.

The fragility of this border must be considered when 'democratic' countries engage in nationwide website filtering, with the backing of consensual causes, such as blocking access to child pornography online. Although no one is willing to defend paedophiles, an ethical issue is to be considered here: is it the role of a country's government to tell its residents what is right or wrong to watch and access? In many European countries (including France and Germany), freedom of speech (thus, correspondingly, freedom of access) is not limitless. Notably, it stops where negationism and incitation to racial hatred start. But at least it is a judge who decides when the boundary is crossed, not a preventive filtering system elaborated secretly by the executive power (as has been the case for child pornography blacklists). To put it simply, it is not the same to be a public apologist for Hitler's *Mein Kampf*, as it is to consult it for the purpose of writing a master's thesis on the rise of fascism in the early 20th century. Website filtering technology, of course, does not even allow for this simple distinction.

Beyond that, in effect, no matter what the original intention was, all secret censorship systems have given rise to anti-democratic drifts. Without invoking examples rooted in the darkest hours of European history, a simple observation of the course of things in countries which implemented anti-child-pornography filters is in itself edifying:

- In December 2008, *Wikileaks*, a site for the freedom of the press and information, published the secret list of sites censored by the Department of Information and Communication Technologies of Thailand. Whereas the system was originally built to prevent access to child pornography, the 1,203 sites on the list are all labelled in the 'lèse-majesté' category, i.e. criticizing the royal family. Seemingly, the lèse-majesté label covers a great deal of topics, since although some sites did criticize King Bhumibhol, some pages had nothing to do with actual lèse-majesté: *Wikipedia* pages, *YouTube* videos, discussion forums, blogs of social critics... [32]
- In March 2009, the secret list of sites censored by the ACMA (Australian Communications Authority and the Media) was also leaked. This time, 2,395 sites were listed. And half of them have nothing do with child pornography. There are 'traditional' pornographic sites, but also, curiously, poker sites, *YouTube* videos, *Wikipedia* pages, gay sites, sites on euthanasia, sites of 'marginal' religions (e.g. some Satanist sites), anti-abortion sites (containing images of aborted foetuses) and finally, the site of a dental practice in the province of Queensland. In short, an inspiring mix of themes which may have seemed morally dangerous to the eyes of some censor, and of gross errors. The list of the ACMA must serve as the basis for the next screening system put in place at the Australian Internet Service Providers. At the time of writing, all Australian sites bearing a hyperlink to a site from the list incur a fine of $11,000 per day. [33]
- In January 2009, Finland's secret list was published on *Wikileaks*. Again, many sites were not pornography, of course, but more worryingly, it contained an anti-censorship site, created by an opponent of the law [34].

The list goes on, proving that the unaccountability of secret censorship systems leads to nothing very democratic. As for the impact on the prevalence of child-pornography websites and the actual abuse of children tied to it, it remains a mystery – unsurprisingly, perhaps: no one besides the actual paedophiles with proxies can access them, so no one is going to inquire about that, right?

Ironically, in the press kit of the 'Loppsi 2' project of law distributed by the French government in May 2009, establishment of a nationwide website filtering system is justified by a line stating 'as numerous other democracies have already done'... There is therefore a sensible gearing up in censorship, with countries backing each other up, while at the same time shaking the scarecrow figure of the paedophiles – thereby cutting down any possibility of public debate (intentionally or not). At this point, it is worth recalling a quote by the famous American journalist and writer H.L. Mencken:

> 'The trouble with fighting for human freedom is that one spends most of one's time defending scoundrels. For it is against scoundrels that oppressive laws are first aimed, and oppression must be stopped at the beginning if it is to be stopped at all.'

He may have found a couple of scoundrels to defend here. It is certainly important to keep this in mind when making laws on cybercrime.

Trojan-factory.gov

Another scary figure is the terrorist one. So much so that various governments have attempted to pass laws and bills to empower police officers with the ability of planting Trojan horses on suspects' computer systems; the goal is to spy on data (including screen display, keystrokes, and possibly microphone and webcam data) in a 'live' fashion. The process is claimed to be limited to particular cases involving terrorism.

The 'Magic Lantern' Trojan horse project, born in the wake of the 9/11 events in the USA is one such case. Public knowledge suggests that it was abandoned – although the FBI uses a 'light' monitoring tool called CIPAV [35]. Back in 2007, the German federal police came up with their own 'Bundestrojaner' (federal trojan) project, but faced mitigation by the Federal Constitutional Court: the latter stated in February 2008 that trojanizing a suspect's computer was 'constitutionally permissible only if actual evidence of a concrete danger' existed, and that it was to be conducted only under judicial authorization (i.e. requiring a warrant) [36]. The French government learnt the lesson, and included that judge-control factor in their own law project [37] (pending at the time of writing) from the beginning. Austria and Switzerland are said to have similar projects in the pipeline [38].

Given the tremendously intrusive nature of Trojan horses, the ethical issue raised here clearly deals with privacy, the protection of which is the main barrier against the risks of global surveillance 'à la 1984'. In this precise case, it must be noted that at first sight, within the frame of exceptional measures (such as terrorist attack risks), it is not particularly shocking that all possible means of spying be utilized. Indeed, it is already the case with 'traditional' surveillance involving wire-tapping, microphone bugs and hidden cameras. However, let us point out that a few differences exist, and that they may be worth considering:

- **No scale effect**: first of all, unlike traditional surveillance gear, Trojan horses are immaterial, mere pieces of software. Hence they are not subject to costs of scale, and can be replicated indefinitely. Installing them on the computers of a large number of citizens would therefore involve very low costs, and acceptable effort, since it can easily be automated – should the installation be done via system flaws exploitation, emails, or man-in-the-middle attacks via a component at the ISP level that would automatically booby-trap all user downloads with the trojan (which, if I understood correctly, was a strategy considered by the German federal police, albeit not on a wide scale, of course [38]). In theory, judiciary control over the use of Trojan horses should prevent anything of this flavour from happening; yet, it is worth pointing out that such a risk of drift towards a global surveillance operation does not exist with traditional surveillance gear, for practical reasons. And it is a major difference.
- **Increased risk of backfire**: very few people have microphone-bugs and wiretap detection gear at home, whereas a lot of them have anti-virus software installed. The goal of anti-virus software precisely consisting of spotting Trojan horses – and the AV industry being very hostile to the idea of cooperating by 'whitelisting' policeware [39] – one may reasonably think a presumed terrorist running AV gear (especially those featuring behavioural malware analysis) could very well be alerted to the presence of the police trojan. What might happen next is purely conjectural, but technically, it would be possible (and not extremely difficult, with virtual machine technology, for instance) to transmit fake information, possibly accusing an innocent third party.
- **Ease of evidence tampering**: unfortunately, the planting by counter-intelligence or law enforcement of physical, material evidence of guilt in the house of innocent citizens during surveillance operations may have happened in the past. But doing so with immaterial evidence remotely, via the trojanized computer of a non tech-savvy suspect (before his computer is seized and examined by the prosecution parties) is certainly easier, quicker, cheaper and safer. In a nutshell: it's one click away.
- **Spread of trojan development skills**: Trojan horses are a core technology of cybercriminal activity. Development of the 'know-how' in trojan conception, boosted by governmental tenders (and funded by governments), is certainly not good news for malware fighters. It gives a strong signal that 'trojans can be good', which may serve as a pretext for trojan-programming courses to flourish (online or not). And possibly for companies to specialize in that field.
- **Lowers the suspect's security**: even the finest pieces of software contain bugs, flaws and vulnerabilities. Whether attackers discover them depends on how much time and effort they put into it. Adding a piece of software, especially one allowing remote access and functioning at kernel level (in the very core of the operating system, which is almost mandatory for a spy tool), and especially without the knowledge of its administrator, logically undermines the system's security. Traditional surveillance does not particularly lower the security level of the suspect's mansion: it does not open a hole in the roof to let a camera through.

Taking a position for or against the use of government trojans is not in the scope of this paper. As a matter of fact, from a neutral point of view, upgrading the surveillance gear to cope with the technology seems natural, logical, and necessary. However, while doing so, new challenges and dangers arise, inherent to the said technology. They should certainly be known and taken into account when lawmaking.

HADOPI: how to address the 'an IP is not an individual' pitfall in the worst possible way

An iconic case where ethical issues were blatantly ignored in the course of a lawmaking attempt is the HADOPI case in France. The infamous acronym (standing for 'High Authority for the Diffusion of Art Works and the Protection of Copyright on the Internet') is a nickname for the bill of law 'favouring the diffusion and protection of creation on the Internet'. In effect, it is an attempt to preserve the traditional business model of the entertainment industry (major record companies, etc.), based on the premise that P2P networks are responsible for the losses in their revenue.

Discussing the legitimacy of this attempt, or the veracity of the premise it is based on is beyond the scope of this paper. The practical means it employs to do so, however, are worth discussing here, for they highlight a series of fundamental ethical pitfalls that arise when lawmaking in the cyberworld.

Those means are fairly straightforward: in a nutshell, copyright holders or their representatives (i.e. private agencies paid by majors) collect IP addresses observed to participate in peer-to-peer networks (which, by the way, does not involve any breach of privacy: it suffices to connect nodes to the said P2P networks to collect those), and proceed with the denunciation of those addresses to the administrative body known as HADOPI. The latter, based on these logs, take action against individuals to whom the IP addresses were allocated (by their ISP), ultimately ending with suspension of their Internet connection for one year. This is done without possible judicial recourse, and billing is not halted during suspension.

This, at first, raises the recurrent issue of the very false equation: 'an IP address = an individual'. Among numerous points, let us highlight three essential reasons why this is a fallacy that must be combated tirelessly:

- **Principles of Internet routing**: for architectural reasons highlighted in 'Technical Challenges' above, IP address masking is common on the Internet. In particular, bot-infected machines are used as proxies. For example, if, say, child pornography is hosted via fast-flux technology, from the point of view of the actual web server hosting the material, connections come from nodes of the fast-flux network, which are mere bot-infected machines of innocent users.
- **WiFi connections**: wireless access can either be easily stolen (a survey conducted by *Sophos* in December 2007 revealed that out of 560 computer users, 54 per cent had stolen WiFi connectivity [40]) or shared: beyond hotspots, some companies such as *FON* in the UK and *Neuf Telecom* in France provide systems relying on the sharing of subscribers' WiFi connections among themselves.
- **IP address injection**: regarding the specific case of P2P networks, it must be clear that injecting bogus IP addresses in P2P networks is trivial, for any 'peer' of the network. American researchers Michael Piatek, Tadayoshi Kohno and Arvind Krishnamurthy demonstrated this in an academic paper [41]. This could, of course, result in false accusations (during their research, they managed to get letters from the DMCA addressed to their printer, after injecting the IP of the latter in P2P networks).

The HADOPI law project actually timidly half-acknowledged this: while no judicial recourse was possible, a warned user could prove his innocence by installing a piece of software (sometimes referred to as 'securing software', sometimes as 'connection control software' [42]) on her computer. This software, meant to ensure that the user was not doing anything illegal, was set to be non-interoperable (i.e. not cross-platform), paid for by the user herself, and 'in constant connection with a remote server' [42].

At this point, it may be useful to draw a concrete comparison, in order to seize the implications of this directive: a private agency working for an industry syndicate denounces you to an administrative body, claiming that you are trafficking in your living room. Based on those claims, the administration threatens to send you to jail for a year. There is no further investigation, but to prove your innocence, you can pay for the installation of cameras and microphones in your living room, controlled by the administration. Yet, this surveillance gear is only adapted to houses: should you live in an apartment or a condo, you would have to move to a house to prove your innocence. If you refuse, you are sent to jail for a year. There is no possible judicial recourse and you keep paying your rent while in jail. Meanwhile, the actual people engaged in trafficking keep trafficking in their kitchen, leaving their living room unused (i.e. they install the 'control software' inside a virtual machine that does nothing).

Nonetheless, the law project was voted in by parliament. It was only the Constitutional Council of France that, as a last resort, censored the freshly voted law in June 2009. Two constitutional principles were invoked:

- According to the Universal Declaration of the Rights of Man and of the Citizen of 1789, access to information is a fundamental right. Internet access falls into that category and as such, it cannot be altered automatically by an administration, and suspending thereof requires a judge.
- Reversing the charge of the proof, which implies presumption of guilt, is anti-constitutional: a suspect remains innocent until proven otherwise.

The points above set an interesting jurisprudence. Yet, the very fact that two constitutional chambers (in Germany and in France), the last bastion against totalitarian drift in a republic, have had to censor laws dealing with the cyberworld in the past two years is worrying. If anything, it may be a sign that governments feel helpless, and are prone to attempt to solve the problems radically; while endangering fundamental liberties in the process.

As for HADOPI, at the time of writing, it was promulgated after being stripped of the censored parts (which made it essentially useless), while the government is looking for ways to get around the Constitutional Council's concerns with 'add-ons'. One such plan is to empower the HADOPI administration with the ability to fine Internet users up to 1,500 euros, should they perform illegal downloads themselves or if 'by negligence, by the means of her Internet access, a third party commits counterfeit' [43]. In other words, the 'one IP is not an individual' issue is solved radically: it is the legal responsibility of users to secure their systems.

This would set a dangerous legal precedent, prone to generate conviction of innocents in all the domains of cybercrime. Indeed, securing a computer system is something even security professionals have a hard time doing. Otherwise, there would not be data breaches involving the leaking of hundreds of millions of credit card transactions [44], and the customer bases of high profile companies such as *SalesForce* would never be compromised [45]. Thus, how could the law require this competence from Mrs Van de Kramp, 64 years old, who finds it hard enough using *MS Word* for the manuscripts of her kitchen books?

guilty for not securing her wifi
Wifi? I don't see what my dog has to do with this!
guilty for trusting his kids
Shouldn't have watched the football game...
guilty for not being a C.S. Major
WEP key ain't enough?
6'6"
6'0"
5'6"
5'0"
4'6"
4'0"
NE STRESSEZ PAS : L'IRRESPONSABILITÉ A UN PRIX! VOTRE FAI VOUS EXPLIQUERA..

Figure 5: 'The new face of cybercriminals' by DR [46].

On awareness and political action (Pt. 2)

Beyond all philosophical debates on business models involving immaterial artworks, whether we like it or not, such artworks have been 'de facto' freely available on the Internet for years. There is a whole generation of Internet users who grew up in this situation, and now consider it as normal. As a consequence, attempts to revert to the previous situation is felt like an aggression by a large part of the population. Following the Pirate Bay trial in Sweden, the Pirate Party (a party whose crest is a pirate sail) gathered 7.1% of Swedish votes for the 2009 European Parliament election, hitting a symptomatic estimate of 21% support amongst people aged 18 to 29 [47].

Let us dare to say it, criminalizing such a large part of the population with multiple laws and directives is counter-productive in the struggle against cybercrime. At best, it further blurs the comprehension of it by the public (which, as we have suggested in Pt. 1, does not help political action), and at worst, it severely undermines the public feeling that it is necessary, by letting a majority of people think they are on the side of cybercriminals.

CONCLUSION

If anything, it seems that everyone agrees on one point about cybercrime: because of the very essence of the Internet, there is no panacea, no magical formula that will definitely cure the Internet of cybercrime. Creating a supra-national police or re-engineering Internet core protocols from scratch are mere fantasist ideas. Much like there is no Final Ultimate Solution to the Spam Problem (FUSSP), no technical, legislative, market-based or vigilante solution will eradicate it tomorrow.

Yet, it can be combated, diminished, cornered. The first step towards that objective may be a wider acceptance of the Convention on Cybercrime, which allows for expedient international cooperation and harmonization of cybercriminal offences amongst legal systems, two pillars of the anti-cybercrime struggle. This will certainly require a wider public awareness of the situation, and will take time and effort; for instance, the Universal Declaration of Human Rights, although adopted in 1949 by the United Nations, the largest inter-governmental organization in the world, is still far from being enforced everywhere on the planet, 60 years later.

But as pertinent as it may be, and as widely as it may be accepted, a convention alone will not suffice to address the issue efficiently. There must be an actual political and governance will to use the tools it implements; this holds especially true in emerging countries, already confronted by a myriad of problems in a tense economic situation. As the struggle progresses, some 'cyber-havens' will undoubtedly persist. The international struggle against financial havens for money launderers, however, shows that solutions exist to limit this phenomenon, to a certain extent. Further, user education, industry/law enforcement partnerships and tackling the attractiveness of cybercriminal business models by the market are all additional leads to explore.

Finally, the complexity of the challenges standing in the way of fighting cybercrime must not serve as a pretext to drift towards a post-panoptic society, locked by an invisible ubiquitous surveillance, and deprived of individual liberties. The Internet has taken such a preponderant place in the life of millions of people, that controlling it has become a political challenge, and recent events show that danger exists. Benjamin Franklin once said 'any society that would give up a little liberty to gain a little security will deserve neither and lose both'. While fighting cybercrime is an absolute necessity due to its gargantuan range of impact (from emptying your wallet to funding terrorism and endangering the power grid of your country), we ought to be frequently reminded of his and Mencken's words. In a rapidly changing global society, this may actually be a vital challenge.

REFERENCES

[1] http://threatchaos.com/2009/03/stay-calm-people-cyber-crime-does-not-reap-1-trillion-in-profits/.

[2] http://www.theregister.co.uk/2005/11/29/cybercrime/.

[3] http://www.tmcnet.com/usubmit/2009/03/20/4072706.htm.

[4] http://www.fortiguardcenter.com/papers/VB2006_Dirty_Money_on_the_Wires.pdf.

[5] http://www.fortiguardcenter.com/papers/VB2007_Menace_II_the_Wires.pdf.

[6] Survey by Aon Ltd, 2005.

[7] http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html.

[8] http://en.wikipedia.org/wiki/50_Cent_Party.

[9] Dupuis-Danon, M.-C. Finance Criminelle.

[10] http://counterterrorismblog.org/House%20Homeland%203-31-09%20Statement.pdf.

[11] http://en.wikipedia.org/wiki/Internet_censorship_in_Iran.

[12] http://news.bbc.co.uk/2/hi/middle_east/8099579.stm.

[13] http://en.wikipedia.org/wiki/Internet_censorship_in_the_People's_Republic_of_China.

[14] http://en.wikipedia.org/wiki/Golden_Shield_Project.

[15] http://en.wikipedia.org/wiki/Green_Dam_Youth_Escort.

[16] http://www.messagelabs.co.uk/mlireport/MLI_Report_March_Q1_2008.pdf.

[17] http://telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html.

[18] Verdelho, P. The effectiveness of international co-operation against cybercrime: examples of good practice. For the Project on Cybercrime of the Council of Europe, 2008.

[19] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[20] Interview with the author, 2009.

[21] In its 2008 Internet Crime Report, the IC3 (the US computer crime online report platform for the public) reckons it received 275,284 complaints in 2008 and referred 72,940 of those to law enforcement agencies. In the report only six resolved cases are documented, five of which pertain to auction fraud, and all involve perpetrators located in the US.

[22] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&CL=ENG.

[23] Interview with the author, 2009.

[24] Interview with the author, 2009.

[25] http://profmgmt.wordpress.com/2007/04/16/is-google-money-laundering/.

[26] Blanchiment et financement du terrorisme, Ludovic Francois, Pascal Chaigneau, Marc Chesney, Editions Ellipses (2004).

[27] http://en.wikipedia.org/wiki/Financial_Action_Task_Force_on_Money_Laundering.

[28] http://en.wikipedia.org/wiki/Non-Cooperative_Countries_or_Territories.

[29] http://www.imf.org/external/pubs/ft/weo/2009/01/weodata/groups.htm#oem.

[30] http://en.wikipedia.org/wiki/Accession_of_Romania_to_the_European_Union.

[31] http://www.rsf.org/List-of-the-13-Internet-enemies.html.

[32] http://www.wikileaks.org/wiki/Thailand_official_MICT_censorship_list,_20_Dec_2008.

[33] http://wikileaks.org/wiki/Australian_government_secret_ACMA_internet_censorship_blacklist%2C_6_Aug_2008.

[34] http://wikileaks.org/wiki/Talk:797_domains_on_Finnish_Internet_censorship_list,_including_censorship_critic,_2008.

[35] http://en.wikipedia.org/wiki/Cipav.

[36] http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

[37] http://www.interieur.gouv.fr/sections/a_la_une/toute_l_actualite/securite-interieure/loppsi/downloadFile/attachedFile_1/Loppsi_projet_loi.pdf.

[38] http://de.wikipedia.org/wiki/Online-Durchsuchung.

[39] http://www.spiegel.de/netzwelt/web/0,1518,492184,00.html.

[40] http://www.itpro.co.uk/165633/users-will-steal-wi-fi-to-bypass-file-sharing-crackdown.

[41] Piatek, M.; Kohno, T.; Krishnamurthy, A. Challenges and directions for monitoring P2P file sharing networks – or: why my printer received a DMCA takedown notice. Proceedings of the 3rd Conference on Hot Topics in Security. Dept. of Computer Science and Engineering, Univ. of Washington. Publisher: USENIX Association Berkeley, CA, USA.

[42] http://www.numerama.com/magazine/12221-Big-Brother-Albanel-confirme-le-spyware-de-l-Hadopi.html.

[43] http://fr.news.yahoo.com/12/20090624/ttc-hadopi-et-maintenant-les-amendes-maj-549fc7d.html.

[44] http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9126379.

[45] http://blog.washingtonpost.com/securityfix/2007/10/database_theft_leads_to_target.html.

[46] http://lucileb.com/ejcm/politique-eco/tant-pis-pour-hadopi-1312.

[47] http://www.dn.se/fordjupning/europa2009/piratpartiet-far-tva-mandat-i-ny-matning-1.879371.

[48] http://www.npr.org/templates/story/story.php?storyId=102549504.