In pursuit of cybercriminals

Jacques Martinon,
Mission de Lutte contre la Cybercriminalité (MLC)

Abstract:
What characterizes cybercriminals is their adaptation in real time to changes in the digital environment so as to take advantage of technical flaws and turn legitimate uses into an opportunity for obfuscation or even social engineering to the detriment of their victims. They also benefit from a criminal ecosystem that, by becoming professional (cybercrime as a service), very much facilitates the logistics and diversification of cyberattacks. Some attacks have extremely well-crafted business models (*e.g.*, ransomware). In parallel, judicial authorities must quickly adapt their strategies, methods and organization in order to fight more effectively against cybercriminality. France did not really begin its own adaptation till 2015 following a landmark report on protecting cybernauts from cybercriminality. Despite the undeniable progress, it is necessary to pursue these efforts and hone judicial tools that, dreaded by cybercriminals, can be put to use for the purpose of cyberdefense.

Most cybercriminals are delinquents who want to optimize earnings and try to profit from the many opportunities opened in the digital realm.[1] The "community" is an important aspect of this phenomenon, since specialists are now offering "cybercrime as a service" in a well-established business environment. Nonetheless, some cybercriminals have other motives. They are backed, even weaponized, by more or less secretly backed by governments. In a context of undeclared economic warfare (cyberespionage) or demonstrations of power (cybersabotage), they do the work of pre-positioning within critical systems. Threats are hybrid; and the distinction between cyberdefense and cybercriminality is blurred.[2]

As a consequence, judicial services for fighting against cybercriminality must adapt their strategies, methods and organizations fast and make them more effective. France actually started moving on this issue in 2015, as a followup to the report by an interministerial task force on protecting cybernauts from online criminality.[3] Despite undeniable progress, efforts must be sustained to develop a judicial leverage for cyberdefense that these criminals will dread.

[1] This article, including any quotations from French sources, has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in March 2020.

[2] As pointed out in SGDSN (2018) *Revue stratégique de cyberdéfense* of 12 February, 167p., available via http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

[3] A task force directed by Marc Robert, attorney-general: GROUPE DE TRAVAIL INTERMINISTÉRIEL SUR LA LUTTE CONTRE LA CYBERCRIMINALITÉ (2014) *Protéger les internautes, rapport sur la cybercriminalité*, 30 June (Paris: ministries of Justice, the Economy and Interior), 482p., available via https://www.vie-publique.fr/sites/default/files/rapport/pdf/144000372.pdf.

Although all jurisdictions might have to examine offenses committed in the digital realm, the court of first instance in Paris enjoys national competence for cyberattacks.[4] A penal policy for fighting against cyberdelinquency is being consolidated with priority given to the most worrisome trends that affect the population of France and its economy.

After presenting the principal characteristics of cybercriminality, this article will discuss the strategic and organizational adaptations made by the justice system and the new relations that its agents have with cybersecurity.

Cybercriminality

The typology of cybercriminality is still an intellectual exercise, since the traditional approach to qualifications under penal law is far from perfect. Under French penal law however, nearly all offenses in cyberspace are misdemeanors instead of crimes. “Cyberattack” refers to several phenomena (such as cyberespionage, cybersabotage and randomware) distinct as to their operations and motivations. The terms “cybercriminality” and “cyberdelinquency” are used herein interchangeably, even though the first is more current given its closeness to “cybercrime” in English-speaking publications.

In the main, cybercriminality is still cryptic, since traditional statistical methods are *de facto* not operational for assessing it and its trends. In addition, there is the classical problem of the blind spot and of e-evidence.

Cybercriminality: Evolving and polymorphous

Among the major characteristics of cybercriminality is its polymorphous, changing nature, which enables it to profit from the dynamics of digital technology.

A tricky classification

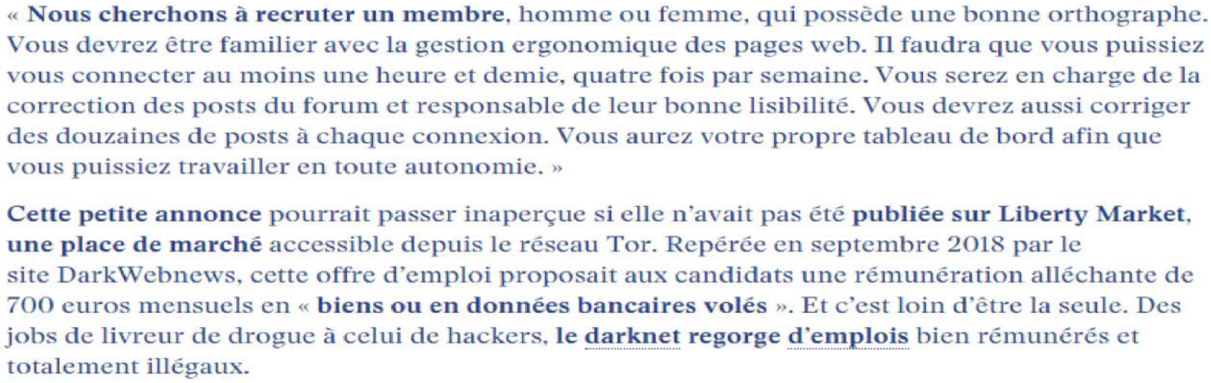
In penal law, cyberdelinquency in the strict sense of the word refers to phenomena related to an attack on an automated data processing system (articles 323-1, 323-2, 323-3 and 323-4 of the Penal Code). In practice, a distinction is made between attacks of low and high intensity. High intensity refers to sophisticated attacks on the nation’s fundamental interests or with an international dimension, or that have (actually or presumably) a large number of victims. Low intensity is a category grouping phenomena conveyed or facilitated by an automated data processing system. This is cyberdelinquency in the broad sense, which covers many sorts of scams. Offenses in this category also include the unlawful activities on darknets (the best known being TOR protocol: The Onion Router).

[4] Article 706-72-1 of the Code of Penal Procedure (under Act n°2016-731 of 3 June 2016): “*For the prosecution, examination and judgement of offenses in fields covered by Article 706-72, the public prosecutor, the pole of investigation, the criminal court and the trial court in Paris exercise a competence concurrent with that which results from applying articles 43, 52 and 382.*”

New job offers in cybercrime

Cybercriminality is thriving. New jobs regularly crop up, whence the talk about "cybercrime as a service" (in analogy with traditional online services), such as: the rental or sale of botnets (a network of "zombies" — connected devices or computers — under a so-called command-and-control server),[5] malware (including ransomware, which has made a fierce comeback in attacks against firms and local authorities), crypter/packer services (for improving the stealth of malware), money mules (or smurfers: persons who launder money via transfers in behalf of third parties), and mixer/blender operations (for laundering cryptocurrencies).[6] Cryptocurrencies provide a slue of opportunities: thefts on cryptocurrency platforms or from individuals, or the "cryptojacking" of computers to use their computational capacity for "mining" cryptocurrencies in the hacker's behalf.

Figure 1: A job offer for darknet administrator
Source: www.ladn.eu



« **Nous cherchons à recruter un membre**, homme ou femme, qui possède une bonne orthographe. Vous devrez être familier avec la gestion ergonomique des pages web. Il faudra que vous puissiez vous connecter au moins une heure et demie, quatre fois par semaine. Vous serez en charge de la correction des posts du forum et responsable de leur bonne lisibilité. Vous devrez aussi corriger des douzaines de posts à chaque connexion. Vous aurez votre propre tableau de bord afin que vous puissiez travailler en toute autonomie. »

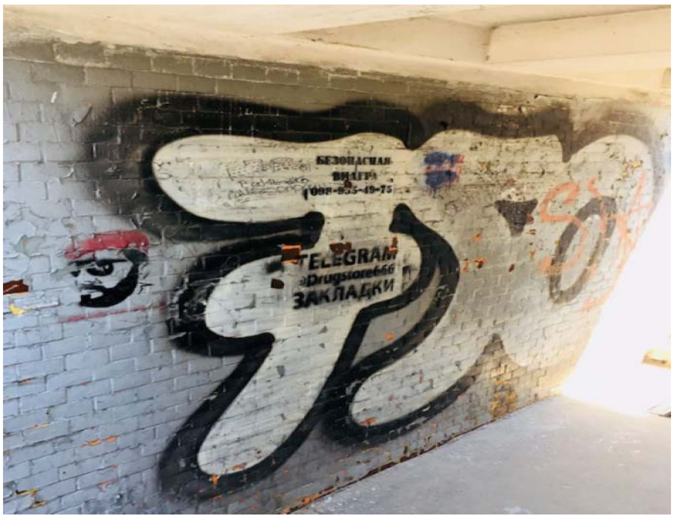
Cette petite annonce pourrait passer inaperçue si elle n'avait pas été **publiée sur Liberty Market, une place de marché** accessible depuis le réseau Tor. Repérée en septembre 2018 par le site DarkWebnews, cette offre d'emploi proposait aux candidats une rémunération alléchante de 700 euros mensuels en « **biens ou en données bancaires volés** ». Et c'est loin d'être la seule. Des jobs de livreur de drogue à celui de hackers, **le darknet regorge d'emplois** bien rémunérés et totalement illégaux.

What is new are the recruitment campaigns with job offers (*e.g.*, for positions as darknet administrator, *cf.* Figure 1). Yet another example: persons are paid to simply "tag" certain zones in urban areas with instructions about how to join a dealer's thread on Telegram (Figure 2) — an "uberization" of the drug trade. The consumer orders a drug directly on his smartphone using an encrypted messaging application with round-the-clock home delivery any day of the week. As a result, "dealerships" will probably no longer be territorialized, given the visibility, stealth and popularity of the dealer's electronic communications. Other worrisome trends seem to be taking shape around applications for decentralized, anonymous cryptocurrency transactions (*e.g.*, Openbazaar and Haven).

[5] A notorious case: botnets from the malware Mirai in 2016 were used for DDoS (distributed denial of service) attacks against OVH and Dyn. The attack against Dyn struck a critical part of the Internet, namely the management of DNS (domaine name system) services. In August 2019, C3N (the National Gendarmerie) successfully dismantled the Botnet Retadup, a network of 500,000 infested machines.

[6] A joint operation conducted by Europol and Dutch investigators shut down Bestmixer.io with sales amounting to an estimated €200 million.

Figure 2: An example from Ukraine: pay is $15/day in a country where the monthly minimum wage is $140.
Source: Trustwave



Cybercriminality: Cryptic

Several factors hamper the fight against cybercriminality, in particular the large number of offences left unreported to the justice system and the contingent nature of evidence.

The blind spot in statistics

Some high-intensity cybercrimes (involving, for example, espionage or sabotage) are not reported to authorities owing to their sensitive nature.[7] News about a cyberattack against a firm can tarnish its image. The EU General Data Protection Regulation (GDPR) offers a sign of hope, since breaches of personal data have to be reported within 72 hours to the National Commission on Informatics and Liberty (CNIL: Commission Nationale de l'Informatique et des Libertés).[8] As for individuals, they have various reasons for not reporting cyberoffenses. Sometimes breaches are imperceptible; sometimes users have the (mistaken) impression that it is useless to file complaints; and in many cases, there is very little material damage.

Raising the awareness of the public about this issue is necessary, whence the national procedure of assistance to the victims of cyberacts of criminal intent[9] and the measures for making it easier to file complaints. The future platform THESEE (under a program conducted by the Ministry of the Interior) is likely to improve our statistical knowledge of certain types of cybercriminality. The recent program act for the Ministry of Justice provides for filing complaints on line (Article 15-3-1 of the Code of Penal Procedure).

[7] In this respect, the policy of the United States is different, judging from the recent activism of the Department of Justice against Chinese or Russian nationals.

[8] *Cf*. the case of Airbus in January 2019.

[9] https://www.cybermalveillance.gouv.fr/

E-evidence: Going dark and extraterritoriality

Encryption has significantly raised the level of cybersecurity, but it has also had collateral damage by, for instance, making it harder to conduct judicial investigations. This is often described as “going dark”, which, in the armed forces, refers to the sudden loss of knowledge of the enemy’s communications (in this case, due to the use of encryption). As instant messaging applications with robust protocols for end-to-end encryption are being routinely used, the problems mount. The generalization of full-disk encryption on computer terminals and smartphones has made it difficult to use data forensically. Furthermore, as already mentioned, network architectures of a TOR type are used to obfuscate criminal acts on darknets.

The professionals who fight cybercriminality are alarmed by the announced merger of messaging applications and cryptocurrencies. For instance, Telegram announced TON (a blockchain) and GRAM (a cryptocurrency) for the last quarter of 2019, the initial coin offering (ICO) amounting to $1.7 billion. Facebook has announced the cryptocurrency Libra, which will have a systemic impact given the number of potential users. All this has, however, spurred a strong political reaction that should lead to concrete regulations against money-laundering (AML) and know-your customer (KYC) procedures.

To complete this already grim list, I might add the difficulty of establishing proof in digital cases since, because of cloud computing, evidence is now often stored outside national borders.

However the sun manages to come out from behind this grimacing cloud. A revolution is under way: the future EU regulation on e-evidence along with the so-called “representative directive”, which establishes the judicial principle that European law will be applicable to global firms with business in Europe. The aforementioned GDPR, though using different criteria, has laid the cornerstone for this regulatory framework.

This topic has created diplomatic tensions with the United States. A dialog is indispensable between the United States and the European Commission in order to settle eventual conflicts between laws and jurisdictions. Meanwhile, negotiations are making headway about a second protocol to be added to the Budapest Convention on Cybercriminality (Council of Europe).

In the meantime and in anticipation of these fundamental changes in crossborder access to e-evidence, certain giants on the Internet (like Google) have recently modified their policies by transferring the handling of some legal matters in France from their headquarters in the United States to their subsidiary under Irish law. In fact, nearly all of the Californian high-tech firms have offices in Ireland, eventually in order to optimize taxes.

Adapting judicial strategies and the organization of justice

An investigation of cybercrime has specific characteristics. The distribution of the victims over a large territory means that the justice system has to rationalize its handling of cases. The bunker mentality in public administrations has to make way for exchanges between institutions, since cybercrime spans many fields.

An overview of judicial strategies

I shall mention but a few examples of judicial strategies herein, given the lack of space to discuss them fully and, too, my decision not to say too much. Readers will understand that cybercriminals are on the lookout for any information they can turn to account, evidence of this being the posts about penal procedures on darknets. Let me start by recalling what has been said about civil lawsuits: “*Although low blows are forbidden, simple ‘ruses de guerre’ are not.*”[10]

Retrieving e-evidence often necessitates, prior to actual searches, identifying and locating back-end servers, where key evidence might be dissimulated behind a slue of proxy servers. In many cases, the server to be searched will be in a foreign country, whence the need for close, international cooperation. One investigatory technique is to use a pseudonym. Software on the market can help track the use of cryptocurrencies, like bitcoins. When suspects are questioned, priority is to be given to “live forensics”, *i.e.* an urgent investigation of their digital devices so as to minimize technical difficulties (due to encryption) later on.

The admissibility of the evidence obtained from foreign sources is a complicated topic. Jurisprudence in this matter has shifted about. The Cour de Cassation, the final court of appeal in France, has ruled that creating a fake pedophile website (by American authorities) constituted an incitement to commit an offense. As a consequence, it voided a French criminal procedure (Cass. Crim., 7 February 2007, n°06-87.753). In 2014 however, it upheld evidence collected via a forum on credit card scams created by the FBI (Cass. Crim., 30 April 2014, n°13-88.162). Legal arguments will be drawn out since authorities in certain countries are using “honeypots” to attract hackers.

Judicial authorities and cybersecurity

The organization of the French judicial system in 2019

While avoiding details about the territorial competence of judicial authorities in cases of cybercriminality, I would like to point to the key role played by the court of first instance in Paris (*tribunal de grande instance*). Since an act of 3 June 2016, it has national competence in cases related to attacks on automated data processing systems and crimes of sabotage against computer systems (Article 706-72-1 of the Code of Penal Procedure). This reform has consolidated the “F1 section”, which, created in 2015 within the Paris office of prosecution, is devoted to handling complex cases of cybercriminality. This section now has more personnel; in September 2019: three magistrates, an assistant and a clerk. The situation on the bench is less reassuring: there is no specialized investigating magistrate. The Mission de Lutte contre la Cybercriminalité, part of the DACG (Direction des Affaires Criminelles and des Grâces), has released dispatches about centralizing the handling of certain cybercrimes.[11]

Specialized interregional jurisdictions (JIRS) are handling more and more litigation involving organized cybercriminality.[12] Furthermore, magistrates who are “resource persons on cybercrime” are forming a network, a bridge between ordinary courts, appeal courts and JIRSs. The Paris prosecutor’s office and the DACG organized the first national meeting of these magistrates on 14 June 2019.

[10] CARBONNIER J. (1997) *Droit civil. Introduction* (Paris: Presses Universitaires de France), p. 363.

[11] The DACG is a division of the central administration of the Ministry of Justice. I cite as examples the DACG dispatches of 10 May 2017 and 22 June 2018: the one about making operational the national competence of the Paris office of prosecution in matters involving attacks against automated data processing systems or ransomware; the other about the handling of scams for “repairing” information systems.

[12] For instance, Main Noire, a darknet platform, was dismantled under the supervision of the JIRS in Lille.

Tightening relations between judicial authorities and cybersecurity professionals

The central administration (DACG) of the Ministry of Justice is, via the Mission de Lutte contre la Cybercriminalité, contributing to both the strategic work done by the Center of Coordination of CyberCrises (C4, set up following the 2018 issue of the *Revue stratégique de Cyberdefense*) and the meetings of the Groupe de Contact Permanent (GCP). This permanent contact group, steered by the ministerial Delegation in charge of Trusted Industries and the Fight against Cybermenaces (DMISC), has the goal of improving the dialog with private operators (such as Apple, Google, Twitter, Microsoft, Facebook and, more recently, Dropbox) and fostering a constructive, shared view.

The DACG also sits on the board of ACYMA (cybermalveillance.gouv.fr, a public interest partnership: *groupement d'intérêt public*, GIP). It also participates in the joint training program on "Digital sovereignty and cybersecurity" along with the IHEDN (Institut des Hautes Études de la Défense Nationale) and INHESJ (Institut National des Hautes Études de Sécurité et de Justice). Participants in this program are top white collars from the public or private sectors and from NGOs.

Conclusion

Figure 3:
Source: Gunshow, KC GREEN

Judicial leverage should increase as these various organizations mature. Undeniable progress is being made. International cooperation, in particular with Europol, Eurojust and Interpol, is a key to success. Cyberthreats should not be left without a response, even less so since the attack surface is constantly expanding with potentially systemic consequences on the economy and even on the physical integrity of citizens. This remark might seem overdrawn; but what reaction is to be adopted when ransomware will paralyze a hospital or take charge of a connected vehicle driving at full speed on a superhighway? Till now, all is (nearly) fine, as indicated in the cartoon.