The fight against cybercriminality: The state's new role and the issues

Thierry Delville,
PricewaterhouseCoopers (PwC)

Abstract:
Innovations have always benefitted criminals before reaching the public. The digitization of society during the past decades is no exception to this: the context is propitious for cybercriminals to benefit from the offenses they commit. The race to adapt the law to digital technology and incriminate new behaviors, an insufficient international harmonization of the law, the persistent difficulty of gauging and knowing the phenomenon…these are a few of the issues that the government must address to fight more effectively against a delinquency that is undergoing its own digital revolution. Added to these difficulties are questions about
closer coordination and dialog between state authorities and private parties. Cybercriminality raises the stakes related to sovereignty, economic protection, intelligence and national defense. Seeing to security and justice in cyberspace is more than ever the occasion to rethink how to mobilize society so as to prevent, detect and repress actions that weigh ever more heavily on our fellow citizens' everyday lives.

Cybersecurity is now a central preoccupation of leaders, wether public officials or corporate executives.[1] During the last three years, opinion polls regularly rank cybersecurity as third, fourth or fifth among the major sources of preoccupation, alongside terrorism, geopolitics, the increase in regulations or even climate change.[2] It will soon be 45 years since the first computer virus was identified on what was not yet the Internet: Creeper was launched on the ARPANET in 1971. Nowadays, hyperconnectivity and the digital transformation of the economy and society have turned cyberspace into the fifth field of conflict where most major armies are now staking out positions.

Given the sociology of cybercriminality, these criminals have profited from this new space in a very favorable context: the absence of borders; an evolving, diversifying population of criminals; and the switch from the quest for easy profits to actions, better prepared and targeted, to which more sophisticated means are being devoted. Espionage and interference in behalf of private organizations with governments or other principals as accomplices have lasted, crystallizing into a literal "cold war". All of this motivates actions with a return on investment far higher than what is made on types of delinquency outside the cyberrealm.

To fight against cybercriminality, apprehend, investigate and judge perpetrators, state authorities have a key role to play by protecting fundamental rights and freedoms. Nonetheless, it is ever more evident that accomplishing this assignment calls for other forms of intervention.

[1] This article, including 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 February 2020.

[2] https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2019.html

Improving our knowledge of cyberthreats and trends

In a report in 2014, a French interministerial task force directed by Marc Robert, attorney-general, stated that cybercriminality seemed like a "*nebula all the harder to define because it involves inherently evolving technical processes that, steered by initiates, traditional statistical procedures have trouble detecting.*"[3] Drawing on several definitions, national and international (but none of which help us enough to understand the phenomenon), this report suggested a generic definition: "*Cybercriminality groups all the penal offenses attempted or perpetrated against or through a system of information and communication, mainly the Internet.*"

It is necessary to know the reality of this phenomenon before assessing the actuality of the threat. As Sun Tzu wrote in *The Art of War*, "*If you know your enemies and know yourself, you will not be imperiled in a hundred battles.*" Knowing the reality of cybercriminality despite the lack of a precise legal definition is a challenge. In a report in 2019, the Ministry of the Interior recalled how difficult it is to distill a view of this phenomenon out of the statistics.[4] Working out a shared view is to be encouraged. Knowledge of the "cybercriminal topography" nationwide necessitates aggregating data from several sources. This aggregation can be done only if we have a view broad enough to see beyond the data from our institutional services. Just as we frequently talk about the "black box" of delinquency with, in mind, the crimes and offenses that are left unreported to authorities, several experts have described as a "black hole" the unreported crimes and offenses committed in cyberspace.

Regulations require that certain categories of victims report incidents affecting their information systems to ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). This interministerial regulatory authority's role has been bolstered over the past few years. In line with the armed forces program act for 2013-2019 and the EU's NIS directive on "*network and information systems*", the phrases "*operator of vital interests*" (OIV under the French act) and "*operator of essential services*" (OES under the EU directive) refer to strategic firms subject to obligations about their computer equipment and about reporting incidents to regulators. Other "less sensitive" firms are not subject to these requirements.

These rules do not *de facto* require filing a complaint nor opening an investigation. Prosecuting offenses relies on a synergy between the state's technical or legal services and the willingness of victims, who still far too often fear for their reputation or are afraid of eventual sanctions. Under the EU's General Data Protection Regulation (Article 83.4) for instance, a firm that does not report a data theft faces a stiff fine that can amount to as much as 2% of its sales.

Encouraging organizations to use new procedures for filing complaints,[5] raising the awareness of all stakeholders about cybercriminality, systematically exchanging data among state services, laying the conditions for gathering information (in particular with the private sector)… these are the ways to ensure an exhaustive followup on cybercriminality.

---

[3] 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.

[4] https://www.interieur.gouv.fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019. For the full report: MINISTÈRE DE L'INTÉRIEUR (2019) *L'état de la menace liée au numérique en 2019*, report n°3, May, 142p., available via https://www.interieur.gouv.fr/content/download/117535/942891/file/Rapport-Cybermenaces2019-HD-web-modifi%C3%A9.pdf.

[5] https://www.interieur.gouv.fr/Archives/Archives-ministres-de-l-Interieur/Archives-Gerard-Collomb-mai-2017-octobre-2018/Communiques-du-ministre/Ouverture-de-la-plateforme-Percev-l-Signalement-des-fraudes-a-la-carte-bancaire.

Better known, better prevented

Obtaining knowledge and sharing information are key points for fighting effectively against cybercriminality. For the state, effective action means, above all, prevention, awareness and information.

Identifying threats and the technical responses to them are activities that ANSSI shares with CERT, the Computer Emergency Response Team network.[6] This essential source of technical support for cybersecurity experts is not yet well known outside the professional community. Out of the three million firms in France, how many rely on this source of knowledge?

Other major programs have been carried out in recent years. For instance, the platform cybermalveillance.gouv.fr registers incidents affecting firms or individuals before bringing the victims into contact with certified technicians on the website. This public interest partnership (*groupement d'intérêt public*, GIP) diffuses through the social media messages of information and alerts. Among other programs, I might mention: e-enfance (on cyberharassment), stop-jihadisme (about online propaganda), Perceval (for reporting scams involving credit or debit cards) and the platform PHAROS (which has been listing unlawful contents for nearly ten years now).

Prevention is being organized, but it is crucial for us to see farther and plan a collective effort to help spread knowledge:

- foster feedback by branch of the economy from firms that have been attacked so as to advance in updating knowledge about the evolution of cyberthreats;
- encourage feedback from the service-providers certified under the authority of ANSSI and other state services in order to provide information about new menaces and work habits; and
- develop new practices and methods so as to be prepared for massive, systemic attacks.

Many preparations have been made, but much more is yet to do for preparedness!

Adapting our legal tools

Should we assume that "*the law has been exhausted by the pursuit of digital evidence with bounds that are always pushed farther away*"?[7] For sure, lawmakers are ceaselessly responding to new digital risks. In the past three years, laws have been passed against cyberharassment, revenge porn, the incitement to commit suicide; and the list goes on….. The PACTE Act has recently introduced rules for fighting against the new fund-raising scams based on cryptocurrencies. These ongoing adjustments to evolving digital practices and the need to create new criminal counts are not about to come to a halt in the coming years.

The means and techniques for conducting investigations are also being adapted. The offer of digital forensic services has changed. Investigators are not overlooking the major advances made in interceptions, geolocation and the processing of big data when they conduct searches on location (as during the terrorist attacks that took the headlines in 2015). This trend also carries benefits for the private service-providers that intervene during crises or during remedial work after emergencies.

Expectations have arisen about changes in the law with regard to: data storage (after the decision in December 2016 by the Court of Justice of the European Union in a case involving Télé2), the means used by investigators to work around techniques that make data anonymous, and faster crossborder data exchanges. The bedrock in these cases lies beyond the reach of national law by itself.

---

[6] See the security alerts at https://www.cert.ssi.gouv.fr/.

[7] QUEMENER M. (2018) *Le Droit face à la disruption numérique. Adaptation des droits classiques, Émergence de nouveaux droits* (Paris: Éditions Gualino).

In effect, much of the fight against cybercriminality is referred to the international level. Evidence of this are: Europol's growing capacity in this domain, since the creation in 2013 of the European Cybercrime Center (EC3,[8] which has shone through its actions for managing unlawful contents on the Internet and setting up the European platform IRU), the European Commission's many texts (including the NIS directive and GDPR), Cyberact,[9] the reinforcement of the European Union Agency for Cybersecurity (ENISA) for the certification of trusted solutions in the EU. All these advances clearly indicate that the future fight against cybercriminality has to be conducted on a European and, even farther, an international scale.

Penal policy must also have more visible effects. More magistrates have to have specialized training for handling cybercriminality. These effects must be visible in sanctions that are proportional to the seriousness of incidents so that cybercriminality no longer be perceived as a joke. The sanctions decided by courts in serious cybercriminal cases must set an example, but without imitating the very heavy sanctions applied in the United States (*cf*. the case brought against Ross Albricht).[10]

More forces mobilized in the fight against cybercrime

France became aware of the importance of cybercrime soon enough to pass legislation and organize a riposte. As of 1994, the Prefecture of Police set up a service of investigation in charge of frauds based on information technology: BEFTI.[11] Soon afterwards, the police and gendarmerie created units (OCLCTIC, C3N) that, now internationally recognized as centers of expertise, are capable of conducting investigations under the control of a few specialized magistrates. Other services of investigation in the customs administration and Tracfin have, over the years, formed teams committed to the fight against cybercriminality.

As for the judiciary, the appointment of "referent" magistrates and the creation of a specialized section in charge of cybercriminality in Paris (Section F1 of the prosecutor's office) and of the JIRSs outside Paris also reflect this trend. Setting up a specialized prosecutor's office (like the PNF or PNAT) would go a step farther toward a better adapted judicial response.

Other state authorities are also actively involved in the fight against cybercriminality. ANSSI has described cybercriminality as a "*vast subject that concerns, first of all, the ministries of the Interior and Justice, in close collaboration with ANSSI.*"[12] This agency's clearly defined role has not been questioned; and its technical expertise is an essential asset for detecting threats and analyzing incidents. Intelligence services are also active. The DGSI (General Directorate for Internal Security) has the power to conduct judicial inquiries into attacks that jeopardize firms or other targets related to national defense or the country's vital or strategic interests. The *Revue stratégique de cyberdefense* of 2018 recommended allowing technical data to be exchanged between investigators in cybercriminality and experts in cyberdefense: ANSSI, COMCYBER in the Ministry of Defense and the DGSE (General Directorate for External Security).[13]

---

[8] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[9] https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_fr

[10] https://en.wikipedia.org/wiki/Ross_Ulbricht

[11] Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information.

[12] https://www.ssi.gouv.fr/particulier/principales-menaces/cybercriminalite/

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

Cyberattacks bring the criminal world into contact with intelligence and defense services. Given this hybrid dimension, certain events call for diplomatic handling. As several significant events, such as WannaCry, NotPetya or other affairs across the Atlantic or nearer to us in the Netherlands[14] have shown, the situation is moving judicially and diplomatically: a finger is being pointed at individuals or even at presumably criminal states[15] — the practice of "name and shame". A finger is also being pointed at insufficiently protected companies that are victims in waiting.

Other actors, not among the least, in this fight are the private service-providers who are heavily involved in tasks of prevention and remediation. They are core players in the crisis experienced by most victims of cyberattacks. Labeling or certification procedures are increasingly being used to declare them to be trusted parties. In relation to this expertise, the state must undertake actions ranging from the exchange (in both directions) of information as accurate as possible with the goal of foiling menaces to the exercise of its power of control in cases of proven distortions or loopholes. This ecosystem of experts must have a facilitator. This is an issue for the sector of information and communications technology and too a matter of sovereignty.

Preparedness for challenges in cyberspace

The history of cybercriminality has just started. Several legal texts at the national level will be drafted to redefine the limits set on investigators' work, to incriminate new practices, to draw attention to the need for vigilance, to determine the responsibilities of operators, and so forth. The fight against crime in digital environments of the future will depend on the means devoted to research and development. Shortly before the G7 summit in Biarritz, Catherine de Bolle, Europol's new executive director, emphasized that the advent of 5G, the Internet of things (IoT) and artificial intelligence (AI) represent a progress that raises questions about investigators' capacities, whether in matters of interception or investigation.

Apart from the question of these new tools and new issues, we need to be present in the drafting of new international regulations. The Budapest Convention on Cybercrime, the founding act of international assistance in this field, dates back to 2001 but has not yet been ratified by the fifty or so member states. The call by the president of the Republic in November 2018 for confidence and security in cyberspace has not received support from China, the United States or Russia.[16] As pointed out at the G7 summit in Biarritz in August 2019, we must work better together… but the way is still long from words to deeds.

In the coming years, the state's role will be central to the fight against cybercriminality; but this fight will no longer be based on, as it used to be, a clear-cut separation between state authorities, on the one hand, and experts, on the other. The fight against crime in the digital realm involves networking; and information-sharing will be a cardinal virtue. Awareness, prevention, sharing, these are and will be the keys for fighting cybercrime with weapons that, though perhaps unequal, are at least comparable to those used by criminals.

---

[14] https://www.huffingtonpost.fr/2018/10/04/derriere-laffaire-de-la-cyberattaque-aux-pays-bas-le-puissant-gru-le-service-de-renseignement-militaire-russe_a_23551536/

[15] https://www.theguardian.com/politics/2018/may/23/uk-threatens-to-name-and-shame-state-backers-of-cyber-attacks

[16] Availble via https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf.