Confronting Cybercrime through Criminology

Xavier Raufer[A]

As far as cybercrime is concerned, we are still on terra incognita, or nearly so. "*Hic sunt dracones*," is found cautiously inscribed on medieval maps that are supposed to depict the heart of Africa. "Digital dragons" are ever more abundant today. Faced with these challenges, in the as yet uncharted territory of cybercrime, the only way forward is to think as criminologists and no longer as technicians. Why?

Look! Open Your Eyes!

As of the beginning of 2015, Internet advertising in France (25 percent of the market) has now surpassed advertising in the press (24 percent). Today, there are close to 1.2 billion Facebook users on mobile devices—an increase of 74 percent since 2012.

Humanity is becoming more connected than ever—standardized, formatted, remote-controlled. This is taking place in the developed countries and in the megalopolises, on a planet where stability is being worn thin, giving way to dynamism. In this society of perpetual acceleration, the intoxication of speed is felt ever more strongly.

What snares lie in wait for us! Notwithstanding the fairy-tales propagated by the titans of the Net, technology is not neutral, and algorithms are subtly partial. And listen to what British sociologist Zygmunt Bauman tells us of these fabulous mutations: "Unlike solids, liquids cannot maintain their form when subjected to an external force, however light it might be. Links between particles are too weak to resist any pressure. For Bauman, this is precisely the characteristic of human relationships in a liquid society."[1]

And we speak of mastery? This is a loss of control. We shower praise on emancipatory high-tech inventions? Yet cyber-servitude continues to grow. Obviously, all of this is criminogenic: fragilization, disorganization, and loss of attention are a veritable bonanza for thieves and fraudsters. These are the intrinsic perils attendant upon the system itself. But there are also hardcore criminals, cyber-predators who do not act thoughtlessly or cynically—but for the quickest and most hefty possible profit.

[1] Translator's note: Adela Abella, "Psychoanalysts Facing New Technologies in a World of Liquid Modernity," in *Psychoanalysis Online 2: Impact of Technology on Development, Training, and Therapy*, ed. Jill Savege Scharff (London: Karnac, 2015), 70. See Z. Bauman, *Liquid Modernity* (Cambridge: Polity, 2000).

[2] Translator's note: This quotation was back-translated from the French version.

doi: 10.18278/ijc.3.2.4

As an example, let's look at one of the Russian-Ukrainian cyber-gangs, one among many in the ex-Eastern bloc, as described at the end of 2014 by Group-IB and Fox IT. Calling itself "Carberp" after the "Trojan Horse" software of the same name, and starting in early 2013, this cyber-gang infiltrated its targets' systems by way of malware-laced e-mails that appeared to come from so-called trusted partners (the Russian Central Bank and others), and then proceeded to plunder the targets' bank accounts. Now it also preys on the systems themselves, which are heavy and inert, myopic, and even blind; it also attacks the computers in ATM devices.

Since its creation, "Carberp" has plundered fifty banks and ATMs in Eastern Europe, looting 25 million dollars. Since summer 2014 the gang has become even bolder, attacking businesses and banks in Western Europe and the US, thanks to a new "malware" package called "Anunak," which brings together a dozen tools used to steal passwords, break codes, enable remote cyber-theft, and more. Finally, "Carberp" practices criminal insider trading by stealing sensitive information relating to the targeted companies, so as to exploit it on various financial markets and stock exchanges, as well as in other ways.

Silent and invisible, great wild beasts like "Carberp" prowl a cyber-jungle where humans have so far struggled to deal with them. There is a bright future ahead for cybercrime. And what can mere technology do when faced with such beasts? Not a lot. We saw this recently when pirates ravaged the digital systems of the television channel TV5Monde, with all of the channel's anti-piracy IT staff entirely unable to see or do anything.

Confronted with this cybercrime, still barely understood, and now capable of striking whenever it pleases, as it pleases, cyber-criminology must prevail. A new criminology, one dedicated to mobility. A cyber-criminology forsaking the stable and the fixed in favor of fluxes and networks. A cyber-criminology of movement and motion, at ease swimming in Bauman's famous "liquid modernity." A cyber-criminology dedicated to understanding better, learning more about, and facing up to the emergent cyber-dangers—and alone capable of doing so.

Cyber-Criminology: What Does it Mean, and What Can it Do?

The objective of cyber-criminology is to tell us what criminals do in the cyberworld; here are its four foundational theses:

- *Diagnosis 1*: In the compound term "cybercrime," "crime" is dominant. Analyzing the world of cybercrime reveals that it has not invented anything new. In their own milieu, up to the present, cybercriminals have merely reproduced variants of physical criminality.

- *Diagnosis 2*: Cybercrime will not decline as a result of yet more advanced technology, but only through political will. An all-guns-blazing-style, headlong charge would provoke, in this domain, a disaster analogous to that of the inept high-tech war in Iraq.

- *Treatment 1*: What the cyberworld needs is a highway code—just as the society of the automobile, in its time, gave rise to its own. This code must be developed and enforced by a coalition of powerful nations, in the reasonable hope that it will be enforced worldwide. Another possible image for this indispensable normative superstructure would be that of the control tower.

- *Treatment 2*: The Highway Code applies to every vehicle, be it a luxury model or a more modest car. Similarly, only a code of the cyberworld would effectively penalize the predators, financial raiders, giants of the net, and others who plunder it with impunity and exploit its users.

An Agile Worldwide Digital Infrastructure? No, a Fragile One.

Today, the global system of automated data-processing constitutes a worldwide superstructure. Cyberspace represents a new continent, a new world. And these new information and communication technologies (ICT) alter the way in which populations think, believe, behave, and learn.

This applies to the whole population: honest folk, but also wrongdoers. Now, as always, when humans conquer a new area, it is not long before we see theft, fraud, crime, propagandist activities, fakery, and lies, among other forms of deviance from social norms. Cybercrime does indeed exist, and therefore cybercriminals also: in 2013, Interpol found that, on a global scale, more than 80 percent of online criminality can be attributed to transnational criminal groups. Today, this cybercrime is the Holy Grail for every felon. Consider the following:

- A total dissociation of time and distance, offering the ability to commit a crime at a distance of 10,000 kilometers (cyber-theft).

- Youth that are hypnotized, easy to dupe and infiltrate, in so far as they see “the world as a set of applications, and their own world as a series of applications—sometimes even as one single application, extending from cradle to grave.”

- Cybercriminal masterminds, gang chiefs, or network bosses with almost guaranteed impunity—today only peripheral stooges are arrested.

- Limited costs for considerable gains.

- A simple methodology, exploiting two fundamental factors: human weakness (such as naivety) and technical vulnerabilities (such as flaws open to exploits)

Ultimately, in the ambient Internet world, we hear nothing regarding crime. Sometimes we speak of the effects of crime (attacks, intrusions. . .), but never, or almost never, of flesh-and-blood criminals—who they are and where they really come from. This is a dramatic omission. For if one thing is obvious, it is the need to start out by naming that which one wishes to understand, and subsequently deal with. Thus the discreet power of nomination is a formidable one: "Naming enables us to know. . . Naming unveils. . . By virtue of exhibiting, names attest to their magisterial sovereignty over things,"[2] as Martin Heidegger said.

In medicine, for example, failing to name a serious illness condemns the patient: in strategy, likewise, failing to give a precise name to a threat most often condemns the victim.

Cybercrime, Cyberterrorism: The Three Big Questions

Is cybercrime more dangerous than terrorism?

Quite recently James Comey, director of the FBI, declared: "The threat is so dire that cyber security . . . for the second consecutive year, surpass[es] both terrorism and espionage—even the threat posed by weapons of mass destruction."[3] Seriously? Let us understand the FBI director: he lives in a society formatted by, and intoxicated by, media hype. When speaking to the cream of Silicon Valley, any announcement that falls short of the first (digital) world war would inevitably trigger yawns of boredom.

Nevertheless, the threat of cybercrime is real. Today, the digital world is like the Bank of France minus the safety deposit boxes: generally, in most cases hackers of all stripes need only help themselves. In the past year, hackers were able to gain access to the systems of an American retail giant and steal almost all the confidential personal data of seventy million payment cards (those of its entire, massive customer base)—that is, a third of all cards currently in use in the US. Recently in France we saw the hijacking of TV5Monde: for a period of hours, the wholesale capture of a huge television network, its servers and diffusion channels, its accounts on social networks, and other places—something that was, for France, as huge a "strategic shock" in the virtual world as last January's killings (at Charlie Hebdo and Hyper-Cacher) were in the physical world.

After the TV5 hijack: Is France well-protected?

France lacks any mechanism for the early detection of dangers and threats. All too often, our official services react to a drama that is already underway, a crime already

[3] Translator's note: James Comey, "The FBI and the Private Sector: Closing the Gap in Cyber-Security," address to the RSA Cyber Security Conference, February 26, 2014, accessed October 8, 2015, https://www.fbi.gov/news/speeches/the-fbi-and-the-private-sector-closing-the-gap-in-cyber-security.

[4] Translator's note : Xavier Raufer, *Cyber-criminologie* (Paris: CNRS, 2015).

committed, but do not operate—do not yet have the knowledge, and therefore cannot operate—in a preventative register. Yet there is no spontaneous generation in the strategic realm, no more than there is in biology. The preparations for a violent act like the attack on Charlie Hebdo (in the physical world) or that on TV5Monde (in the cyberworld) will necessarily leave traces; what are called weak signals or "deviations from the ambient background," analogous to what ancient Greek wisdom called "epiphanies."

These are what we need to detect before the drama unfolds. In the months preceding September 11, 2001, multiple warning signs were reported to the authorities. But these signs were not understood in time. Essentially, their meaning was only realized on September 12, when the catastrophe had already occurred. This is what must be avoided. In strategic terms, what we need to do is simply allow France to apply concretely the popular wisdom of the proverb: "Prevention is better than cure."

An overexcited media often speaks to us of "cyber-prediction": can we take this seriously?

There is a generational question here: those who govern know little of the cyberworld and the perils it contains. In particular, they are entirely ignorant of the pernicious ideology of Silicon Valley, a highly toxic cocktail of scientism (Max Planck: "only the measurable is real") and hyperliberalism (so-called "libertarianism") bordering on pure and simple anarchism. The dominant idea in the propaganda of this anarcho-capitalism is that only information technology can protect us from the perils of the world. Thus it is affirmed, with unprecedented force: "There is no Alternative (TINA)." And consequently—so Silicon Valley tells us—the future lies in prediction via information technology.

Now of course this is absurd, because true uncertainty can no more be modeled today than it could in Aristotle's time. Otherwise, everyone would win the lottery or at the racetrack. This is absurdity verging on intellectual fraud, peddled to dupes by the giants of Silicon Valley. I expose all of it in my book *Cyber-Criminologie*.[4] Read it, and see what you can learn!