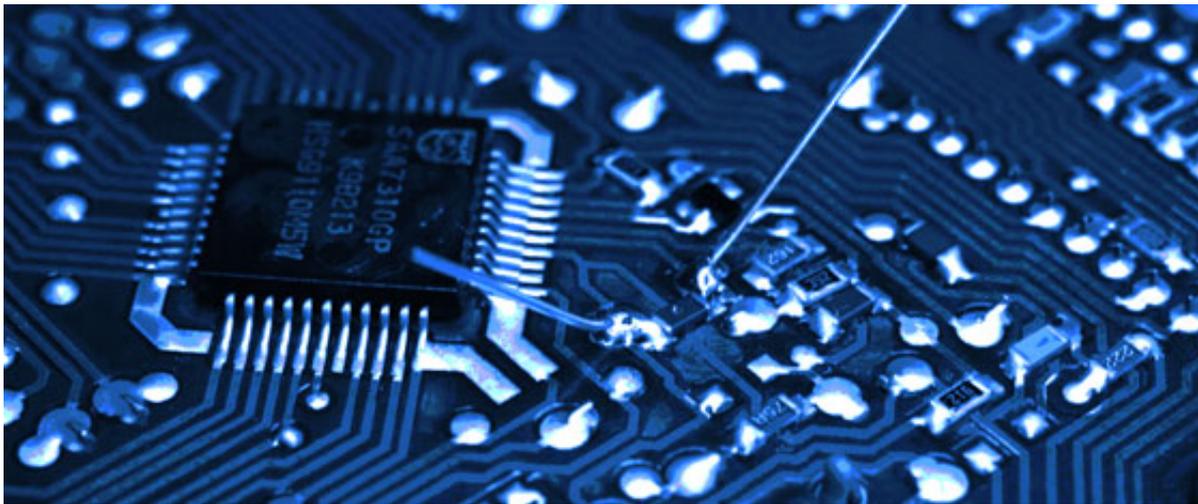


CYBERCRIME - COUNTERFEITING

The Issue of "Real-Virtual" Interactions

Most professionals define cybercrime as: "Any illegal action in which a computer is the tool or object of the criminal offence.(1) "However, this definition has the disadvantage of not taking into account the "offline world". It means that many stakeholders, such as the French Customs, tend to broaden the de facto concept of cybercrime to acts that involve criminal flows, both in the real world and on the Internet, by using a computer.



This broader view of cybercrime has the advantage of acknowledging - in theory - this type of crime in both the real and the virtual field. While the Internet is a difficult network to observe, assess and to conceptualize without technical intermediaries, it is reasonable to consider or assume that this broader view of cybercrime leads to a better understanding of the cyber phenomenon and its criminological implications. The well known phenomena of the counterfeiting of physical goods such as luxury goods (watches, cosmetics or accessories) and in the leisure industry (DVDs, video games or music), and its ramifications on the intersection of the real (factories and distribution networks) and the virtual (Internet), would then be especially relevant to unearthing many issues pertaining to cybercrime. Yet, with this hybrid vision of cybercrime it is quite the opposite that happens because reality tends rather to reflect the fragility of the binomial "Cybercrime - counterfeiting."

Indeed, according to the multiple available sources (academic studies, French, European or American official reports and the international press), we cannot help noticing that counterfeiting reveals, on the contrary, a strong misunderstanding of cybercrime. Like the Canadian researcher Stéphane Leman-Langlois,(2) we can consider that cybercrime is proving to be a relative scientific impasse or, as the British researcher Majid Yar(3) describes, is a result of statistical constructs. This critical view of cybercrime takes its full dimension in the case of counterfeiting, because it's shown especially in the French case:

- The inability/incapacity of computer experts to work in a transversal way with legal-oriented experts. The latter, being closer to political power, tend to address the fight against cybercrime in the framework of restrictive intellectual property rights for counterfeit products. The result: growing and widely unjustified legislation on cybercrime issues, bringing on dedicated rents of judicial expertise, having as consequence an inadequate fight.
- The available sources do not confirm the very real concept of transnational criminal organization plying in counterfeiting.

The cases most often reported by the press are those related to certain criminal organizations matching the Palermo Convention criteria, but most available information supports the theory that most cases primarily involve certain micro-organizations or isolated individuals who use the Internet without understanding the gaps in protection for illegally trafficked counterfeit goods. The Chinese case (with counterfeit websites based in Hong Kong and the factories in China) is rarely discussed in a factual manner and information on this sensitive area is less frequently reported by the media. On the other hand the grey areas where the legal economy overlaps with the criminal economy or "mafia" remain a huge blind spot in the public debate on counterfeiting. One of the few credible descriptions of this overlap is the testimony of the famous journalist Roberto Saviano(4) in his book Gomorra, which accurately describes the extent to which luxury manufacturers (whose names he does not mention) have cooperated (and still cooperate?) with the Camorra on a global scale.

In such a context there is evidence of the opacity of some grey areas in the real world even if we can assume, as the Academic David S. Wall(5) details for the fashion industry, that "that the counterfeiting economy works more likely in parallel with the legitimate fashion industry with "separate sub-markets- as a sort of assemblage." Regarding the role of Internet in such a configuration any precise information suggests that it is at the heart of the organizational logistics. The web has more likely accompanied and accelerated the gap to the real world, which has grown with globalization.

Despite the large opacity of the Chinese counterfeiting industry and the many grey areas, computer users sanctions continue to be carried out primarily on a local basis against less skilled Internet users, rather than on territories like China and Russia, which are more distant but potentially major markets. A more "comfortable" local cybercrime perpetration must also be interpreted as a bad anticipation of the challenges of Internet, to which luxury or cinema corporations have been belatedly adapted. The Internet expresses less of a "cybercrime risk" (transgression of a rule by buying goods known to be counterfeits from Asia) than the strategic importance for industrialists to be able to manage an optimal presence in the information flow network, particularly taking into account semantic parameters (such as keywords). Parameters that new economy corporations such as Google and eBay have been able to better anticipate and integrate within their business model. Some major "old economy" manufacturers, well supported by pressure groups and custom services searching for additional tax revenues, thus are encouraging local cybercrime sanctions, mainly aimed to control through "a kind of administration of fear" a new form of economic consumption that still remain poorly understood, or at least integrated somehow into their business models.

However, we can assume that, with globalization, the systemic failures within the real (outsourcing, manufacturing; fragmentation; product designing difficulties) and the virtual (digital paradise where there are few inquiries on hosting servers) offer a wide range of possibilities for malicious activity. But within the dyad/duet "real - virtual", it is probably the "real" one that presents the highest opacity and the most numerous grey areas. The Internet often serves as a mobilization resource within certain industrial lobbies and especially to divert the public debate away from very opaque issues of the real world which should be better identified. So what is the solution? The sociologist Saskia Sassen(6) emphasizes the development of concepts that contribute to assessing the interactions between the virtual and the real world. The most radical (or simply lucid/clear?) minds will remain skeptical about such theoretical approaches being difficult to apply, and will consider, as the French magistrate Jean de Maillard(7) does, that the fight against cybercrime is most of all a "cosmetic" struggle, where actors are mostly concerned with the conservation of capitalist income and are paradoxically also slightly interested in the present anarchy. From such a perspective, the repressive law enforcement tightening of the "cybercrime - counterfeiting" binomial should be decrypted within a broader geopolitical and capital framework, where emerging Countries (both future competitors and subcontractors) could have a major role and where cyber-consumers, even any "criminal organizations," seem to "play a part" beyond their genuine commitment.

Eric Przywa - (eric.przywa@wanadoo.fr) is a researcher, risks consultant and the editor of risk05 (<http://www.risk-05.com>). He is the author of the recently published book "Cybercrime and Counterfeiting", FYP and writes for various magazines.

He holds degrees in International Relations and Economics and conducts research on risk assessment at CRC - Mines ParisTech.

-
- 1 Olivier Itéanu, Tous cybercriminels, Jacques-Marie Laffont éditeur, 2004.
 - 2 Stéphane Leman-Langlois, « Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberspace commercial », *Criminologie*, vol. XXXIX, n°1, printemps 2006.
 - 3 Majid Yar, *Cybercrime and society*, Sage Publications, 2006.
 - 4 Roberto Saviano, *Gomorra. Dans l'empire de la camorra*. Gallimard, 2009.
 - 5 David S. Wall, Jo Large, « Jailhouse frocks. Locating the public interest in policing counterfeit luxury fashion goods », *British Journal of Criminology*, vol. L, n° 6, July

- 6 Saskia Sassen, *La Globalisation. Une sociologie*, Gallimard, 2009.
- 7 Interview with Jean de Maillard, magistrate, 29th October 2009.