Economic and Social Analyses of Cybercrimes

Coriolano de Almeira Camargo*

Renato Leite Monteiro**

***Summary*:** This article exposes an analyses on economic and social incentives considered by perpetrators of cybercrimes, and it concludes for the necessity of cooperation among the different sectors of the society aiming at diminishing such stimulus.

Key Words: *Cybercrime, Economic Analyses, Fiscalization.*

I. INTRODUCTION

In order to plan the level of necessary resources to fight the data-processing crimes we need to cleverly understand the costs they cause. At the same time, to understand the incentives glimpsed by the cybercriminals, it is equally important to investigate the virtual attack proceedings.

II. THE ECONOMY OF CRIMINALITY: *LATO SENSU ANALYSES*

The basic scenery of the economy applied in the study of illegal acts arise from the conjecture that the perpetrators of such acts react to incentives. crime is considered a social choice, despite the moral and ethical aspects, or even the deviation of responsible individuals' behavior. Grounded on this hypothesis, Gary Becker [1] developped a model that considers the gains and costs that motivate the crime, and the options to control criminality, its social cost. Becker shapes the offender's option as a function of the illegal act gains, the probability of aprehension and the severity and type of the punishment. His purpose is to minimize the net social cost produced by the crimes, as the costs attributed to the victims and to the judiciary surmount any benefit earned by the criminals, causing instability in the economy. Becker demonstrates that to maximize the social revenue added, the good sanctions opposed to criminals shall be the in the form of fines. He argues that pecuniary fines are more efficient in the repression than the liberty restriction penalties, for the latter still includes a cost for the state.

Becker's model was expanded for a myriad of sceneries. One of the fundamental extensions is the offense market and the analyses of their associated balance. The market model consists (i) supply of offenses (crime rates, for example); (ii) demand – supply of illegal goods and services as drugs, deviation of stolen products, etc; and (iii) negative demand – potential victims of criminal actions that require public intervention, as the correct application of the legal provisions and administration of justice or of private protection.

The supply of offenses consists in the study of benefits and costs to offenders, as opportunities of gains, personal aversion to crimes and individual perception as to the probability of apprehension. Social interactions are also considered a fundamental part, as they influence the crime rates in society [2]. One of the conclusions of Becker' studies is that the expenses in activities with the purpose of crime reduction shall be

considered in long term, as the criminal rates are influenced by previous rates [3], thus, any strategy to fight crimes may take generations to obtain any noticeable result. Another important point is the expectation of increase of crime rates in a measure in proportion to a community social unbalance, for two reasons: (i) the ones in the inferior social levels have low costs to commit crimes; (ii) the presence of individuals who earn high incomes provides highly profitable targets.

The study of public demands for the law application deals directly with the optime distribution of resources to the legal system. The measures utilized for the optimization of the problems are normally based on social incomes added. However, some include justice concepts. Most part of the models start from a social plan whose option is to influence the probability of apprehension and conviction of na individual, the severity of the punishment and the sanctions imposed to offenders. However, in reality, there is no social plan and the persons responsible for the correct application of the law are only worried about their own social well-being, what may give rise to corruption [4].

Potential victims have also incentives to protect themselves, to reduce the victimization risks, to acquire insurances, in order to reduce their losses if they become victims [5]. One of the main issues in this context is if private protection reduces crime levels, or only deviates the risks to less protected victims. The study of the offense market assumes that the frequency in which each type of crime happens reflects in the implicit balance between the supply and the demand of such acts [6]: the supply added of illegal acts, criminality rates, for example, is proportional to the return expected for offense, that diminishes with the private protection used by the potential victims, and due to the expected legal sanctions.

Market models have also been used to estimate the criminality sócia costl [7]. Marginal markets may lead to a high level of crimes. As the barters are illegal, it is impossible to make explicit contracts that may be solved by the legal system, and this leads to disputes that end in violence. Another market analyses considers the public as suppliers of opportunities for the criminals, and potential victims [8]. One of the conclusions is that the criminals react to the opportunities, and the supply of these offered by the public determines the criminality rates. While the majority of market models take into consideration unorganized groups, dealing with organized criminality requires different models, once the latter represents an entity that tries to function as a monopoly, and restricts the flow of illegal transactions. In addition, they take part in the artificial raise of prices and in the undervaluation of the efforts for law application [9].

III. THE SOCIAL COST OF THE CYBERCRIMES

There is a lack of understanding about the exact magnitude of the cybercrime and its impact due to the fact that these crimes are not always detected or reported. The reason why they are not denounced includes the financial impact in the market, reputation and damages to the mark, concern with possible legal suits, the fact that the report of a failure sends green signal to new attacks, incapability to supply information, worries related to employment loss by professionals responsible for the company security, and a noticeable lack of law enforceability by the State.

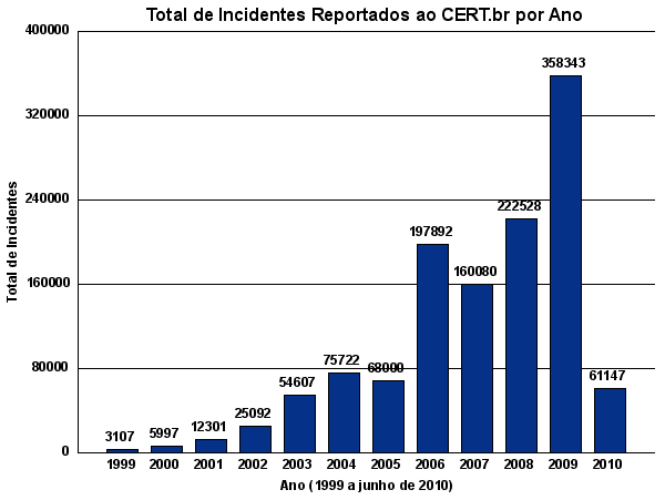
The data related to the costs of the cybercrimes are easy to obtain in some cases of notorious security failure. For example, the security failure of TJX company cost nearly 200 million dollars [10]. The Heartland Company had a total loss of almost 40 million dollars due to its failure that exposed thousands of medical backgrounds. However some of these costs came indirectly when the company faced legal suits and potential civil responsibility claims [11].

Besides the data arisen from big security failures, it is very difficult to obtain reliable registers in minor cases. The methodology used by the cybercriminals aims at users of a great variety of sceneries, with access to different financial services. However, while each individual case may seem simple and less significant, the amount accumulated of cyberfrauds may be spread through several entities and will not be identified by any institution separately. There are many estimates made by different entities of the most diverse jurisdictions [12]. However, studies, point out that losses may surpass the cipher of 01 trillion dollars a year [13]. While such estimates are valuable, they are not completely reliable, as they present great differences without apparent explanation and some institutes do not inform their sources or the methodology used to make their estimate [14]. Besides, many security companies receive incentive to artificially inflate such estimate [15].

Nowadays, one of the most reliable statistics internationally are the catalogued and collected by the Inter Crime Complaint Center (IC3). The 2009 annual report disclosed that the number of online denounces reached a record, receiving a total of 336.665 complaints, an increase of 23% if compared to the previous year. The total amount of virtual frauds surpassed the 559 million dollars [16]. The annual average was 931 dollars. Despite showing the seriousness of the cybercrimes, such estimates are only a small fraction of the real losses for several reasons: Many companies prefer not to report the attacks, for the motives above exposed; victims may not be known and the IC3 compiles only the data from the United States of America – USA.

The United Kingdom has estimated losses in the amount of 610 million pounds related to losses arisen from credit card frauds, which include practices in which the crime occurred without the physical presence of the cards. Such number represents a continuous increase since 2004 when they started to be measured. While that year the frauds carried out with the presence of physical cards were similar to when they were inexistent, now the virtual frauds are the primary source of such modalities of crimes, suffering an increase of 243%. In the same period the total of transactions only in the electronic commerce, has increased 524%.

In Brazil, the institute responsible for the data collection e for receiving the denounces of security failure and cybercrimes is CERT.br [17] (Computer Incident Response Team of Brazil). The 2009 year received a total of 358.343 denounces, number superior to the one received by American organizations. The enormous growth of the Brazilian economy and the fragility of the data processing systems that sustain such economy was one of the motives of the massive increase of the cybercriminality in the Brazilian territory.



While the reports of these institutions may supply solid data for the estimate of the losses arisen from cybercrimes, much more has to be done so that the reliable prospectings are made. Nowadays, we cannot identify accurately the real scenery of the problem. We can only state categorically that it exists, but without real estimates we cannot measure if the actions taken by public and private initiative have worked.

A possible way to know better the real costs of the cybercrimes is to enforce, through the law and frequent fiscalization (*enforcement*), banks, financial institutions, internet service providers, and other companies to disclose the registers and costs associated to the attacks to their systems, including the volume of money involved in the crimes. Some American states already have legislation that determines that any security failure must be reported, under the penalty of civil responsibility in the amount of the losses if it is posteriorly discovered that the institution had not informed the incident [18]. To report the incident will facilitate the elucidation of the failures and trends, and also create a market to deter the frauds, where the institutions may find means to protect their users[19].

IV. POTENTIAL FUND COLLECTION OF CYBERCRIMES

To be possible to develop an economic model of the data processing crimes it is also necessary to estimate the potential benefits. This shall help to understand the incentives glimpsed by potential criminals and the total social loss: in what amount the profit margin surpasses the dangers arisen from a legal and safe system.

While some cases may supply a basic material on different activities, it is still hazy how representative these cases are in relation the marginal economy, as only a fraction of the incidents are reported, investigated and processed. To obtain a better view of the real amount that enters such economy it is necessary more transparency from public and private institutions, in reporting their losses arisen from data processing crimes. Estimating the cybercrime gains is different from working the pecuniary damages, as these damages are extended not only to lost information, but they are also distributed among their recuperation, legal suits, depreciation of the valor of the marks and other collateral effects. If the institutions were obliged to inform such direct losses we might be able to estimate the real flow of money that sustains the marginal economy of data processing crimes.

V. PUBLIC PROTECTION

The public protection may influence the supply of offenses, when reducing the incentives of the cybercriminals' acts. The variables that the law application and the

legislation may influence are: (i) the probability of apprehension of the cybercriminals; (ii) and the penalties associated to the cybercrimes. In relation to the apprehension probability, several factors contribute for the low risky nature of the cybercrimes. For example, it is highly improbable that the law applicators get involved with the cases involving identity theft, as the majority of the victims does not report such crimes to the authorities [20] This may also be the case of bank accounts theft, as the victim normally solves the problem through a contact with the bank without continuing the procedures related to the incident. Even when a consumer tries to contact the police, some authorities are still reluctant to receive the denounces. Some understand that the victims might be the financial institution. Or in case the theft occurred in another jurisdiction, the authorities may require the offended to file the claim in another place. On the other side, private entities do not receive any incentive to report security incidents.

The scenery is more complicated for the authorities priorities and *expertise*. In a local level, the police normally have no resources or knowledge to identify effectively the persons responsible for the data processing crimes. This leads to an interaction problem between public and private entities, when the latter, in many cases, perform functions eminently public in order to solve the cases. In the federal sphere, only the cases of great importance are investigated, the others are filed for lack of cause. In 2003 it was estimated that the cybercriminals have one chance in seven hundred to be arrested by the Police authorities[21], while in ordinary more serious crimes the probability raises from one to five [22]. This lack of authorities' response induces, even more, the victims not to report the incidents.

Even if the authorities decide to investigate and start a legal procedure, the no bounds nature of these types of crimes increase the ambiguities of jurisdiction and the difficulties associated to the process. Most parto f the penalties in Brazil attributed to data processing crimes are soft and there is no alternative penalties. As previously referred, the more efficient penalties are the pecuniary ones, modality that is not commonly used in Brazilian jurisdiction. In cases in which the responsible receives a liberty restriction penalty, besides the fact that this penalty is more expensive for the State, the imprisonment may contribute for the malicious behavior when it is aggregated to a community of persons that might share techniques and create criminal nets. Two classic cases may illustrate the argumentation. John Draper, one of the most famous *phreakers*, *crackers* who used his knowledge to access telephonic systems, was arrested in the USA in 1972 due to fee frauds. When He was released from prison, he informwd that when he entered the prison system he had to teach everyone in prison how he performed his frauds. The method spread and the telephonic companies registered higher losses [23]. In the same way, Max Butler began its activities as a recreative hacker. However, when he entered the Pentagon computers, he was arrested. In prison, he knew a professional fraud criminal that introduced him to the *carding* world. When he served his sentence, he started to attack systems of banks, markets and others *crackers* to steal credit card numbers, which were sold to *carders*[24].

VI. PRIVATE PROTECTION

In the cooperation pattern among private and public entities, the computer security industry may contribute for the reduction of virtual offenses increasing the cost for the beginning and the maintenance of the cybernetic attacks. While the computer security industry is traditionally focuzed in prevention technologies, firewall, antivirus, encryption, authentication, etc, there is an emerging market for attack detection and recuperation. Private entities have already been responsible for many cases of cybernetic criminal organizations squandering. In the same way, some companies are using mark monitoring and antifraud solutions, that include disconnection systems, which consist in tracking the malicious servers and make contact with the responsible

providers so that the offensive content is withdrawn. One of the main questions is if the private protection diminishes crime levels or only deviates them to less protected victims.

VII. SHAPING THE DECISION MAKERS INCENTIVES

Internet service providers have different approaches when managing their users' security level that is directly related to their hierarchy and interconnection principle. The up to date Internet consists in multiple semi-independent nets that share an IP number [25] in common and a global structure of traffic routing that supplies directly or indirectly the connectivity to these nets.

Motivated internet access suppliers can apply a large number of measures to improve the nets security, for example: (i) preventive acts to protect the clients from attacks offering accessible security software; (ii) active response, applying automatic quarantine and repair of detected failures; (iii) net defense through local and interconnected net traffic; (iv) and collaboration, shared net defenses implementation and creation of united combat groups.

However, it is important to notice that even the most vigilant internet providers do not have always the conditions to provide security to their users without collaborative initiatives. Firstly, many threats do not manifest in the connection layer, but in the application layer, as example of what happens in the credential theft through phishing. Secondly, many countries, like Brazil, have strict privacy legislation that prohibits the internet access providers to monitor their users' actions, therefore they can just act after receiving abuse notices. Technologies that automatically identify such threats may reduce the logistic of denounces.

In relation to companies and domestic users, it is necessary to evaluate the possible roles that they may perform to combat data processing crimes. It is important to mention that different classes of users have different incentive levels to invest in security.

The success of cybercrimes schemes frequently depends on the lack of security investments among domestic users and small businesses. Domestic users are rarely aware of the risks and fail in the adoption of the necessary adequate security measures due to the complexity of the effective measures [26]. For example, they may open malicious files annexed to e-mails or may not install updating of the subscriptions against virus, even being aware that such acts may lead to financial losses and misfortunes. Still, most part of users to whom differed security services are offered chooses to maintain basic plans due to financial problems. Another motive is the lack of responsibility when the users and business are negatively reached by compromised machines [27]. Unfortunately, residential users combined with the lack of preventive actions may result in a substantial increase in collective damage [38].

Users may also act in a passive way for being protected from the damages that may arise from cybercrimes. For example, the consumer's legislation protects the consumer from being held responsible for theft in his bank accounts. Decisions on the contrary are still rare, even when the victims fault has been proved. However, there are some incentives for the victims to apply security measures in their nets, in order to avoid inconveniences and occasional monetary losses.

Large companies, including financial and electronic commerce institutions normally invest in security to protect their operational procedures and industrial secrets. They may count on the cooperation of the Internet access providers to defend them from

large scale attacks. They are also interested in maintaining strict security polices, that normally include operation in separate nets.

In opposition, companies have also incentives to dim the cybercrimes identity and credential thefts; for fear that the value of their marks is affected. In addition, the exposition of severe losses due to security incidents may lead to regulatory acts undesired by the market. High levels of fraud may diminish the financial institution credibility, beginning a chain movement that may lead to the whole market instability.

Still, malicious users pay for differed services to fraudulent internet providers, receiving in exchange the possibility of conducting their activities longer without having their contents reached or withdrawn.

The Software industry is an interesting case in cybercrimes analyses. While most companies are made responsible for the security of their products, the current practice of the software industry is non attribution of the responsibility for the software quality through the user license agreement. The court decisions in contrary are rare.

VIII. CONCLUSION

We can conclude that data processing crimes are still advantageous under the economic and social incentive analyses which lead to their practice. The lack of adequate fiscalization, the high profitability, the great possibility that the criminals will not be found, the habit of the victims not to report the incidents and small penalties are incentives for the occurrence of such crimes. Only the cooperation among the different spheres will make the diminishing of such incentives possible.

REFERENCES

[1] BECKER, Gary S. Crime and punishment: An economic approach. Journal of Political Economy, vol. 1968, p. 169.

[2] GLAESER, Edward; SACERDOTE, Bruce; SCHEINKMAN, Jose. **Crime and social interactions**. Quarterly Journal of Economics, 2:507–548, 1996.

[3] SAH, Raaj K. **Social osmosis and patterns of crime**. Journal of Political Economy, vol. 99. 1991, p.1272–1295.

[4] FRIEDMAN, David. **Why not hang them all: the virtues of inefficient punishment**. Journal of Political Economy, vol.107. 1999, p. 259–269.

[5] LAKDAWALLA, Darius; ZANJANI, George. Insurance, self-protection, and the economics of terrorism. Journal of Public Economics, vol. 89. 2005, p. 1891–1905.

[6] EHRLICH, Isaac. On the usefulness of controlling individuals: an economic analysis of rehabilitation, incapacitation, and deterrence. American Economic Review; vol. 71. 1981, p. 307–322.

[7] ANDERSON, David.**The aggregate burden of crime**. Journal of Law and Economics, vol. XLII. 1999, p. 611–642.

[8] COOK, Philippe. **The demand and supply of criminal opportunities**. Crime and Justice. vol.7. 1986, p. 1–27.

[9] GAROUPA, Nuno. **The economics of organized crime and optimal law enforcement**. Economic Inquiry. vol.38. 2000, p. 278–288.

[10] TJX hacker was awash in cash; his penniless coder faces prison. Available at: <http://www.wired.com/threatlevel/2009/06/watt>. Acessed in: 15 jul 2011.

[11] Payment Processor Breach May Be Largest Ever. Available at:<http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html>. Acessed in: 15 jul 2011.

[12] ITU Study on the Financial Aspects of Net- work Security: Malware and Spam. Available at:<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ itu-study-financial-aspects-of-malware-and-spam.pdf>. Acessed in: 15 jul 2011.

[13] Unsecured Economies - Protecting Vital Information. Available in:< http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>. Acessed in: 08 set 2009.

[14] The NGO Safernet (www.safernet.org.br) has valuable data relating to informatics security in Brazil, but it does published its sources and methodology.

[15] ITU Study on the Financial Aspects of Net- work Security: Malware and Spam. Available at:<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ itu-study-financial-aspects-of-malware-and-spam.pdf>.Acessed in: 15 jul 2011.

[16] IC3 2009 Annual Report on Internet Crime Released. Available at:<http://www.ic3.gov/media/2010/100312.aspx>. Acessed in: 10 jul 2011.

[17] http://www.cert.br/stats/incidentes/

[18] Available at: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

[19] HOOFNAGLE, Chris Jay. **Identity theft: Making the known unknowns known**. Journal of Law and Technology, vol. 21, 2007.

[20] Identity theft survey report. Available at:<http://www.ftc.gov/os/2003/09/synovatereport.pdf>.Acessed in: 15 jul 2011.

[21] Underreporting of identity theft rewards the thieves. Gartner Group Research ID: M-20-3244, 2003.

[22] Porque a Lei Não Deve Almejar a Justiça, mas sim o Bem Estar. Available at:<http://www.redel.com.br/~dennisww/lei1.htm>. Acessed in: 15 jul 2011.

[23] Interview with John Draper. First episode of stop H*Commerce. Available at:<http://www.stophcommerce. com>. Acessed in: 15 jul 2011.

[24] Kevin Poulsen. Superhacker max butler pleads guilty. Available at:<http://www.wired.com/threatlevel/2009/06/butler_court/>. Acessed in: 15 jul 2011.

[25] Internet address - IP: number attributed to each internet conection, allowing its individualization.

[26] Managing online security risks. Available at: <http://www.nytimes.com/library/financial/columns/060100econ-scene.html>. Acessed in: 28 jul 2010.

[27] GROSSKLAGS, Jens; CHRISTIN, Nicolas; CHUANG, John. **Secure or insure? A game-theoretic analysis of information security games.** World Wide Web Conference (WWW'08). China. 2008, p. 209–218.

* Lawyer, CEO of the Almeida Camargo Attorneys at Law, Teacher of the Pos-Graduation Program on Electronic Law and Cybernetics Intelligence at FADISP.

**Associated Lawyer at Opice Blum Attorneys at Law. Master on Constituional Law. Teacher of the Pos-Graduation Program on Electronic Law and Cybernetics Intelligence at FADISP.

.