Chapter 2
Simple Economics of Cybercrime and the Vicious Circle

"Today's online data thieves don't just run automatic scanners and jump on any network hole they find. They're more likely to first choose a target that has data they can turn into cash, and then figure out how to break in" (Peter Tippett of Verizon Business, cf. Larkin, 2009, p. 33).

"Law enforcement is presently 5 to 10 years behind the global crime curve in relation to technological capabilities" (Alexander, 2002).

Abstract Cybercrimes are becoming increasingly pervasive and sophisticated and have more severe economic impacts than most conventional crimes. Technology and skill-intensiveness; a higher degree of globalization than conventional crimes; and the newness make cybercrimes structurally different. In this chapter, we examine how characteristics of cyber-criminals, cybercrime-victims, and law-enforcement agencies have reinforced each other and formed the vicious circle. Next, we build on key elements of the vicious circle and some additional characteristics of cybercrimes to assess the cost–benefit calculus of a hacker.

2.1 Introduction

The underlying causal mechanisms may differ across types of crime (Clarke, 1983). A clearer understanding of such mechanisms, that is, the structures of costs, benefits, and attractiveness of cybercrimes, is crucial to combat against this new form of criminality. Three factors contribute to structural uniqueness of cybercrimes: technology and skill-intensiveness; a higher degree of globalization than conventional crimes; and the newness. First, unlike conventional crimes against persons or property such as arson, burglary, and murder, most cybercrimes are very skill-intensive. At this point, it must be emphasized that even script kiddies that use someone else's tools to commit victimless and/or marginal cybercrimes possess more skills than most of their conventional world counterparts do. Second, given the global nature of the Internet, cybercrimes entail important procedural and jurisdictional issues. Third, mostly due to newness of cybercrimes, law-enforcement

N. Kshetri, *The Global Cybercrime Industry*, DOI 10.1007/978-3-642-11522-6_2,

authorities across the world are relatively inexperienced to deal with these crimes. Fourth, another implication of newness is that the legal system is not well-developed to deal with cybercrimes. Brenner (2004, p. 22) notes: "... the traditional model of law enforcement is a compilation of past practices that have been deemed effective in dealing with the phenomena it confronts. The model's general strategy, the reactive approach, is one that has been in use since antiquity." Some scholars argue that "first principles of law" need rethinking in the cyberspace (Katyal, 2001). Moreover, some countries have not yet enacted laws related to cybercrimes. Fifth, still another dimension of newness is a lack of previously developed mechanisms and established codes, policies, and procedures. These factors are likely to result in much less guilt in cybercrimes compared to conventional crimes.

This chapter examines the structure of cybercrimes and assesses the cost–benefit structure of cyber-criminals. From a potential victim's perspective, it is widely recognized that economic analysis can help explain the optimum investment as well as types of measures needed to prevent hackers' cracking into an organization's computer network (Anderson & Schneier, 2005). We offer a simple economic analysis from the perspectives of a cyber-criminal. Such an analysis provides insight into factors encouraging and energizing a cyber-criminal's behavior.

2.2 Economic Factors Affecting Crimes

Prior researchers have suggested that "offences are most imminent if their technological viability coincides with a high level of economic temptation to break the rules" (Hirschauer & Musshoff, 2007, p. 248). People can perceive the criminal law system as legitimate and fair, accept the legitimacy of anti-cybercrime norms and internalize them, but may violate them when they have a powerful temptation (Morgan, 2005). An important question then is: what factors make the commission of a crime tempting?

2.2.1 Target Attractiveness

Target attractiveness depends on offenders' perceptions of victims. Prior research indicates that crime opportunity is a function of target attractiveness, which is measured in monetary or symbolic value and portability (Clarke, 1995). The general affluence of an area as well as the value of a particular target influences attractiveness. Empirical research has demonstrated that in a given area, more affluent residents' cars are more likely to be targeted (Clarke, 1995). Likewise, some goods are "hot products" in terms of being targeted (Clarke, 1999). Target attractiveness is also related to accessibility—visibility, ease of physical access, and lack of surveillance (Bottoms & Wiles, 2002; Clarke, 1995).

Weakness of Defense Mechanisms: Weakness of defense mechanism co-varies positively with the likelihood of becoming a crime victim (Glaeser & Sacerdote, 1999). A low informal surveillance (e.g., not watching out for suspicious-looking activities in a neighborhood) is related to a high crime rate (Taylor, Koons, Kurtz, Greene, & Perkins, 1995). Because of a low surveillance, sparsely populated neighborhoods tend to have a high rate of violent crimes (Browning, Feinberg, & Dietz, 2004; Wilson, 1987). Individuals and organizations, however, can reduce the probability of becoming victims and losses by buying insurance policies or by using safety measures such as anti-burglar systems and safety deposit boxes, or by living in safe neighborhoods (Ehrlich & Becker, 1972). Likewise, middle classes tend to avoid "high crime areas" by moving away from crime hot spots (Lianos & Douglas, 2000).

2.2.2 Economic Conditions Facing an Offender

In general, crime rates are tightly linked to the lack of economic opportunities. Becker (1995, p. 10) comments on the increased number of crimes committed by teenagers: "[L]ow earnings are a factor behind crime, and teenagers have lower earnings and fewer opportunities."

Scholars have examined how certain "land use" types act as crime generators by bringing potential offenders and potential victims together (McCord, Ratcliffe, Garcia, & Taylor, 2007; Swope, 2001). Schuerman and Kobrin (1986) observed a three-stage process in the emergence of a high offender area. The first stage involved an increase in the number of renting and apartment units. Stage II was characterized by changes in population-related feature such an increase in the proportion of unrelated individuals or a higher residential mobility. The final stage concerned a change in socio-economic status such as more unskilled people and a higher proportion of unemployed population (Schuerman & Kobrin, 1986).

Recent studies provide a growing body of evidence to support and extend Schuerman and Kobrin's findings. McCord et al. (2007) found that some businesses, institutions, and facilities act as "crime generators" by bringing potential offenders and victims. Concentrated poverty has been linked to a high crime rate (Kupersmidt, Griesler, DeRosier, Patterson, & Davis, 1995; Oberwittler, 2007; Hawkins et al., 1998; Valdez, Kaplan, & Curtis, 2007). Likewise, Deas and Thomas (2002) reported that poverty and living in an urban environment predicted substance abuse among adolescents.

2.3 Economic Processes Motivating a Cyber-Criminal's Behavior

Unlike conventional crimes against persons or property such as arson, burglary, and murder, cybercrimes are skill-intensive. In industrialized countries, people with IT skills can more easily find legitimate jobs. A large number of cyberattacks originate

from Eastern Europe and Russia because students there are good at mathematics, physics, and computer and have difficulties finding jobs (Blau, 2004). Economies of the former Soviet Union are too small to absorb the existing computer talent (Serio & Gorkin, 2003). Beyond all that, a 1998 financial crash in Russia left many programers unemployed (Serio & Gorkin, 2003). In some countries, organized crime groups reportedly pay up to 10 times as much as legitimate IT jobs to top graduates (Warren, 2007). A self-described hacker from Moscow noted: "Hacking is one of the few good jobs left here" (Walker, 2004). Likewise, regarding computer attacks originating from Romania, the US-based Internet Fraud Complaint Center noted: "Frustrated with the employment possibilities offered in Romania, some of the world's most talented computer students are exploiting their talents online."

Notwithstanding India's huge IT talents, the country accounts for proportionately fewer cybercrimes compared to most developing countries. The primary reason behind India's low cybercrime profile is the development of legitimate IT industry in the country. Speaking of a low rate of cybercrimes in the country, Nandkumar Saravade, director of cybersecurity for India's National Association of Software and Service Companies (NASSCOM) noted: "Today ... any person in India with marketable computer skills has a few job offers in hand" (Greenberg, 2007).

2.3.1 Selection of Targets

Businesses with a high dependence on digital technologies such as online casinos, banks, and e-commerce hubs are the most likely to fall victim to cybercrimes (Kshetri, 2005). These seem to be attractive targets, which provide a powerful temptation to cyber-criminals (Clarke, 1995; Morgan, 2005). A study by IDC indicated that over 60% of cybercrimes targeted financial institutions in 2003 (Swartz, 2004).

It is also apparent that cybercrimes targeting developing economies exhibit a concentration in e-commerce ready industries such as the online gaming industry in China (Greenberg, 2007; Fong, 2008), banking industry in Brazil (Miller, 2008), and the offshoring sector in India (Fest, 2005).

2.4 Structure of Cybercrimes: The Vicious Circle

Characteristics of cyber-criminals, cybercrime-victims, and law-enforcement agencies have reinforced each other and formed the vicious circle of cybercrime. Key elements of the vicious circle are presented in Fig. 2.1.

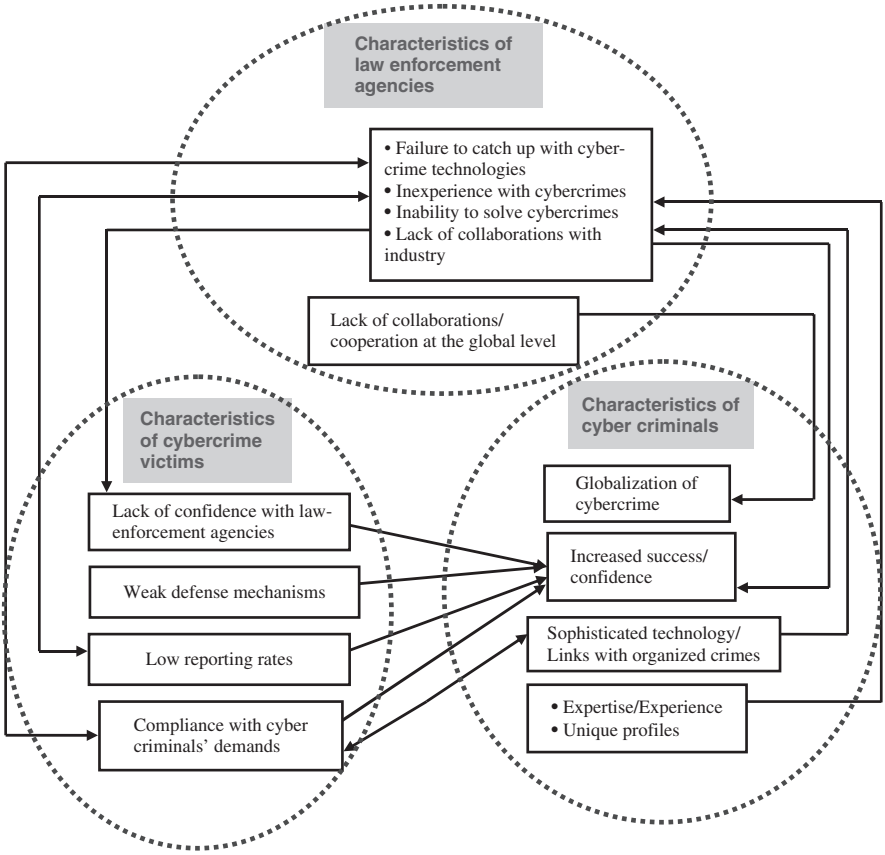

Fig. 2.1 The vicious circle of cybercrimes: a proposed framework

2.4.1 The Cybercrime Market

We begin by considering the "market" for cybercrime. Following, Ehrlich (1996), cybercrime "market" can be considered as a Walrasian market in which "the aggregate behavior of suppliers and demanders is coordinated and made mutually consistent through adjustments in relevant prices." Note that Walrasian market is among the most common models used to describe the operation of the virtual market (Toshiya, Susumu, & Noriyasu, 2003). In Becker's (1968) model of the crime market, criminals and law enforcers are the only actors involved. Interactions between these two sets of actors determine equilibrium. It is important to note that actors other than criminals and law enforcers are also involved in the game. For conventional crimes, they include consumers of illicit and illegally sold goods and services in specific crimes and victims (Ehrlich, 1996).

2.4.2 Law-Enforcement Agencies

First, laws as well as enforcement mechanisms lag in their response to cybercrimes' challenges (Brenner, 2004; Jones, 2007). Law-enforcement agencies such as Police forces and the FBI are inexperienced with these new forms of crimes. Police forces in most countries are highly localized and are not well equipped to deal with the global nature of cybercrimes (Walden, 2005). Alexander (2002) noted: "Law enforcement is presently 5 to 10 years behind the global crime curve in relation to technological capabilities."

The failure to change structures and practices fast enough to deal with the rapidly growing cybercrimes can be attributed to the organizational inertia. Organizational inertia can be defined as formal organizations' tendency to resist internal changes to respond to external changes (Larsen & Lomi, 2002). Prior research indicates that established and matured organizations tend to stick with the traditional business model (Matsumoto, Ouchi, Watanabe, & Griffy-Brown, 2002; Watanabe & Tokumasu, 2003). Wall (2007) comments on police forces' failure to change organizational structures to deal with cybercrimes: "But, it is one thing to possess the technological capabilities and another to be able to utilize them, and there are a number of institutional obstacles to this task. The public police, like the other criminal justice agencies are deeply conservative institutions that have been moulded by time-honored traditions, and therefore do not respond readily to rapid change."

They are also facing a short supply of manpower to handle cybercrimes. A senior official of the Internet Crime Complaint Center (I3C) reported in November 2004 that the FBI has been unable to recruit and retain the best available IT talent. Based on his interviews with current and former agents Blitstein (2007) noted that "there are too few federal cyber-investigators, and that too little is done to retain detectives with advanced technical training."

According to the American Prosecutors Research Institute, the FBI's San Diego lab in 2005 had a 6-month backlog for forensic examinations (Blitstein, 2007). Moreover, cybercrimes are increasingly sophisticated and new forms and methods of such crimes are developing at an increasing rate. Law-enforcement agencies lack resources and have failed to catch up with technologies enabling such crimes. Grow and Bush (2005) note: "[C]ops don't have all the weapons they need to fight back [cyber-criminals]. They clearly lack the financial resources to match their adversaries' technical skills and global reach."

As is the case of any transnational crime, dealing with cybercrimes, especially those with international dimensions, is a resource intensive task (Walden, 2005). As noted above, cybercrime investigations are highly complex, as well as resource and expertise intensive. Many small countries thus do not investigate all reported cybercrimes. In Indonesia, for instance, only 15% of reported incidents are investigated. Law-enforcement agencies' lack of ability to solve cybercrimes reinforces cyber-criminal's confidence as well as victims' unwillingness to report such crimes (Fig. 2.1).

There is a lack of collaboration and coordination among various government agencies and between government and the private sector. Rivalries among various

law-enforcement agencies have hindered information dissemination (Joshi, 2009). The US president put the issue this way: "Indeed, when it comes to cybersecurity, federal agencies have overlapping missions and don't coordinate and communicate nearly as well as they should—with each other or with the private sector" (The New York Times, 2009). Given that up to 90% of all critical infrastructures in the United States are owned by private sectors, many cybercrimes cannot be solved without their help. An estimate suggests that 80% of global email traffic including the majority of the spam scams comes via the Webmail services of global providers such as AOL, MSN, and Yahoo. Law-enforcement agencies have expressed concern over service providers' unwillingness to cooperate in cybercrime investigations.

2.4.3 Cyber-Criminals

Cyber-criminals' unique profiles are significantly different from those of conventional criminals. Non-existence of cyber-criminals' database with law-enforcement agencies has also hampered the latter's ability to solve cybercrimes. In Russia, for instance, most hackers are young, highly educated, and work independently and thus do not fit the conventional Police profiles of criminals.

Cyber-criminals are also inventing various forms of markets. Some, for instance, have created a hybrid market consisting of online and offline market activities, with each having different roles. For instance, it was estimated that there were over 300 cashiers in Paris, who regularly steal payment-card details from their customers. Most of the stolen data were sold face-to-face between fraudsters who met online (Sutherland, 2008). Likewise, in first- and second-tier cities in India, data brokers and data merchants reportedly buy data from people working in offshoring companies (Aggarwal, 2009).

Evidence indicates that criminals' skill, intelligence, and experience co-vary positively with the odds of getting away with crimes. Some serious cyber-criminals are highly skillful and thus face very low odds of getting caught. For instance, in recent years, the Russian mafia has developed expertise in cybercrime (Giannangeli, 2008). Russian mafia hack rings are reportedly operated by former KGB agents (Bell, 2002). There is evidence that some less skillful criminals get help from experienced hackers and transnational organized crime groups thereby minimizing the probability of getting caught.

Increased success is making cyber-criminals more brash. Barnes (2004) notes: "There is, then, a justifiable perception among worm authors that only exceptionally careless authors get caught, and this causes authors to deeply discount the occasional law enforcement success." There is some evidence of cyber-criminals becoming disrespectful of law-enforcement agencies. A number of international hackers, for instance, do not even conceal their real identities and the origin of their mailings. What is more, many organized criminals have invested illegally earned incomes in new technologies and to globalize their operations making it further difficult to solve cybercrimes. Experts suggest that international collaboration among cyber-criminals will further grow in the future (Rush, Smith, Mbula, & Tang, 2009).

2.4.4 Cybercrime Victims

Cybercrimes are also among the most under-reported forms of criminality. Cybercrime victims' unwillingness to report such crimes to law-enforcement agencies further encourages cyber-criminals' behavior (Fig. 2.1). Some experts say that less than 10% of cybercrimes are reported (Bednarz, 2004). An FBI report released in January 2006 indicated that only 9% businesses reported cybercrimes to authorities (Regan, 2006). Likewise, another study conducted in the United Kingdom indicated that no formal complaint was made in 90% of online harassment cases (Birmingham Post, 2007). Similarly, a survey conducted among Australian businesses indicated that only 8% of respondents reported computer security breaches to police and most preferred to deal with them internally (Andrews, 2009).

Many victims are unwilling to report cybercrimes because they think going to law-enforcement does not stop an attack. Most Internet fraud victims are embarrassed to report that they have been victimized (Salu, 2004). Other factors contributing to low reporting rates could be the fear of losing customer trust; the damage in corporate credibility; and potential stock prices fall. Especially banks, financial institutions, and others businesses that deal with sensitive data are reluctant to turn over the investigation to the authorities. According to the *Seventh Annual Computer Crime and Security Survey* 70% of those not reporting cybercrimes cited negative publicity as a reason. Difficulties related to documentation and proofs further discourage businesses reporting cybercrimes. Finally, enterprises do not always know when their networks have been attacked, which results in under-reporting of cybercrimes (Regan, 2006). In some cases, it may also take cybercrime victims some time to realize that they have been victims (Wall, 1998; Richtel, 1999). Studies have found that terminologies such as "breaches" or "security incidents" were used to refer to cyberattacks, which meant that businesses were less likely to treat the attacks as cybercrimes (Andrews, 2009).

For many online transactions, the costs of enforcing a contract tend to be higher than the transaction's value (McDonald & Slawson, 2002). For instance, many online auctions are of low value, averaging under US $25 per item (Bauerly, 2009). For many defrauded buyers, the costs of pursuing a claim may outweigh the potential gains of a desired outcome.

Weakness of defense mechanisms co-varies positively with the likelihood of attack. While some weaknesses are technological, others are behavioral or perceptual in nature. The public's lack of education to recognize cybercrime has been a major challenge. Cyber-criminals take advantage of Internet users' ignorance (GAO Reports, 2007). Consider, for instance, phishing—acquisition of personal information fraudulently by tricking an Internet user. Experts say that the key to combat phishing lies in consumer's ability to distinguish between real and fraudulent e-mails. A study conducted by MailFrontier in the early 2003 indicated that 40% of people who read a fraudulent Citibank e-mail considered it as a real one (Salkever, 2003). Another study suggested that 60% of people clicked on phishing e-mails within the first hour of receiving them (Shiels, 2009).

An understanding of manipulative techniques used by various creatures to fool their enemies is of particular relevance for cybercrimes. In particular, a phenomenon proposed by Dawkins (1982) called the *rare enemy syndrome*, provides a helpful theoretical perspective for understanding how victims often fall to new unfamiliar baits or lure. The basic idea behind rare enemy syndrome is simple. The enemy's manipulation is so rare that evolutionary development has not yet progressed to the point that the victim has an effective counter poison (de Jong, 2001). Similar processes happen in the cyberworld. Many targets and victims lack a strong protection against cyber-criminals' novel manipulation tactics. Several examples provided by Schneier (2009), which have been used by fraudsters to frame their enemies, are rare manipulations. For instance, Google's anti-fraud systems detect and shut down advertisers if they attempt to inflate their commission by repeatedly clicking on their own AdSense ads. In response, some fraudsters built bots, which repeatedly clicked on their competitors' AdSense ads. To take another example, Google penalizes a website's search engine rankings if the site is linked with bad sites such as adult or gambling sites, blog spam, and link farms.[1] Some fraudsters spotted an opportunity to build link farms, where they posted blog comment spam to their competitors' sites (Schneier, 2009).

Beyond all that some criminal organizations are highly skillful in carrying out cybercrime activities. For instance, the Russian group, Rock Phish, which is estimated to be responsible for over half of all phishing sites worldwide, arguably has a " proven technical prowess" and sends "baited hooks written in perfect English—as well as French, German and Dutch" (Fong, 2008). Rock Phish uses "impeccable" counterfeit design of brand logos and styles of financial companies, retailers, and government agencies (Bulkeley, 2008; Fong, 2008). The Riga, Latvia-based company, Real Host, which was found to have 3.6 million PCs involved in a botnet called Zeus, was reported to have links to Rock Phish (The Baltic Times, 2009).

Similarly, a survey by the US National Cyber Security Alliance (NCSA) found that 61% of computers were infected with adware and spyware but only 8% of users knew that they were infected (Edelman, 2007). In another study conducted by McAfee and the NCSA, about half the respondents erroneously believed their computers were protected by anti-virus software and 71% never heard the word "botnet" (Claburn, 2008).

Moreover, some companies choose to negotiate with cyber-criminals by paying ransom. Estimates suggest that online gambling sites alone have paid millions of dollars to cyber-extortionists. To take one example, in September 2003, Antigua-based World Wide Tele-Sports (BetWWTS.com) paid ransoms as high as US $30,000 to cyber-extortionists after attacks to the company's networks resulted in customers not being able to place wagers estimated at US $5 million. Similarly, UK's National Hi-Tech Crime Unit (NHTCU) estimated extortion of "hundreds of thousands of pounds" paid by UK-based online bookmakers during October 2003–January 2004. For some companies, it is cheaper to pay up to online extortionists than to face an attack. For instance, estimates suggest that a few hours downtime on a peak time (e.g., Super Bowl weekend) costs online casinos up to US $1 million.

2.4.5 Inter-jurisdictional Issues

In the conventional world, most crimes are committed close to home. Criminals travel far only if there are sufficient incentives to leave known territory (van Koppen & Jansen, 1998). Some crimes such as kidnapping, attacking a bank are "attractive" enough to do so. These crimes require much more planning. Crimes in the digital world differ significantly on this dimension. Most cybercrimes, on the other hand, are conducted away from a criminal's home. For instance, in California, which accounted for most reported cyber-fraud cases in the United States in 2007, only in 18.3% of the cases, both the victim and perpetrator lived in the state (IC3, Internet Crime Complaint Center, 2007). A high proportion of cybercrime investigations thus have significant jurisdictional issues. In many cases, cybercrimes crossing borders slow down responses to such crimes.

National boundaries have thus created serious obstacles to law-enforcement agencies. Collaborations and cooperation among law-enforcement agencies in different jurisdictions are far from sufficient to solve cybercrimes. To take one example, although Russia has signed an agreement with the United States to help in investigating a number of crimes, cybercrimes are not among them (Lemos, 2001). In 2000, the FBI arrested two Russian hackers by luring them to the United States with job offers. FBI Agents handling the case later downloaded data from the two hackers' computers located in Chelyabinsk, Russia. In 2002, Russia filed hacking charges against the FBI arguing that it was illegal to download data from computers physically located in Russia. Similarly, in 2001, the US Department of Justice requested the help of Russian authorities but received no response. More recently, US law-enforcement officials have reported improving cooperation from Russian authorities. In 2005, it was reported that US law-enforcement officials received help from their Russian counterparts on about one out of six cybercrime-related requests (Bryan-Low, 2005).

The police's association with corruption and crime association with corruption in some countries further complicate the problems. Law-enforcement agencies from other countries tend to be reluctant to share information with them (Joshi, 2009).

There is also a high degree of international heterogeneity in cybercrime laws. The Council of Europe's Convention on cybercrime is, for example, the first international treaty on cybercrimes. As noted in Chap. 1, although 46 nations signed the treaty as of August 2009, only 26 members had ratified it by that time (COE, 2009). Likewise, industrialized countries are discussing about international cooperation to combat cybercrimes, many poor countries are not yet involved in the discussions. What is more, many countries have not yet enacted cybercrime laws. One estimate suggested that in 2000, more than 60% of Interpol members lacked the appropriate legislation to deal with cybercrimes (cnn.com, 2000). Likewise, as of May 2008, out of the 35 Organization of American States (OAS) member states, only 15 had "substantive cybercrime legislation in place" and only 12 had enacted procedural cybercrime legislation (Caribbean Press Releases, 2008). In April 2008, Bryan Tan,

director of Keystone Law Corporation, noted that in many countries in Asia, laws to deal with cybercrime are "either are very basic or have not been passed" (Ye, 2008).

A lack of cross-border collaboration in cybercrime investigations, international heterogeneity in cybercrime laws, and weakness and even non-existence of such laws in some countries have facilitated the globalization of cybercrimes. A report released by the UK government at its first national security strategy noted how the Internet is being used by spies, terrorists, and transnational organized criminal groups: "Organized crime groups are becoming more organized and professional and increasingly operate a portfolio approach, switching focus to wherever risk is lowest and profit highest" (Grant, 2008). It is, for instance, reported that some Japanese gangs hire Russian hackers to attack law-enforcement agencies' databases. Likewise, some Australian swindlers have established links with Russian and Malaysian organized crime networks to transfer stolen money from overseas banks they have cracked into (Foreign Policy, 2005).

2.5 A Cyber-Criminal's Cost–Benefit Calculus

In this section, we integrate key elements of the simplified framework representing the vicious circle discussed above and some additional characteristics of cybercrimes to examine a hacker's perceived cost–benefit structure. Following the economic approach, a cyber-criminal weighs benefits and costs to make decision about engaging in a crime (Becker, 1968; also see Probasco, Clark, & Davis, 1995). A cybercrime is committed if

$$M_{\mathrm{b}} + P_{\mathrm{b}} > O_{\mathrm{cp}} + O_{\mathrm{cm}} P_{\mathrm{a}} P_{\mathrm{c}} \tag{2.1}$$

where

M_{b} = The monetary benefits of committing the crime;
P_{b} = The psychic benefit of committing the crime;
O_{cm} = Monetary opportunity costs of conviction;
O_{cp} = Psychic costs of committing a cybercrime;
P_{a} = The probability of arrest;
P_{c} = The probability of conviction.

The product term in the right side: $O_{\mathrm{cm}}\ P_{\mathrm{a}}\ P_{\mathrm{c}}$ in (2.1) is also referred as the expected penalty effect. Equation (2.1) captures costs and benefits associated with macro- and micro-level factors such as arrest, stigma, and illegal earnings, which are found to influence an individuals' engagement in a crime (Aguilar-Millan, Foltz, Jackson, & Oberg, 2008; McCarthy, 2002).

2.5.1 The Benefit Side

2.5.1.1 Monetary Benefits

The cybercrime landscape is rapidly changing in terms of hackers' monetary motives. A Russian hacker employed as a security expert noted: "There is more of a financial incentive now for hackers and crackers as well as for virus writers to write for money and not just for glory or some political motive" (Blau, 2004). For instance, IT graduates with legitimate job in Romania earn about US $400 per month compared with several thousand per month in the cybercrime economy. A "security exploiter" can earn 10 times as much a security researcher (Claburn, 2008). Terri Forslof of TippingPoint Technologies put the issue this way: "Over a ten year period hack for fun and hack for fame has become hack for profit" (Webwire, 2008).

2.5.1.2 Psychic Benefit (P_b)

The potential psychological benefits provide strong incentives for some individuals to engage in cybercrimes. Psychological benefits can be better explained in terms of intrinsic motivations. For instance, maverick hackers testing their skills and looking for fun act for purely psychological rather than monetary benefits. As noted in Chap. 1, acting on the basis of principle is also a form of intrinsic motivation. First, the respect of one's peer hackers acts as a source of psychological benefit for some hackers.

Second, a feeling of vindication against symbolic enemy also provides psychological benefits to hackers. Many ideological hackings fall in this category. An organization becomes a hacking unit's symbolic foe for many reasons. In addition to nationalism and religion, hackers' interests are also framed by fight against global capitalism. Such hackers are likely to attack networks of big multinationals.

Government backed cyber-wars in some countries also fall in this category. A number of such wars are fought for intangible goals such as dominance and prestige rather than material goals.

2.5.2 The Cost Side

2.5.2.1 Psychic (Psychological) Costs of Committing a Cybercrime (O_{cp})

Psychological costs are intangible, but can, however, be considered as costs. These costs are associated with the psychological and mental energy needed in committing cybercrimes. They result from the fear or apprehension of punishment, guilt, etc. A potential criminal's taste or distaste for crime, and moral values also influence O_{cp} (Ehrlich, 1996). Some scholars argue that moral values, which are associated with social costs, are more important than monetary opportunity costs of conviction (O_{cm}) related to imprisonment and loss of wages (Nagin, 1998).

An important question is: Do cyber-criminals have a feeling of guilt or remorse after cracking into a victim's computer? Experts argue that most of those who make

unethical uses of computer networks arguably do not really perceive the ethical implications of their actions (Kallman & Grillo, 1996). Put differently, the novelty of the technology; a lack of previously developed mechanisms and established codes, policies, and procedures; and non-existence of an easily identifiable victims in many cases (Phukan, 2002) are likely to lead to much less in cybercrimes guilt compared to conventional crimes. An official of India's Cyber Crime Investigation Cell (CCIC) noted that many young people in the country have committed cybercrimes for fun "without actually realising the gravity of their actions" (cf. Sawant, 2009).

Some argue that widely shared norms, values, and beliefs of Napster users contradicted the existing copyright laws and legitimized file-swapping services provided by the company (Webb, Tihanyi, Ireland, & Sirmon, 2009). Napster users did not feel guilty about their file sharing activities.

In the medical world, for instance, there arguably is a lack of clear guidelines as to what constitutes an unethical or unprofessional online conduct for physicians (Lagu, Kaufman, & Asch, 2008; Thompson et al., 2008). In a survey conducted among US medical schools to assess professionalism in medical students' online posts, 60% of the respondents reported incidents of their students posting online content that were unprofessional and 13% violated patient confidentiality (Chretien, Ryan, Chretien, & Kind, 2009). The study also found that only few schools had policies to deal with such violations. Illegal or questionable activities such as violation of patient confidentiality are taking place in the cyberspace without the violators' intent.

Likewise, it is argued that online child pornography "reduces the social stigma" as individuals do not have to go to stores, which eliminates the chance of meeting other criminals engaged in child pornography (Shelley, 1998). Others note that "consumer indifference to the stigma of intellectual property theft" has contributed to such crimes (McIllwain, 2005, p. 35). This is contrary to most conventional crimes such as drug dealings, which are characterized by social stigma (Whitlock, 1979; Harler & Fox, 1992).

Research on crimes in the conventional world has indicated that socio-cultural practices and political and economic systems are tightly linked to crimes. We thus hypothesize that the feeling of guilt is not equally pervasive across hackers in different socio-cultural backgrounds. Put differently, the psychological cost of a cybercrime is a function of a cyber-criminal's socio-cultural background.

2.5.2.2 Monetary Opportunity Costs of Conviction (O_{cm})

It is the foregone monetary income incurred by serving out a criminal sentence. For instance, if a hacker is sentenced to a 3-year prison term, and if he/she could legally earn US $20,000 per year, the sentence would cost US $60,000. In recent years, many countries have enacted stricter laws against cybercrimes, which have increased the opportunity costs of conviction. Nonetheless, many countries have no laws enacted to fight cybercrimes, which means a very low or no opportunity cost of conviction. To take one example, when a Philippino hacker launched the "Love Letter" virus in 2000, estimated loss of damage in the United States was in the range

of US $4–15 billion. But the US government could not do anything to prosecute the hacker or to recover the damages because at that time the Philippines had no laws prohibiting such crimes (Adams, 2001). In sum, costs to criminals of their deviant behaviors on the Internet have been remarkably low (Shelley, 1998).

As noted above, crime rates are related to the lack of economic opportunities. Additionally, unlike conventional crimes, most cybercrimes are skill-intensive. The most relevant issues thus concern expectations from education. Note that if societal expectations related to educational attainment are unmet, people are likely to engage in crimes (McCleary, 2008).

Cybercrimes are thus likely to originate if the legitimate IT industry is too small to absorb available talents. Consistent with history and theory, serious cyber-criminals tend to be from countries that emphasize on physics, mathematics, and computer science educations, but lack high-paying legitimate IT jobs (Sullivan, 2007).

Speaking of emphasis on mathematics in Romania, a scientist in Bucharest put the issue this way: "The respect for math is inside every family, even simple families, who are very proud to say their children are good at mathematics" (Wylie, 2007). In the former Soviet Union economies, computer specialists gained experience in "disassembling, examining and hacking American systems to see how they worked in order to make them functional on Soviet systems" (Serio & Gorkin, 2003).

2.5.2.3 The Probability of Arrests (P_a) and the Probability of Conviction (P_c)

As discussed above, only a small proportion of cybercrimes are reported. For small transactions in Internet auctions, for instance, buyers often avoid criticizing sellers for their opportunistic behavior because they are afraid of possible reprisal from the seller (Clemons, 2007). Because of concerns related to retaliation by the seller, buyer satisfaction statistics published by websites tend to be higher than the actual satisfaction level (Dellarocas & Wood, 2008).

Among reported crimes, arrest rates are vanishingly small. Arrest entails identifying the pool of potential suspects and narrowing the pool by eliminating innocents. The structure of cybercrimes discussed in the previous section makes it difficult to identify the pool of potential suspects. The FBI estimates that the probability of cyber-criminal's being caught is less than 1 in 20,000 (Gabrys, 2002). Another estimate suggests that the proportion of identity thefts (most of which employ the Internet) that are even investigated is estimated to be fewer than 1 in 700 (Boal, 2005).

The low probability of arrests can also be attributed to the huge global e-marketplace with a large number of vendors (Webb et al., 2009). This means that most informal and underground economy entrepreneurs that operate online are invisible to law-enforcement agencies (Zimmerman, 2006).

In order to minimize the probability that they are caught, some cyber-criminals avoid victimizing people in the country where they live. Benjamin Edelman of Harvard Business School noted: "By declining to hurt people in their own country, they discourage law enforcement from pursuing them" (cf. Messmer, 2009).

The conviction phase of a cybercrime is equally complex. Difficulties related to documentation and proof compound the problems at this phase (Casey, 2004). The newness of cybercrimes has also presented a challenge to the court system. For small cases, it is difficult to find an attorney in who takes cyber-fraud cases. Experts also say that explaining Internet-related crimes to judges is difficult. Estimates suggest that if a cyber-criminal is caught, the probability that the criminal would be convicted is 1 in 22,000 (Gabrys, 2002).

The situation is worse in developing countries. Mohammad Khairuddin Abdullah, Malaysia's HeiTech Padu Berhad's director noted: "As long as they [cyber-criminals] are within the country, the criminals can be brought to court, but you'll be lucky if you can find the judge, who can write the warrant and understands the issue. Even though cyberlaws are in place, you need to have people who are able to apply the laws, as most cybercrime cases will get cold in just 24 hours" (cf. Ismail, 2008).

2.6 Concluding Comments

The above discussion indicates that there is a temptation to engage in opportunistic behavior in the cyberspace. Compared to the physical world, the detection of opportunism is difficult in the cyberworld. Some also commit a cybercrime due to ignorance.

The concept of manifest and latent functions (Merton, 1968) can be very helpful in understanding the behaviors of some cyber-criminals. Manifest functions are explicitly stated and understood by the participants in the relevant action and the consequences can be observed or expected. Latent functions, on the other hand, are those that are not explicitly stated by the people involved (Merton, 1968). In the Napster example above, for instance, the manifest posture may be the users' argument that free file sharing services provided by Napster are consistent with their norms, values, and beliefs. Below the surface deeply ingrained, however, may be a powerful economic temptation of free music (latent function).

In the absence of appropriate measures, the elements of the vicious circle reinforce each other and lead to public distrust of law-enforcement agencies and increased confidence of cyber-criminals, which results in more and serious cybercrimes. A Global Security Survey conducted by *Deloitte Touche Tohmatsu* in 2003, for instance, found that respondent companies spent 6% of their IT budgets on security. Nevertheless, cyberattacks are increasing rapidly.

Where should we start to break the vicious circle of cybercrime and to alter the cost/benefit calculus associated with committing cybercrimes? There is no pure technological solution for security-related problems involving technologies. Micro- and macro-level measures combining technological and non-technological fixes are thus needed to combat cybercrimes.

In the conventional world, individuals and organizations can reduce the probability of becoming victims and their losses by buying insurance policies or by using

safety measures such as anti-burglar systems and safety deposit boxes, or by living in safe neighborhoods (Ehrlich & Becker, 1972). Not all of these have their equivalents in the cyberworld. As noted above, certain "land use" types act as crime generators (McCord et al., 2007; Swope, 2001). While formal control mechanisms such as "hot spots policing" can be used to deal with land uses associated with high crime rates (Weisburd, Bushway, Lum, & Yang, 2004), there are no equivalents of such mechanisms in the cyberspace.

At the macro-level, development of national technological and manpower capabilities; enactment of new laws; a higher level of industry-government collaborations; and international coordination are critical for combating this new form of crime. Investment in the skills of law-enforcement authorities is likely to enhance national capabilities to fight cybercrimes and thus increasing the probability of arrest and conviction. Like most other criminals (Becker, 1995), we can assume that cyber criminals are risk takers, not risk avoiders. Measures taken so far have mainly emphasized on increasing penalty rather than on increasing the probabilities of arrest and conviction. This is arguably because law-enforcement agencies have been unable to catch up technologically with cyber-criminals (Downes, 2007). It is suggested that private citizens may be especially effective at combating cybercrimes as the costs are much less for individuals and private firms to protect their electronic records than those for the government to identify and prosecute criminals (Katyal, 2001; Mikos, 2006).

Note

1. A link farm is "any group of web sites that all hyperlink to every other site in the group" (Wikipedia definition of Link farm, http://en.wikipedia.org/wiki/Link_farm, accessed 19 October 2009).

References

Adams, J. (2001, May/June). Virtual defense. *Foreign Affairs,* 98–112.

Aggarwal, V. (2009). Lead: Cyber crime's rampant, Express Computer, 03 August 2009. http://www.expresscomputeronline.com/20090803/market01.shtml. Accessed 1 October 2009.

Aguilar-Millan, S., Foltz, J. E., Jackson, J., & Oberg, A. (2008). The globalization of crime. *Futurist, 42*(6), 41–50.

Alexander, D. (2002, June). Policing and the global paradox. *FBI Law Enforcement Bulletin, 71*(6), 6–13, 00145688.

Anderson, R., & Schneier, B. (2005). Counterpane internet security guest editors introduction: Economics of information security. *IEEE Security & Privacy, 3*(1), 12–13.

Andrews, L. (2009, June 9) Online scams go unreported and unpunished. *Cybercriminals beating the law Canberra Times (Australia) SECTION: A*, p. 5.

Barnes, D. A. (2004). Note, Deworming the Internet, 83 TEX. L. REV. 279, 322–329.

Bauerly, R. J. (2009). Online auction fraud and ebay. *Marketing Management Journal, 19*(1), 133–143.

Becker, G. (1968). Crime and punishment: An economic approach. *Journal of Political Economy, 76*(2), 169–217.

Becker, G. S. (1995, Fall). The economics of crime. *Cross Sections*, 8–15. http://www.rich.frb.org/pubs/cross/crime/crime.pdf. Accessed 1 October 2006.

Bednarz, A. (2004). Profiling cybercriminals: A promising but immature science, Network World, November 29. http://www.nwfusion.com/supp/2004/cybercrime/112904profile.html?page=2. Accessed 1 October 2005.

Bell, R. E. (2002). The prosecution of computer crime. *Journal of Financial Crime, 9*(4), 308–325.

Birmingham Post. (2007). Politics: Cybercrime victim every 10 seconds, 4.

Blau, J. (2004). Russia - a happy haven for hackers, 26 May 2004. http://www.computerweekly.com/Article130839.htm. Accessed 1 October 2005.

Blitstein, R. (2007, November 14). Cybercops: US targets terrorists as online thieves run amok. *San Jose Mercury News*.

Boal, M. (2005). Being Bill Gates Steven Spielberg, Martha Stewart, George Soros Charles Schwab: How the Most Brazen Identity Thief In US Almost Get Away With It. *Readers Digest*, 161–173.

Bottoms, A. E., & Wiles, P. (2002). Environmental criminology. *Oxford Handbook of Criminology*, 620–656.

Brenner, S. W. (2004). Toward a criminal law for cyberspace: A new model of law enforcement? *30 Rutgers Computer and Technology Law Journal, 30*, 1–9.

Browning, C. R, Feinberg, S. L., & Dietz, R. D. (2004). The paradox of social organization: Networks, collective efficacy, and violent crime in urban neighborhoods. *Social Forces, 83*(2), 503–534.

Bryan-Low, C. (2005, July 13). Fraud Inc.: As identity theft moves online, crime rings mimic big business; Russian-led Carderplanet steals account numbers; Mr. Havard hits ATMs; 'Common Punk' to 'Capo'. *Wall Street Journal*, A.1.

Bulkeley, W. M. (2008). Quiz; Tech IQ: How well do you know...the digital world. *Wall Street Journal*, R.14.

Caribbean Press Releases. (2008). Trinidad and Tobago to Host OAS Cyber-Crime Workshop, 13 May 2008. http://www.caribbeanpressreleases.com/articles/3236/1/Trinidad-and-Tobago-To-Host-OAS-Cyber-Crime-Workshop/Page1.html. Accessed 1 October 2009.

Casey, E. (2004). *Digital evidence and computer crime.* Cambridge: Academic Press.

Chretien, K. C., Ryan, G. S., Chretien, J. P., & Kind, T. (2009). Online posting of unprofessional content by medical students. *JAMA, 302*(12), 1309–1315.

Claburn, T. (2008). The Cybercrime Economy, April 9, 2008. http://www.informationweek.com/blog/main/archives/2008/04/the_cyber_crime.html. Accessed 1 October 2009.

Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. In M. Tonry & N. Morris (Eds.), *Crime and justice: An annual review of research* (p. 14). Chicago: University of Chicago Press.

Clarke, R. V. (1995). Situational crime prevention. In M. Tonry & D. P. Farrington (Eds.), *Building a safer society. Strategic approaches to crime* (pp. 91–150). University of Chicago Press.

Clarke, R. V. (1999). Hot products: Understanding, anticipating, and reducing demand for stolen goods. *Police Research Paper 112*. London: Home Office.

Clemons, E. K. (2007). An empirical investigation of third-party seller rating systems in e-commerce: The case of buySAFE. *Journal of Management Information Systems, 24*(2), 43–71.

CNN.com. (2000, July 26). Many countries said to lack computer crime laws. CNN.com. http://www.cnn.com/2000/TECH/computing/07/26/crime.internet.reut.

COE. (2009). Convention on Cybercrime: CETS No.:185. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG. Accessed 1 October 2009.

Dawkins, R. (1982). *The extended phenotype.* Oxford University Press.

de Jong, W. M. (2001). Manipulative tactics in budgetary games: The art and craft of getting the money you don't deserve. *Knowledge, Technology & Policy, Spring, 14*(1), 50–66.

Deas, D., & Thomas, S. (2002). Comorbid psychiatric factors contributing to adolescent alcohol and other drug use. *Alcohol Research and Health, 26*, 116–121.

Dellarocas, C., & Wood, C. A. (2008). The sound of silence in online feedback: Estimating trading risks in the presence of reporting bias. *Management Science, 54*(3), 460–476.
Downes, L. (2007, March 6). Cybercrime treaty: What it means to you. *Baseline.com*.
Edelman, B. (2007, January 25). Why I can never agree with adware and spyware. *The Guardian*.
Ehrlich, I. (1996). Crime, punishment, and the market for offenses. *Journal of Economic Perspectives, 10*(1), 43–67.
Ehrlich, I., & Becker, G. (1972). Market insurance, serf-insurance and serf-protection. *Journal of Political Economy, 80*(4), 623–648.
Fest, G. (2005, September 1). Offshoring: Feds take fresh look at India BPOs; Major theft has raised more than a few eyebrows. *Bank Technology News, 18*(9), 1.
Fong, C. (2008, May 8). Fighting the agents of organized cybercrime. *CNN.com*.
Foreign Policy. (2005, March/April). Caught in the net: Australian teens, 92.
Gabrys, E. (2002). The international dimensions of cyber-crime, Part 1. *Information Systems Security, 11*(4), 21–32.
GAO Reports. (2007). Public and private entities face challenges in addressing cyber threats, RPT-NUMBER: GAO-07-705.
Giannangeli, M. (2008, June 8). Are we ready for Russian Mafia's crime revolution? *Sunday Express*, Scottish Edition, 3.
Glaeser, E. L., & Sacerdote, B. (1999). Why is there more crime in cities? *The Journal of Political Economy, 107*(6), Part 2, 225–258.
Grant, I. (2008, March 19). The UK's dependence on the internet is putting more than half of its economy at risk, says the government. *ComputerWeekly.com*. http://www.computerweekly.com/Articles/2008/03/19/229932/uk-government-warns-of-economys-reliance-on-internet.htm. Accessed 1 October 2009.
Greenberg, A. (2007). The top countries for cybercrime, Forbes.com. http://www.forbes.com/2007/07/13/cybercrime-world-regions-tech-cx_ag_0716cybercrime.html. Accessed 1 October 2008.
Grow, B., & Bush, J. (2005, May 30). Hacker hunters. *Business Week*, 74.
Harler, C., & Fox, B. (1992). Network security communications news. *Nokomis, 29*(1), 20–24.
Hawkins, J. D., Herrenkohl, T., Farrington, D. P., Brewer, D., Catalano, R., & Harachi, T. W. (1998). A review of predictors of youth violence. In R. Loeber & D. P. Harrington (Eds.), *Serious & violent juvenile offenders: Risk factors and successful interventions* (pp. 106–146). Thousand Oaks, CA: Sage.
Hirschauer, N., & Musshoff, O. (2007). A game-theoretic approach to behavioral food risks: The case of grain producers. *Food Policy, 32*(2), 246–265.
Internet Crime Complaint Center. (2007). Internet Crime Report, 2007. http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf. Accessed 1 October 2008.
Ismail, I. (2008, February 18). Understanding cybercriminals. *New Straits Times* (Malaysia), 12.
Jones, B. R. (2007). Comment: Virtual neighborhood watch: Open source software and community policing against cybercrime. *Journal of Criminal Law & Criminology, 97*(2), 601–629.
Joshi, V. (2009, October 12). Officials: Criminals cooperate better than police. *The Boston Globe.* http://www.boston.com/news/world/asia/articles/2009/10/12/officials_criminals_cooperate_better_than_police/ Accessed 27 October 2009.
Kallman, E. A., & Grillo, J. P. (1996). *Ethical decision making and information technology*, 2e. New York: McGraw Hill.
Katyal, N. K. (2001). Criminal law in cyberspace. *University of Pennsylvania Law Review, 149*(4), 1003–1114.
Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management, 11*(4), 541–562.
Kupersmidt, J. B., Griesler, P. C., DeRosier, M. E., Patterson, C. J., & Davis, P. W. (1995). Childhood aggression and peer relations in the context of family and neighborhood factors. *Child Development, 66*, 360–375.
Lagu, T., Kaufman, E. J., & Asch, D. A. (2008). Armstrong, K. Content of weblogs written by health professionals. *Journal of General Internal Medicine, 23*(10), 1642–1646.

Larkin, E. (2009). Organized crime moves into data theft. *PC World, 27*(7), 33–34.
Larsen, E., & Lomi, A. (2002). Representing change: A system model of organizational inertia and capabilities as dynamic accumulation processes. *Simulation Model Practice and Theory, 10*(5), 271–296.
Lemos, R. (2001, May 1). FBI "hack" raises global security concerns. *CNet News*. http://news.com.com/2100-1001-950719.html
Lianos, M., & Douglas, M. (2000). Dangerization and the end of deviance. *The British Journal of Criminology, 40*(2), 261–278.
Matsumoto, K., Ouchi, N., Watanabe, C., & Griffy-Brown, C. (2002). Optimal timing of the development of innovative goods with generation. *Technovation, 22*(3), 175–185.
McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology, 28*, 417–442.
McCleary, R. M. (2008). Religion and economic development. *Policy Review, 148*, 45–57.
McCord, E. S., Ratcliffe, J. H., Garcia, R. M., & Taylor, R. B. (2007). Nonresidential crime attractors and generators elevate perceived neighborhood crime and incivilities. *Journal of Research in Crime and Delinquency, 44*(3), 295–320.
McDonald, C. G., Slawson, C. V., Jr. (2002, October). Reputation in an internet auction market. *Economic Inquiry, 40*(4), 633–650.
McIllwain, J. S. (2005). Intellectual property theft and organized crime: The case of film piracy. *Trends in Organized Crime, 8*(4), 15–39.
Merton, R. (1968). *Social theory and social structure*. New York: Free Press.
Messmer, E. (2009, October 6). Malware flea market pays hackers to hijack PCs. *The Industry Standard*. http://www.thestandard.com/news/2009/10/06/malware-flea-market-pays-hackers-hijack-pcs. Accessed 14 October 2009.
Mikos, R. A. (2006). "Eggshell" victims, private precautions, and the societal benefits of shifting crime. *Michigan Law Review, 105*(2), 307–351.
Miller, N. (2008). Casting a wide net for cyber crimes. *The Age.* Melbourne, Australia.
Morgan, P. M. (2005). Taking the long view of deterrence. *Journal of Strategic Studies, 28*(5), 751–763.
Nagin, D. S. (1998). Criminal deterrence–research at the outset of the twenty-first century. In M. Tondry (Ed.), *Crime and justice: A review of research, 23*, 1–42.
Oberwittler, D. (2007). The effects of neighborhood poverty on adolescent problem behaviors: A multi-level analysis differentiated by gender and ethnicity. *Housing Studies, 22*, 781–803.
Phukan, S. (2002, June). IT ethics in the Internet age: New dimensions. *InSITE*. http://proceedings.informingscience.org/IS2002Proceedings/papers/phuka037iteth.pdf
Probasco, J., Clark, R., & Davis, W. L. (1995). A human capital perspective on criminal careers. *Journal of Applied Business Research, 11*(3), 58–64.
Regan, K. (2006). FBI: Cybercrime causes financial pain for many businesses. *TechNewsWorld*. http://www.technewsworld.com/story/48417.html. Accessed 1 October 2009.
Richtel, M. (1999, June 2). Federal cybercrime unit hunts for hackers. *New York Times*, A16.
Rush, H., Smith, C., Mbula, E. K., & Tang, P. (2009). Crime online: Cybercrime and illegal innovation, Research report: July 2009, CENTRIM, University of Brighton. http://eprints.brighton.ac.uk/5800/01/Crime_Online.pdf. Accessed 1 October 2009.
Salkever, A. (2003, October 21). "Phishing" is foul on the Net. *Business Week Online*. http://www.businessweek.com/technology/content/oct2003/tc20031021_8711_tc047.htm. Accessed 1 October 2004.
Salu, A. O. (2004). Online crimes and advance fee fraud in nigeria – Are available legal remedies adequate? *Journal of Money Laundering Control, 8*(2), 159–167.
Sawant, N. (2009, October 5). Virtually speaking, crime in the city on an upward spiral. *The Times of India*. http://timesofindia.indiatimes.com/news/city/mumbai/Virtually-speaking-crime-in-the-city-on-an-upward-spiral/articleshow/5087668.cms.

Schneier, B. (2009, October 15). Why framing your enemies is now virtually child's play. *The Guardian*. http://www.guardian.co.uk/technology/2009/oct/15/bruce-schneier-internet-security.

Schuerman, L., & Kobrin, S. (1986). Community careers in crime. In A. J. Reiss, Jr. & M. Tonry (Eds.), *Communities and crime* (pp. 67–100). Chicago: University of Chicago Press.

Serio, J. D., & Gorkin, A. (2003). Changing lenses: Striving for sharper focus on the nature of the 'Russian Mafia' and its impact on the computer realm. *International Review of Law*, *Computers and Technology, 17*(2), 191–202.

Shelley, L. I. (1998). Crime and corruption in the digital age. *Journal of International Affairs, 51*(2), 605–620.

Shiels, M. (2009, October 1). US urges 'cyber hygiene' effort, BBC News. http://news.bbc.co.uk/2/hi/technology/8279867.stm. Accessed 1 October 2009.

Sullivan, B. (2007). Who's Behind Criminal Bot Networks?, April 10. http://redtape.msnbc.com/2007/04/whos_behind_cri.html. Accessed 1 October 2008.

Sutherland, B. (2008). The Rise of Black Market Data; Criminals who steal personal data often don't exploit it. Instead, they put it up for sale on one of the many vibrant online markets. *Newsweek (International ed.), 152*(24).

Swartz, J. (2004, October 21). Crooks slither into Net's shady nooks and crannies crime explodes as legions of strong-arm thugs, sneaky thieves log on. *USA Today*. www.usatoday.com/printedition/money/20041021/cybercrimecover.art.htm. Accessed 1 October 2005.

Swope, R. E. (2001). Criminal theory on the street: Analyzing why offenses take place. *Law and Order, 49*(6), 121–128.

Taylor, R. B., Koons, B., Kurtz, E., Greene, J., & Perkins, D. (1995). Streetblocks with more nonresidential landuse have more physical deterioration: Evidence from baltimore and philadelphia. *Urban Affairs Review, 30*, 120–136.

The Baltic Times. (2009, August 4). Cyber criminals found in Latvia. http://www.baltictimes.com/news/articles/23283. Accessed 1 October 2009.

The New York Times. (2009). Text: Obama's Remarks on Cyber-Security. http://www.nytimes.com/2009/05/29/us/politics/29obama.text.html?pagewanted=2. Accessed 1 October 2009.

Thompson, L. A., Dawson, K., & Ferdig, R., Black, E., Boyer, J., & Coutts, J. (2008). The intersection of online social networking with medical professionalism. *Journal of General Internal Medicine, 23*(7), 954–957.

Toshiya, K., Susumu, F., & Noriyasu, Y. (2003). A validation on Pareto optimality of Walrasian virtual market. *IEIC Technical Report (Institute of Electronics, Information and Communication Engineers), 102*(613), 13–18.

Valdez, A., Kaplan, C. D., & Curtis, R. L. (2007). Aggressive crime, alcohol and drug use, and concentrated poverty in 24 US urban areas. *American Journal of Drug and Alcohol Abuse, 33*, 595–603.

Van Koppen, P. J., & Jansen, R. W. J. (1998). The road to the robbery: Travel patterns in commercial robberies. *The British Journal of Criminology, 38*(2), 230–246.

Walden, I. (2005). Crime and security in cyberspace. *Cambridge Review of International Affairs, 18*(1), 51–68.

Walker, C. (2004, June). *Russian Mafia extorts gambling websites.* http://www.americanmafia.com/cgi/clickcount.pl?url=www.americanmafia.com/Feature_Articles_270.html. Accessed 1 October 2005.

Wall, D. S. (1998). Catching cybercriminals: Policing the internet. *International Review of Law, 12*(2), 201–218.

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice & Research, 8*(2), 183–205.

Warren, P. (2007, November 15). Hunt for Russia's web criminals. The Russian Business Network – Which some blame for 60% of all internet crime – Appears to have gone to ground. *The Guardian*. http://www.guardian.co.uk/technology/2007/nov/15/news.crime. Accessed 1 October 2009.

Watanabe, C., & Tokumasu, S. (2003). Optimal timing of R&D for effective utilization of potential resources in innovation. *Journal of Advances in Management Research, 1*(1), 11–27.

Webb, J. W., Tihanyi, L., Ireland, R. D., & Sirmon, D. G. (2009). You say illegal, I say legitimate: Entrepreneurship in the informal economy. *Academy of Management Review, 34*(3), 492–510.

Webwire. (2008, June 25). First told of Chinese PC hijack explosion. http://www.webwire.com/ViewPressRel.asp?aId=68776. Accessed 1 October 2009.

Weisburd, D., Bushway, S., Lum, C., & Yang, S. M. (2004). Trajectories of crime at places: A longitudinal study of street segments in the city of Seattle. *Criminology, 42*(2), 283–320.

Whitlock, R. A. (1979). Witch crazes and drug crazes: A contribution to the social pathology of credulity and scapegoating. *Australian Journal of Social, 14*(1), 43–54.

Wilson, W. J. (1987). *The truly disadvantaged*. Chicago: University of Chicago Press.

Wylie, I. (2007, December 26). Internet; Romania home base for EBay scammers; The auction website has dispatched its own cyber-sleuth to help police crack fraud rings. *Los Angeles Times*, C.1.

Ye, V. (2008, April 15). Asia hindered by lack of cybercrime laws. *businessweek.com*. http://www.businessweek.com/globalbiz/content/apr2008/gb20080415_220378.htm?campaign_id=rss_daily. Accessed 12 October 2009.

Zimmerman, A. (2006, October 25). Creative crooks: As shoplifters use high-tech scams, retail losses rise; Theft rings alter bar codes, work gift-card swindles; Fencing the loot online; Target snares a Lego bandit. *Wall Street Journal*, A1.

http://www.springer.com/978-3-642-11521-9

The Global Cybercrime Industry
Economic, Institutional and Strategic Perspectives
Kshetri, N.
2010, XXI, 252 p., Hardcover
ISBN: 978-3-642-11521-9