Chapter 8
Structure of Cybercrime in Developing Economies

At the moment, cybercriminals see Africa as a safe haven to operate illegally with impunity (Hamadoun Toure, secretary-general of the ITU, cf. Africa News, 2007).

"Even in 2001, I was meeting judges who thought cyber-crime was someone stealing a computer" (eBay's Albena Spasova, who worked in promoting law reform in Moldova and Bulgaria, cf. Wylie, 2007).

Abstract Cybercrime's footprints across the developing world are getting bigger. In this chapter, we examine the structure of cybercrimes in developing economies. Specifically, we analyze economic and institutional factors facing cyber-criminals and potential victims in the developing world. The findings indicate that formal institutions related to cybercrimes are thin and dysfunctional in a developing economy; a cyber-criminal is less likely to be stigmatized in a developing economy than in a developed economy; and organizations' and individuals' technological and behavioral defense mechanisms are likely to be weaker in a developing economy than in a developed economy.

8.1 Introduction

With the Internet's rapid diffusion and digitization of economic activities, cybercrime has gained momentum in developing economies. Many developing countries are top cybercrime sources (see Tables 7.1, 7.2, and 8.1). Businesses and consumers in developing countries have also become victims of domestic as well as international cybercrimes. Since most of the growth in the global PC market in the near future is likely to be from the developing countries (Miller, 2008), cybercrimes in these countries deserve special attention. Analyzing the trend of cybercrime activities across countries, analysts have suggested 10–15% Internet penetration as the threshold level for the generation of significant hacking activities (Reilly, 2007). It is important to note that Internet penetrations in many developing countries have reached this level.

N. Kshetri, *The Global Cybercrime Industry*, DOI 10.1007/978-3-642-11522-6_8,

Table 8.1 Cybercrime situations in selected developing countries

Country	Internet users (% of population 2005)	International cybercrimes originated	Cybercrime victims
Brazil	19.5	2003: World’s 10 most active cyber-criminal groups were based in Brazil (Smith, 2003) 2004: Two-thirds of the world’s pedophile pages were hosted in Brazil (Leyden, 2004)	• Online financial fraud exceeds the loss through bank robberies (Leyden, 2004) • 2006: Over half of firms with Internet access were virus-attack victims (ITU, 2007)
China	8.5	According to a Symantec report, 5% of the world’s malware-infected computers were in Beijing in 2006 Overtook the United States in the number of malware hosts	• 2007: Attacks on PC rose by 2125% (WEBWIRE, 2008) • 2004: 58% of large government, educational, and commercial entities experienced cybercrimes (US, Commercial Service, 2004)
India	5.5	Data frauds have been reported in call centers in Pune, Hyderabad, Bangalore, and Gurgaon (tribuneindia.com 2005; Schwartz 2005, Fest 2005)	• The Cyber Crime Investigation Cell (CCIC) recorded 159 cases in 2006, 344 in 2007, 775 in 2008, 718 in the first 8 months of 2009 (Sawant, 2009) • 2006: 565 people arrested on cybercrime-related charges (Expressindia, 2008) • Cybercrime cases increased by 200% in Delhi in 2007 and credit card fraud in the city went up by 500% (hindu.com, 2008) • August 2007: Bank of India’s network was attacked with Mpack-created virus, which forwarded financial data to Russian Business Network (RBN) (Krebs, 2007) • Mid-2007–mid-2008: 10 ministry websites were attacked (Raghav, 2008) • During September 2007–September 2009, Indian banks experienced over 1,000 unique phishing attacks (Indiatimes, 2009) • Cybercrime cases in Mumbai: 142 in 2005, to 159 in 2006, 344 in 2007, and 775 in 2008 (Hindustan Times, 2009)

Table 8.1 (continued)

Country	Internet users (% of population 2005)	International cybercrimes originated	Cybercrime victims
Panama	6.4	Over 100 portals with child pornography content hosted in 2007 (Frayssine, 2007)	
Poland	26.2	An ISP produced 5% of the world's spam in 2007 (Greenberg, 2007)	
Romania	20.8	Cybercrime industry is bigger than drug smuggling or human trafficking industries (Wylie, 2007)	
Russian Federation	15.2	Russians have a profitable niche in Internet dating fraud (Wylie, 2007)	• 2005: About 12,000 computer crimes were registered (BBC Monitoring International Reports, 2006)
South Africa	10.9		• Cybercrime is the fastest growing white collar crime • 2007: PricewaterhouseCoopers' biennial Global Economic Crime Survey: 72% companies became cybercrime victims in the previous 2 years (Africa News, 2007)
The Philippines	5.4	A Philippino hacker launched the "Love Letter" virus in 2000. Estimated damage in the US: $4–15 billion (Adams, 2001)	• 2007: More than 330 cyberattacks per day, the sixth highest cybercrime target country in the world (Conti, 2007)

The underlying notion in this chapter is that cybercrimes in developing and developed countries are characterized by important structural differences. The sources, targets as well as other ingredients structurally differ in developing and developed countries. First, as we have demonstrated, economic factors facing cyber-criminal and cybercrime victims are significantly different in developing and developed countries. They include nature and quality of hardware, software, and infrastructure; targetability of victims; stock of cybercrime skills; and associated opportunity costs and benefits.

A second, probably more significant factor, relates to formal and informal institutions in these economies. As explained in Chap. 3, cyber-criminals' activities can be explained in terms of Baumol's (1990) destructive entrepreneurship. The society's "rules of the game," known as institutions affect the extent of such activities (Baumol, 1990; North, 1990, 1996).

Institutions can be better understood in the context of the tasks for which they were created (Holm, 1995). Relevant institutions from the standpoint of cybercrimes include the availability of jurisdictional arbitrage and strength of rule of law and stigmatization issues associated with becoming a cyber-criminal or a cybercrime victim.

A final reason why cybercrimes in developing and developed countries are likely to differ is related to cognitive factors. Cyber-criminals as well as cybercrime victims in these two groups of countries are likely to differ in terms of confidence, skills, and experiences.

8.2 A Brief Survey of Cybercrimes in Developing Countries

Tables 7.1 and 7.2 (Chap. 7) presented quantitative indicators related to cybercrimes in developing countries. Table 8.1 presents some qualitative indicators. In some cities such as Mumbai in India, there have been more cybercrime cases being registered with the police than conventional crimes such as murder, burglary, and arson (Hindustan Times, 2009).

An increasing number of cyberattacks targeting developing countries are international in nature. For instance, it is reported that cyber-criminals from Malaysia, Japan, Korea, the United States, and China have targeted computers in the Philippines (Conti, 2007). In a well-publicized case, it was found that Canada-based hackers employed about 100,000 poorly protected "zombie" computers mainly in developing countries such as Poland, Brazil, and Mexico and stole US $44 million (Harwood, 2008). Experts argue that this is an indication of a change in the victim/victimizer pattern and an unusual case of role reversal.

In Chap. 1, we discussed Gordon and Ford's (2006) classification of Type I and Type II cybercrimes. Because of their lower digitization, Type II cybercrimes, which mainly involve human elements are likely to be proportionately higher in developing countries compared to those in industrialized countries. For instance, many

Indians are reported to be victims of various versions of "Nigerian 419"[1] fraud, which involve criminal–victim interaction (Srivastava, 2009).

8.2.1 Broadband Connections and Increase in Cybercrimes

In a discussion of cybercrimes in developing economies, the rapid proliferation of broadband connections in these economies deserves special attention. At this point, we should emphasize that one reason why US computers are attractive targets for cyber-criminals is because they are always online and have broadband connections. Note that serious cybercrimes require bandwidth intensive applications. A related point is that African networks do not attract the same level of attention from hackers as other regions of the world because of the low level of connectivity of the region and low broadband penetration. From the criminal's standpoint, the African environment is thus highly unreliable for carrying out cyberattacks effectively (Reilly, 2007). Not that typical "bot-herders" control tens of thousands and even millions of "zombie" computers.

Not long ago, most African economies lacked fiber-optic cable and relied on slower satellite links to connect to the World Wide Web, which meant longer time to attack local websites (Kinyanjui, 2009). In June 2009, East Africa got its first fiber-optic submarine cable. Two additional companies are expected to complete similar projects by the end of 2009. The project is expected to speed up the connections in Kenya, Burundi, Rwanda, Tanzania and Uganda, Somalia, Ethiopia, and Sudan. Analysts argue that Africa and other developing countries are likely to experience a rapid growth of cybercrime as broadband technology takes off in these economies (Africa News, 2007; The Economist, 2009). For instance, Kenya experienced about 800 bot attacks per day in July 2009, which is expected to increase to 50,000 per day after the fiber connectivity goes live (Kinyanjui, 2009b).

Most obviously, cybercrime proliferation is associated with and facilitated by the growth of broadband networks. In the early 2000s, estimates suggested that about one-third of spam came from zombie computers with broadband connections (Kotadia, 2003). Estimates suggested that in recent years, Zombie computers are almost always connected to broadband Internet.

A number of developing countries are experiencing rapid broadband growth. Analysts argue that increased penetration of broadband in developing countries is likely to make these countries a fertile ground for hackers. It is argued that rise of cybercrime in China can be mainly attributed to the rapid growth of broadband users in the country (Business Daily Update, 2006). China's broadband subscriber base, for instance, grew by 114% in 2004, 57% in 2005 and 38% in 2006 and is expected to experience a double-digit growth for the next few years. China's broadband subscriber base is expected to surpass that of the United States in 2008 (Chan, 2007).

Likewise, broadband connections in Latin America increased by 41% in 2007 and by 2013, average consumer broadband penetration in the region is expected to reach 30 % (Screen Digest, 2008). In particular, in Peru, the number of broadband subscribers rose by over 80% annually during 2001–2006 and it reached about half a million in 2006 (ITU, 2007).

8.3 Economic and Institutional Factors Related to Cybercrimes in Developing Economies

8.3.1 Formal Institutions: Permissiveness of Regulatory Regimes

Most cybercrimes in recent years are committed by organized criminal groups. To understand organized criminal groups' operations, it may be helpful to consider them as rational economic actors with profit maximization goal (Becker, 1968; Ehrlich, 1973; Freeman, Grogger, & Sonstelie, 1996; Sjoquist, 1973; Viano, 1999). Their profit depends upon capability to emulate market mechanisms. This may require formation of strategic alliances, making appropriate capital investment decision, identifying new growth areas, investing in R&D, adopting modern accounting systems, and insuring against risks (Mittelman & Johnston, 1999).

The research literature provides abundant evidence that like multinational firms, organized crime groups consider a number of factors to make decisions related to geographic location of their activities. Perhaps the most important factor influencing the location decision is the strength of the rule of law. A person's decision to participate in an illegal activity is a function of the expected probability of apprehension and conviction and the expected penalty if convicted (Ehrlich, 1996). Many developing countries' weak rule of law and permissiveness of regulatory regimes provide a fertile ground for criminal activities (Mittelman & Johnston, 1999; Vassilev, 2003).

Developing economies are at different degrees of readiness in terms of regulative institutions to deal with cybercrimes. In Africa, for instance, as of September 2009, Kenya and Rwanda recognized electronic signature and electronic crimes. In Tanzania and Uganda, on the other hand, the bills to recognize electronic signature and electronic crimes were at the parliament level (Mark, 2009).

While an increasing number of developing economies have enacted laws to deal with cybercrimes, they lack enforcement mechanisms. As one might expect, developing countries lack judges, lawyers, and other law-enforcement manpower, who understand cybercrimes. For instance, Malaysia's HeiTech Padu Berhad's director noted that out of the country's 40,000 lawyers, only four were able to handle cybercrimes (Ismail, 2008). Similarly, in 2004, of the 4,400 police officers in India's Mumbai city, only five worked in the cybercrime division (Duggal, 2004).

Cybercrime awareness level is very low among the law-enforcement community. For instance, it was reported that when a police officer was asked to seize the hacker's computer in an investigation of a cybercrime in India, he brought the hacker's monitor. In another cybercrime case, the police seized the CD-ROM drive from a hacker's computer instead of the hard disk (Aggarwal, 2009). Likewise, eBay's Albena Spasova, who worked in promoting law reform in Moldova and

Bulgaria noted: “Even in 2001, I was meeting judges who thought cybercrime was someone stealing a computer” (Wylie, 2007).

Regulative institutions in developing economies are also insufficient and impractical to deal with some forms of cybercrimes. Experts, for instance, say that Indian law on computer crime is “fuzzy” (Ribeiro, 2006). India’s IT Act 2000, for instance, did not cover phishing, cyberstalking, and cyberharassment (Hindustan Times, 2006). The IT (Amendment) Act 2008, however, has specific provisions on how various cybercrimes such as publishing sexually explicit material, cyber-terrorism, Wi-Fi hacking, sending and viewing child pornography, identity theft, and spam are punished (Deshpande, 2009).

Similarly, due to a lack of cybercrime laws, Indonesian police used a “red book,” a manual to conduct credit card investigations available since 1997, to handle Internet credit card fraud (Darmosumarto, 2003). Likewise, according to Brazil’s legislation enacted in 1988, a hacker cannot be charged for breaking into a site, or distributing a virus, unless it is proven that the action resulted in a crime (Smith, 2003). In the same vein, Romanian law requires cybercrime victims to send police a signed complaint and be represented at the hearing (Wylie, 2007). It is thus virtually impractical for most US-based eBay fraud victims to bring a case in the Romanian courts.

In Indonesia, only 15% of reported incidents are actually investigated (Shubert, 2003). In India about 10% cybercrimes are reported of those reported about 2% is actually registered. The conviction rate is as low as 2% (Hindustan Times, 2006). As of 2006, no one charged for data fraud in India was convicted (Ribeiro, 2006). As of August 2009, only four people were convicted for cybercrime (Aggarwal, 2009).

One reason why industrialized economies are forced to develop legal and regulatory infrastructures to deal with cybercrimes is because they experience more cybercrimes compared to developing economies. In industrialized countries, while most laws have focused in increasing the severity of punishment for cyber-criminals (Walker, 2004), some also require businesses to enhance defense against cybercrimes. An estimate suggested that US banks spent US $60 million in 2002 on technology to comply with the requirements of the Patriot Act (McGeer, 2002).

Although criminals in general are emboldened if laws are weak, a much higher degree of jurisdictional arbitrage is available in digital crimes. Not surprisingly, organized cybercrimes are initiated from countries that have few or no laws directed against cybercrimes and little capacity and willingness to enforce existing laws. Commenting on Africa’s currently low level but high-growth potential of cybercrimes, Hamadoun Toure, secretary-general of the ITU put this issue this way: “At the moment, cybercriminals see Africa as a safe haven to operate illegally with impunity” (Africa News, 2007).

We noted above that national level institutions dealing with cybercrimes in developing countries are thin and dysfunctional. Equally problematic are institutions at industry and inter-organizational levels. For instance, there is no insurance company in India that offers a comprehensive anti-cybercrime policy for a company (Syed and D’monte, 2008).

8.3.1.1 Resources to Fight Cybercrimes

Developing economies lack resources to build institutions to combat cybercrimes (Cuéllar, 2004). For instance, consider Ramnicu Valcea town of Romania, where a large number of eBay fraud cases originate. In 2005, two law-enforcement officers in the town were dealing with over 200 eBay cases with a 9-year-old computer that had no Internet connection. And to connect to the Internet they had to use the same cafes as used by cyber-criminals for eBay fraud (Wylie, 2007). Similarly, in the ITU Regional Cybersecurity Forum for Eastern and Southern Africa held in Zambia in 2008, an expert from Democratic Republic of Congo stated that factors such as the lack of legal experts in ICT and poor understanding of ICTs and its added value in the national economy hindered the adoption of cybersecurity-related legislation in the country (ITU, 2008). Likewise, in Bangladesh cellphones with unregistered subscriber identity module (SIM) cards have been increasingly used for extortion activities. However, the cybercrime unit of Dhaka Metropolitan Police (DMP) has not been equipped to handle such crimes (The New Nation, 2009).

8.3.1.2 Cyber-Criminals' Confidence

Increased success is sending positive cognitive messages and making cyber-criminals more brash and disrespectful of law-enforcement agencies (Kshetri, 2005). Because of weak law-enforcement machinery in developing countries, cyber-criminals in these countries are more confident than those in developed countries. A computer forensics expert in Sao Paolo, Brazil noted that Internet crime gangs in the country do not use techniques to hide themselves (Warren, 2007). Likewise, it is reported that many developing world-based hackers targeting the US networks do not conceal their real identities or origin of their mailings (Vardi, 2005).

8.3.2 Informal Institutions: Social Legitimacy and Cybercrime

We noted above how regulative permissiveness has been a driving force behind the growth of the crime industry. But the more immediate—and also the more foundational—reason behind the rapidly rising global cybercrimes relates to the degree of social legitimacy to such crimes. As discussed in Chap. 5, condemnation of an act such as a cybercrime leads to internalization of norms against the act among the "condemners" and as well as the "condemned" (Kahan, 1996). Proponents of "gay rights" legislation, for instance, argue that the real battle centers on gaining social and cultural acceptability, achieving social legitimacy of such rights (Hu, 2001; Shilts, 1991), and stigmatizing "orthodox religious believers" (Duncan, 1994).

As noted in Chap. 2, various factors lead to less guilt in cybercrimes compared to conventional crimes (Kallman & Grillo, 1996; Phukan, 2002). Most obviously, these conditions are more pervasive in developing countries as many Internet users in these countries are connected to the Internet for the first time (redherring.com, 2005). A related point is that developing and developed countries may also differ in terms of social stigma associated with becoming a cybercrime victim. In sum, cybercrimes tend to be more justifiable in developing countries than in developed countries.

8.3.3 Defense Mechanisms Against Cybercrimes

Countries across the world differ in the deployment of security products to address such holes. In 2002, North America accounted for 58% of the global security product market (Europemedia, 2002).

An estimate suggested that in 2006, about 3 million of Brazil's small- and medium-sized enterprises (SMEs) lacked anti-virus software in their PCs (Business Wire, 2006). Likewise, 60% of Kenyan banks are reported to have insecure systems (Kinyanjui, 2009).

The concept of "hollow diffusion" of Internet and e-commerce technologies among firms in developing economies such as China may help understand weak defense mechanisms (Otis and Evans, 2003: 49). The basic idea behind "hollow diffusion" is simple: Many companies adopting e-commerce, especially in developing countries, lack technological and human resources, and other fundamental ingredients needed for long-term success. In short, they lack true depth of Internet adoption. "Hollow diffusion" can take place in human terms (lack of skill and experience) as well as in technological terms (failure to use security products) (Otis & Evans, 2003). It is argued that organizations that adopt Internet technologies without considering the costs and efforts needed to maintain those systems generate a negative externality (Otis & Evans, 2003). A related point is that compared to dominant multinationals, ICT vendors in developing countries tend to be smaller businesses and later entrants into the global ICT market (Denardis, 2007).

8.3.3.1 Hardware and Software Used in Developing Economies

Of equal importance in the discussion of cybercrimes in developing countries that follows below is the nature of hardware and software in these countries. According to the product-cycle approach, ICT products are adapted in developing countries to meet the conditions of local markets and processes to local technological capacity (Nordas, 1996). Most ICT products targeted for developing countries are low-cost versions as advanced features make them unaffordable (Dairy Industries International, 1998). At the same time, universities and other organizations are taking measures to make products available at low cost in developing countries. For instance, Universities Allied for Essential Medicines (UAEM) has called for "open-access" patents from universities to increase low-income countries' access to medicines (Kim, 2007). In some cases, entirely new products are developed for developing world-based consumers. A case in point is Whirlpool's launch of the world's cheapest automatic washer in the US $150–200 price range (Jordan & Karp, 2003).

As an example of entirely new products designed for developing world-based consumers, the One Laptop per Child (OLPC) program deserves special attention. The program aims to provide low-cost computers to children in developing countries. The goal of the OLPC project was to deploy 100 million laptops in the first year (Naraine, 2006). While this goal has not been materialized, the OLPC program has made a significant progress. As of the early 2008, there were an estimated 250,000 children from developing countries across the world, who owned laptops under the OLPC program (South Africa: The Good News, 2008). These computers run on Linux and have a security system called BitFrost (Reilly, 2007). BitFrost's built in features prevent viruses and other programs from "damaging the computer, stealing files, or spying on the user" (Brandt, 2007). It has been robust against viruses so far. Analysts however, argue that hackers may find previously unknown flaws in BitFrost (Reilly, 2007). To substantiate this claim, we draw a parallel with recent intensification of cybercrimes targeting Macs. It is worth noting that cybercriminlas have extended their efforts beyond Windows and such efforts are becoming more sophisticated over time. For instance, while some viruses targeting Macs existed before, Apple's computers experienced financially motivated attacks from organized criminal groups for the first time in 2007 (sophos.com, 2008).

The OLPC program is facing a competition from Intel's low-cost Classmate computers designed for children in developing countries (Clark 2008). Intel sold "tens of thousands" of its first generation of Classmate PCs, which were launched in the early 2007 (thestate.com, 2008). The company announced its plan to start selling a new generation of Classmate PCs starting April 2008. The Classmate computers operate on Windows' cut-down versions (Reilly, 2007). As noted above, most viruses and botnets attack Windows.

8.3.3.2 Internet Users' Skills

Another problem is related to the lack of skills. Many Internet users in developing economies such as China are inexperienced and not technically savvy. A high proportion of them are getting computers and connecting them to the Internet for the first time (redherring.com, 2005). A majority of new Internet users in developing countries also lack English language. While the developments of user-friendly software and interfaces have reduced the complexity and consumer learning requirements (Gatignon & Robertson, 1985) for computer and Internet use, such developments have not taken place in the development of security products.

Most of the information, instructions, and other contents for security products are available in English language only (Information Today, 2008). Many Internet users in developing countries are unable to use IT security products developed in English language. For instance, even if Microsoft publishes a security bulletin in Chinese, it is unlikely to do so in all the 20 dialects of China (redherring.com, 2005).

8.3.3.3 International Hierarchical Pattern in the Diffusion of Security Products

It is also important, in this context, to look at the connection between a country's market size and the availability of technology products in the country. Most developing countries lack market and infrastructures for such products (Brown, Malecki, & Spector, 1976). Put differently, international diffusion of technology products exhibits a "hierarchical pattern" (Gatignon & Robertson, 1985, p. 858). As is the case of other technologies, commercial distributors of IT security products often find developing countries unprofitable for their markets, which lead to adverse international hierarchical pattern of such products. A related point is that the international "hierarchical pattern" is more adverse for security products. While the top security software firms are US-based, businesses and consumers in some developing countries (e.g., Southeast Asia), mainly because of nationalism, prefer to buy domestically manufactured software (Information Today, 2008).

8.3.4 Concentration of Crimes

Deutsch, Hakim, and Weinblatt (1984) suggested that the return to crime is positively related to the concentration of criminals in a neighborhood. Criminals tend to focus their efforts in a few neighborhoods, or crime hot spots, "overwhelming" the law-enforcement agencies and police forces in those neighborhoods (Freeman et al., 1996; Weisburd, Bushway, Lum, & Yanz, 2004). As middle classes tend to avoid "high crime areas," crime hot spots tend to be inner city low-income neighborhoods (Lianos & Douglas, 2000). It is also suggested that sparsely populated neighborhoods are associated with a high rate of violent crimes (Browning, Feinberg, & Dietz, 2004; Wilson, 1987). Note that 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).

It was apparent from our review that cybercrimes targeting developing economies exhibit a heavy concentration in specific industry sectors. In China, businesses in the online gaming industry and gamers have been attractive targets for hackers (Kshetri, 2009b). These hackers steal gamers' passwords and login information (e.g., World of Warcraft). The stolen virtual items and identities are then auctioned online (Greenberg, 2007). Experts say that an online gaming account in China can be sold for up to US $1,000 compared to US $5–10 for stolen credit card data (Fong, 2008).

In Brazil, a large number of cybercrimes involve malicious codes, most notably keylogging viruses, designed to steal banking passwords (Greenberg, 2007). E-mail spam is getting more personalized (ITU, 2007). Cyber-criminals also use sophisticated social engineering scams to trick Brazilians into giving up personal information. According to the Brazilian Banks Association, estimated losses associated with virtual fraud in 2005 were US $165 million (PR Newswire, 2008). Cyber-criminals also make a rapid adaptation in password-stealing malware to the changes made by banks (PR Newswire, 2008). Likewise most high-profile and widely publicized cybercrimes in India are concentrated in the offshoring sector (Hindustan Times, 2006). For instance, data frauds have been reported in call centers in Pune, Hyderabad, Bangalore, and Gurgaon. The British Tabloid, Sun, reported that an Indian call center employee sold confidential information of 1,000 bank accounts to its reporter working as an undercover (tribuneindia.com, 2005; Hindustan Times, 2006). In another case, call center workers at Pune, India, subsidiary of Mphasis, a provider of outsourcing services, transferred about US $500,000 from four Citibank customers' accounts to their personal accounts (Schwartz, 2005; Fest, 2005). It is reported that in major Indian cities, there are "data brokers," who obtain data illegally from people that are working in offshoring companies (Aggarwal, 2009).

The common denominator to the above examples is that businesses and consumers in leading e-commerce sectors in a developing economy are more likely to be cybercrime targets compared to other less e-commerce ready industries. In China, for instance, online games generated US $1.8 billion in 2007 (China Daily, 2008). Buying and selling of virtual items has been a "mini-economy" in China (Nystedt, 2004).

Similarly, a majority of Brazilians do banking activities online (PR Newswire, February 21, 2008). Indeed, financial services are among the leading e-commerce sectors and banks are positioned to be leaders in e-marketplaces and in e-payment solutions in Brazil and other Latin American countries (Kshetri & Dholakia, 2002). Likewise, Indian offshoring industry's revenue grew from US $4.8 billion in fiscal year 1997–1998 to US $47.8 billion in 2006–2007 (Indo-Asian News Service, 2007).

8.3.5 Path Dependence Externalities Generated by Conventional Crimes and Cybercrimes

As discussed in Chap. 4, due to path dependence of crimes, other things being equal, the more a particular type of crime a society previously had, the higher the odds of observing crimes of the type in the society.

Given the cybercrime environment and feedback loops, increasing returns could manifest themselves in many ways. For instance, cyber-criminals may "invent" sophisticated and new tools that law-enforcement agencies face increased difficulty in tracing. Cyber-criminals could also operate from countries with weak cybercrime laws (Kshetri, 2009a). The externality could also arise because at a given level of law-enforcement resources, an increase in the number of cyber-criminals reduces the probability that a cyber-criminal will be caught (Freeman et al., 1996).

As discussed in Chap. 4, developing countries also differ in terms of leadership in a cybercrime category and the patterns of international cybercrimes originated from these countries. More fully developed examples of cybercrimes are found in East European countries. In Chap. 4, we discussed Romanian and Ukrainian cyber-criminals' specialization in Internet auction frauds and online credit card related crimes (Wylie, 2007). Bulgarian and Chinese cyber-criminals have reportedly specialized in intellectual property theft (Vardi, 2005). For instance, in 2005, a Trojan horse code named Myfip was sending data from the networks of US-based companies to an Internet user in Tianjin, China. Myfip reportedly sent sensitive documents such as CAD/CAM files that stored mechanical designs, electronic circuit board schematics, and layouts (Vardi, 2005). In 2005, a Chinese intern working in Valeo was detained in France for alleged "illegal database intrusion" aimed at intellectual property theft (Luard, 2005).

8.3.6 Cybercrime Business Models in Developing Economies

Developing world in general lags behind the developed world in the availability of IT skills. There are, however, highly skillful organized crime groups in some developing countries. Note that specialized organized crime groups are increasingly engaged in cybercrime activities (Hawser, 2007; Giannangeli, 2008). Indeed, cybercrime has been one of the most important revenue sectors for global organized crime groups (M2 Presswire, 2007). In many cases, organized criminals also buy high-skilled coders as well as low-skilled IT workforce to engage in cybercrimes.

To launder funds stolen through cybercrime operations, organized crime groups often lure and recruit money mules. The mules help to move stolen money from one account to another. Most often they take the stolen funds into their own account before sending as a wire transfer to the criminal groups (Sullivan, 2007). They receive commissions for doing that. For instance, most of Romanian cyber-criminals' auction fraud victims are in the United States, Canada, Britain, Spain, or Italy. Romanian mules are found to pick up money in these countries. In 2006, US law-enforcement agencies arrested an eBay fraud ring in Chicago, which was traced to have connections with cyber-criminals in Pitesti, Romania (Wylie, 2007).

Here is why "money mules" are needed. Cyber-criminals know that credit card transactions initiated from Eastern Europe and some developing countries have a low probability of success. In such cases, they recruit "money mules" in countries where the credit card holder is located (e.g., United States). A US-based "money mule", for instance, uses the stolen credit card to make a transaction in a US bank and then sends the money to the cyber-criminal. One estimate suggested that international cybercrime groups had set up about 44,000 post office boxes and residential addresses in the United States in 2004 (Acohido & Swartz, 2005). US-based online retailers are cautious of shipping across borders. Cybercrime groups, however, know that if an online transaction is approved, shipments inside the United States are rarely scrutinized. They thus recruit US-residents as mules, whose homes are used as shipment drop points.

In some cases, money mules are unaware that they are engaged in illegal activities. Worse still, the mules themselves could become scam victims (Claburn, 2008). To take another example, consider the Nigerian check scam. In this type of scam, Nigerians send fake documents, which look like Wal-Mart money orders, Bank of America checks, US Postal Service checks, and American Express traveler's checks[2] (Gohring, 2008). They provide a money mule with instructions on filling out the checks and where they would go. The mule cashes the checks and sends most of the check amount to Nigerian cyber-criminals. However, when the check is found to be a fake one, the mule would be responsible for the entire amount.

Location and number of money mules and functions they perform also vary across the type of cybercrimes. Some transactions involve "money mules" located in a number of countries. In a case reported in Sullivan (2007), a cybercrime victim, an online CD and DVD retailer, paid a ransom of US $40,000 to a hacker based in Balakov, western Russia. The fund was wired to 10 different bank accounts in Riga, Latvia. The mules then wired the money to accounts in St. Petersburg and Moscow. Another set of mules brought the money to Balakov. The computer server used by the Balakov-based hacker to launch the botnet attacks was in Houston.

In an interesting pattern of international division of labor, in the early 2008, a criminal group involved in botnet attacks set up offices in India to process applications that cannot be completed automatically (Arnott, 2008). IT workers in the India offered help to facilitate signing up of free e-mail accounts.

8.3.7 Motivations Behind Cybercrimes

As noted in Chap. 2, crime rates are tightly linked to the lack of economic opportunities. A large number of cyberattacks originate from Eastern Europe and Russia because there are a large number of students good at mathematics, physics, and computer (Blau, 2004). Speaking of the social emphasis on mathematics skills among Romanians, a senior research scientist at the Institute of Mathematics 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).

Consistent with history and theory bot herders and other types of cyber-criminals tend to be from locations where high-paying legitimate IT jobs are unavailable (Sullivan, 2007). In industrialized countries, people with IT skills can easily find legitimate IT jobs. In many developing economies, IT job growth is lower than Internet penetration growth (Sulaiman, 2007). The primary reason why some people are attracted into cybercrime in Eastern Europe and Russia is because of high unemployment and low wages. Organized crime groups in countries such as Russia, Romania, and Brazil are thus tapping into the technical skills available in those countries to expand their operations.

The combination of over-educated and under-employed computer experts has made Russia and other Eastern European countries fertile ground for hackers. While IT industries are developing in these economies, the growth rate is far from enough to absorb students and the workforce with IT skills. Students good at mathematics, physics, and computer science are having difficulties to find jobs in these countries (Blau, 2004). Beyond all that, in Russia a financial crash in 1998 left many computer programmers unemployed. In Russia, top university graduate are paid by organized crime groups up to 10 times as much as from legitimate IT jobs (Warren, 2007).

A related point is that notwithstanding India's huge IT talents, the country accounts for proportionately fewer cybercrimes compared to other developing countries. For instance, according to Sophos researchers, the United Kingdom and India together contributed 1.3% of the world's malware. While they could not separate malware originated from the United Kingdom and India as both use British English, the United Kingdom is considered to account for more crimes than India (Greenberg, 2007). 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 noted: "Today ? any person in India with marketable computer skills has a few job offers in hand" (Greenberg, 2007).

8.4 Concluding Comments

This chapter has contributed to the conceptual and empirical understanding of the structure of cybercrimes in the context of the developing world. The analyses indicated that the nature of the source of a web attack is a function of the nature of institutional legitimacy to a cyber-criminal; and stocks of hacking skills relative to the availability of economic opportunities; and potential victims' defense mechanisms. Table 8.2 presents economic and institutional factors facing cybercrime offenders and victims in a developing economy.

Anti-cybercrime institutions are developing rapidly in industrialized economies because of exogenous shocks, pressures to change organizational logics and other

Table 8.2 Economic and institutional factors facing offenders and victims

	Economic factors	Institutional factors
Offender	[1] • Lack of availability of other economic opportunities	[3] • Jurisdictional arbitrage: No or few laws dealing with cybercrimes • More confident cyber-criminals • Novelty factor and stigmatization • Path dependence and specialization in specific crimes
Victim	[2] • Heavy concentration of cybercrimes in specific industry sectors • Hierarchical pattern of the diffusion of security products • Hollow diffusion of Internet and e-commerce	[4] • Stigmatization • Lack of strong security mechanisms • Less experienced computer users—weak psychological/behavioral defense

forces of gradual changes. In many developing economies, on the other hand, formal institutions are weak because these countries lack laws that recognize cybercrime, they lack judges, lawyers, and other law-enforcement manpower who understand cybercrimes, and they lack resources to build institutions to combat cybercrime. Governments' measures to combat cybercrimes too often remain pure lip service. One reason for this problem is a lack of resources to build formal institutions to deal with cybercrimes (Cuéllar, 2004). Equally problematic are institutions at industry and inter-organizational levels. Because of weak law-enforcement machinery in developing countries, cyber-criminals in these countries are more confident than those in developed countries.

Cybercrimes may be more justifiable if informal institutions (or social and internalized norms) against them are weaker in a society. These conditions are more pervasive in economies, in which many Internet users are connected to the Internet for the first time (redherring.com, 2005). Moreover, cybercrime victimization level is relatively low in these economies.

As noted earlier, most people involved in using computer networks unethically and illegally do not perceive their actions' ethical implications. Factors giving rise to such conditions are stronger in developing countries. This is because the Internet is new for many users in developing countries. A related point is that many organizations and individuals are unaware of cybercrimes. Cybercrimes are more justifiable in developing countries than in developed countries. As pointed out by social identity theory argues (Hamner, 1992; Tajfel & Turner, 1986), as more and more individuals and organizations become cybercrime victims and they belong to the in-group of cybercrime victims the perceived social stigma associated with a cyber-criminal may increase and that of becoming a cybercrime victim may reduce. Based on above discussion, the following proposition is presented.

Many Internet users in developing economies are inexperienced and not technically savvy. Most organizations adopt these technologies without considering security and other related problems. Even if organizations are willing to secure their systems, because of the adverse international "hierarchical pattern" for security products, these products are less likely to be available in these economies.

Thin and dysfunctional institutions and a lack of resources are among the biggest roadblocks for combating cybercrimes in developing countries. A lack of international cooperation and coordination is equally problematic in fighting cybercrimes originated in developing countries.

Yet, notwithstanding the political, legal, cultural, and economic barriers, some economies are making some great leaps. Some developing countries are also modernizing their crime-fighting efforts. It was, for instance, reported in 2006 that Kenya was in advanced stages for assembling a cybercrime laboratory, which could be used by police in Eastern African countries (Kornakov, 2006). In September 2009, Antigua opened a state-of-the-art cyberforensics facility to serve the entire Caribbean region to fight cybercrimes. Montserrat, Barbados, St Kitts Nevis, and Antigua and Barbuda would use the lab. The United States provided over US $500,000 to establish the lab and US $200,000 to train the workforce (caribbean360.com, 2009).

Indian offshoring industry provides a remarkable example of industry-government collaboration in combating against cybercrime (Box 8.1). Especially the National Association of Software and Services Companies (NASSCOM) has played an exemplary role in bringing institutional changes in cybercrime-related institutions (Kshetri & Dholakia, 2009).

Box 8.1 NASSCOM's Efforts in Fighting Cybercrimes in the Indian Offshoring Industry

Indian offshoring industry provides a remarkable example of industry-government collaboration in combating against cybercrime. India's National Association of Software and Services Companies (NASSCOM) works with police officers, lawyers, and industry bodies to ensure enforcement. NASSCOM meets with bar councils in different cities to educate legal communities. It also educates police officers about cybersecurity and trains them to recognize and prosecute cybercrimes (Ticoll, 2004). NASSCOM started working with Mumbai police since 2003 (Saravade & Saravade, 2007). NASSCOM helped police departments of Mumbai and Thane in establishing a cybercrime unit and in training officers to investigate data theft (Indo-Asian News Service, 2006). In 2005, NASSCOM announced a training initiative for Pune's cybercrime unit, which caught data crime perpetrators from MphasiS, a major ICT company (Cone, 2005). A third cybercrime unit established in Bangalore in January 2007 has resources to train more than 1,000 police officers and other law-enforcement personnel annually (COMMWEB, 2007). Similar units were planned for other cities. NASSCOM also offered to work with authorities in the United Kingdom and India to investigate cases involving identity theft (tribuneindia.com, 2005).

The Data Security Council of India (DSCI), a self-regulatory member organization set up by NASSCOM, has the ability to expel non-compliant members or call in police (McCue, 2007). Companies that fail to secure their data may have to pay up to US $1 million (Hindustan Times, 2006). NASSCOM has also established a CyberCop committee and a member of the committee serves as a technical advisor to the Indian CyberCrime Investigation Cell.

NASSCOM asked the Indian government to create a special court to try people accused of cybercrimes and other violations of the country's Information Technology Act. The Indian government is considering NASSCOM's request in establishing such courts (Ribeiro, 2006). NASSCOM has also launched a registry of IT employees, which allows employers to perform background checks on existing or prospective employees (Hindustan Times, 2006; Trombly, 2006; Trombly & Yu, 2006). Creation of criminal and public records databases has been a part of the program (Fest, 2005).

In September 2007, the Indian government announced a grant of US $900 thousand to Central Bureau of Investigation (CBI) for combating cybercrime (BBC Monitoring South Asia, 2007).

NASSCOM's measures have paid off brilliantly. Studies conducted by Forrester Research and by the UK's Banking Code Standards Board indicated that security standards in Indian call centers are among the best in the world and there were more security breaches in the United Kingdom and the United States in 2005 than in India (Precision Marketing, 2006).

We noted above that growth of Internet and broadband penetrations in developing countries is likely to lead to a more rapid growth of cybercrimes in these countries than in developed countries. Other economic factors related to cybercrimes such as availability of resources to fight cybercrimes and availability of economic opportunities are likely to change at slower rates. Institutions related to cybercrimes are even slower to change, especially informal institutions.

On the bright side, developing world-based firms have also increased investments in security. The security market in China showed a 24% increase during 2006 (Hope, 2008). Factors such as the 2008 Olympics in Beijing, the 2010 World Expo in Shanghai, and a steady rise in broadband usage as a vehicle for online entertainment have boosted the growth (Hope, 2008). Likewise, small and medium businesses in Brazil spent an estimated US $260 million in 2007 on IT security solutions (Business Wire, 2006).

Cybercrimes catching international attention have been an important trigger for the strengthening of cybercrime laws in some developing economies. For instance, the Philippine Republic Act 8792 came following the love bug virus attack. The act laid out how cybercrimes should be punished in the country (Evans, 2000).

Other developing countries are also taking some measures against cybercrimes. In November 2006, the Bangladesh hosted a regional cybercrime seminar to exchange experience on combating cybercrime and foster future cooperation, leading towards a strong regional response to cybercrime. Experts dealing with cybercrime issues from Australia, Hong Kong, Sri Lanka, and Nepal participated. The Australian Federal Police supported the seminar (Asia Pulse, 2007).

It is also important to include developing economies in international level policy initiatives. In the first UN forum on Internet governance some developing countries such as Iran and South Africa complained that they had not been given an opportunity to adequately express their views on ethical issues and other concerns (RTÉ, 2006).

Economic factors related to cybercrimes such as hardware and software used, broadband connections, stock of cybercrime skills, availability of economic opportunities, diffusion of security products are changing in developing economies. Institutions related to cybercrimes, on the other hand, tend to be persistent (Parto, 2005), durable (Hodgson, 2003), and stable (Scott, 1995, 2001) and hence are slower to change. Moreover, in most cases, compared to formal institutions, de-institutionalization and re-institutionalization of social practices, cultural values, and beliefs occur very slowly (Clark & Soulsby, 1999; Ibrahim & Galt, 2002, p. 109; North 1990; Zweynert & Goldschmidt, 2006). Informal institutions such as those related to stigmatization of a cyber-criminal and a cybercrime victim are thus likely to change more slowly than formal institutions such as strength of rule of law.

Notes

1. Nigerian 419 fraud is named for a section of the Nigerian criminal code.
2. Edna Fiedler of the Washington State pleaded guilty in March 2008 for a scam of this type.

References

Acohido, B., & Swartz, J. (2005, July 11). Cybercrooks lure citizens into international crime. *USA Today*. http://www.usatoday.com/tech/news/2005-07-10-cyber-mules-cover_x.htm. Accessed 5 October 2009.

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

Africa News. (2007, October 24). South Africa; Internet banking fraud on the increase.

Aggarwal, V. (2009, August 3). Cyber crime's rampant. *Express Computer*. http://www.expresscomputeronline.com/20090803/market01.shtml. Accessed 27 October 2009.

Arnott, S. (2008, March 22). Cyber crime stays one step ahead. http://www.independent.co.uk/news/business/analysis-and-features/cyber-crime-stays-one-step-ahead-799395.html. Accessed 27 October 2009.

Asia Pulse. (2007, November 6). Cybercrime cost is a burden on developing countries: Bangladesh.

Baumol, W. J. (1990). Entrepreneurship: Productive, unproductive, and destructive. *Journal of Political Economy, 98* (5), 893–921.

BBC Monitoring International Reports. (2006, September 30). Kazakhstan Russian police chief urges cis efforts against cybercrime.

BBC Monitoring South Asia. (2007, September 15). India takes steps to tackle cybercrime.

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

Blau, J. (2004, May 28). Viruses: From Russia, with love? *IDG News Service*. http://www.pcworld.com/news/article/0,aid,116304,00.asp. Accessed 27 October 2005.

Brandt, R. L. (2007). Ivan Krstic, 21. *Technology Review, 110*(5), 54–55.

Brown, L., Malecki, E., & Spector, A. (1976). Adopter Categories in a Spatial Context: Alternative explanations for an empirical regularity. *Rural Sociology, 41*, 99–118.

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.

Business Daily Update. (2006, September 28). China tops globe in robot PCs.

Business Wire. (2006, November 20). SMBs in Brazil to Spend $260USM on IT Security in 2007; – Up to 72% of Brazil-based MBs Cited Enhanced Data Security and Privacy as Key Factors Influencing IT Purchases, AMI Partners Study Finds.

caribbean360.com. (2009, September 28). Regional cyber lab opens in Antigua. http://www.caribbean360.com/News/Caribbean/Stories/2009/09/28/NEWS0000008964.html. Accessed 27 October 2009.

Chan, I. (2007, July 26). China's Disturbing Broadband Decline: A digital divide between saturated urban areas and underserved rural markets is behind the slowdown. http://www.businessweek.com/globalbiz/content/jul2007/gb20070726_579284.htm?campaign_id=rss_as. Accessed 27 October 2009.

China Daily. (2008, May 5). China gets its game on. http://www.chinadaily.com.cn/bizchina/2008-05/05/content_6661519.htm. Accessed 2 October 2008.

Claburn, T. (2008, April 9). The Cybercrime Economy. http://www.informationweek.com/blog/main/archives/2008/04/the_cyber_crime.html. Accessed 7 October 2008.

Clark, D. (2008). PC makers race to market with low-cost 'Netbooks'. *Wall Street Journal* (Eastern edition), B.1.

Clark, E., & Soulsby, A. (1999). *Organisational change in post-communist Europe*. London: Routledge.

COMMWEB. (2007, January 4). India will train police to catch cybercriminals.

Cone, E. (2005). Is offshore BPO running around? *CIO Insight, 53*, 22.

Conti, M. K. C. (2007). Firms warned vs. cybercrimes. *BusinessWorld*, S1/7.

Cuéllar, M. (2004). The mismatch between state power and state capacity in transnational law enforcement. *Berkeley Journal of International Law, 22*(1), 15–58.

Dairy Industries International. (1998). No fuss printing basics assist third world trade, *63*(2), 48.

Darmosumarto, S. (2003, December 8). Battle on Internet credit card fraud still long. *The Jakarta Post*. http://www.crime-research.org/news/2003/12/Mess0802.html. Accessed 27 October 2005.

Denardis, L. (2007, November 11). Internet standards and developing countries: Problems and opportunities. Giganet second annual symposium, Rio De Janeiro, Brazil. http://www.igloo.org/community.igloo?r0=community-download&r0_script=/scripts/document/download.script&r0_pathinfo=%2F%7B58dacb33-31ea-4219-9124-89a75ffe71d0%7D%2FPublic%20Library%2Fpapers∼1%2Fdenardis&r0_output=xml. Accessed 27 October 2009.

Deshpande, S. (2009, October 28) New cyber law casts its net wide. *The Economic Times*. http://economictimes.indiatimes.com/infotech/internet/New-cyber-law-casts-its-net-wide-/articleshow/5170897.cms. Accssed 29 October 2009.

Deutsch, J., Hakim, S., & Weinblatt, J. (1984). Interjurisdictional criminal mobility: A theoretical perspective. *Urban Studies, 21*, 451–458.

Duggal, P. (2004). What's wrong with our cyber laws? http://www.expresscomputeronline.com/20040705/newsanalysis01.shtml

Duncan, R. (1994). Who wants to stop the church: Homosexual rights, legislation, public policy, and religious freedom. *Notre Dame Law Review, 69*, 393.

Ehrlich, I. (1973). Participation in illegitimate activities: A theoretical and empirical investigation. *Journal of Political Economy, 81*, 521–565.

Ehrlich, I. (1996). Crime, punishment, and the market for offenses? *Journal of Economic Perspectives, 10*(1), 43–67.

Europemedia. (2002, June 13). Terrorist attacks mean bid e-security spending, 1.

Evans, J. (2000). Cyber-crime laws emerge, but slowly. http://archives.cnn.com/2000/TECH/computing/07/05/cyber.laws.idg. Accessed 27 October 2005.

Expressindia. (2008, January 7). Cyber crime in India on the decline: Report. http://www.expressindia.com/latest-news/Cyber-crime-in-India-on-the-decline-Report/258638/.

Fest, G. (2005). 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. http://www.cnn.com/2008/TECH/05/08/digitalbiz.cybercrime. Accessed 27 October 2009.

Frayssine, F. (2007). Latin America: New 'Cyber Paradise' for Paedophiles and Racists? *ipsnews.net* http://ipsnews.net/news.asp?idnews=40072. Accessed 11 April 2010.

Freeman, S., Grogger, J., & Sonstelie, J. (1996). The spatial concentration of crime. *Journal of Urban Economics, 40*(2), 216–231.

Gatignon, H., & Robertson, T. S. (1985). A propositional inventory for new diffusion research. *Journal of Consumer Research, 11*, 849–867.

Giannangeli, M. (2008). Are we ready for Russian Mafia's crime revolution? *Sunday Express*, Scottish Edition, 4.

Gohring, N. (2008, June 25). Woman gets two years for aiding Nigerian internet check scam. *PC World*. http://www.pcworld.com/businesscenter/article/147575/woman_gets_two_years_for_aiding_nigerian_internet_check_scam.html.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*, 13–20.

Greenberg, A. (2007, July 17). The top countries for cybercrime. *Forbes.com*. http://www.forbes.com/2007/07/13/cybercrime-world-regions-tech-cx_ag_0716cybercrime.html. Accessed on 9 April 2008.

Hamner, K. M. (1992). Gay-bashing: A social identity analysis of violence against Lesbians and Gay Men. In G. M. Herek & K. Berrill (Eds.), *Hate crimes: Confronting violence against Lesbians and Gay Men* (pp. 179–190). Newbury Park, CA: Sage.

Harwood, M. (2008, February 22). Quebec police break up hacking syndicate. *Security Management*. http://www.securitymanagement.com/news/quebec-police-break-hacking-syndicate.

Hawser, A. (2007). Banks on the spot over internet fraud. *Global Finance, 21*(8), 8.

Hindustan Times. (2006, October 22). Securing the web.

Hindu.com. (2008, April 1). Delhi Police to train officers on combating cyber crime. http://www.hindu.com/thehindu/holnus/002200804011653.htm

Hindustan Times. (2009, October 24). Wired for trouble. http://www.tmcnet.com/usubmit/2009/10/24/4442635.htm. Accessed on 29 October 2009.

Hodgson, G. M. (2003). The hidden persuaders: Institutions and individuals in economic theory. *Cambridge Journal of Economics, 27*, 159–175.

Holm, P. (1995). The dynamics of institutionalization: Transformation processes in Norwegian fisheries. *Administrative Science Quarterly, 40*(3), 398–422.

Hope, C. (2008, March 20). UK security threat from cyber crime. http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/03/19/nterror319.xml. Accessed 27 October 2008.

Hu, V. T. (2001). Nondiscrimination or secular orthodoxy? Religious freedom and breach of contract at Tufts University. *Texas Review of Law & Politics, 6*(1), 289–333.

Ibrahim, G., & Galt, V. (2002). Bye-bye central planning, hello market hiccups: Institutional transition in Romania. *Cambridge Journal of Economics, 26*(1), 105.

Indiatimes. (2009, September 24). Phishing attacks on Indian brands rising. *Symantec*. http://economictimes.indiatimes.com/infotech/software/Phishing-attacks-on-Indian-brands-rising-Symantec/articleshow/5051231.cms. Accessed 27 October 2009.

Indo-Asian News Service. (2007, January 23). Indian IT revenue grows 10-fold in decade. *NASSCOM*.

Information Today. (2008, February). Challenges in the East. *25*(2), 22.

Ismail, I. (2008). Understanding cybercriminals. *New Straits Times* (Malaysia), 12.

ITU. (2007). *World Information Society Report 2007*, International Telecommunication Union. http://www.itu.int/osg/spu/publications/worldinformationsociety/2007. Accessed 27 October 2009.

ITU. (2008). ITU Regional Cybersecurity Forum 2008 Lusaka, Zambia, Meeting Report: ITU Regional Cybersecurity Forum for Eastern and Southern Africa, Lusaka, Zambia, 25–28 August 2008, 29 August 2008. http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/lusaka-cybersecurity-forum-report-aug-08.pdf. Accessed 5 October 2009.

Jordan, M., & Karp, J. (2003). Machines for the masses; Whirlpool aims cheap washer at Brazil, India and China; Making due with slower spin. *Wall Street Journal*, A.19.

Kahan, D. M. (1996). What do alternative sanctions mean? *63 U. Chicago Law Review, 591*, 603–604.

Kallman, E. A., & Grillo, J. P. (1996). *Ethical decision making and information technology, 2e*. New York: McGraw Hill.

Kim, J. Y. (2007). Toward a golden age. *Harvard International Review, 29*(2), 20–25.

Kinyanjui, K. (2009). High speed Internet exposes Kenya to cybercrime. http://www.businessdailyafrica.com/-/539444/638794/-/rx1rgv/-/. Accessed 5 October 2009.

Kinyanjui, K. (2009b, September 8). Watchdog warns of increased cybercrime threat. http://www.businessdailyafrica.com/Company%20Industry/-/539550/654440/-/u765i9z/-/. Accessed 5 October 2009.

Kornakov, K. (2006, September 8). Police forces in East Africa will have a new hi-tech lab. http://www.viruslist.com/en/viruses/news?id=197753850. Accessed 27 October 2007.

Kotadia, M. (2003, December 3). Report: A third of spam spread by RAT-infested PCs. *CNET News.com*. http://www.news.com/Report-A-third-of-spam-spread-by-RAT-infested-PCs/2100-7355_3-5113080.html. Accessed 27 October 2005.

Krebs, B. (2007, October 13). Taking on the Russian business network. http://blog.washingtonpost.com/securityfix/2007/10/taking_on_the_russian_business.html. Accessed 27 October 2008.

Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management, 11*(4), 541–562.

Kshetri, N. (2009a). Positive externality, increasing returns and the rise in cybercrimes. *Communications of the ACM, 52*(12), 141–144.

Kshetri, N. (2009b). The evolution of the chinese online gaming industry. *Journal of Technology Management in China, 4*(2), 158–179.

Kshetri, N., & Dholakia, N. (2002). Determinants of the global diffusion of B2B e-commerce. *Electronic Markets, 12*(2), 120–129.

Kshetri, N., & Dholakia, N. (2009). Professional and trade associations in a nascent and formative sector of a developing economy: A case study of the NASSCOM effect on the Indian Offshoring industry. *Journal of International Management, 15*(2), 225–239.

Leyden, J. (2004, September 23). US credit card firm fights DDoS attack. http://www.theregister.co.uk/2004/09/23/authorize_ddos_attack. Accessed 27 October 2005.

Lianos, M., & Douglas, M. (2000). Dangerization and the end of deviance. *The British Journal of Criminology, 40*(2), 261–278.

Luard, T. (2005, July 22). China's spies come out from the cold. http://news.bbc.co.uk/2/hi/asia-pacific/4704691.stm. Accessed 27 October 2007.

M2 Presswire. (2007, July 13). Frost & Sullivan: Correction: Cybercrime drives growth and increased competition in the global anti-malware market.

Mark, O. (2009). ICT experts gear up for war against e-crime. http://www.businessdailyafrica.com/Company%20Industry/-/539550/655032/-/u75jcqz/-/. Accessed 5 October 2009.

McCue, A. (2007, June 7). India gets offshore cyber crime watchdog. *silicon.com.* http://services.silicon.com/bpo/0,3800004865,39167417,00.htm.

McGeer, B. (2002). Security: Bankers fight a new battle it adjustments, purchases Part of Patriot Act. *Bank Technology News, 15*(11), 1.

Miller, N. (2008). Casting a wide net for cyber crimes. *The Age* (Melbourne, Australia), 6.

Mittelman, J. H., & Johnston, R. (1999). The globalization of organized crime, the courtesan state, and the corruption of civil society. *Global Governance, 5*(1), 103–126.

Naraine, R. (2006). Money Bots: Hackers cash in; Research group details how lucrative PC hijacking can be. *eWeek*, 27.

Nordas, H. K. (1996). South African manufacturing industries – Catching up or falling behind? *The Journal of Development Studies, 32*(5), 715–733.

North, D. C. (1990). *Institutions, institutional change and economic performance*. Cambridge, MA: Harvard University Press.

North, D. C. (1996). Epilogue: Economic Performance Through Time. In L. J. Alston, T. Eggertsson, & D. C. North (Eds.), *Empirical studies in institutional change* (pp. 342–355). Cambrige, PA: Cambridge University Press.

Nystedt, D. (2004). Online gaming growing fast in China, study says. http://archive.thestandard.com/movabletype/datadigest/archives/003210.php. Accessed 27 October 2005.

Otis, C., & Evans, P. (2003). The Internet and Asia-Pacific security: Old conflicts and new behavior. *Pacific Review, 16*(4), 549–550.

Parto, S. (2005). Economic activity and institutions: Taking stock. *Journal of Economic Issues, 39*(1), 21–52.

Phukan, S. (2002, June). IT ethics in the Internet age: New dimensions. *InSITE*. http://proceedings.informingscience.org/IS2002Proceedings/papers/phuka037iteth.pdf. Accessed 27 October 2005.

PR Newswire. (2008, February 21). New McAfee research shows regionalized malware rising; More attacks tailored to different cultures and technologies.

Precision Marketing. (2006, October 6). India call centres set to triple US Bank work. *18*(42).

Raghav, K. (2008, June 26). Cyber attacks will be disruptive, not destructive. http://www.livemint.com/2008/06/26001839/Cyber-attacks-will-be-disrupti.html. Accessed 27 October 2009.

redherring.com. (2005, April 5). China's Zombie PCs. http://www.redherring.com/Home/11708. Accessed 27 October 2006.

Reilly, M. (2007). Beware, botnets have your PC in their sights. *New Scientist, 196*(2634), 22–23.

Ribeiro, J. (2006, September 7). India's Nasscom calls for special cybercrimes court. *Network World*. http://www.networkworld.com/news/2006/090706-indias-nasscom-calls-for-special.html. Accessed 27 October 2007.

RTÉ. (2006, November 2). Global forum on Web bridges 'cultural gap'. *RTÉ Commercial Enterprises*. http://www.rte.ie/business/2006/1102/internet.html. Accessed 1 October 2009.

Saravade, P., & Saravade, N. (2007). A public-private partnership in India: Broken windows in cyberspace. *The Police Chief, 74*(3), 16.

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. Accessed 27 October 2009.

Schwartz, K. D. (2005). The background-check challenge. *InformationWeek*, 59–61.

Scott, R. (1995). *Institutions and organizations*. Thousand Oaks, CA: Sage.

Scott, R. (2001). *Institutions and organizations*. Thousand Oaks, CA: Sage.

Screen Digest. (2008). Telefonica takes the lead in Latin America. http://www.screendigest.com/press/releases/press_releases_22_01_2008/view.html

Shilts, R. (1991, January). The queering of America. *The Advocate*, 1.

Shubert, A. (2003, February 6). Taking a swipe at cyber card fraud. *CNN.com*. http://www.cnn.com/2003/WORLD/asiapcf/southeast/02/06/indonesia.fraud. Accessed 27 October 2005.

Sjoquist, D. L. (1973). Property crime and economic behavior. *American Economic Review, 63*, 439–446.

Smith, T. (2003, October 27). Technology; Brazil becomes a cybercrime lab. http://query.nytimes.com/gst/fullpage.html?res=9F02E3DA1131F934A15753C1A9659C8B63&sec=&spon=&pagewanted=2. Accessed 27 October 2005.

sophos.com. (2008, July 23). Police crack suspected online extortion ring. *Sophos reports*. http://www.sophos.com/virusinfo/articles/extortion.html. Accessed 27 October 2009.

South Africa: The Good News. (2008, April 8). SA kids benefit from one Laptop per child campaign. http://www.sagoodnews.co.za/education/sa_kids_benefit_from_one_laptop_per_child_campaign_.html. Accessed 27 October 2008.

Srivastava*,* M. (2009, September 14). Pros of con; From credit card fraud to drug peddling and job scams, Nigerians seem to be everywhere in the crime business. *India Today*. http://indiatoday.intoday.in/index.php?option=com_magazine&opt=section&sectionid=36&issueid=127&Itemid=1. Accessed 27 October 2009.

Sulaiman, H. (2007). Quest to fight cybercrime. *New Straits Times*, 13.

Sullivan, B. (2007, April 10). Who's behind criminal bot networks? http://redtape.msnbc.com/2007/04/whos_behind_cri.html. Accessed 27 October 2009.

Syed, F., & D'monte, L. (2008, April 7). India lags in cybercrime insurance. http://www.rediff.com/money/2008/apr/07cyber.htm. Accessed 27 October 2009.

Tajfel, H., & Turner, J. C. (1986). The social identity theory of intergroup behavior. In S. Worchel & W. G. Austin (Eds.), *Psychology of intergroup relations* (pp. 7–24). Chicago, IL: Nelson-Hall.

The Economist. International: It may make life easier and cheaper; East Africa gets broadband. 391(8636), 46.

The New Nation. (2009, October 5). Cell phone crime rise: Extortions go on unabated. Internet Edition. http://nation.ittefaq.com/issues/2009/10/05/news0827.htm. Accessed 5 October 2009.

thestate.com. (2008, April 15). Intel adds new features to low-cost laptops. http://www.thestate.com/business/story/376162.html. Accessed 27 October 2009.

Ticoll, D. (2004, October). IT industry trade associations and the globalization of knowledge work. *Review of NASSCOM and the Irish Software Association*. http://www.itac.ca/Archive/PolicyandAdvocacy/Outsourcing/04OctITIndustryTrade-AReviewofNASSCOM.pdf. Accessed 27 October 2005.

tribuneindia.com. (2005, June 25). Outsourcing crime Call centre expose can wreak havoc. http://www.tribuneindia.com/2005/20050625/edit.htm. Accessed 27 October 2006.

Trombly, M. (2006). India tightens security. *Insurance Networking & Data Management, 10*(1), 9.

Trombly, M., & Yu, W. (2006). Outsourcing resilient in India. *Securities Industry News, 18*(26), 1–21.

US Commercial Service. (2004, October 15). Approximately 58% of China's internet users experience security problems. China Commercial Brief – American Embassy, Beijing, 2(168). http://www.buyusa.gov/china/en/ccb041015.html. Accessed 27 October 2005.

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.

Vardi, N. (2005). Chinese take out. *Forbes*, 54.

Vassilev, R. (2003). De-development problems in Bulgaria. *East European Quarterly, 37*(3), 345.

Viano, E. C. (1999). *Global organized crime and international security*. Burlington, VT: Ashgate Publishing.

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 27 October 2005.

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 5 October 2009.

WEBWIRE. (2008, June 25). First told of Chinese PC hijack explosion. http://www.webwire.com/ViewPressRel.asp?aId=68776. Accessed 27 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.

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

Wylie, I. (2007). 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.

Zweynert, J., & Goldschmidt, N. (2006). The two transitions in Central and Eastern Europe as processes of institutional transplantation. *Journal of Economic Issues, 40*(4), 895–918.