The Simple Economics of Cybercrimes

By: Nir Kshetri

Kshetri, Nir (2006), "The Simple Economics of Cybercrimes", *IEEE Security and Privacy, January/February, 4 (1),* 33-39.

***** Made available courtesy of Institute of Electrical and Electronics Engineers: http://www.ieee.org/**

(c) 2006 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other users, including reprinting/ republishing this material for advertising or promotional purposes, creating new collective works for resale or redistribution to servers or lists, or reuse of any copyrighted components of this work in other works

Abstract:

The characteristics of cybercriminals, cybercrime victims, and law enforcement agencies have a reinforcing effect on each other, leading to a vicious circle of cybercrime. The author builds on key elements of this circle to assess a hacker's cost-benefit calculus, and suggests possible mechanisms for combating cybercrime.

Article:

Cybercrimes are becoming increasingly pervasive and sophisticated and have more severe economic impacts than many conventional crimes. The US Federal Bureau of Investigation (FBI) has reported that cybercriminals have attacked almost every Fortune 500 company at some time (see www.fbi.gov/publications/leb/2002/june2002/june02leb.htm). An estimate from MailFrontier, an email security company, suggested that fraudulent email messages totaled 80 million in September 2003, 43 percent more than in August 2003. [1] And according to a September *Wall Street Journal* article, [2] Internet-related fraud accounted for 53 percent of consumer-fraud complaints made to the US Federal Trade Commission (FTC) in 2004. Cybercrime and cyberterrorism are currently the FBI's number three priority, behind only counterterrorism and counterintelligence.

To combat this growing form of criminality, we need a clearer understanding of cybercrimes' costs, benefits, and attractiveness. Cybercrimes are structurally unique in three main ways:

- They're technologically and skill-intensive.
- They have a higher degree of globalization than conventional crimes (see Table 1).
- They're relatively new.

Unlike conventional crimes against people or property such as arson, burglary, or murder, most cybercrimes require significant skill. Even script kiddies that use someone else's tools to commit victimless or marginal cybercrimes possess more skills than their conventional-world counterparts. Given the Internet's global nature, cybercrimes entail important procedural and jurisdictional issues. Additionally, due primarily to cybercrimes' newness, law enforcement authorities worldwide are relatively inexperienced at dealing with them. All these factors are likely to result in fewer consequences for cybercrimes compared to conventional crimes.

In this article, we assess the cost-benefit structure of cybercriminals. From the potential victims' perspectives, an economic analysis can help explain the optimum investment necessary as well as the measures required to prevent hackers from cracking into their computer networks. [3] Our analysis from the cybercriminal's viewpoint also provides insight into factors that might encourage and energize his or her behavior.

The vicious circle

We define a cybercrime broadly as a crime that employs a computer network during any phase. Examples include critical infrastructure attacks, online fraud, online money laundering, criminal uses of Internet communications, ID fraud, use of computers to further traditional crimes, and cyberextortions.

The characteristics of cybercriminals, cybercrime victims, and law enforcement agencies have created a vicious circle of cybercrime. Figure 1 shows this circle's key elements. Law enforcement agencies such as police forces and the FBI are inexperienced with these new forms of crimes; in fact, localized police forces in most countries aren't equipped to deal with cybercrimes' global nature. They also face shortages of manpower for handling cybercrimes—in November 2004, a senior official from the Internet Crime Complaint Center (I3C) reported that the FBI has been unable to recruit and retain the best available IT talent. According to an article published in *The Washington Post* (17 May 2000, p. A.18), only 2 percent of US police personnel were trained in cyberforensics. Moreover, cybercrimes are increasingly sophisticated, and new forms and methods of such crimes are developing rapidly. Law enforcement agencies lack resources and have failed to catch up to the technologies that enable such crimes. As a *Business Week* article notes, "Cops don't have all the weapons they need to fight back [against cybercriminals]. They clearly lack the financial resources to match their adversaries' technical skills and global reach" (30 May 2005).

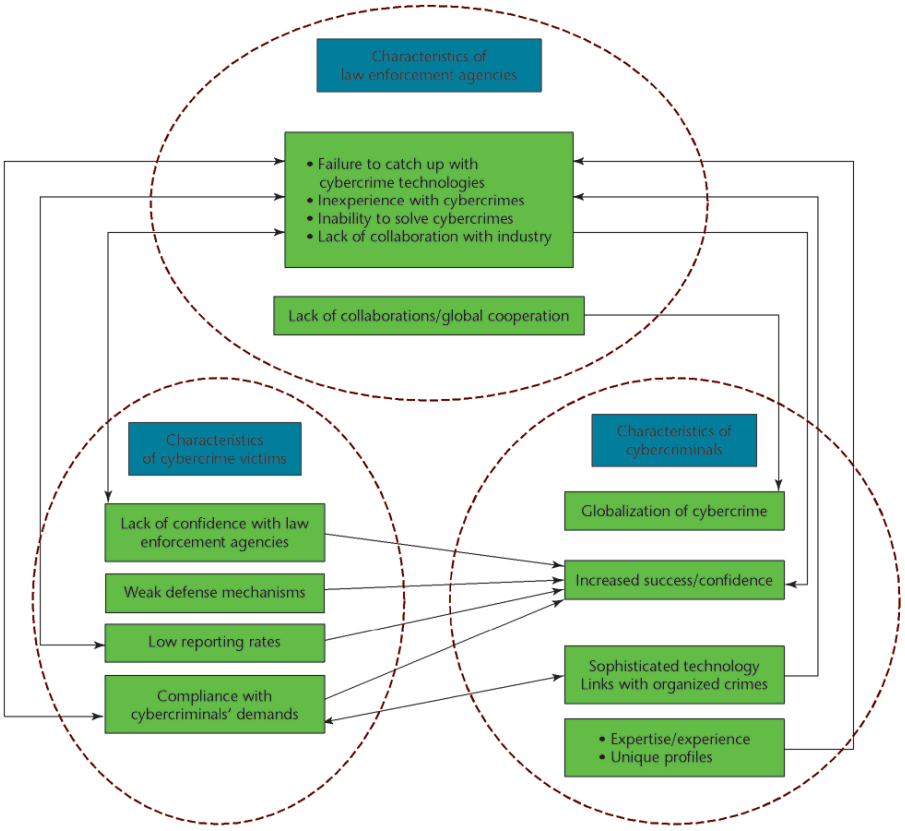

Figure 1. The vicious circle of cybercrimes. The proposed framework outlines how the characteristics of cybercriminals, law enforcement agencies, and cybercrime victims shape the cybercrime landscape.

Cybercrime investigations are highly complex as well as resource- and expertise-intensive, thus many small countries don't investigate all reported cybercrimes. In Indonesia, for instance, law enforcement investigates only 15 percent of reported incidents (see www.cnn.com/2003/WORLD/asiapcf/southeast/02/06/indonesia.fraud/). Accordingly, law enforcement agencies' inability to solve cybercrimes reinforces cybercriminals' confidence as well as victims' unwillingness to report such crimes (see Figure 1).

Cybercriminals' unique profiles are significantly different from those of conventional criminals. No cybercriminal database exists with law enforcement agencies, which further hampers their ability to solve cybercrimes. In Russia, for instance, most hackers are young, educated, and work independently, and thus they don't fit conventional criminal profiles.

In the conventional world, most crimes occur close to criminals' homes. They travel far only if there are sufficient incentives to leave a known territory. [4] Some crimes, such as kidnapping or robbing a bank, make traveling lucrative and require careful planning. Crimes in the digital world differ significantly in this dimension. Information and communications technologies have drastically increased the porosity between national borders. [5] Moreover, the Internet's anonymity superimposes a complex interaction that enables criminal and violent groups, transnational terrorist organizations, and companies engaged in espionage to expand their operations globally without leaving home. A high proportion of cybercrime investigations thus have significant jurisdictional issues. In many cases, cybercrimes that cross borders slow down the responses to such crimes.

National boundaries have thus created serious obstacles for law enforcement agencies. Collaboration and cooperation among agencies in different jurisdictions can help, but this is a far-from-sufficient solution. To take one example, although Russia signed agreements with the US to help investigate numerous crimes, cybercrimes aren't among them. [6] In 2000, the FBI arrested two Russian hackers by luring them to the US with job offers. FBI agents handling the case later downloaded data from the hackers' computers located in Chelyabinsk, Russia. In 2002, however, Russia filed hacking charges against the FBI, arguing that it was illegal to download data from computers located in Russia. Similarly, in 2001, the US Department of Justice requested the help of Russian authorities in prosecuting cybercriminals that attacked US computer networks but received no response. [5] Experts argue that countries such as China and Russia ignore cybercrimes unless such crimes negatively impact their national interests.

Cybercrime laws also have a high degree of international heterogeneity. The Council of Europe's Convention on Cybercrime, for example, is the first international cybercrime treaty. Although 34 countries participated in the ceremonial act of signing the convention in November 2001, most haven't agreed to abide by its rules. As of June 2004, the only countries ratifying the convention were Albania, Croatia, Estonia, Hungary, Lithuania, and Romania (www.epic.org/privacy/intl/ccc.html). Likewise, industrialized countries are working on international cooperation to combat cybercrimes, but poor countries aren't yet involved in these discussions. Many countries haven't enacted any cybercrime laws. Consequently, Japanese gangs hire Russian hackers to attack law enforcement agencies' databases, [7] while Australian swindlers have established links with Russian and Malaysian organized crime networks to transfer stolen money from overseas banks they've hacked into. [8]

Cybercrimes are also among the most underreported forms of criminality. Cybercrime victims' unwillingness to report such crimes to law enforcement agencies further encourages cybercriminal behavior (see Figure 1). One estimate suggests that only 17 percent of companies report cybercrime-related losses to law enforcement (see www.police.govt.nz/events/2001/e-crime-forum/cybercrime_and_its_effects.html). Many victims are unwilling to report cybercrimes because they think that going to law enforcement won't stop an attack. Other factors could be embarrassment, the fear of losing customer trust, the damage in corporate credibility, and potential falling stock prices. Banks, financial institutions, and other businesses that deal with sensitive data are especially reluctant to turn investigations over to the authorities. According to the *Computer Crime and Security Survey*, 70 percent of those not reporting cybercrimes cited negative publicity as a reason. Difficulties related to documentation and proof further discourage businesses from reporting cybercrimes.

Evidence indicates that criminals' skill, intelligence and experience covary positively with the odds of getting away with crimes. Some professional cybercriminals are highly skillful and thus face very low odds of getting caught. For instance, Russian mafia hack rings are reportedly operated by former KGB agents. [9] Additional evidence shows that less skillful criminals get help from experienced hackers and transnational organized crime groups, making them less likely to get caught. [7]

Weakness of defense mechanisms also co-varies positively with the likelihood of attack. Although some weaknesses are technological, others are behavioral or perceptual in nature. Consider, for instance, phishing—acquiring personal information fraudulently by tricking an Internet user. Experts say the key to combating phishing lies in consumers' ability to distinguish between real and fraudulent email. A MailFrontier study from 2003 indicated that 40 percent of people reading a fraudulent Citibank email believed it to be real. [1]

Moreover, some companies negotiate with cybercriminals by paying ransom. Estimates suggest that online gambling sites alone have paid millions of dollars to cyberextortionists. To take one example, in September 2003, Antigua-based World Wide Tele-Sports (BetWWTS.com) paid US$30,000 to cyberextortionists after attacks on the company's networks resulted in customers being unable to place wagers estimated at US$5 million. [10] For some companies, paying extortionists is cheaper than facing an attack. Just a few hours of downtime during peak operations (for example, Super Bowl weekend) might have cost online casinos up to US$1 million (see www.cnn.com/2004/TECH/internet/01/30/internet.crime.reut/index.html).

A lack of industry–government collaboration also hampers law enforcement's ability to solve cybercrimes. Given that private sectors own roughly 90 percent of all critical infrastructures in the US, many cybercrimes can't be solved without their help (see www.govexec.com/features/1103/1103view.htm). An estimate suggests that 80 percent of global email traffic, including most spam, comes via the Webmail services of global providers such as AOL, MSN, and Yahoo. Law enforcement agencies frequently express concern over service providers' unwillingness to cooperate in cybercrime investigations.

Increased success is making cybercriminals more brash and disrespectful of law enforcement agencies. Several international hackers, for instance, don't conceal their real identities or origin of their mailings anymore. Furthermore, many organized criminals have invested illegally earned income in new technologies and in globalizing their operations.

A cybercriminal's cost–benefit calculus

Following the approach used by economists, a cybercriminal must weigh the benefits and costs to decide whether to commit a crime. [11] A cybercrime occurs if

$$M_b + P_b > O_{cp} + O_{cm} P_a P_c, \qquad (1)$$

where M_b equals the monetary benefits of committing the crime; P_b equals the psychological benefits of committing the crime; O_{cm} equals the monetary opportunity costs of conviction; O_{cp} equals the psychological costs of committing the crime; P_a equals the probability of arrest; and P_c equals the probability of conviction. The product term on the right, $O_{cm}P_aP_c$, is also called the *expected penalty effect*.

Monetary benefits

The cybercrime landscape is rapidly changing in terms of hackers' monetary motives. An article published in IDG News Service on May 28 (www.pcworld.com/news/article/0,aid,116304,00.asp) quotes a Russian hacker employed as a security expert: "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." According to market research firm IDC, more than 60 percent of computer hackers targeted financial institutions in 2003 (see www.usatoday.com/printedition/money/20041021/cybercrimecover.art.htm). Moreover, as we've already discussed, some companies comply with cybercriminals' demands and pay ransom, increasing cybercrimes' expected monetary benefits.

Psychological benefits

Few crimes offer as much psychological benefit to criminals as cybercrimes. We can better explain psychological benefits in terms of *intrinsic motivations*—intrinsically motivated individuals do activities for "inherent satisfactions rather than for some separable consequence" and they "act for the fun or challenge

entailed rather than because of external prods, pressures, or rewards." [12] Maverick hackers testing their skills and looking for fun, for example, act for purely psychological rather than monetary benefits.

Some psychologists' conceptualization of intrinsic motivation is broader, [13] and includes acting on the basis of principle. Some hackers are socialized into acting appropriately and in a manner consistent with group norms. Gaining the respect of their peer hackers is a source of psychological benefit for them. The members of the Honker Union of China (or the Red Hackers), for example, are expected to behave according to their organizations' guidelines.

A feeling of vindication against a symbolic enemy can also provide psychological benefits to hackers. An organization becomes a hacking unit's symbolic foe for many reasons. One example is the 1998 attack during which six hackers from the US, the UK, the Netherlands, and New Zealand (identifying themselves as Milworm) attacked the Web sites of India's Bhabha Atomic Research Center and left the message, "If a nuclear war does start, you will be the first to scream" (see www.afsa.org/fsj/sept00/Denning.cfm). In 2001, Cyberjihad, a group of hackers in Indonesia, attacked the Indonesian police's Web site to force them to free a militant Muslim leader. [14] Apart from nationalism and religion, hackers' interests are also framed by the fight against global capitalism. Such hackers attack the networks of the big multinationals.

Government-backed cyberwars also fall in this category. Several such wars are fought for intangible goals, such as dominance and prestige rather than material gain. The US National Security Agency believes that Iran, North Korea, Russia, and China have developed computer attack capabilities and trained hackers in Internet warfare. [15] Observers believe some of these countries are systematically probing US computer networks to find vulnerabilities. Similarly, Burma's government has reportedly built up an advanced cyberwarfare department within the police force, which tracks its online critics and sends viruses attached in emails to exiled activists. [16]

Psychological costs

Psychological costs, like benefits, are intangible, but they're still costs and are associated with the psychological and mental energy needed to commit cybercrimes. They result from the fear or apprehension of punishment, from guilt, and so on.

It's important to ask whether cybercriminals feel guilt or remorse after cracking into a computer. Experts argue that most people using computer networks unethically don't perceive their actions' ethical implications. [17] The technology's novelty; a lack of previously developed mechanisms and established codes, policies, and procedures; and the lack of easily identifiable victims in many cases [18] lead to less guilt in cybercrimes compared to conventional ones.

Research has indicated that sociocultural practices and political and economic systems are tightly linked to crimes. We can thus hypothesize that guilt isn't equally pervasive across hackers from different sociocultural backgrounds. Put differently, a cybercrime's psychological cost is a function of the hacker's sociocultural background. Many Indonesian hackers, for instance, feel cyberfraud is "wrong" but acceptable if a victim is rich and not an Indonesian. A carder (someone who uses stolen credit-card information to buy items online) reportedly said, "I only choose those people who are truly rich. I'm not comfortable using the money of poor people. I also don't want to use credit cards belonging to Indonesians. Those are a carder's ethics." [12]

Monetary opportunity costs

The monetary costs of conviction are incurred when cybercriminals forego monetary income to serve out a criminal sentence. If a hacker is sentenced to a three-year prison term, for example, and if he or she can legally earn US$20,000 per year, the sentence would cost US$60,000. Recently, many countries have enacted stricter laws against cybercrimes that have increased the opportunity costs of conviction. Nonetheless, many countries have no laws at all against cybercrimes—or zero opportunity costs of conviction. As an example, when a Philippino hacker launched the "Love Letter" virus in 2000, the estimated damage in the US was between US$4

and 15 billion. [19] But the US government could do nothing to prosecute the hacker or to recover the damages because at the time, the Philippines had no laws prohibiting such crimes.

In some economies, the lack of employment opportunities results in a low perceived monetary opportunity cost of conviction. A self-described hacker from Moscow told reporters that "Hacking is one of the few good jobs left here." [10] In Russia, many students with outstanding performance in mathematics, physics, and computer science have difficulty finding jobs. The situation is exacerbated by a financial crash in 1998 that left many computer programmers unemployed. Regarding computer attacks originating from Romania, the US-based Internet Fraud Complaint Center, run by the FBI and the National White Collar Crime Center, has reported that "frustrated with the employment possibilities offered in Romania, some of the world's most talented computer students are exploiting their talents online" (see http://ro-gateway.ro/node/185929/comnews/item?item_id=223937/).

The probability of arrests and conviction

Among reported cybercrimes, arrest rates are very low. Arrest entails identifying the pool of potential suspects and narrowing it down by eliminating innocents. Cybercrimes' structure makes it difficult to identify this pool, however. The proportion of investigated identity thefts (most of which employ the Internet), for instance, is estimated to be fewer than 1 in 700. [20]

A cybercrime's conviction phase, which requires proof beyond reasonable doubt, is equally complex. Difficulties related to furnishing documentation and proof to establish that a cybercrime has been committed compound the problem. Additionally, cybercrimes' newness presents a challenge to the court system. For small cases, few attorneys will take cyberfraud cases. Experts also say that explaining Internet-related crimes to judges is difficult.

Mechanisms for combating cybercrimes

Without appropriate measures to combat cybercrimes, the vicious circle's elements reinforce each other and lead to public distrust of law enforcement agencies and increased confidence in cybercriminals, resulting in more and serious cybercrimes. So where should we start to break this circle and to alter the cost ¬benefit calculus associated with committing cybercrimes?

No pure technological solution exists for such security-related problems. Micro- and macro-level measures combining technological and nontechnological fixes are thus needed to combat cybercrimes. At the micro level, ensuring that technological and behavioral factors are given equal consideration during computer networks' design and implementation is crucial. Technological measures range from simply disconnecting databases containing sensitive information from the Internet to deploying sophisticated antifraud technologies such as RF fingerprinting. Similarly, simple behavioral measures can stop some serious cybercrimes. A simple training strategy aimed at improving the ability of consumers, employees, and the public to distinguish a fraudulent email from a real one could reduce a significant proportion of phishing-related cybercrimes. [1]

At the macro level, developing national technological and manpower capabilities, enacting new laws, promoting a higher level of industry-government collaborations, and pushing for international coordination are critical to combating cybercrime. Given cybercrimes' global nature, international institutions especially carry enormous power that we must harness to fight such crimes. More than 25 years ago, Louis Henkin [21] noted that "almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time." As an example, the International Telecommunications Union (ITU) counts both nations and corporations among its members. Thus, it can both influence its corporate members to design systems with specified security standards and persuade national members to enact and enforce cybercrime laws. Another example comes from the UN Commission on International Trade Law (UNCITRAL), which undertook works leading to the adoption of the Model Law on E-Commerce, which attempts to create a more secure legal environment for online transactions. Many countries have enacted new e-commerce laws using the UNICITRAL model law as a guideline. We need more such laws promoting international harmonization to combat cyberattacks.

Investing in training law enforcement authorities could also enhance nations' abilities to fight cybercrimes and thus increase the probability of arrest and conviction. Like other criminals, [22] we can assume that cybercriminals are risk takers, not risk avoiders. Measures taken so far have mainly emphasized increasing penalties rather than increasing arrests. The US Patriot Act, for instance, brought cyberattacks into the definition of terrorism with penalties of up to 20 years incarceration. A punishment's severity is important, but still more critical is the certainty of punishment. [22]

Organizations established to combat cybercrimes—such as the UK's National Hi-Tech Crime Unit (www.nhtcu.org) and the US National White Collar Crime Center (www.nw3c.org)—are far from effective in dealing with cybercrimes that originate in foreign locations. No other crime needs more worldwide collaboration and cooperation. Although some signs of improvement have materialized, nations have a way to go before they can achieve even moderate success. Cooperation among governments in countries with high concentrations of cybercrimes is especially critical (see Table 1). Moreover, societies that have weak or no cybercrime laws, and in which sociocultural practices provide some legitimacy to such crimes, are likely to provide fertile ground for cybercriminals. International measures to help these countries enact cybercrime laws are crucial. Given that most serious viruses, such as the Love Bug, originate in developing countries, the industrialized world can't solve cybercrimes without their help.

Table 1. Worldwide cybercrime statistics.

COUNTRIES GENERATING MOST ONLINE FRAUD*	RANK ACCORDING TO % OF FRAUDULENT ORDERS§	RATE OF ATTACKS (HIGHEST TO LOWEST) PER 10,000 INTERNET USERS†	NUMBER OF ATTACKS PER 10,000 INTERNET USERS‡	TOTAL ATTACKS (%)‡
Ukraine	Yugoslavia (1)	Panama	Kuwait (50.8)	US (40)
Indonesia	Nigeria (2)	Hong Kong	Israel (33.1)	Germany (7.6)
Yugoslavia	Romania (3)	Macau	Iran (30.8)	South Korea (7.4)
Lithuania	Pakistan (4)	Qatar	Peru (24.5)	China (6.9)
Egypt	Indonesia (5)	Israel	Chile (24.4)	France (5.2)
Romania	Macedonia (6)	Turkey	Nigeria (23.4)	Canada (3.0)
Bulgaria	Bulgaria (7)	Bosnia and Herzegovina	Morocco (22.3)	Italy (2.7)
Turkey	Ukraine (8)	Canada	Hong Kong (22.1)	Taiwan (2.4)
Russia	Lebanon (9)	Luxemburg	Puerto Rico (20.8)	UK (2.1)
Pakistan	Lithuania (10)	Spain	France (19.9)	Japan (2.1)
Malaysia			Argentina (19.3)	
Israel			Belgium (17.6)	
			Romania (16.5)	

Sources: *www.ocalasmostwanted.com/online_fraud_stats.htm; §www.msnbc.msn.com/id/4648378/; †last half 2004, www.symantec.ca/region/cz/czpress/download/istr_vii_finalfull.pdf; ‡first half 2002, www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report_vII.20020708.pdf.

An appropriate response to organized crime's investment in cybercrime technologies would be to increase business ¬government collaboration in developing and deploying antifraud technologies and fraud-detection software. Currently, deployment of antifraud technologies is limited to a small, elite group of businesses. We must take measures to accelerate the diffusion of such technologies among small- and medium-sized enterprises.

In the conventional world, research has indicated that the time it takes a victim to report a crime is one of the most important factors in increasing the probability of arrest. This is especially important with crimes for which preserving evidence is critical for a successful prosecution. For many cybercrimes, successfully prosecuting offenders might require us to preserve physical as well as digital evidence. It's thus important to report a cybercrime to law enforcement authorities as soon as possible.

Conclusion

Clearly, more research must occur to fully determine how economic, political, and social factors affect a hacker's assessment of costs and benefits associated with cybercrimes. The preliminary evidence I've discussed

indicates the shift in hackers' motivations from intrinsic to extrinsic. In this regard, another fruitful avenue for future research is to understand the determinants of this turning point. In-depth interviews with extrinsically motivated hackers would help understand how economic and institutional factors transform their motivations for attacking computer networks.

References

1. A. Salkever, "'Phishing' Is Foul on the Net," *Business Week Online*,21 Oct. 2003; www.kroening.com/papers/dsn2003.pdfwww.businessweek.com/ technology/content/oct2003 tc20031021_8711_tc047.htm.
2. D. Bank and R. Richmond, "Where the Dangers Are: The Threats To Information Security That Keep The Experts Up At Night— And What Businesses And Consumers Can Do To Protect Themselves," *Wall Street J.*,18 July 2005, p. R1.
3. R. Anderson and B. Schneier, "Economics of Information Security," *IEEE Security & Privacy*, vol. 3, no. 1, 2005, pp. 12–13.
4. P.J. van Koppen and R.W.J. Jansen, "The Road to the Robbery: Travel Patterns in Commercial Robberies," *British J. Criminology*, vol. 38, no. 2, 1998, pp. 230–246.
5. J.N. Rosenau, "Security in a Turbulent World," *Current History*, vol. 94, no. 592, 1995, pp. 193–200.
6. R. Lemos, "FBI 'Hack' Raises Global Security Concerns," *CNet News*,1 May 2001; http://news.com.com2100-1001-950719.html .
7. "Crime without Punishment: Russian Organised Crime," *The Economist*, vol. 352, no. 134, 28 Aug. 1999, pp. 17–19.
8. "Caught in the Net: Australian Teens," *Foreign Policy*, Mar./Apr. 2005, p. 92.
9. R.E. Bell, "The Prosecution of Computer Crime," *J. Financial Crime*, vol. 9, no. 4, 2002, pp. 308–325.
10. C. Walker, "Russian Mafia Extorts Gambling Websites," June 2004; www.americanmafia.comFeature_Articles_270.html .
11. J.R. Clark and W.L. Davis, "A Human Capital Perspective on Criminal Careers," *J. Applied Business Research*, vol. 11, no. 3, 1995, vol. 58–64.
12. E.L. Deci and R.M. Ryan, *Intrinsic Motivation and Self-Determination in Human Behavior*, Plenum Press, 1985.
13. S. Lindenberg, "Intrinsic Motivation in a New Light," *Kyklos*, vol. 54, nos. 2–3, 2001, pp. 317–342.
14. Antariksa, "I Am a Thief, Not a Hacker: Indonesia's Electronic Underground," *Latitudes Magazine*, July 2001, pp. 12–17.
15. R. Lenzner and N. Vardi, "The Next Threat," *Forbes*,20 Sept. 2000, p. 70.
16. J. Havely, "When States Go to Cyber-War," *BBC News*,16 Feb. 2000; http://news.bbc.co.uk/1/hi/sci/tech642867.stm .
17. E.A. Kallman and J.P. Grillo, *Ethical Decision Making and Information Technology*, 2nd ed., McGraw Hill, 1996.
18. S. Phukan, "IT Ethics in the Internet Age: New Dimensions," *Proc. Informing Science & IT Education Conf.* (InSITE), Informing Science Inst., 2002; http://proceedings.informingscience.org/ IS2002Proceedings/papersphuka037iteth.pdf .
19. J. Adams, "Virtual Defense," *Foreign Affairs*, May/June 2001, pp. 98–112.
20. M. Boal, "Being Bill Gates, Steven Spielberg, Martha Stewart, George Soros, Charles Schwab: How the Most Brazen Identity Thief Almost Got Away with It," *Reader's Digest*, Mar. 2005, pp. 161–173.
21. L. Henkin, *How Nations Behave*, Council on Foreign Relations, 1979.
22. G.S. Becker, "The Economics of Crime," *Cross Sections*, Fall 1995, pp. 8–15; www.richmondfed.org/publications/economic_research/ the_economics_of_crimeindex.cfm .