Positive Externality, Increasing Returns, and the Rise in Cybercrimes

By: Nir Kshetri

Kshetri, Nir (2009) "Positive Externality, Increasing Returns and the Rise in Cybercrimes" *Communications of the ACM, 52(12), 141-144.*

***** Made available courtesy of Association for Computing Machinery: http://doi.acm.org/10.1145/nnnnnn.nnnnnn**

Article:

The meteoric rise in cybercrime has been an issue of pressing concern to our society. According to Federal Bureau of Investigation (FBI), nine out of 10 U.S. companies experienced computer security incidents in 2005 which led to a loss of $67.2 billion. A survey conducted by IBM found that U.S. businesses worry more about cybercrimes than about physical crimes. Internet-related frauds accounted for 46% of consumer complaints made to the Federal Trade Commission (FTC) in 2005. Total losses of Internet fraud victims reporting to FTC increased from $205 million in 2003 to $336 million in 2005. In a July 2007 interview with USA Today, McAfee CEO reported that his company received 3,000-5,000 threat submissions per day from customers and 10% of them were new.

This paper offers an economic analysis to explain cybercrimes' escalation. We define cybercrimes as criminal activities in which computers or computer networks are the principal means of committing an offense. Examples include cyber-theft, cyber-trespass, cyberobscenity, critical infrastructure attacks and cyber-extortions.[6] The most notable features of the cybercrime environment include newness, technology and skill-intensiveness, and a high degree of globalization. Factors such as a wide online availability of hacking tools, information sharing in the cyber-criminal community, availability of experienced hackers' help to less skillful criminals and congestion in law enforcement systems produce externality effects within the cybercriminal community as well as across society and businesses.

We focus on three positive or self-reinforcing feedback systems to examine increasing returns in cybercrime related activities. In this article, we first provide an overview of the positive feedback loops that reinforce cybercriminals' behavior. Then, we describe mechanisms associated with externality in cybercrime related activities.

Increasing Returns and Feedback Loops in Cybercrimes

Increasing returns approach help explain how firms, innovations, industries, and the environment influence each other. The law of increasing returns argues that economies of scale, decreasing costs and feedback mechanisms lead to a further success of already successful entities. W.B. Arthur[1] notes: "Increasing returns are... mechanisms of positive feedback that operate—within markets, businesses, and industries—to reinforce that which gains success or aggravate that which suffers loss." This article explores evidence of increasing returns in cybercrime activities.

There are three types of self-reinforcing feedback systems: economic, sociopolitical and cognitive.[1,7] Cybercrimes' significant financial benefits provide a positive economic feedback to cyber-criminals. An IDG News Service article (May 28 2004) quoted a Russian hacker: "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." A low probability of cyber-criminals' being caught and prosecuted[6] and less severity of punishment give them a high positive economic feedback .[3]

Sociopolitical feedbacks are related to formal and informal institutions.[8,12] Social feedbacks are linked to informal institutions such as sanctions applied by a social group to exclude a cybercriminal from one's circle of friends. Political feedbacks, on the other hand, are applied by regulative institutions.

Cognitive feedback loops are associated with cognitive programs that are built on mental maps of individual hackers. Put differently, cognitive systems influence the lens through which existing and potential criminals view cybercrimes.[12] Effects such as enjoyment from and less guilt in cybercrimes serve as cognitive feedbacks.

Mechanisms Associated with Externality in Cybercrimes

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.

We examine three mechanisms that may give positive feedback to cybercriminals: inefficiency and congestion in the law enforcement system, acceleration of the diffusion of cybercrime know-how and technology and increase in potential criminals' predisposition toward cybercrimes.[5,11] From victims' perspective, there is arguably a vicious circle of cybercrimes linking characteristics of cyber-criminals, cybercrime victims, and law enforcement agencies[6] and a corresponding virtuous circle for cyber-criminals. These externality mechanisms strengthen the elements of the vicious circle for victims and of the virtuous circle for criminals.

Table 1 presents how the externality mechanisms and the feedback systems described here are intertwined.

Table 1: Externality mechanisms and feedback systems producing increasing return in cybercrime related activities

Externality mechanisms → / Feedback system ↓	Inefficiency and congestion in the law enforcement system (Assessment of risks related to cybercrimes)	Diffusion of cybercrime know-how and technology (Ability to commit cybercrimes)	Increased predisposition toward cybercrime (Willingness to commit cybercrimes)
Economic	• Law enforcement agencies' lack of resources. • Sophistication in cybercrimes. • No cyber-criminal database. • Difficult to explain in courts.	• Easily available hacking tools. • Schools teaching hacking skills in some countries.	• Over-educated and under-employed specialists in some countries. • Increasing financial incentive for hackers.
Sociopolitical	• Weak cybercrime laws in some countries. • Jurisdictional arbitrage. • Lack of industry-government collaboration. • Lack of international cooperation.	• Less skillful criminals get help from experienced hackers/crime groups. • Information sharing among hackers.	• Ideological hackers: obligation based intrinsic motivations. • Social obligations. • Cybercrimes are acceptable in some societies.
Cognitive	• Victims' lack of confidence with law enforcement: unwillingness to report cybercrimes.	• Ease of use of hacking tools.	• Enjoyment-based intrinsic motivations. • Compliance with cyber-criminals' demands: more confidence. • Less guilt.

Ineffciency and Congestion in the Law Enforcement System

Congestion and inefficiency in law enforcement systems arise from factors such as newness of cybercrimes, a low governmental priority, a lack of cross-border, and industry-government cooperation and victims' unwillingness to report.[6] In the U.S., attempts to regulate cyberspace to protect children faced oppositions from groups which argue that such measures undermine free speech. Some countries are also slow to enact cybercrime laws.

Law enforcement agencies such as police forces and the FBI are inexperienced with cybercrimes. Cyber-criminals and victims tend to be scattered across the country and the world, posing logistical challenges. At the

same time, while large law enforcement agencies such as FBI have developed some capacity to deal with cybercrimes, localized police forces aren't equipped to deal with national and global nature of cybercrimes. They are also facing manpower shortages. According to a Washington Post article (May 17, 2000), only 2% of U.S. police personnel were trained in cyber-forensics.

Law enforcement agencies lack sufficient resources to fight cybercrimes. For instance, in 2005, FBI spent $150 million on cybercrimes out of its $5 billion budget. Similarly, the U.K.'s National Hi-Tech Crime Unit could not convince cybercrimes' seriousness to the government and secured only half the funds needed. A Business Week article notes: "Cops don't have all the weapons they need to fight back. They clearly lack the financial resources to match their adversaries' technical skills and global reach" (May 30, 2005).

Beyond all that, conventional crimes have diverted law enforcement agencies' attention away from cybercrimes. For instance, at a U.S. Senate Judiciary Subcommittee on Crime and Drugs meeting in May 2007, leaders of national law enforcement organizations noted that budgetary cuts to programs such as the Community Oriented Policing Service (COPS) have led to escalation in violent crimes and "adversely affected local crime prevention and local law enforcement initiatives."

In poorer nations, fighting cybercrime gets a lower priority. In Indonesia, the police say they lack expertise and resources to fight against cybercrimes. The country's Information Technology Sub-Directorate of the Directorate of Special Crimes of the National Police Headquarters had only one dial-up connection in 2002. Moreover, Indonesian police use a 'red book,' a manual to conduct credit card investigations, to handle Internet credit card frauds. Estimates suggest that only 15% of reported incidents are investigated in Indonesia.

Cybercrimes are increasingly sophisticated and new forms and methods are developing rapidly. Law enforcement agencies have failed to catch up with the constant progressive nature of such crimes.

A further congestion in the law enforcement system is caused by unavailability of cyber-criminals' database. Most of the new breed of criminals' profile differs from conventional criminals.' In Russia, for instance, most hackers are young, educated, and work independently and thus do not fit conventional criminal profiles.

Digital criminals are also more difficult to catch and prosecute than conventional ones. In fact, collection and retention of evidence has been a critical challenge facing law enforcement agencies. Estimates suggest that the U.S. Department of Justice declines to prosecute up to 78% of cases mainly because of a lack of evidence.[2]

Cybercrimes' newness has also presented challenges to the court system. For small cybercrime cases, it is difficult to find an attorney. Experts also say that explaining cybercrimes to judges is difficult.

Another point to bear in mind is increasingly transnational and international nature of cybercrimes, which benefit from jurisdictional arbitrage. Organized cybercrimes are initiated from countries with few or no laws and little enforcement capacity. For instance, the U.S. couldn't prosecute the Philippino hacker, who launched the "Love Letter" virus in 2000 because the Philippines had no laws prohibiting cybercrimes that time. Due to newness, jurisdictional arbitrage is higher for cybercrimes compared to conventional crimes.

Additional externality effects concern national boundaries. Collaborations and cooperation among law enforcement agencies in different jurisdictions are insufficient. For example, Russia and the U.S. have signed agreements in many crimes, but not in cybercrimes. Experts also argue countries such as China and Russia ignore cybercrimes unless such crimes jeopardize their national interests.

A lack of industry-government collaboration has also hampered law enforcement agencies' ability to solve cybercrimes. For instance, estimates suggest that 80% of global email traffic including most spams come via Web mail services of global providers such as AOL, MSN and Yahoo. Law enforcement agencies have expressed concern over these providers' unwillingness to cooperate.

Proportionally less cybercrimes than conventional crimes are reported. Some estimates suggest that less than 10% of cybercrimes are reported to authorities. Most businesses don't report cybercrimes because they are embarrassed; think doing so would undermine their credibility, likely lead to bad public relations and damage reputation; and fear their stock prices would drop. Especially financial institutions and businesses dealing with sensitive data such as e-commerce companies are reluctant to turn over the investigation to authorities. Complications related to documentation and proofs further discourage reporting cybercrimes.

Diffusion of Cyber Crime Know-How and Technology

How do cybercrime know-how and technology diffuse? What factors lead to increased width and depth of cybercrime adoption among criminals? Diffusion of cybercrimes can be explained in terms of *relative advantage, compatibility, complexity, observability, and trialability*.[10]

Cybercrimes' principal source of relative advantage stems from the fact that such crimes are less likely to be caught and prosecuted. An estimate of PricewaterhouseCoopers indicated that only about 5% of cyber-criminals are caught. Moreover, cybercrimes can be committed without leaving home. This is contrary to most conventional crimes, for which criminals leave a known territory only for sufficient incentives.

Next, consider compatibility. The Internet has facilitated carrying out of most traditional crimes. The Internet has thus become most criminals' tool.

The natures of the technology and of hacking communities and organized crime groups have greatly reduced the complexity of cybercrime know-how and technology. Most hacking tools are widely available online and require little or no expertise. Less skillful criminals also get help from experienced hackers.

Information sharing in the cybercriminal community also reduces the complexity. Members in the community help fellow hackers accessing a router and getting through a firewall. Moreover, in some countries, specialized schools teach hacking skills. There are also reports that U.S.-based low-end criminals get cybercrime-related helps from Russian and Eastern European professional criminals.

Cybercrimes also induce a perception of a high degree of observability for criminals as they are easy to commit and rewards are high. Some criminals in the conventional world are cashing in on the trend of increased sophistication in cybercrime technologies. For instance, Russian hack rings are reportedly operated by mafia and former KGB agents.

Online availability of hacking tools offers risk-free trial to would be hackers. Recently, quantity and availability of hacking tools have increased, and the quality has improved. Some sources of externalities thus exist in the technology. Evidence also indicates that many college students pirate software and gain illegal access to a computer system to browse and/or exchange information. Such experiences provide 'trial-ability' and help them get their foot in the door of the cybercrime world.

Increased Predisposition Toward Cybercrime

What factors contribute to an individual's willingness to commit cybercrimes? First, crime rates are linked to economic opportunities. Gary Becker3 comments on crimes committed by teenagers: "[L]ow earnings are a factor behind crime, and teenagers have lower earnings and fewer opportunities." According to a March 2007 *McAfee Virtual Criminology Report* produced with the U.S. and European high-tech crime units, 88% of computer science students at a U.S. university admitted committing an illegal act online. A McAfee analyst noted that Crime gangs are recruiting and training teenagers as young as 14 for cybercrimes.

In some economies, the lack of employment opportunities has led to increase in cybercrimes. In Russia and Eastern Europe, students good in mathematics, physics, and computer science are having difficulty to find jobs. Evidence indicates that parents and teachers encourage certain computer crimes such as software piracy thereby

providing social legitimacy to cybercrimes. Cybercrimes are even more justifiable in some societies. An IDG News Service article describes how a Russian hacker-turned-teacher and his friends hacked programs and distributed for free: "It was like our donation to society, it was a form of honor; [we were] like Robin Hood bringing programs to people."

Behaviors of ideological hackers interested in political goals can be explained by obligation/community based intrinsic motivations. Chinese hackers, for instance, have expressed patriotic and nationalistic longings in cyber-wars. They have fought cyberwars with Taiwanese, Indonesians, Japanese and U.S. hackers. Chinese hackers involved in cyber-wars argued that they were patriotic and didn't do anything wrong. Patriotism and nationalism thus provided cognitive legitimacy of these hackers' activities. Other factors energizing ideological hackers include motivation to fight against global capitalism and religion.

Technological, behavioral and perceptual weaknesses in defense are tightly linked with cybercrimes. Cyber-criminals are taking advantage of computer users' ignorance. A 2003 Mail-Frontier study indicated that 40% of people reading a fraudulent Citibank email believed it to be a real. Similarly, a 2005 survey by America Online and the National Cyber Security Alliance found that 80% of the respondents' computers were infected by spyware and almost all were unaware of it. Another survey found that 56% of U.S. home computers have either no or outdated anti-virus software.

At the same time, children's online activities aren't sufficiently monitored. For instance, many parents don't know availability of parental controls options at latest versions of operating systems such as Microsoft's Vista and Apple's Mac OS X Tiger.

Some companies negotiate with cyber-criminals by paying ransom. Estimates suggest that online gambling companies have paid millions of dollars to cyber-extortionists. Increased success is sending positive cognitive messages and making cyber-criminals disrespectful of law enforcement agencies. Many international hackers, for instance, don't conceal their real identities or mailings' origin.

Do cyber-criminals feel guilt after cracking into a computer? Experts argue that most people using computer networks unethically don't perceive their actions' ethical implications. Technologies' novelty; a lack of previously developed mechanisms, codes, policies, and procedures; and the lack of easily identifiable victims lead to less guilt in cybercrimes compared to conventional ones.[9] It is also argued that standards of rules and conducts guiding actions are based on the notion of face-to-face relations. Compared to conventional crimes, people involved in cybercrimes are thus less likely to see their actions' negative impacts. A final concern regards the trend of declining morality. For instance, in the U.S., two-thirds of respondents in a 2004 USA Today/CNN/ Gallup Poll said that "the state of moral values is getting worse."[4] A government-sponsored survey in China reported in the early 2007 found similar trend in the country. Rise in cybercrime is associated with and facilitated by declining morality.

Conclusion

Cybercrimes are costing businesses, especially banks and credit-card companies, and consumers billions of dollars every year. For instance, in 2006, the cost of identity theft, a significant proportion of which is facilitated by the Internet, was estimated at over $50 billion to U.S. businesses plus $5 billion in out-of-pocket expenses. We examined synergies between increasing return activities in cybercrimes. Our analysis of economic, sociopolitical, and cognitive legitimacy to cyber-criminals, which influence the degree of increasing to returns to these criminals, leads to a number of managerial and policy implications.

The battle against cybercrimes must be waged on many fronts. Technological and non-technological measures can reduce the externality effects. At micro level, technological and behavioral factors should be considered in design and implementation of computer networks to provide negative cognitive feedback to cyber-criminals. Technological measures range from disconnecting databases containing sensitive information from the Internet to the deployment of sophisticated antifraud technologies such as eBay's 'spoof detector,' which enables users

to receive alerts when eBay/PayPal pass words are entered in inappropriate login screens and some financial companies' deployment of dummy accounts to trap phishers and tools to detect fake e-commerce/bank Web sites. Similarly, behavioral measures such as trainings to enable consumers, employees and the public to identify fraudulent email messages may reduce phishing.

Research indicates that time taken to report a crime is among the most important factors affecting the probability of arrest. This is especially important for crimes for which preserving evidence is critical for successful prosecutions. Preservation of physical and digital evidence is important to successfully prosecute cyber-criminals. Timely reporting of cybercrimes to authorities thus sends negative cognitive feedback to criminals.

Development of national technological and manpower capabilities; enactment of new laws; a higher level of industry-government collaborations; and international coordination may give cyber-criminals negative cognitive feedbacks. Given cybercrimes' global nature, international institutions especially carry enormous power that must be harnessed.

References

1. Arthur, W.B. Increasing returns and the new world of business. Harvard Bus. Rev. (Jul-Aug. 1996), 101-109.
2. Banisar, D. Computer hacker's sentence spotlights high-tech crime prosecutions. Criminal Justice Weekly, (Aug. 3, 1999).
3. Becker, G. S. The economics of crime. Cross Sections, (Fall 1995), 8-15; http://www.rich.frb.org/pubs/cross/ crime/crime.pdf.
4. Drinkard, J. Nation's moral values declining, most say; Poll: Majority see USA as deeply split. USA Today, (Nov. 23, 2004), A.11.
5. Gaviria, A. Increasing returns and the evolution of violent crime: The case of Colombia, Journal of Development Economics 61, 1, (2000), 1.
6. Kshetri, N. The simple economics of cybercrimes. IEEE Security and Privacy 4, 1 (2006), 33-39.
7. Noda, T. and Collis, D.J. The evolution of intraindustry firm heterogeneity: Insights from a process study, Academy of Management Journal 44, 4 (2001), 897- 925.
8. North, D. C. Institutions, Institutional Change and Economic Performance Cambridge University Press, Cambridge, U.K., 1990.
9. Phukan, S. IT ethics in the Internet age: New dimensions, InSITE, June (2002); http://proceedings. informingscience.org/IS2002Proceedings/papers/ phuka037iteth.pdf.
10 .Rogers, E.M. Diffusion of Innovation, 4th edn. Free Press: NY, 1995.
11. Sah, R. Social osmosis and patterns of crime. Journal of Political Economy 99, 6 (1991), 169–217.
12. Scott, R. Institutions and Organizations, Sage, Thousand Oaks, CA, 2001.