

An Economic Map of Cybercrime

(Working Paper)

Alvaro A. Cárdenas,¹ Svetlana Radosavac,² Jens Grossklags,¹
John Chuang,¹ Chris Hoofnagle¹

¹ University of California, Berkeley

² DOCOMO Communications Laboratories USA, Inc.

1 Introduction

The rise of cybercrime in the last decade is an economic case of individuals responding to monetary and psychological incentives. Two main drivers for cybercrime can be identified: (1) the potential gains from cyberattacks are increasing with the growth of importance of the Internet, and (2) malefactors' expected costs (e.g., the penalties and the likelihood of being apprehended and prosecuted) are frequently lower compared with traditional crimes. In short, computer-mediated crimes are more convenient, and profitable, and less expensive and risky than crimes not mediated by the Internet. The increase in cybercriminal activities, coupled with ineffective legislation and ineffective law enforcement pose critical challenges for maintaining the trust and security of our computer infrastructures.

Modern computer attacks encompass a broad spectrum of economic activity, where various malfeasants specialize in developing specific goods (exploits, botnets, mailers) and services (distributing malware, monetizing stolen credentials, providing web hosting, etc.). A typical Internet fraud involves the actions of many of these individuals, such as malware writers, botnet herders, spammers, data brokers, and money launderers.

Assessing the relationships among various malfeasants is an essential piece of information for discussing economic, technical, and legal proposals to address cybercrime. This paper presents a framework for understanding the interactions between these individuals and how they operate. We follow three steps.

First, we present the general architecture of common computer attacks, and discuss the flow of goods and services that supports the underground economy. We discuss the general flow of resources between criminal groups and victims, and the interactions between different specialized cybercriminals.

Second, we describe the need to estimate the social costs of cybercrime and the profits of cybercriminals in order to identify optimal levels of protection. One of the main problems in quantifying the precise impact of cybercrime is that computer attacks are not always detected, or reported. Therefore we propose the need to develop a more systematic and transparent way of reporting computer breaches and their effects.

Finally, we propose some possible countermeasures against criminal activities. In particular, we analyze the role private and public protection, and the incentives of multiple stake holders.

2 The Cybercrime Ecosystem

Creating an economic map of cybercrime with all the possible entities and their interactions is non-trivial. Computer attacks are implemented in many different forms and their profitability will frequently depend on the specific system under attack. In this paper, we do not attempt to give a complete description of computer crimes; instead, we focus on *pervasive, large scale, and automated* types of computer crime: the use of Trojans to steal credentials from victim computers, and the infrastructure needed to run a botnet. In describing these crimes we also need to describe a large ecosystem of criminals, including exploit writers, malware distributors, and cashiers.

In this section we describe different specialized roles played by cybercriminals in order to support their underground infrastructure and operations. While it is possible that a single person may take on most or all of these possible roles, it is likely that these roles are divided among many entities with different expertise.

2.1 Vulnerability Researchers: Developers of Exploit Tools

Exploiting software vulnerabilities in order to obtain control of multiple computers is the fundamental step in most large-scale cybercrime enterprises. Finding vulnerabilities (especially zero-day exploits [41, 16, 56]) and writing exploit software is one of the difficult aspects of computer attacks (compared to other cybercrime roles). Therefore, it has become a specialized task.

As with many other parts of the cybercrime ecosystem, there are several specialized software tools used to compromise machines (e.g., Luckysploit, Gumblar, Mpack, Zeus, Neosploit, etc.). Therefore, while advanced attackers can write their own exploit code, many other criminals can make use of these readily available tools. While many of these tools can be bought in underground markets (e.g., Neosploit used to provide customer support and also took steps to prevent the spread of pirated copies), other tools are developed and used by closed criminal groups which may consider that selling exploits would give competitive advantage to other criminals.

In addition, a vulnerability researcher may simply sell information about the vulnerability to let others write the exploit code [59]. This case is more likely to happen if the vulnerability researcher is not well connected to underground groups.

The revenue that can be generated from exploiting a vulnerability is a combination of the size of the installed base of vulnerable hosts and the value to an attacker of controlling each host.

2.2 Malware Distributors: Affiliate Programs

Once attackers have access to exploit tools, they still need to find vulnerable computers to exploit.

Traditionally, there were two main methods to find these vulnerable computers: (1) an attacker would probe networks to identify vulnerable computers, or (2) an attacker

would send spam with malware attachments. While these two ways of finding vulnerable computers are still active, currently, the most common way to compromise new computers is through web-based malware. In this kind of attack, cybercriminals take over a web server, turn it into a drive-by-malware site, and “entice” users of vulnerable computers to visit their website.

In order to “entice” users to visit their server, cybercriminals use affiliate programs that pay other criminals for the amount of traffic referred to their malware server [33]. A very popular approach for directing traffic to the malicious server is by infecting legitimate websites and adding an iframe pointing to the malicious server [66, 46]. In addition, cybercriminals may convince rogue website developers to embed malicious code in their websites, or they can distribute malicious “free” third party widgets (such as a website visitor counter) that web site developers incorporate into their own site [66]. 80% of the websites flagged as malicious by antivirus and search engine indexes are legitimate businesses who were abused into redirecting traffic to malicious sites [63].

Some criminals do not know (or do not care) how their software is installed; therefore they will pay other people who compromise computers and install their software [43]. Affiliate programs are not only used to refer web traffic: developers of Trojans, scareware, botnet command and control, and many other types of malware usually pay a network of affiliates for each installation of their programs. Affiliate programs have also been very successful for installing scareware (programs that bombard the victim with fake warnings, indicating that their computer is infected with malware, and urging the victim to pay for a license to the scareware program). Affiliates earn a variable amount for each installation and commissions between 58-90% for completed sales [50].

In addition, some attackers may not want to control the machines after infecting them (or may not have the time or manpower to design campaigns for monetizing the compromised computers); therefore they can sell compromised machines.

2.3 Botnet Herders: Monetizing Compromised Computers

Once an attacker exploits a vulnerability in a computer, it gains control over it and can install any program. One of the first programs attackers install is software with the ability to keep track of all their compromised computers. A set of compromised computers under the control of a single authority is usually called a *botnet*.

By controlling a botnet, an attacker has many ways of monetizing compromised computers. Sources of income include the theft of private information, extortion demands through DDoS attacks, spamming, search engine poisoning, and click fraud [58, 38].

While spamming, phishing, and DDoS attacks can be considered part of the botnet business model, we describe them in more detail in separate sections due to their popularity.

2.4 Phishers, and credential-stealing Trojans

Phishing started as an e-mail fraud method where the perpetrator sends legitimate-looking emails containing links to spoofed web sites in an attempt to obtain confidential financial information from recipients. Web sites that are frequently spoofed by phishers include PayPal, eBay and most well known financial institutions in the US. Users are frequently tricked into giving out confidential information by clicking on links in emails seemingly originating from legitimate financial institutions asking them to update their contact and login information. Once that information is recorded, cyber-criminals can gain the control of the account.

While several phishing attacks are still conducted this way, phishing attacks are now being replaced by credential-stealing trojans. This type of trojan uses keyloggers (and screenloggers) installed in the victims' computers to collect personal information. Clampi, Zeus, and Torpig are some of the many examples of trojans that steal users' data.

In addition to passive monitoring, many of these trojans actively elicit sensitive information from their victims. For example, whenever the infected machine visits one of the domains specified in the configuration file of the trojan (e.g. a banking website), Torpig issues a request to an injection server which provides a form in the login page, asking the user for sensitive information. These – sometimes called man-in-the-browser attacks – are essentially man-in-the-middle attacks between the user and the security mechanisms of the browser [26].

Besides banking credentials, these trojans collect other information. For example, the command and control server for Torpig distributes modules that are injected into popular applications in the infected computer. Applications include the device control manager, web browsers, ftp clients, email clients, instant messengers and system programs. After the injection, Torpig can inspect all the data handled by these programs and can identify and store interesting information, such as credentials for online accounts and stored passwords [70]. Once the trojans has intercepted information of interest, they upload it to “drop sites”. For example, Torpig contacts its drop server every 20 minutes to upload stolen data [70].

Phishing and credential-stealing trojans are at the center of many criminal activities. Fig. 1 shows some of the relations that phishers and trojans have with other cybercrime partners. First, in order to install their trojans in computers they require exploit tools, pay for affiliate programs, or buy botnets from herders. They also need to pay ISPs and domain name registrars to host contact command and control servers and drop locations. Phishers also need to use spam services to advertise their fraudulent websites. Finally, after confidential information is collected from unsuspecting users, they need to either sell this information, or use the services of mules, cashiers or carders.

2.5 Spammers

While spam is generally associated with unsolicited email (typically sent by a botnet), spam can be generally defined to include many of the ways cybercriminals attempt

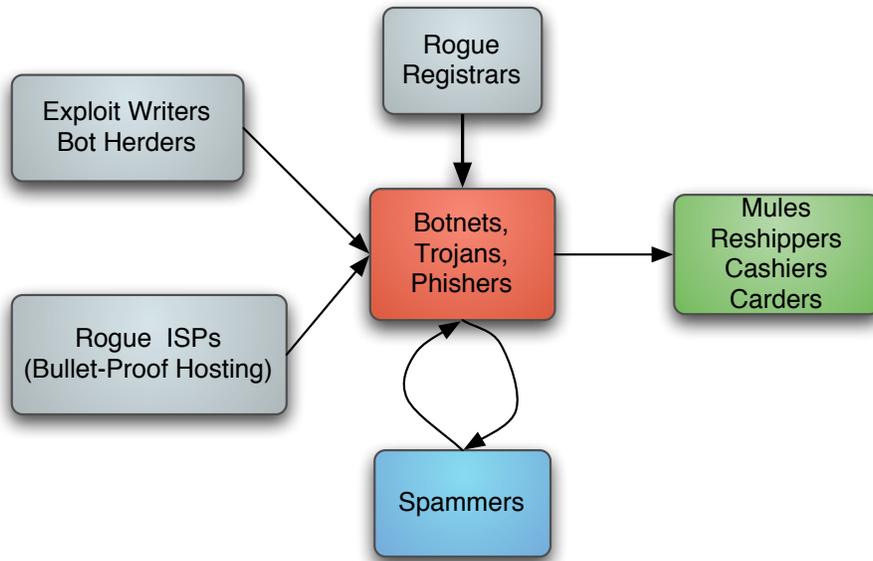


Fig. 1. Arrows represent the flow of goods and services.

to contact users (e.g., via email, blog posts, comments in Web 2.0 applications, or by poisoning of search engine results).

The primary goal of spam is to convince users to visit a specific web site (typically used for malware distribution, phishing, or for the sale of merchandise of questionable quality or pirated goods). Spam is also used to recruit money mules, or to engage the user in a conversation with a swindler (e.g., a 419 scam).

There is a large variety of tools that swindlers can use to send spam. In a recent account, a swindler describes how “He got tools: formats, or FMs, for letters; mailers, or accounts that send e-mails in bulk; and huge lists of e-mail addresses, bought on-line” [9]. The sophistication of some spam sending tools is impressive. An example of an infamous spam sending tool was Reactor Mailer. Computers infected with the Reactor Mailer client periodically downloaded message templates and lists of email addresses, independently generated and transmitted their messages, and then reported the results to the Reactor Mailer server. Additionally, it could create messages indistinguishable from popular email clients, automatically generate and obfuscate images, and was easily configurable with the help of macros [69].

2.6 DDoS Attackers

In a DDoS attack, the master of a botnet issues commands ordering bots (compromised computers) to flood a target with high volume of traffic, essentially blocking every path from the Internet to the victim. DDoS attacks are frequently used to express certain political views (as the recent attacks in Estonia, and Georgia confirm) or to damage

business competitors (cybercriminals sometimes target security companies with DDoS attacks). However, the most likely economic incentive of DDoS attacks is blackmail. In such cases, botmasters either launch a short DDoS attack and ask for a certain amount of money in order not to bring down the target server/website/business or contact the web site owner asking for money before launching a DDoS attack. Popular targets of such attacks are online gambling or betting web sites whose viability depends on being available to customers at all times and which are often located in jurisdictions with less-developed Internet laws and enforcement [61].

2.7 Rogue Domain Registrars

The IT infrastructure for running most criminal campaigns depends on victims being able to contact key criminal servers, such as malware distribution sites, drop-sites for trojans, command and control servers for botnets, phishing websites etc. These servers are located by resolving Internet domain names, and by contacting the ISPs hosting these computers.

A security researcher trying to take down these criminal servers will usually contact the ISPs and the domain name registrars associated with these servers. However, removing these servers from the Internet is not always easy. For example, the command and control architecture of the Koobface botnet relied on 24 domain names during a 3-month period in 2009 [57]. A security researcher trying to take down Koobface would need to make all 24 domains unavailable. Alternatively, the researcher may try to take down the computers associated with the IP addresses that are temporarily associated with the domain names. In this example, during the 3-month period, these domains resolved to 4 fixed IP addresses spread around the world. The addresses belonged to three ISPs; located in Malaysia, China, and the Czech Republic, respectively [57].

Even if a security vigilante manages to contact all domain name registrars and ISPs associated with a given criminal activity, some domain name registrars and ISPs might not cooperate with the takedown requests. Some “rogue domain registrars” do not investigate or eliminate their malicious domains after receiving complaints about these activities. According to KnujOn³, the top 10 rogue registrars account for 83% of the world’s concentration of illicit sites and spam domains.

Rogue domain name registrars are a pervasive problem. For example, ICANN sends several enforcement notices per month to rogue domain name registrars, following complaints from the community⁴. Furthermore, even if ICANN terminates the accreditation of the registrars for global top-level domains (gTLD) such as “.com”, each country has administrative control over country-code top level domains (ccTLD). In order to reliably shut down malicious ccTLD domains better international communications and procedures are required.

³ <http://www.knujon.com/registrars/>

⁴ <http://www.icann.org/en/compliance/>

2.8 Rogue ISPs and Web Hosting Companies

When a server is being used for spam or to spread malicious software, security researchers usually report the server to the ISP, who can then remove it from the Internet. Bulletproof servers are services provided by rogue ISPs who simply ignore these take-down requests [53]. Besides bulletproof servers, there are other special contracts between criminals and rogue ISPs. One particular version of these dealings are *pink contracts*. In a pink contract, the rogue ISP exempts spammers from the usual terms of service prohibiting spamming. Rogue ISPs charge premium prices to cybercriminals for the use of these special services.

The Russian Business Network (RBN) – an organization previously based in St. Petersburg – is probably the best known cyber-criminal service hosting organization. With the exception of child pornography, RBN’s primary targets were financial institutions and their customers [34, 7]. Because RBN rarely targeted victims in Russia, local law enforcement agencies felt minimal pressure to prosecute RBN’s activities. At the end, the organization shut down without any related charges filed [34].

McColo, Atrivo, Triple Fiber Network, and Real Host are recent examples of misbehaving (rogue) ISPs [44, 52]. These ISPs provided bulletproof hosting servers for several illegal activities, including the command and control servers for major botnets. In 2008, McColo and Atrivo were de-peered from their respective upstream providers when researchers publicized evidence of malicious activities. Triple Fiber Network was shut down in 2009 by an FTC order, and Real Host was disconnected by its upstream provider, Junik, in 2009, after TeliaSonera (Junik’s peering ISP) threatened Junik with sanctions. The enforcement action against Real Host is the first time the internet community put pressure on upstream providers to take action on an allegedly rogue ISP in eastern Europe [47].

Despite these recent takedowns, there are still many other rogue ISPs that act as safe heavens for criminal activities [17]. As long as there are cybercriminals willing to pay premium prices for hosting services there will be a supply of rogue ISPs willing to provide these services.

2.9 Payment Processors

Rogue domain registrars and rogue ISPs are part of a larger set of businesses that cybercriminals use as their infrastructure, and who later claim that they were providing a service to an unknown client who turned out to be a scammer. Another example of this infrastructure are the payment processors that cybercriminals need to process the credit card transactions of users who buy their products. For example Chronopay – an online payment processor based in the Netherlands – was the preferred payment processor of a network of scareware distributors. The extent of their involvement in the crime is in question, but they insist they were not aware of the scareware distributors intentions [39].

2.10 Identity Theft, Fencing, and Money Mules: Monetizing Stolen Credentials

In order to monetize the confidential information gathered by trojans, keyloggers, and phishing campaigns, cybercriminals require the help of cashiers, carders, identity thieves, and many other professional swindlers and fraudsters.

Identity theft is broadly defined,⁵ and the term is used to describe several different types of fraud, including variations such as “criminal identity theft,” where an impostor masquerades as another to avoid accountability for a crime. We deal here with variations of financial identity theft, of which there are two main flavors, in “new account fraud,” an impostor opens lines of credit using personal information of another. This may include new credit card accounts, mortgages, or utilities, such as wireless phone accounts. In “account takeovers,” an impostor uses one of the victim’s existing accounts. For instance, the impostor may steal or phish a credit card number from the victim and use it without authorization.

A number of economic factors shape the landscape of identity theft. Identity theft is a low-risk and lucrative crime, but it is labor intensive when performed on a large scale. Small-scale thieves may opportunistically use another’s card, or make charges on their own accounts and claim that they were made by impostors. Large-scale operations require cooperation from multiple actors and some technical expertise.

In new account frauds, the impostor attempts to obtain lines of credit. To start this process effectively, the impostor should obtain credentials in the names of the victims, arrange mail drops for collection of credit cards, and obtain telephone accounts for activation of the cards. Impostors can either create fake credentials or obtain real credentials from a state authority, but both of these options are increasingly expensive and difficult to accomplish, because of advances in credential technology and anti-fraud measures at motor vehicle authorities (nationwide, 37 motor vehicle agencies use facial recognition technologies [54]). Under Postal Service regulations, post office box customers must be identified, and are only supposed to receive mail under authenticated names.⁶ The impostor must, therefore, maintain many different boxes, or through a scheme known as “synthetic identity theft,” [32] use victim names that are very similar, such that the mailbox owner would see different names as acceptable variations, rather than a fraud scheme. Once this infrastructure is in place, the impostor can apply for credit and other accounts, directing them to the postal boxes.

Criminals monetizing account takeovers have similar labor-intensive, technical challenges. A typical way to monetize bank accounts is to recruit *cashiers* and *money mules*. A cashier uses the stolen account to transfer funds from the stolen account to the account of a mule. The mule then transfers a percentage of the money to the cashier, typically via an untraceable money transfer.

⁵ 18 USC §1028

⁶ USPS, Domestic Mail Manual, 508 §4.3.2, available at <http://pe.usps.com/text/dmm300/508.htm>

Money mules are often victims of scams as well [40]. A common way of recruiting money mules is to target people looking for jobs, and offer them a job as a payment processor or as a mystery shopper.⁷

In a recent example, cyber criminals were able to obtain the bank credentials of the treasurer of Bullitt County, Kentucky, by installing a keylogger (the Zeus trojan) on his PC. To get the money from the bank, they hired 25 people in the U.S. (at least two of them were contacted after they placed their resumes on careerbuilder.com). The cybercriminals pretended to be a company – Fairlove Delivery Service – in need of a representative in the U.S. to receive payments from its clients. The job of the U.S. representatives was to receive the money into their bank accounts, and then transfer it via Western Union to a bank account in the Ukraine [42].

While monetizing stolen credentials may be easy for an experienced fraudster, it is still a major bottleneck for monetizing large numbers of stolen credentials. The series of steps involved in extracting money from banks and credit cards, and the higher probability of apprehension faced by these criminals helps explain why massive data breaches may result in a relatively small number of cases of identity theft. Even with personal information or credit cards of millions of individuals, the practical logistics of identity theft acts as a brake on massive new account and account takeover frauds.

3 Social Cost of Cybercrime

In order to plan the appropriate level of resources to fight cybercrime, we need a better understanding of the costs of cybercrime. Similarly, to understand the incentives of cybercriminals, it is equally important to investigate the proceeds from computer attacks.

3.1 Losses

There is a lack of understanding about the precise magnitude of cybercrime and its impact because computer attacks are not always detected or reported. Reasons for not reporting cybercrime include, financial market impact, reputation or brand damages, litigation concerns, the fact that reporting sends a signal to other potential attackers, inability to share information, fears of job security by the people responsible for computer security within the attacked firm, and a perceived lack of law enforcement action [71].

Anecdotal data on the costs of cybercrime is relatively easy to obtain for some of the more publicized security breaches. For example, TJX's breach cost the company \$200 million according to its 2009 SEC filing [75]. Similarly, Heartland's breach costs reached \$32 million in the first half of 2009. Heartland will see a net after tax loss attributable to the breach for the first six months of 2009 of some \$5.1 million. Interestingly, several of

⁷ More information on money mules: <http://www.bobbear.co.uk/> and <http://joewein.net/fraud/spam-fraud-paypal.htm>.

the costs were indirect, and dealing with legal proceedings, potential liabilities etc. At the moment it is unclear how much did the breach cost the financial services or other entities involved with direct losses.

Besides data from large security breaches, it is very difficult to obtain reliable data for smaller cases of fraud. In particular, the cybercrime operations described in the previous section target users from a wide variety of backgrounds with access to many different financial services; therefore, while each individual case may look small, the cumulative amount of fraud that cybercriminals can spread across many different entities will not be identified by any single institution. There are, however, some reports attempting to estimate the cumulative effects of cybercrime. The U.S. Government Accountability Office (GAO) collected in 2007, a list of different estimates by different entities on the losses due to computer breaches [71]. In Europe, the International Telecommunication Union also published a report in 2008 which summarized some of the estimates by different entities [36]. While this data is very valuable, it may not be very reliable: the estimates presented have large—and unexplained—differences. In addition, some of the agencies do not report their method for estimating these losses. A large portion of the costs of cybercrime are estimated by security service providers; however, while these estimates are useful, security service providers have incentives to over-estimate security problems [36].

Currently, some of the more reliable statistics are collected at the Internet Crime Complaint Center (IC3). The 2008 Annual Report states that complaints of online crime hit a record high in 2008. IC3 received a total of 275,284 complaints, a 33.1% increase over the previous year. The total dollar loss linked to online fraud was \$265 million, about \$25 million more than in 2007. The average individual loss amounted to \$931⁸. While these reports are very useful, these estimates are just a fraction of the losses on cybercrime for many reasons: many companies prefer not to report losses due to computer attacks (for the reasons stated above), victims of computer crime may not know about the IC3, and IC3 compiles only data from the United States.

The United Kingdom has another source of reliable statistics. Fraud loss figures released in 2009 by APACS, the UK payments association, show that card fraud losses totalled £609.9m in 2008. More than half of the losses—£328.4m—were due to “card-not-present fraud,” which includes Internet, phone, and mail-order fraud. The losses due to card-not-present continue growing: £150.8m in 2004 £183.2m in 2005 £212.7m in 2006 £290.5m in 2007, and £328.4m in 2008 [4]. While in 2004 the losses due to card-not-present were very similar to the losses due to stolen/lost credit cards, or due to counterfeit cards, it is now clear that online and phone fraud are the primary means of card fraud. From 2001 to 2008 card-not-present fraud losses rose by 243 per cent; over the same time period, the total value of online shopping transactions alone increased by 524 per cent (up from £6.6 billion in 2001 to £41.2 billion in 2008).

While the IC3 and the APACS reports provide some solid foundation for estimating cybercrime losses, much work needs to be done to estimate reliably the social costs of

⁸ http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

cybercrime. Currently we do not know the scope of the problem. We do know that it is a big problem and that the losses are estimated in the tens of billions in the U.S.; however, without better estimates of the costs of cybercrime we cannot tell whether the market is addressing the problem.

One possible way to improve our knowledge on the cost of cybercrime is to require banks, financial institutions (and possibly other stake holders, such as ISPs or e-commerce sites) to disclose more fraud data and costs associated with computer attacks, including the volume of money involved in the crimes. Reporting will elucidate the scope of the problem and its trends, as well as create a market for fraud prevention, where banks could compete on ways to protect customers [32].

3.2 Proceeds of cybercrime

To develop an economic model of cybercrime we also need to estimate the benefits of cybercrime for potential miscreants. This will help us understand the incentives of potential criminals, and the net social loss: by what margin do costs on victims and the justice system exceed the benefits of perpetrators and security service providers.

We can obtain anecdotal data on some of the earnings of cybercrime from prosecution cases.⁹ Currently one of the most high-profile cases is the prosecution of Max Butler. From this case we know that authorities found in his hard-drive, 1.8 million stolen credit card numbers belonging to 1000 different banks. The banks tallied the fraudulent charges on the cards at \$86.4 million US dollars [64]—however, Max Butler stole several numbers from other cybercriminals, so the fraudulent charges may not be directly attributable to him. Similarly, Chris Aragon, a carder who bought cards from Butler, is accused of earning at least \$1 million dollars in the business [64].

While prosecution cases can give us some ground truth on different activities, it is unclear how representative of the underground economy are these anecdotal reports (after all, only fraction of crimes are reported, and of the reported cases only a fraction are investigated and prosecuted). To obtain a better idea of the amount of money entering the underground economy we require (again) more transparency from institutions reporting their losses on cybercrime. While estimating the earnings of cybercriminals is different than estimating the losses due to cybercrime—only a fraction of the losses of cybercrime translate to earnings for cybercriminals; the remaining part of the losses are distributed among recovery, litigation, brand damage, and many other side-effects—if we require financial institutions to report direct losses from cybercrime (i.e., non-recoverable fraudulent charges on stolen accounts), we may be able to estimate the inflow of cash that supports the underground economy.

⁹ Some current cases include \$100,000 earnings from affiliate programs <http://www.cybercrime.gov/maxwellPlea.htm> and \$50,100 for selling software for pump & dump schemes <http://www.usdoj.gov/opa/pr/2009/July/09-crm-664.html>. In general, the Department of Justice and the FTC maintain a different list of cases <http://www.cybercrime.gov/> and <http://www.ftc.gov/os/caselist>.

4 Countermeasures

A final challenge for developing a model for the market of offenses is to identify the mechanisms that may reduce the supply of offenses. In this context we study the demand for public and private protection, and the incentives of stake holders.

4.1 Public Protection

Public protection can influence the supply of offences by reducing the incentives for cybercrime activities. The main variables that law enforcement and legislation can influence are: the probability of apprehending cybercriminals, and the penalties associated with cybercrimes.

Probability of Apprehension Several factors contribute to the low-risk nature of cybercrime. For example, law enforcement is highly unlikely to become involved in identity theft cases for a variety of reasons. The FTC has found that most victims of ID Theft do not report the crime to criminal authorities [21]. This may especially be the case with account takeovers, because the victim usually resolves the issue with a call to the institution without further incident. Even where a consumer victim does try to contact police, some law enforcement agencies are reluctant to take reports. They may view the lending institution as the victim [29]. Or, in cases where the theft took place in another jurisdiction, they may tell the victim to file the report elsewhere. In turn, police in the other jurisdiction then tell the victim to file where she lives. This runaround has caused California to require law enforcement by statute to take reports from victims.¹⁰

Businesses have no incentives for reporting identity theft to law enforcement. The landscape is further complicated by law enforcement priorities and expertise. On the local level, police often do not have the resources or expertise to effectively deliver an identity theft case to a prosecutor. Federal law enforcement will not even begin an investigation until a fraud scheme reaches a certain severity, law enforcement will not begin an investigation. For instance, even a fraud event resulting in \$50,000 in loss will not necessarily trigger an investigation in Southern California.¹¹ This problem interacts with concerns over brand tarnishment: federal law enforcement only investigates major cases, but at the same time, businesses are resistant to publicly declare the amount of money lost in a criminal proceeding. In limited cases, identity thieves are pursued and restitution may be collected for the costs, but these situations are rare. The Gartner Group estimated in 2003 that criminals still have a one out of 700 chance of getting caught by federal authorities [49]. This lack of response from law enforcement causes some commercial victims to not report the crime.

¹⁰ See e.g. Cal. Penal Code 530.6(a)(2007).

¹¹ Remarks of Joe Majka, Vice President, Risk Management and Fraud Control Department, Visa, Teaming Up Against Identity Theft, A Summit on Solutions (Feb. 23, 2006).

Finally, even if law enforcement decides to investigate and prosecute a case, the border-less nature (several crimes are committed across country borders) of most cybercrimes increase the jurisdictional ambiguities associated with the investigation.

Penalties Many of the penalties associated with cybercrime are monetary. In general, monetary sanctions are the best penalties for many crimes [6]. Not only is imprisonment more costly to the state, but in many cases, imprisonment may only be contributing to malicious behavior by gathering a community of people to share techniques and to create criminal networks. Two cases help us illustrate this case.

John Draper, one of the most famous phone phreaks was arrested in 1972 on toll fraud charges. He later reported that “once I got busted, I had to tell everybody else in jail how to do it: the cat got out of the bag and immediately they [phone companies] started losing lots and lots of money ... as more and more hackers get thrown to jail, the more opportunities for criminals to get connected to the right kind of hackers”.¹²

Similarly, Max Butler started as a “recreational” hacker. However, when he broke into computers in the Pentagon, he was apprehended and sent to prison. In prison he met a professional swindler who introduced him to the world of carding. After his release he started hacking banks, merchants and other hackers to steal credit card numbers, which he sold to carders [64].

4.2 Private Protection

The computer security industry can also reduce the supply of offenses by increasing the cost of launching and maintaining successful attacks.

While the computer security industry has traditionally focused on prevention technologies (e.g., firewalls, anti-virus, encryption, authentication, etc.) there is an emergent industry focusing on detection of attacks and recovery. Internet vigilantes created the cases that brought down criminal ISPs such as McColo and Atrivo. Similarly several entities are using brand-monitoring and anti-fraud solutions, which include takedown companies.¹³ Takedown companies track down malicious servers connected to the Internet, and then request ISPs and domain registrars to remove the offending content.

One of the main questions raised by the economics of crime regarding private protection is whether private protection reduces crime levels, or just shifts the risks to less protected victims [68].

4.3 Shaping the Incentives of Stakeholders

Internet Infrastructure: ISPs and Domain Registrars ISPs have different approaches when managing the level of (in)security of their users that is directly related to

¹² Interview with John Draper. First episode of stop H*Commerce, available at <http://www.stopcommerce.com>

¹³ <http://www.antiphishing.org/solutions.html>

the ISP hierarchy and interconnection principles. The current Internet consists of multiple semi-autonomous networks which share a common IP addressing and global BGP routing framework providing direct or indirect connectivity of those networks. Networks are classified in three tiers according to the nature of the connection to other networks. Tier 1 operators (who frequently have international coverage) own the operating infrastructure that forms the backbone and interconnect via settlement free peering to obtain access to the entire Internet routing table. By definition, Tier 2 ISPs have to enter into contractual (transit) agreements with at least some Tier 1 ISPs to provide global access to their customers. However, Tier 2 ISPs may also enter into peering agreements with their peers to reduce transit costs. Finally, Tier 3 ISPs mostly focus on local markets and are customers of more sizeable ISPs.

Tier 1 ISPs usually invest in large bandwidth networks with significant over-provisioning to provide service guarantees and to protect against a variety of failures [12]. As a result, the incentives to respond to specific security problems that mostly affect lower-tiered ISPs and end users is limited. For example, malware traffic may not represent a large enough burden to engage in countermeasures, in particular, since the cost for service calls is significant (i.e., estimates suggest about 16 Euros per call [72]). While large ISPs may act upon abuse notifications, data shows that only a small number of customers is contacted regarding security issues (i.e., the so called “two percent rule” is applied [72]).

Lower tier ISPs are motivated to avoid transit costs as well as upgrade investments to last-mile connection capacities necessitated by unsolicited and malicious communications. Further, disregarding abuse notifications may result in blacklisting or cutoff of selected resources or users. Due to their size and importance Tier 1 ISPs are generally safe from being blacklisted. Therefore, higher-tier ISPs can implicitly or explicitly delegate security management to lower-tier ISPs by exercising market power [60]. It is therefore not surprising that several Tier 1 ISPs have been cited in industry top 5 lists concerning malware and spam traffic.

Motivated ISPs may undertake a number of actions to improve their network security:

1. Prevention: Protect customers from attacks by offering discounted or free security software,
2. Active response: Automatic quarantine and patching when infection is detected,
3. Network defense: Monitoring local and interconnection network traffic.
4. Collaboration: Implement joint network defenses and create inter-ISP network management teams.

However, it is important to note that even the most vigilant ISPs are not always able to provide strong security to their users without collaboration. First of all, many threats do not manifest themselves on the network layer but rather on the application layer (e.g., stealing personal data of users via phishing). Secondly, many countries have strict privacy laws that prohibit ISPs from monitoring user activity (e.g., the European Union)

so that ISPs are only able to actively respond to malicious behavior after receiving abuse notifications (which happens in less than 10% of total infections [72]). Technologies that reduce the cost of reliably identifying malicious hosts can ease the burden of notification [74].

Businesses and residential customers In order to evaluate possible roles of customers of ISPs in the fight against cybercrime, it is important to mention that different classes of users have different incentives to invest into security.

The success of cybercrime schemes often depends on the lack of security investments among *residential and small business customers*. Home users are often not aware of risks to themselves or fail to respond adequately due to the complexity of effective countermeasures [2]. For example, they may open malicious email attachments or do not install updated virus checking templates, even though their actions can result in significant nuisances or financial losses. Further, an overwhelming majority of users who are offered premium services with enhanced security by their ISPs choose instead basic services [72]. Inactivity is also caused by the lack of liability when other users and businesses are negatively affected by compromised machines [73]. Unfortunately, residential customers combined lack of actions can result in an substantial increase in collective risk [28].

Users may also act passively because they are shielded from damages that may have originated from cybercrime. For example, a variety of consumer protection laws and self-regulatory practices limit liability for financial account takeovers.¹⁴ For example, consumers can dispute fraudulent charges and have them removed from a bill, even if the consumer was negligent in protecting a credit card number. However, consumers do have some incentives to avoid fraud, because of the inconvenience and opportunity costs it poses. Some research supports the allegation that consumers do lose money in identity theft. In 2004, according to Gartner, consumers recovered 80% of losses from Phishing attacks. In 2005, only 54% recovered the full amount of fraud [51]. In the U.S., consumers are not liable for unauthorized transactions against their bank accounts; however, this provision does not apply to business account holders.

Large companies including financial services and ecommerce usually invest in security to protect their operational processes and business secrets. They may rely on collaboration with their ISPs to defend against large-scale attacks. They are also interested in maintaining strict security policies, which often include operating on separate networks.

In contrast, businesses also have incentives to obscure cybercrime such as identity theft, for fear of brand tarnishment. The Identity Theft Resource Center has observed: “Unfortunately, many commercial victims do not report the crime to law enforcement, considering it more fiscally advantageous to *write off the loss*” [35]. Collins and Hoffman note that, “...even though this crime became epidemic on the last decade, many companies remain reluctant to report the thefts of their employees’ or customers’ identities

¹⁴ See e.g. Regulation Z, 12 C.F.R. §226; Regulation E, 12 C.F.R. §205.

for fear of losing business” [14]. In addition to tarnishing a company’s brand, severe identity theft losses are likely to attract unwanted regulatory attention. High levels of fraud may bring lending institutions’ security and soundness into question, triggering examinations and costly compliance duties. As a result, the lack of vigilance concerning the protection of customer data (caused by these muddled incentives) has led to breach notification laws in many states [55].

Finally, *malicious users* pay willing ISPs for a “premium” service, which in exchange allows them to conduct their business for a longer duration without being taken down by abuse complaints.

Software Industry The software industry is an interesting case in the analysis of cybercrime. While most companies are held accountable for the safety of their products, the current practice in the software industry is to disclaim responsibility for the quality of their software through the user license agreement.

To address this lack of accountability, the American Law Institute (ALI) is currently proposing model laws making software vendors liable for knowingly shipping buggy software. In a very rare event, Microsoft and the Linux Foundation have joined forces against this proposal arguing that the laws would stifle innovation, raise the cost of software, and hurt small developers.

5 Related Work

5.1 The Economics of Crime

The outline of this paper was influenced in great part by the literature on the economics of (traditional) crime. We believe that the study of cybercrime can leverage several ideas from this area.

The basic economic framework for crime is based on the assumption that offenders—on average—respond to incentives: crime is considered a social choice, despite unethical, immoral, or even deviant behavior of some of its perpetrators. Under this assumption, Gary Becker [6] developed a model that considers the costs and gains that motivate crime, and the options to control crime (and their social cost). Becker models the offender’s choice as a function of the gains from crime, the probability of apprehension, and the severity (and type) of punishment. His goal is to minimize the net social loss produced by crime (crime generates an external diseconomy because costs on victims and the criminal justice system exceed any benefit produced by the perpetrators). He shows that to maximize the aggregate social income, the optimal sanctions against criminals should take the form of fines. He argues that fines are a better deterrence for crime than imprisonment (as imprisonment is costlier to impose).

Becker’s model has been expanded in a variety of ways. One of the fundamental extensions is the market of offenses and its associated equilibrium analysis [19, 20]. The market model consists of 1) supply of offenses (crime rate), 2) demand—provision of illegal goods and services such as drugs, fencing of stolen goods, etc.—and 3) negative

demand—potential victims of crime demand public (law enforcement and administration of justice) and private protection. We now describe each of the components of the market in more detail.

The supply of offenses consists on the study of benefits and costs to the offenders, such as earning opportunities, personal aversion to crime, and individual perception about the probability of apprehension. Social interactions are also considered a fundamental part of the supply of offenses, as they influence crime rates in society [67, 27, 62, 11]. One of the insights in the study of crime rates is that the spending on activities to reduce crime should be considered as a long-term process because crime rates are also a function of past crime rates [67], so any possible strategy against crime may take generations to yield observable benefits. Another important observation is that crime is expected to increase with a community's income inequality for two reasons¹⁵: 1) those at the bottom have low opportunity costs for committing crimes, and 2) the presence of high-income individuals provide profitable targets.

The study of public demand for law enforcement deals with the optimal distribution of resources in the criminal justice system. The metrics used for the optimization problems are usually based on the aggregate social income; however, some of them include concepts of fairness. Most models assume a social planner who has a choice of influencing the probability of apprehension and conviction, the severity of punishment and the sanctions inflicted on perpetrators. In practice, however, there is no social planner, and individual enforcers are concerned with their own welfare (which leads to corruption) [24]. A seminal work in the study of the role of government in crime and the social costs of crime was given by the 1967 President's commission on law enforcement and administration of justice [65].

Potential victims also have the incentives to protect themselves (to reduce the risk of victimization) and to purchase insurance (to reduce the loss if they are victimized) [5, 13, 45]. One of the key questions in private protection is whether protection reduces crime levels, or just shifts the risks to less protected victims [68].

The study of the market of offenses assumes that the frequency of offenses of each specific kind of crimes reflects an implicit equilibrium between the supply and demand of offenses [18]: the aggregate supply of offenses (i.e., the crime rate) is proportional to the expected return per offense, which in turn decreases with self-protection by potential victims, and by the expected legal sanctions. Market models have also been used to estimate the social cost of crime [3]. Underground markets can also lead to higher level of crime: since trades are illegal, explicit contracts are impossible to make, and disputes are often resolved by violence¹⁶. Another market analysis considers the public as “providers” of crime opportunities, and potential victims [15]. One of the conclusions is that rehabilitating or incapacitating criminals will have less than the expected influence on crime rates in the long run to the extent that potential criminals are responsive

¹⁵ this is similar to cybercrime

¹⁶ also similar to cybercrime?

to opportunities and that the public's provision of opportunities is responsive to the crime rate.

While most of the market models consider uncoordinated groups of offenders (the competitive nature in the market for offenses), dealing with organized crime requires different models. Organized crime represents an entity which attempts to act as a monopoly, and thus restricts the flow of illegal transactions. In addition, organized crime participates in curtailment of sales to raise prices and to limit the law enforcement efforts (i.e., to stay under the radar of law enforcement) [10, 25].

5.2 Cybercrime Studies

There is an emerging trend to consider economic aspects in the study of cybercrime.

Brenner and Clarke [8] provide a summary of efforts to deter cybercrime and propose a new distributed security model for discouraging cybercrime. The distributed security proposes a set of incentives so that Internet users accept a higher-degree of responsibility on cybercrime. Abad describes in detail phishing campaigns and argues that while it is easy to obtain credential information, it is hard to extract monetary value from these credentials [1].

Ford et.al. propose a model for attacking the ad-revenue stream of botnets [22]. Li et.al., [48] model an attacker who gets a profit by launching DDoS attacks on a server, and botnet master who can rent part of its botnet to participate in the attack. The authors argue that by infiltrating the botnet and making some of the bots unreliable (machines that will not participate in the DDoS attacks) reduces the profitability of the botnet market and the probability of DDoS attacks.

Herley and Florencio [30] consider the economic similarities between phishing and open access fishing grounds. They argue that phishing is an example of the tragedy of the commons, since each phisher independently seeks to maximize his returns, the resources is over-grazed and yields far less than it is capable of; in fact, the pool of available dollars shrinks as a result of the efforts of the phishers. In a follow up paper [31] the authors argue that the lower-tier criminals who use IRC underground (lemon) markets for trading goods and services are almost certainly cheated by other members. They also argue that the majority of the proceeds from cybercrime are obtained from gangs who do not trade openly.

While most of the research has focused on models for cybercrime, there are some detailed empirical studies. These include the analysis of the activity of an underground carder forum [23], a study of the economics of spam by infiltrating the Storm botnet [37], and the operation of the Torpig Trojan [70].

6 Conclusions

To develop an economic model of cybercrime we need to (1) understand the attackers, their incentives and risks, (2) estimate the social cost, or losses due to cybercrime, and (3) identify the optimal amount and distribution of the resources to spend in the fight

against cybercrime. In particular, we need to identify sustainable ways to combat cybercrime, and to identify metrics to evaluate the success of legislation or law enforcement.

References

1. C. Abad. The economy of phishing: A survey of the operations of the phishing market. *First Monday*, 10(9), September 2005.
2. A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1):26–33, January–February 2005.
3. D. A. Anderson. The aggregate burden of crime. *Journal of Law and Economics*, XLII(2):611–642, October 1999.
4. APACS. Press release. 2008 fraud figures announced by apacs. http://www.apacs.org.uk/09_03_19.htm, March 2009.
5. A. Bartel. An analysis of firm demand for protection against crime. *Journal of Legal Studies*, 4(2):443–478, 1975.
6. Gary S. Becker. Crime and punishment: An economic approach. *Journal of Political Economy*, 76(2):169, 1968.
7. David Bizeul. Russian business network study. http://www.bizeul.org/files/RBN_study.pdf, November 2007.
8. S. Brenner and L. L. Clarke. Distributed security: A new model of law enforcement. *John Marshall Journal of Computer & Information Law*, 2005.
9. K. Brulliard. Worldwide slump makes Nigeria’s online scammers work that much harder. <http://www.washingtonpost.com/wp-dyn/content/article/2009/08/06/AR2009080603764.html>, August 2009.
10. J. M. Buchanan. A defense of organized crime? In *The Economics of Crime and Punishment*, pages 119–132. American Enterprise Institute for Public Policy Research, 1973.
11. A. calvo armengol and Y. zenou. Social networks and crime decisions: the role of social structure in facilitating delinquent behavior. *International Economic Review*, 45(3):939–958, August 2004.
12. C. Chuah. A Tier-1 ISP perspective: Design principles & observations of routing behavior. Available at: http://sahara.cs.berkeley.edu/jun2002-retreat/chuah_talk.pdf. Presentation at the SAHARA Retreat, Bi-annual Meeting, University of California, Berkeley, Networking & System Group, June 2002.
13. C. Clotfelter. Private security and public safety. *Journal of Urban Economics*, 5:388–402, 1978.
14. J.M. Collins and S.K. Hoffman. Identity theft: Predator profiles. Manuscript available from Judith Collins judithc@msu.edu, 2004.
15. P. J. Cook. The demand and supply of criminal opportunities. *Crime and Justice*, 7:1–27, 1986.
16. D. Danchev. Remote code execution exploit for Firefox 3.5 in the wild. <http://blogs.zdnet.com/security/?p=3743>, July 2009.
17. Dancho Danchev. Bad, bad, cybercrime-friendly ISPs. <http://blogs.zdnet.com/security/?p=2764>, March 4 2009.
18. I. Ehrlich. On the usefulness of controlling individuals: an economic analysis of rehabilitation, incapacitation, and deterrence. *American Economic Review*, 71(3):307–322, June 1981.
19. I. Ehrlich. Crime, punishment, and the market for offenses. *Journal of Economic Perspectives*, 10(1):43–67, Winter 1996.
20. I. Ehrlich and Z. Liu, editors. *The economics of crime*, volume 1. Edward Elgar Publishing Limited, 2006.
21. Federal Trade Commission. Identity theft survey report 9. <http://www.ftc.gov/os/2003/09/synovatoreport.pdf>, September 2003.
22. R. Ford and S. Gordon. Cent, five cent, ten cent, dollar: Hitting botnets where it really hurts. In *Proc. of the New Security Paradigms Workshop (NSPW 06)*, pages 3–10, Schloss Dagstuhl, Germany, September 2006.
23. J. Franklin, V. Paxson, A. Perrig, and S. Savage. An inquiry into the nature and causes of the wealth of internet miscreants. In *ACM Conference on Computer and Communications Security CCS*, October 2007.
24. D. Friedman. Why not hang them all: the virtues of inefficient punishment. *Journal of Political Economy*, 107(6):S259–S269, December 1999.
25. N. Garoupa. The economics of organized crime and optimal law enforcement. *Economic Inquiry*, 38(2):278–288, April 2000.

26. Philipp Ghring. Concepts against man-in-the-browser attacks, June 2006.
27. E. L. Glaeser, B. Sacerdote, and J. A. Scheinkman. Crime and social interactions. *Quarterly Journal of Economics*, 2:507–548, 1996.
28. J. Grossklags, N. Christin, and J. Chuang. Secure or insure? A game-theoretic analysis of information security games. In *Proc. of the 2008 World Wide Web Conference (WWW'08)*, pages 209–218, Beijing, China, April 2008.
29. Hearing before the U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information (testimony of Beth Givens, Director, Privacy Rights Clearinghouse). Identity theft: How it happens, its impact on victims, and legislative solutions. http://www.privacyrights.org/ar/id_theft.htm, July 2000.
30. C. Herley and D. Florencio. A profitless endeavor: Phishing as tragedy of the commons. In *New Security Paradigms Workshop*, Lake Tahoe, CA, USA, September 2008.
31. C. Herley and D. Florencio. Nobody sells gold for the price of silver: dishonesty, uncertainty and the underground economy. Technical Report MSR-TR-2009-34, Microsoft Research, June 2009.
32. C.J. Hoofnagle. Identity theft: Making the known unknowns known. *Journal of Law and Technology*, 21, 2007.
33. R. Howard, editor. *Cyber Fraud: Tactics Techniques and Procedures*, chapter IFrame Attacks—An examination of the Business of IFrame Exploitation. CRC Press, April 2009.
34. R. Howard, editor. *Cyber Fraud: Tactics Techniques and Procedures*, chapter The Russian Business Network: The Rise and Fall of a Criminal ISP. CRC Press, April 2009.
35. Identity Theft Resource Center. Identity theft: The aftermath. <http://www.idtheftcenter.org/idaftermath.pdf>, September 2003.
36. International Telecommunication Union. ITU Study on the Financial Aspects of Network Security: Malware and Spam. <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf>, July 2008.
37. C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage. Spamalytics: An empirical analysis of spam marketing conversion. In *15th ACM Conference on Computer and Communications Security (CCS)*, Alexandria, VA, USA, October 2008.
38. B. Krebs. The scrap value of a hacked pc. http://voices.washingtonpost.com/securityfix/2009/05/the_scrap_value_of_a_hacked_pc.html, May 2000.
39. B. Krebs. Following the money: Rogue anti-virus software. http://voices.washingtonpost.com/securityfix/2009/07/following_the_money_trail_of_r.html, July 2009.
40. B. Krebs. The growing threat to business banking online. http://voices.washingtonpost.com/securityfix/2009/07/the_pitfalls_of_business_banking.html, July 2009.
41. B. Krebs. Microsoft: Attacks on unpatched Windows flaw. http://voices.washingtonpost.com/securityfix/2009/07/microsoft_internet_explorer_ex.html, July 2009.
42. B. Krebs. PC invader costs Ky. county \$415,000. http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html, July 2009.
43. B. Krebs. Web fraud 2.0: Franchising cyber crime. http://voices.washingtonpost.com/securityfix/2009/06/web_fraud_20_franchising_cyber.html, June 2009.
44. Brian Krebs. FTC sues, shuts down N. California web hosting firm. http://voices.washingtonpost.com/securityfix/2009/06/ftc_sues_shuts_down_n_calif_we.html?wprss=securityfix, June 4 2009.
45. D. Lakdawalla and G. Zanjani. Insurance, self-protection, and the economics of terrorism. *Journal of Public Economics*, 89(9–10):1891–1905, September 2005.
46. J. Leyden. Blue chip FTP logins found on cybercrime server. http://www.theregister.co.uk/2009/06/26/ftp_malware_hack/, June 2009.
47. J. Leyden. Plug pulled Latvian cybercrime hub. http://www.theregister.co.uk/2009/08/05/cybercrime_takedown/, August 2009.
48. Z. Li, Q. Liao, and A. Striegel. Botnet economics: uncertainty matters. In *Workshop on the Economics of Information Security WEIS*, 2008.
49. A. Litan. Underreporting of identity theft rewards the thieves. Gartner Group Research ID: M-20-3244, July 7 2003.
50. J. Markoff. Antiviral “Scareware” Just One More Intruder. http://www.nytimes.com/2008/10/30/technology/internet/30virus.html?_r=1, October 2008.
51. R. McMillan. Consumers to lose \$2.8 billion to phishers in 2006, experts say phishing attacks continue to rise, getting more costly. <http://www.pcworld.com/article/id,127799/article.html>, Nov. 9 2006.

52. R. McMillan. After links to cybercrime, Latvian ISP is cut off. <http://www.networkworld.com/news/2009/080509-after-links-to-cybercrime-latvian.html>, August 2009.
53. Robert McMillan. In china, \$700 puts a spammer in business. http://www.computerworld.com.au/article/302617/china_700_puts_spammer_business, May 11 2009.
54. N. Miroff. As if it needed to, Virginia bans smiles at the DMV. <http://www.washingtonpost.com/wp-dyn/content/article/2009/05/27/AR2009052703627.html>, May 28 2009.
55. D. Mulligan. Information disclosure as a light-weight regulatory mechanism. Available at: <http://dimacs.rutgers.edu/Workshops/InformationSecurity/slides/mulligan.ppt>. Presentation at the DI-MACS Economics of Information Security Workshop, Rutgers University, January 2007.
56. A. Mushtaq. Who is exploiting the Adobe Flash 0-day? <http://blog.fireeye.com/research/2009/07/who-is-exploiting-the-flash-0day.html>, July 2009.
57. Atif Mushtaq. Killing the beast ... part II. <http://blog.fireeye.com/research/2009/06/killing-the-beastpart-ii.html>, June 17 2009.
58. Y. Namestnikov. The economics of botnets. <http://www.viruslist.com/en/analysis?pubid=204792068>, July 2009.
59. R. Naraine. Researcher: WMF exploit sold underground for \$4,000. <http://www.eweek.com/c/a/Security/Researcher-WMF-Exploit-Sold-Underground-for-4000>, February 2006.
60. W. Norton. The art of peering: The peering playbook, 2002.
61. K. O'Connell. Online casinos will experience cyber-extortion during SuperBowl betting. http://www.ibls.com/internet_law_news_portal_view.aspx?id=1967&s=latestnews, January 2008.
62. Paul Ormerod. *Crime: Economic Incentives and Social Networks*. IEA Hobart Paper No. 151, 2005.
63. D. Pauli. Security filters often flag legit but infected sites. http://www.pcworld.com/businesscenter/article/144485/security_filters_offten_flag_legit_but_infected_sites.html, April 2008.
64. Kevin Poulsen. Superhacker max butler pleads guilty. http://www.wired.com/threatlevel/2009/06/butler_court/, June 2009.
65. President's Commission on Law Enforcement and Administration of Justice. The challenge of crime in a free society. U.S. Government Printing Office, 1967.
66. N. Provos, D. McNamee, P. Mavrommatis, K. Wang, and N. Modadugu. Ghosnet in the browser: Analysis of web-based malware. In *Proceedings of the first USENIX workshop on hot topics in Botnets*, April 2007.
67. R. K. Sah. Social osmosis and patterns of crime. *Journal of Political Economy*, 99(6):1272–1295, December 1991.
68. S. Shavell. Individual precautions to prevent theft: Private versus socially optimal behavior. *International Review of Law and Economics*, 11(2):123–132, 1991.
69. H. Stern. A survey of modern spam tools. In *Proc of the fifth conference on email and anti-spam*, 2008.
70. Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Chris Kruegel, and Giovanni Vigna. Your botnet is my botnet: Analysis of a botnet takeover. Technical report, University of California, Santa Barbara, 2009.
71. United States Government Accountability Office. Cybercrime. public and private entities face challenges in addressing cyber threats, June 2007.
72. M. van Eeten and J. M. Bauer. Economics of malware: security decisions, incentives and externalities. Technical report, STI Working Paper, May 2008.
73. H. Varian. Managing online security risks. <http://www.nytimes.com/library/financial/columns/060100econ-scene.html>, June 2000.
74. Y. Xie, F. Yu, and M. Abadi. De-anonymizing the Internet using unreliable IDs. In *Proc. of ACM SIGCOMM*, Barcelona, Spain, August 2009.
75. K. Zetter. TJX hacker was awash in cash; his penniless coder faces prison. <http://www.wired.com/threatlevel/2009/06/watt>, June 2009.