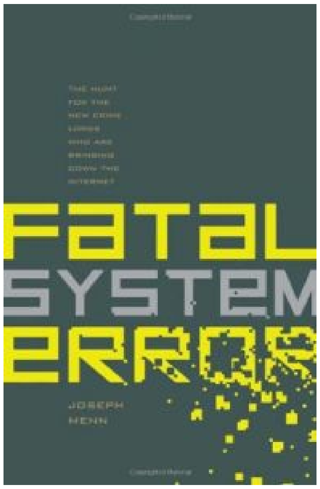
THE HUNT FOR THE NEW CRIME LORDS WHO ARE BRINGING DOWN THE INTERNET
FATAL
SYSTEM
ERROR
JOSEPH MENN

Book Fatal System Error

The Hunt for the New Crime Lords Who are Bringing Down the Internet

Joseph Menn
Public Affairs, 2010
Listen now

- play
- pause

00:00
00:00

Recommendation

The Internet has become the ultimate mob hangout, a dangerous venue where U.S. Mafiosi, vicious Russian gang members and illegal hackers from many nations, especially from Eastern Europe, ply their dirty deeds. Cybersecurity reporter Joseph Menn examines cybercrime, exposing the bad guys while telling exciting stories about two intrepid investigators – Barrett Lyon, a U.S.-based “white hat” security hacker, and Andy Crocker, a British cybersecurity agent – who have successfully waged war against cybercriminals. Menn’s book is both fascinating and disturbing, with its discussion of “zombie armies” of computers, and its exotically named online desperadoes, like CumbaJohnny. *BooksInShort* recommends this gripping saga to those who want to protect themselves from cybercrime. This outstanding book’s only deficiency is, ironically, its remarkable, overwhelming abundance of complex detail. If you think you need a cast list, tech manual and dictionary of arcane online terms, never mind; just hang on for a scary, revealing ride.

Take-Aways

- Cybercriminals use the Web in many illegal ways, costing victims $1 trillion annually.
- Online criminals threaten the security and safety of you and your company.
- Their crimes include identity theft, child pornography, commercial scams, financial data theft, illegal gambling and extortion.
- “‘Distributed’ denial-of-service” (DDoS) attackers electronically seize private computers to use as “bots” or “zombies” to flood and close the servers of online firms.
- Cybercriminals blackmail their victims – often gambling sites – and extort big payoffs.
- U.S. cybercrime expert Barrett Lyon and British security agent Andy Crocker have helped companies and governments fight cybercriminials.
- As cybercrime develops geopolitical motives, it morphs into cyberwarfare.
- The Internet “is not designed for security; it’s designed for fault-tolerance,” leaving companies susceptible to attacks.
- Making the Internet less vulnerable might require changing its basic structure, but meanwhile governments need to invest more resources in fighting cybercrime.
- To avoid cyberattacks, use robust firewalls and regularly update your antivirus software.

Summary

Barrett Lyon

The Internet provides a cornucopia of connections, communication, education and other remarkable benefits. Unfortunately, it provides even more opportunities for breaking the law – extortion, identity theft, child pornography distribution, commercial fraud, theft of financial data, gambling and more. Cybercriminals and hordes of hackers plague the Internet. How serious is online crime? In 2005, hackers illegally downloaded as many as 45 million credit and debit card numbers from TJX, the parent company of retailer T.J.Maxx. By 2009, approximately 30% of Americans had experienced identity theft. People and companies suffer estimated annual losses of $1 trillion at the hands of cybercrooks.

> "As the world connected to more computers and depended on them for more things, the bad guys were wreaking havoc."

Computer genius Barrett Lyon has achieved remarkable success thwarting these criminals. He is a leading expert on shutting down "'distributed' denial-of-service" (DDoS) attacks. In these online assaults, cybercriminals use malicious software to invade and control thousands of individual Web-connected computers. The software autonomously converts these computers into "zombie networks" called "botnets" and directs them to flood targeted commercial Web sites with a tornado of activity that overwhelms their servers and knocks them offline. The criminals then extort money, up to hundreds of thousands of dollars, from the besieged sites. They hit online betting sites just before major sports events, when they must be online. If the site owners pay, the cybercriminals recall the zombie attackers until the next time, often just before the next big game.

> "The only way to create a secure Internet is to start over."

In 2003, Lyon helped one gambling site, Bet Costa Rica International Sports, known as BetCRIS, thwart vicious DDoS attacks that cost it as much as $5 million a day and could have put the company out of business if it hadn't made extortion payments. Lyon used vast bandwidth and a battery of innovative techniques to repel the zombie botnets. Impressed with his solution's success, the site's principals funded a DDoS-defense firm that Lyon organized, Prolexic Technologies, Inc. He provided technical expertise for the firm, which soon had many clients, including other betting services, but he was dismayed to learn just how shady his partners turned out to be.

> "With little public attention, viruses were morphing from an occasional annoyance to a key criminal tool."

In his fight to repel DDoS attacks against offshore gambling sites like BetCRIS (which are illegal in the U.S.), Lyon discovered that many assaults originated in Eastern Europe and some involved the notorious Russian mob. He found that the U.S. Mafia was also quite active in cybercrime, including online betting, "identity theft and Web fraud." He learned unhappily that, at the time, the U.S. Federal Bureau of Investigation (FBI) was lukewarm about eliminating cybercrime. However, the agents of Britain's National Hi-Tech Crime Unit (NHTCU) were passionate about attacking it. Both Queen Elizabeth II and then-Prime Minister Tony Blair understood the vital importance of electronic commerce, so the British government provided NHTCU with the funding, personnel and technical resources it needed to fight cybercrime.

> "Online scams and identity theft soared, and an entire underground industry grew."

To dissociate himself from his disreputable partners, who seemed to be turning Prolexic into a mob money-laundering operation, Lyon tried to sell them his interest in the firm. When they refused to buy him out, he discontinued his day-to-day involvement. He teamed up with venture capitalist Perry Wu to form a new company, BitGravity, an online video delivery service. Lyon also began to testify to the FBI about his Prolexic partners' activities and their unsavory relationships with organized crime. Eventually, Prolexic's investors sold the firm. Lyon received a $400,000 payout, a third of the sum his erstwhile partners had once promised.

Andy Crocker

Just as Lyon successfully fought DDoS attacks for his clients, British agent Andy Crocker managed to shut down criminal hackers operating from the former Soviet Union. His investigation of Ivan Maksakov, a Russian criminal hacker known online as "eXe," led to the "greatest international cybercrime prosecution in history." When Russian hackers hit U.K. betting companies in a DDoS extortion scheme, Crocker was on the case, but he knew his investigation would be difficult: Russian authorities did not work well with outside cybercops.

> "The bad guys...had taken over hundreds of thousands of PCs for a 'distributed' denial-of-service, or DDoS, so that malicious traffic came from everywhere at once."

Crocker discovered that funds from some Russian illegal online activities were going to terrorists in Chechnya, including some who allied with "anti-American jihadists." Crocker turned his Russian data over to an FBI agent, who showed minimal interest. Crocker "gave up hope" about the FBI. Instead, he met with Russian Ministry of the Interior colonel Igor Yakovlev, who assigned an agent to monitor Maksakov. In 2004, armed with the evidence he and Crocker needed, Yakovlev and his team arrested Maksakov and other extortion suspects.

> "Cybercrime is much worse than you thought."

Maksakov confessed to his involvement in the extortion scheme. He had been "running bots off [his] server." He said two Russian men he had recently met online were creating a self-replicating "bot" that would "spread by itself among computers, enslaving them as it went." The two men, known to him only as "Milsan" and "Zet," advertised their criminal services ("DDoS for hire") online. They had paid Maksakov a total of $4,000 for his help with three DDoS attacks. Maksakov also identified a criminal hacker known as "Bra1n," the suspected head of the DDoS extortion ring. Bra1n eluded Crocker and Yakovlev, but they brought a case against Maksakov and two other cybercriminals, Alexander Petrov and Denis Stepanov. Although Crocker couldn't catch the scheme's masterminds, he dug deeper into Russian organized crime than any Western agent since the end of the Cold War.

> "In 2004, very few U.S. hackers had been arrested, and the ones who had been caught were usually dumb teens who had broken into Web sites and then bragged about it on Internet Relay Channels."

As the trial began in January 2006, Crocker and Yakovlev briefed Russian prosecutor Anton Pohamov on the evidence against the cybercriminals and the pertinent "technology issues." Crocker was pleased that Pohamov had an honorable reputation and spoke excellent English. And Pohamov was glad to have Maksakov's formal confession plus "logs of his monitored chats with others in the [extortion] ring." Then, Maksakov withdrew his confession and entered a not-guilty plea. Nevertheless, after a 10-month trial, Judge Igor Grigoriev, who had been offered a bribe to rule for the defendants, found that Maksakov and his colleagues were guilty of DDoS attacks using up to "600,000 simultaneous Web connections." His 120-page verdict sentenced the three men to eight years of hard labor. Despite bringing Maksakov, Petrov and Stepanov to justice, Yakovlev and Pohamov have not advanced much in their careers.

From Russia with Love

Cybercriminals wreak enormous damage worldwide. They turn millions of computers into zombie slaves and commit massive fraud that drives a stake through the heart of online commerce. Many cybercriminals hail from Russia and Eastern Europe, where low pay and a "significant predisposition toward corruption" make fraud endemic, and where strong technical education programs graduate skilled techies into a very weak market for computer jobs. Some Eastern Europeans resent Americans' relative wealth and see them as justifiable targets for identity theft and other online frauds.

> "People have shown that they will continue to gamble on the Internet, even if they must entrust their money to obvious crooks operating in shady jurisdictions."

Even more distressing: The national governments of Russia, China and some other countries now ally themselves with cybercriminals. In Russia, where gangsters and the Mafia have extremely deep roots, "state-sponsored cybercrime" is practically the status quo. Russia's Federal Security Service, the organization that replaced the KGB, may even have been behind the development and spread of the notorious SoBig virus that attacked computers worldwide in 2003. At the time, it "overwhelmed law enforcement and the growing ranks of [Internet] security professionals."

> "Annual online poker revenue soared from $90 million in 2002 to $2.4 billion in 2005."

Nations like Russia and China can steal millions through cybercrime, seriously disrupting Western economies by using computer attacks as "geopolitical weapons." Thus, expensive cybercrime mutates to dangerous cyberwarfare. Indeed, Russian computers may have initiated a 2008 cyberattack on U.S. Defense Department computers. The Chinese have been able to breach computer security at the U.S. Army Information Systems Engineering Command and other U.S. government agencies. However, Russia, China and Eastern European nations are not the only sources of cybercrime. In 2009, a splinter political group used Israeli computers in a DDoS assault on Palestinian Web sites. Conversely, a Russian legislator thanked hackers for attacking Israeli sites. Islamic terrorists frequently employ cybercrime. The infamous "Bali nightclub bomber" applauded credit card fraud as an effective way to raise funds. In 2007, three British jihadists spent $3.5 million drawn from 37,000 stolen credit cards to help other terrorists.

> "Players in most of the professional leagues were betting on their own games."

Though Lyon has successfully fought DDoS attacks, they continue widely. In 2009, more than 1,000 DDoS attacks hit governments, businesses and "activists" each day. Such assaults are remarkably easy to orchestrate. A Canadian teenager who disliked an online commentator closed U.S.-based Digg, a popular news site. Lyon, a friend of the site's CEO, restored it in five minutes in exchange for a pizza. Authorities caught the teen when he bragged online about his crime.

Fighting Cybercrime

Governments need to mount a concerted push to apprehend cybercriminals and develop mechanisms for disabling their technological tools. Governments must find ways to block cybercriminals from reaching their victims on the Web. U.S. regulators should realize that people will gamble online, despite the law, and should legalize betting sites to drive mobsters out of the business. The U.S. could earn money by taxing online gambling, while instituting tight regulations to protect gamblers. For now, Internet users should learn how to shield their computers' security. This means creating robust firewalls and regularly updating your antivirus software.

> "Retailers, not banks, generally absorbed losses caused by identity thieves wielding pilfered credit card numbers."

Additionally, schools should teach children how to use computers safely so their machines don't become infected with viruses or infiltrated by criminals. Software manufacturers should clean up the security flaws in their products and develop "rapid patching procedures" users can deploy in the event of an attack. Banks must be more vigilant in demanding secure identification before providing credit or authorizing online transactions. Most importantly, governments, companies and other influential entities should wake up to this security emergency and work together to protect the Internet. Countries should organize "Computer Emergency Response Teams" with the national authority to close criminal sites. Governments should hire and train "cybercrime agents."

> "The fight against the bots is now unwinnable."

The Internet's security problems are so comprehensive that these helpful measures are only palliatives. The Web's basic structure was created to be open and accessible, not closed and secure. This creates serious structural security flaws. Lyon now advises, "The engine of the world economy is based on this really cool experiment that is not designed for security; it's designed for fault-tolerance. You can reduce your risks, but the naughty truth is that the Net is just not a secure place for business or society." Lyon, Crocker and other cybercrime experts believe the only path to real security is to restructure the Internet and its basic protocols.

> "If the worst criminals had improved their technology to the point that they could leave denial-of-service-attacks behind, a whole new war was opening up."

Unfortunately, governments and other entities have made only laughably small investments in fixing cybersecurity. Those who are most informed about the growing danger of cybercrime are discouraged about law enforcement. The U.S. government's response to fighting cyberthreats was weak during the Bush presidency and is only slightly better in the Obama administration. The 2008 U.S. Cybersecurity Enhancement Act is a step in the right direction toward tougher protective legislation. And, in another mark of progress, the U.S. Defense Department opened a new Cyber Command within the National Security Agency in 2009. That year, Andy Crocker, who retired from government service, told a secret meeting of "more than 100 top spies" that Al Qaeda and its ilk would find it simple to use "criminal service providers to attack the U.S."

At the same conference, Barrett Lyon explained about the Internet's systemic vulnerability. He eventually left BitGravity, the company he founded after Prolexic. A major Pentagon executive asked him to develop a "menu of offensive weapons to destroy enemy computer networks." But Lyon, once dedicated to shutting down cybercriminals and their zombie armies, refused. Instead, he is developing a new "content-delivery" company, 3 Crowd Technologies, to enable computer network owners to sell extra capacity, that is, to let remote operators use their computers during downtime. Barrett Lyon believes this could "put him at the helm of the world's biggest botnet."

About the Author

Joseph Menn covers technology issues, including cybersecurity, for the *Financial Times*. He also wrote *All the Rave: The Rise and Fall of Shawn Fanning's Napster*.