Volume 10 (2010)

Interface: The Journal of Education, Community and Values

3-1-2010

Fatal System Error. The Hunt for the New Crime Lords Who Are Bringing Down the Internet

Jeffrey Barlow
Pacific University

Fatal System Error. The Hunt for the New Crime Lords Who Are Bringing Down the Internet

Description

Review of *Fatal System Error. The Hunt for the New Crime Lords Who Are Bringing Down the Internet*

Fatal System Error. The Hunt for the New Crime Lords Who Are Bringing Down the Internet.

Posted on **March 1, 2010** by **Editor**

Review by Jeffrey Barlow

Joseph Menn's work, *Fatal System Error*, is an extremely detailed and very well researched investigation into organized cyber crime, with a focus on the years from about 2004-2008. Mr. Menn is well qualified to write this book. A former technology reporter for *The Los Angeles Times*, he has written several other significant works related to the Internet, notably, *All The Rave*, *The Rise and Fall* of Shawn Fanning's Napster. He was twice nominated for the Pulitzer prize.

The topic is an inherently exciting one. The author focuses upon the protagonists in organized cybercrime, both the "white hats" and the "black hats." The first of the former is an American hacker, Barrett Lyon, who turned from initially protecting gambling sites from Denial of Service Attacks to broader work assisting law enforcement internationally in uncovering criminal cartels. The second white hat is Andy Crocker, an English police officer who came up in the British forces during a period when the Blair government intended to make Britain a model for the protection of on-line commercial activity. The author worked closely with them in researching and writing *Fatal System Error*.

Through Lyon and Crocker's work, often done cooperatively, the reader also meets numerous criminals, some in their real-world identities, others as shadowy pseudonyms on the net. These operate most frequently out of Russian and other former Soviet republics, may of which have effectively become an alliance between organized crime and corrupt local, and apparently, national governments.

Menn [1] worked closely with dozens if not hundreds of actors on both sides of the legal divide and has been able to discuss highly technical details of the endless fight between offense and defense in cybercrime, while simultaneously bringing the individuals alive. The author manages to

walk some very tight lines in doing so. It is clear that Lyon has a very mixed past and at some points came very close to himself being a criminal, an issue which Menn skirts while pointing out how very frequently other individuals have worked both sides of the street, now an FBI informant, now a master criminal.

Some might idealize the criminals discussed here. After all, part of the charm of computer crime is that it is white-collar work and intellectually challenging. There is also a sort of pleasure, I am sure, in the power that breaking and entering other's computer systems, not to mention their lives, brings. But these criminals are not Robin Hoods.

The gangs rob the poor as well as the rich; in fact, as the book points out, the poor, or at least the middle class, are much easier to rob than the rich, who have a tendency to spend money to protect their money, sometimes vengefully so. The gangs also murder…daughters of complainants are kidnapped, never to be seen again; those who turn on the gangsters die accidently in the custody of corrupt police forces, and if angered the gangs may destroy your business simply to make an example of you. Even those who write about them may find their lives and those of their family members threatened. The difficulties (and dangers) of the author's research should not be underestimated.

We assume that at least the readers of *Interface* are aware how very serious a problem cybercrime has become. As bad as you might think it is, Menn is able to point out how very much worse the reality has become. The agencies which should be protecting consumers, particularly the banking industry, have managed to make accommodations—such as passing losses onto merchants who in good faith accept bad credit cards—to the point where they now often oppose stricter legislation intended to prevent such crimes in the first place.

Governments, for their part, have found the struggle much too difficult (fewer than one percent of cybercriminals are ever convicted) and have in effect given up. It is telling that both Lyon and Crocker, although young in at least Lyon's case, and both at the top of their game, have essentially retired from the struggle and gone into private industry where they see some hope of making headway. They, like the author, have very low expectations of governmental agencies.

In his last chapter, "Fixing What's Fixable," Menn discusses possible solutions, but like many of the experts whom he interviews, he believes that the current Internet is broken and may have to be supplanted with a new two-track system in which participants either accept restrictions on their privacy or risk being robbed or otherwise exploited.

Of the positive actions which Menn suggests, one is the education of consumers. At *Interface*, we have long argued that such education must be undertaken at the public level as soon as computers begin to appear in the curriculum at any given school. This will mean, as Menn's work suggests, educating future "black hats" as well as future "white hats," but the problem can hardly be worse. At present, the "black hats" are clearly winning and the "white hats," are, as one of Menn's experts puts it, "losing faster."

In addition to those simply interested in cybercrime, the work is worth reading by those who work in the industry. Menn does an excellent job of outlining the rapid evolution of the use of technology by the gangs—among his villains are all the familiar big name companies which refuse to take responsibility for bad software which is distributed with known weaknesses.

These firms, like the banks, have supported laws which relieve them of responsibility. As the consumer does not "buy" the product but in effect "rents" or licenses it, the legal exposure to the producer is far less. The consumer pays at every point. Finally, as the author points out, both the recovery of lost funds and the prosecution of perpetrators is extremely difficult, despite the assurances we are constantly given from the business dependant upon digital transfers of funds:

A Gartner survey found that 30 percent of Americans had been victimized by identity fraud by 2009. They got back an average of 86 percent of the money drained from credit cards and 77 percent of the money stolen from ATM and debit cards. Victims of bogus account transfers, though, recovered only 54 percent of their losses. Small businesses were increasingly targeted in account transfers, and the banks often refused to make up the losses. As for the banking industry's red ink, that was anyone's guess. Convictions remained an extreme rarity, striking far less than half of 1 percent of the perpetrators. [2]

Many of Menn's solutions are perhaps counter-intuitive, another value of the book. The issues are so complex that most of us may choose to oppose legislative proposals which initially might seem ineffective or perhaps even likely to worsen the situation. For example, Menn supports the legalization of on-line gambling on the grounds that on-line gamblers are such fools that they are going to gamble anyway, and that it would be better to license and tax it than simply turn so many sheep over to the wolves annually.

His arguments are compelling. For many years individuals have chosen to gamble on-line with firms that have shown, statistically at least, to simply ignore the players' odds of winning by manipulating the hands dealt. The player turns up three aces; the software is programmed to finally, after betting is closed, deal itself four of a kind, however long the odds against that occurring in fact are. The player whispers "almost!" and plays again.

Fatal System Error shows us a terrible truth about the Internet. It truly is in an important sense, broken. Or perhaps more importantly, it has broken many of our laws and institutions, particularly when viewed internationally. Nation states are simply not sufficiently cooperative to deal with cross-border gangs.

Menn fears that the result may one day be that it will be necessary for given states to isolate themselves from other states where criminals—or politically oriented nationalist hacker groups—flourish. [3] But even this is only a partial solution. Ironically, most gangs choose to operate in the U.S. or Europe where the bandwidth is better and the pickings richer.

The book is not without its flaws. While the author has done tremendous research and made

much of it available on the Internet, to see his sources as one reads requires, at least in my Kindle edition, the reader to prowl through the chapter notes at the back, not knowing if the source is, in fact, cited—there are no notes to indicate such. There is a key word index, but not searchable in the Kindle edition [4] and there are no page numbers added to the key word—the reader knows the topic is covered, but not where nor to what extent.

Some readers are going to find the author's prose a bit breathless…lest the reader miss the significance of the topic or the scale of the research, Menn reminds us frequently in words such as these:

Their (Barrett and Crocker) combined stories shine by far the brightest light yet into a shadow economy that is worth several times more than the illegal drug trade, that has already disrupted national governments, and that has the potential to undermine Western affluence and security. This book is about the triumph of two men who went where none like them had gone before. [5]

Also, the work is not truly up to date. Although the publication date is 2010, the coverage pretty much ends before 2009, though there are a few references to events in 2009. While this early history is necessary to understand the present, we can only hope for periodic updates. This is, of course, a great deal to ask from any author. We all get bored with any one topic, and as exciting as investigating cyber crime must be—the author did on site research in the former Soviet Union, for example—the prospect of a career spent on one topic is a daunting one at best.

At *Interface* we have reviewed several previous works on hackers, and while each has its value, this is by far the most comprehensive of them. See Nuwere, Ejovi and David Chanoff. *Hacker Cracker*. At: http://bcis.pacificu.edu/journal/2004/02/nuwere.php. See also Mitnick, Kevin D. and William L. Simon. The Art of Intrusion. at: http://bcis.pacificu.edu/journal/2005/07/mitnick.php

Endnotes

[1] See Menn's home page at: http://www.josephmenn.com/index.php

[2] Loc. 2889-93 (Kindle edition)

[3] China comes in for much criticism by the author. While it is clear that Chinese nationalist hackers have been very active, I myself think that the tolerance of the PRC for truly organized crime is very low. Such groups have too often been rivals for power and authority in China to be tolerated at more than a local level.

[4] While, as I have often made clear, I find our Berglund Kindle a great aide in reading and writing, the increasing tendency of Amazon to release Kindle editions without searchable indexes negates one of the great advantages of the format.

[5] Loc. 58-60 (Kindle edition)

This entry was posted in Uncategorized by **Editor**. Bookmark the **permalink [http://bcis.pacificu.edu/interface/?p=3743]** .