

America lies at the heart of a

Contributed by Harris Badar
Friday, 20 March 2009

An estimated 350 million dollars a year in illegal drug money is laundered through the American banking system. That one figure alone is more than the total receipts of crime in all the other countries in the world put together. This figure also makes America the most corrupt country in the world, because criminal activities on this scale cannot take place without the connivance of thousands of corrupt law enforcement officials – many of whom are drug addicts or drug pushers themselves.

The huge amount of drug money laundered through the US banking system is of a piece with the fact that America is the biggest market for illegal drugs in the world. American is the main market for the heroin produced in Afghanistan (which has shot up many fold since US troops invaded and occupied the country) and the cocaine produced at secret locations in the jungles of the South American country of Colombia (where the drug mafia runs a virtually parallel government of its own, complete with private armies).

An estimated 350 million dollars a year in illegal drug money is laundered through the American banking system. That one figure alone is more than the total receipts of crime in all the other countries in the world put together. This figure also makes America the most corrupt country in the world, because criminal activities on this scale cannot take place without the connivance of thousands of corrupt law enforcement officials – many of whom are drug addicts or drug pushers themselves.

The huge amount of drug money laundered through the US banking system is of a piece with the fact that America is the biggest market for illegal drugs in the world. American is the main market for the heroin produced in Afghanistan (which has shot up many fold since US troops invaded and occupied the country) and the cocaine produced at secret locations in the jungles of the South American country of Colombia (where the drug mafia runs a virtually parallel government of its own, complete with private armies).

If there was no demand for illegal drugs in America, the drug producers in Afghanistan, Colombia, Myanmar (Burma), Thailand and other countries would soon be out of business. Successive US governments have been throwing large sums of money at the supply end of the problem in the form of more money for helicopters for the US Drug Enforcement Agency (DEA), more patrol boats for the US Coast Guard and more weapons for US Border Guards in an effort to reduce the flow of drugs into America – but all to no avail. Instead of going down, the demand for drugs in America has continued to go up, with organised crime syndicates raking in huge profits.

Relatively little money, however, has been spent by successive US governments on the user end of the problem in their own country. It is at this user end of the problem that the answer to reducing the market for drugs in America lies. Yet this is an aspect of the problem that has continued to be mostly ignored ever since the 1980s when then-US President Ronald Reagan launched his so-called “War Against Drugs”. That war was a miserable failure, and has continued to be a failure ever since then.

One of the results of this failure has been the huge rise in the number of prisoners in American jails. This number now exceeds 2.6 million, the highest figure by far for any country in the world. America now has a population of 300 million people. The 27 EU member countries have a combined population of roughly the same number of people. Yert the total number of jail inmates in all the EU countries put together is less than 15 per cent of the number of jail inmates in America.

According to official figures compiled by all the US federal, state and local law enforcement agencies, the number of reported crimes in America now totals over 15 million a tear – far more than the number in any other country. This is yet another illustration of the fact that America is the crime capital of the world. And the story doesn’t end there because numerous crimes go either unreported or undiscovered.

Another aspect of the worldwide web of organised rime has to do with the fact that billions of impoverished people living in developing countries still have no idea what the Internet is and what it does. But some others elsewhere know what it is only too well and are using their knowledge to profit from it illegally in the shape of cyber-crime. Until recently, cyber-crime was largely a sport for lone wolves and teenagers with a twisted mentality, or for small groups with a taste for mischief and danger. Organised-crime groups largely left the Internet alone. But security experts are worried that Net crime across borders will quickly proliferate. The reason: Low risk of apprehension and the potential for big rewards.

Now, however, those worries are finally starting to come true, according to the US’s National Infrastructure Protection Commission (NIPC) – an American federal watchdog that works with the FBI to protect the US national infrastructure.

The NIPC says that Eastern European hackers have now infiltrated Web servers running versions of the Microsoft NT operating system, grabbing millions of credit-card numbers and other personal information from US financial institutions.

After lifting this data, the gang has allegedly attempted to extort money from their victims by threatening to post the information on the Internet.

Law enforcement officials say there's plenty of blame to go around for this crime wave. They say many companies have clearly fallen down in enforcing basic security policies for their Internet operations. Some have never fixed vulnerabilities. Software vendors are also at fault for selling flawed products.

John Gilligan, chief information officer for the US Air Force's computer networks, says, "The increasing reliance of our economy on information technology requires that we have software systems that have much higher levels of security."

In August 2000, media mogul Michael Bloomberg (who is currently the Mayor of New York City) helped police apprehend two Kazakhs who had stolen his personal information from his company's computer networks. And in January 2000, a still-at-large Russian hacker dubbed "Maxus" posted for public consumption on the Internet 25,000 credit-card numbers stolen from online music retailer CD Universe, after the company refused to pay his six-figure extortion money demand.

Malicious hackers have long had easy access to automated tools designed to find flaws in Web servers and other software exposed to the public Internet. But the timing of the NIPC warning came amidst a raft of bad Net-security news. The same week, hackers published a free programme that makes it easy to compromise encrypted passwords on computers running older versions of e-commerce software from IBM, which expressed frustration that customers weren't applying readily available patches.

A survey released by the US Computer Security Institute (CSI) shows that 65 per cent of the 538 companies and large institutions it polled acknowledged suffering financial losses due to computer breaches in the previous year. The majority of those breaches came over the Internet, according to the CSI survey. Of those entities, the 186 that were willing to tally their losses admitted that the hacking had cost them \$ 378 million, up 42 per cent and the highest number since the CSI started these eight years ago.

The CSI study likely downplays the real figure. Many companies are loath to admit to anyone that they've been hacked. Likewise, the NIPC is probably understating the number of companies facing extortion threats. "According to Alan Paller, director of research for the US Systems Administration Networking & Security Institute, the actual number of extortion victims could be much higher.

This comes as no surprise. The amount of commerce and financial transactions now passing over the Internet means that it's now a far more enticing environment for organised hackers in which to operate. And that's precisely what the Eastern European crime ring appears to be doing.

Allegedly based in Russia and Ukraine, the group appears to use three well-known security holes to ransack systems and then come back with ransom demands. One press report quotes Shawn Henry, the chief of computer crime investigation for the NIPC, as saying, "We began to see a correlation between many investigations that we been conducting. We had victims who had reported that their systems had been compromised, and there had been extortion demands placed against them."

The question is: What should be done? First of all, software companies that fail to safeguard their products should be subject to legal action for damages. At the same time, they should help create better solutions to the existing systems of applying patches to flawed programmes. Overwhelmed systems administrators often apply a dozen or more of these patches each week — and the patches themselves often conflict with other critical software, says a press report.

The complexities that are inherent in mixing and matching different software systems, provides business revenues for dozens of multibillion-dollar consulting companies. "Every systems administrator is the equivalent of the head of maintenance for an airline. His job is to not only maintain the planes, but create the blueprints for the planes, too. That's just insane," a press report quotes Paller as saying.

The report says that all this cries out for big changes in the system — changes that software and e-commerce companies fear would impose a heavy financial burden on them. But building in safety measures need not be so heavy-handed. The US Lawrence Livermore National Laboratory is already testing a system called SafePatch that would automate the patching process and smooth over many of the conflicts inherent in the process.