

Federal Computer Week

FBI goes global on threats

By Ben Bain

Jan 12, 2009

Law enforcement officials continue to face in the age of global interconnectedness and criminal behavior that operates without regard to national borders.

Last May, the Justice Department announced charges against 38 people for their alleged involvement in a computer and credit card fraud scheme that spanned the globe. It was a case the FBI could not have solved without close coordination with officials in Romania, because the international crime ring had a significant base in Bucharest.

The defendants were charged with crimes related to phishing, tricking people into revealing personal information and passwords that allowed the criminals to defraud them of millions of dollars. Several of the defendants have pleaded guilty. Romanian authorities, coordinating with the FBI, conducted several searches of homes that uncovered crucial evidence necessary to prosecute the defendants, said Mark Filip, Justice's deputy attorney general. Indeed, the Romanian authorities' active cooperation with the FBI now serves a model when U.S. law enforcement officials discuss international cooperation on cyber crime.

"The Romania prosecution is a good example of our ability to deal with cyber criminal activity cutting across national borders," Filip said.

The case was a relatively simple one, but even so, it took close and careful cooperation between U.S. and foreign officials to solve. It's a good example, Filip said, of the challenges that law enforcement officials face in the age of global interconnectedness and criminal behavior that operates without regard to national borders. Fostering cooperation and sharing of information is difficult enough among U.S. counterintelligence agencies.

When dealing with other countries — which have a wide variety of laws, enforcement capabilities and degrees of willingness to help — the equation becomes dramatically more complex. "Many traditional organized crime figures who in the past committed crimes such as narcotics smuggling or extortion are now setting up shop online, and these figures are less constrained by national borders or geographic location," said Filip, speaking at the International Conference on Cyber Security (ICCS) 2009 held by the FBI and Fordham University last week in New York City.

Now, "they use the global reach and seeming anonymity of the Internet to carry out their schemes," he said. And cyber crime tactics are rapidly advancing, challenging law enforcement organizations to keep up.

"The sophistication has grown exponentially," said Shawn Henry, an FBI assistant director who heads the bureau's cyber division. "And it really is a case where the offense sometimes outpaces the defense — the ability of attackers to exploit known vulnerabilities or to develop new tools, techniques, tradecraft to exploit emerging vulnerabilities is significant."

As if cyber crimes directed against financial institutions and corporations — and the individuals who do business with them — were not worrisome enough, terrorist groups want to use the technology to attack networks, Henry said. They already use online networks to communicate, spread propaganda and raise funds, he said.

“There is no shortage of groups or countries that are interested in the intelligence that is contained on U.S. networks,” he said.

Other than a nuclear device or some other type of destructive weapon, Henry added, “the threat to our infrastructure, the threat to our intelligence, the threat to our computer networks is the most critical threat that we face.”

The weakest link

Officials from more than 40 countries that have varying capabilities and experience in mitigating cyber threats attended the New York conference. Experts pointed to the disparity in laws and technical capabilities as the biggest obstacles to dealing with a cyber crime.

The first order of business is getting many countries to view cyber crime as a criminal justice issue.

“In many countries cyber crime is not a crime” as it is in the United States, said Veni Markovski, a senior adviser to Bulgaria’s Agency for Information Technology and Communications. He is president and chairman of the board for Internet Society, a Bulgarian nongovernmental organization.

The ICCS event is an example of the FBI’s efforts to change that situation, creating a venue for U.S. law enforcement officials to proselytize on the dangers of cyber crime. Other efforts include programs to train foreign law enforcement counterparts, case coordination through the 75 legal attachés and suboffices the bureau has in countries around the world, and Justice’s efforts in the Group of Eight’s (G8) Subgroup on High-Tech Crime.

That G8 subgroup is chaired by Christopher Painter, who recently joined the FBI as a deputy assistant director in the cyber division after a long legal career working on cyber issues at Justice.

The subgroup runs a 24-hour, seven-day-a-week network that allows officials to contact colleagues from other countries for help with cyber crime matters. The network includes 55 countries, and Painter said it helps countries learn about what they should do internally and how they can cooperate internationally.

“When [other countries] can do cyber investigations better, then we can, too,” Painter said.

Painter added that work is ongoing to expand the network and that ideally every country would be represented in it, with the caveat that they must have the necessary expertise and cyber laws in place.

Claudio Peguero Castillo, who founded the cyber crime unit of the Dominican Republic’s national police and now serves as an adviser to the chief of police, said a key to international collaboration on cyber crime is building relationships with foreign colleagues. “The secret of international

cooperation — and it's a tricky part — is you have to know the person on the other side of the phone or the e-mail," he said.

The Dominican Republic, which is part of the G8 24-hour network, was the first country to develop a national cyber law that was totally compliant with the Council of Europe Convention on Cybercrime, Castillo said. That accord lays out guidelines for governments to develop legislation directed at cyber crime. Many nations, including some not in Europe, have signed or ratified the treaty or passed similar national laws.

Howard Schmidt, a former top cybersecurity adviser in the Bush White House and now president of the Information Security Forum, said that getting more countries to ratify the Council of Europe convention would provide significant progress forward by allowing countries to know that what is against the law in one country is also against the law in another country. Experts say harmonization of laws is important because if a country has weak or no laws against cyber crime, the nation can be used as a haven or pass-through for cyber crime and attacks.

"Any country that doesn't have its laws up to snuff — the [criminals] are going to be smart — they are going to route their attacks through that country to make it more difficult to trace it," Painter said.

Even when cyber crime laws are tough, cyber crime still poses unique challenges to law enforcement. Attribution in the cyber realm is notoriously difficult, with criminals using tools such as botnets, which can hijack thousands of computers all over the world to launch cyberattacks or scams, according to law enforcement officials.

How President-elect Barack Obama will alter the overall U.S. cyber strategy or approach to engagement with foreign partners remains to be seen. But speakers at the conference expressed hope that lawmakers and the incoming administration understood the seriousness of the cyber threat and its international components.

"It's not a U.S. problem, it's not a Mexican problem, it's not a Dutch problem, it's not a German problem — it's a problem for our society, all of us," Henry said. "The threats that we see are threats to all of us."