THE HOMELAND SECURITY *NEWS CLIPS*

PREPARED FOR THE DEPARTMENT OF HOMELAND SECURITY BY BULLETIN NEWS WWW.BULLETINNEWS.COM/DHS

TO: THE SECRETARY AND SENIOR STAFF

DATE: FRIDAY, FEBRUARY 25, 2011 7:15 AM EST

TODAY'S EDITION

[redacted]

[redacted]

To Probe "Dark Spots" Where Cybercrooks Lurk, FBI Wants New Tools (FOX)

By John Brandon

FOX News, February 25, 2011

Living on the edges of the Internet, cyberstalking sex addicts, terror suspects, and spambot purveyors communicate through secret chat boards and instant messaging tools, send real-time communiqués through Facebook, talk over Web phone services like Skype, and generally live off the grid.

It's called "going dark," and the FBI wants to put an end to it. Now.

The challenge? The standard techniques for dealing with criminals online -- normal Internet surveillance, which typically involves scanning e-mail messages, data stores, and other “static” info held on servers across the U.S. -- doesn't work with cybersavvy crooks.

“The old ways of combating cybercrime through service provider monitoring is a failing endeavor,” said Marc Maiffret, the CEO of eEye Digital Security, a vulnerability assessment company. “It's very simple to create encrypted and obscure forms of communication that will simply go underneath the FBI's radar."

"We've monitored malicious attackers communicating across Internet-based games -- and even the Xbox,” Maiffet told FoxNews.com.

Last week, the Bureau announced a new strategy to deal with these almost untraceable criminals. Valerie Caproni, general counsel for the FBI, explained the growing "dark spot" problem at a special congressional subcommittee. In one case, a pimp was soliciting kids on a social-networking site and luring them into child prostitution. Caproni said the site did not have the technology to track real-time communication -- so there wasn't enough evidence to get a court order and track down the criminal.

At issue is what the FBI calls intercept capabilities -- that is, the agency's ability to capture real-time communication. Take for example the "hacktivist" group Anonymous, which tends to use private chat forums that are nearly untraceable.

“In order to enforce the law and protect our citizens from threats to public safety, it is critically important that we have the ability to intercept electronic communications with court approval,” Caproni said in an official statement. “Without the ability to collect these communications in real or near-real time, investigators will remain several steps behind, and leave us unable to act quickly to disrupt threats to public safety or gather key evidence that will allow us to dismantle criminal networks."

Security experts have been warning about the “going dark” problem for years. Those who monitor security for companies or who manage the Web servers used for the Internet say plenty of cybercrime happens outside the scope of the official watchdog groups.

“The telecommunication back doors are notoriously insecure,” said James Kelley, a technology consultant with Kelley Consulting Company. “They were designed in a way to prevent different law enforcement agencies from knowing the other is tapping the subject. Since the systems use default passwords, Hacker Joe can use the system as well.”

“The FBI is committed to working with industry toward a solution that would allow us to comply with court orders,” said Jenny Shearer, an FBI spokeswoman.

Shining a light on the problem

The implication in the FBI report to Congress is that the agency will develop new tools to monitor criminal activity on the Internet. One of the existing methods, based on the Communications Assistance for Law Enforcement Act (CALEA) in 1994, is to work with telecommunication providers like AT&T to monitor subversive behavior. Caproni noted that this law is now quite outdated: Not only did Facebook not exist back in 1994, but the Internet was a shadow of what it is today.

Ron Meyran, a product director at Radware, a company that develops security products for business, says the solution is for the FBI to use existing security tools to monitor real-time communication -- for example, using algorithms that can decrypt the private communications on chat boards. Meyran says the issue is not that the decryption tools are so complex or not available, but that the social networking services, Internet phone companies, and chat services have been unwilling to let government agencies install necessary surveillance tools, calling them a violation of privacy policies.

Another problem with installing government monitoring tools, said Benjamin Wright, an attorney, security expert, and teacher at the SANS Institute, is that this method also creates a potential back door for criminals to gain access to private networks as well.

“A back door for the FBI may also become a back door for another, possibly repressive foreign government that wants to spy on political opponents,” says Wright.

Wright says the “going dark” problem is not as complex as it might seem -- people leave tracks everywhere, even online video games. He explained a recent case in Indiana where a court asked the makers of the popular multiplayer game World of Warcraft for information about one of their users, a suspected drug dealer.

“Even the most well-trained terrorist leaves an ever-enlarging trail of digital footprints,” Wright said, “Increasingly these footprints are accessible through public search engines. They are also accessible through subpoenas or search warrants for things like credit or debit card transactions.”

To deal with criminals who have “gone dark,” the FBI may simply have to learn more inventive ways to track down criminals.

“The FBI would do well to innovate and, every day, make itself more creative,” Wright said.