

By: April 2008 Botezatu, Hardware Editor

FBI to Snag Criminals in the Internet Backbone

The government agency will push the line between public and private cyberspace

During the Judiciary Committee of the House of Representatives meeting held on Wednesday, the US Federal Bureau of Investigations has offered a sneak preview of its upcoming actions to fight crime in the cyberspace. During the meeting, the US congressman Darrell Issa tackled the topic of online crimes and of how the FBI could protect civilians, government agencies and military structures from malicious Internet users. More than that, he asked the Bureau whether they needed additional legal privileges to get proof of the attacks and start the attackers' prosecution. "I think legislation has to be developed that balances, on one hand, the privacy rights of the individuals who are receiving the information, but on the other hand, given the technology, the necessity of having some omnibus search capability utilizing filters that would identify the illegal activity as it comes through and give us the ability to preempt that illegal activity where it comes through a choke point as opposed to the point where it is diffuse on the Internet," claimed FBI director Robert Mueller in his testimony. At the moment, the FBI is constantly monitoring some parts of the Internet, including chat rooms, websites and P2P networks, in order to detect and stop illegal activities. However, their power is geographically limited, which leaves other portions of the global infrastructure open to such activities. According to Mueller, criminal activity could be centralized no matter of the attackers' geographical location by tapping into the Internet backbone. All the Internet activity, be it legal or illegal, passes through backbone hubs located in hosting facilities across the country. FBI wants the legal authorities to rummage through all the traffic using automated software and to search for illegal aspects. It's not a secret anymore that the FBI is currently reading emails, instant messaging conversations or other types of private data, but such a law would give the Bureau the legal foundation to re-place privacy second after security concerns.