



Home ■ Transport / Border ■ Biometrics ■ Continuity / Recovery ■ Infrastructure / IT ■ Biodefense ■ Surveillance ■ Detection ■ Sci / Tech ■ Markets ■ Policy ■ Energy ■ Search

#### IT security

### Hackers' attacks on U.S. government systems are frequent, serious

Published 8 August 2008

**U.S. government computer systems under frequent and serious attacks by other governments and organizations; James Finch, assistant director of the FBI's cybercrime division: "We're not worried so much about the noisy attacks as we are about the quiet ones"**

Here is more from the Black Hat 2008 Las Vegas event: Remember last year's cyber attacks on Estonia which brought many parts of the small Baltic country to stand still for a couple of days? It is still unclear who launched the massive attacks, but since they occurred after the Estonian government decided to move a statue commemorating Russian soldiers who died during the Second World War from the center of the capital to a more remote location, suspicion fell on Russian nationalist organizations -- and even on the Russian secret service itself. The fact is, U.S. government agencies are exposed to similar attacks. *Dark Reading's* Tim Wilson [reports](#) that at the annual "Meet the Feds" session at the Black Hat conference, top federal officials said the threat of cyber attack against the United States is very real -- and, in fact, is already happening. "There are countries that have [cyber] capabilities equivalent to ours, and in some cases, that exceed ours," said James Finch, assistant director of the FBI's cybercrime division. "There are countries that are knocking on our door every day -- and they are a threat to our national security." Finch declined to name any specific countries or threats. But when asked about recent public cyber attacks that reportedly emanated from China and Russia, he said, "We're not worried so much about the noisy attacks as we are about the quiet ones."

There have been numerous reports of attacks by Chinese hackers on other governments, including a break-in of Congressional computers that was [reported](#) in June. Russian attackers have been credited with attacks on several former Soviet republics expressing anti-Russian sentiments, including Estonia, Lithuania, and Georgia (see [President of Georgia's Site Under Attack](#)). The capabilities of other countries and splinter groups should not be underestimated, said the National Security Agency's Rich Marshall. "We have to be careful about assuming the technological superiority of the United States," he said. "That's the height of arrogance. These attacks don't necessarily require a lot of skill or technology. All they need is access to the Internet."

Government agencies are wrestling with many of the same problems as the private sector, because so many of their systems and communications rely on private-sector infrastructure, the officials said. For example, the speakers bristled at the notion that the government should bear responsibility for protecting critical infrastructure systems, such as the power grid, from cyber attack. "We work with the power companies to come up with sound backup plans, and we work with the other entities that operate our critical infrastructure. But if you're operating systems for a profit, and making money from them, then it's not government's responsibility alone to protect them." Similarly, it is not possible for many government agencies to create a separate, "safe" network that is divorced from the Internet, officials said. "We're delivering services to the public using the same infrastructure they are," said Mischel Kwon, director of U.S. CERT.

While much of the discussion focused on cyber defense, several attendees also leveled questions at the speakers regarding privacy and recent legislation that expands the rights of law enforcement to conduct electronic surveillance. "The last thing I would do is apologize for protecting our national security through the use of court-authorized wiretaps," said the FBI's Finch. "I would prefer a lot more privacy in the United States, and there will always be instances of abuse [of wiretap privileges]. But I can't apologize for surveillance that's done in the interest of national security."

About us | Subscribe | Advertise | Contact us | ©2008 HS Daily Wire