

August 13, 2008

## Before the Gunfire, Cyberattacks

By [JOHN MARKOFF](#)

Weeks before bombs started falling on [Georgia](#), a security researcher in suburban Massachusetts was watching an attack against the country in cyberspace.

Jose Nazario of Arbor Networks in Lexington noticed a stream of data directed at Georgian government sites containing the message: “win+love+in+Rusia.”

Other Internet experts in the United States said the attacks against Georgia’s Internet infrastructure began as early as July 20, with coordinated barrages of millions of requests — known as distributed denial of service, or D.D.O.S., attacks — that overloaded and effectively shut down Georgian servers.

Researchers at Shadowserver, a volunteer group that tracks malicious network activity, reported that the Web site of the Georgian president, [Mikheil Saakashvili](#), had been rendered inoperable for 24 hours by multiple D.D.O.S. attacks. They said the command and control server that directed the attack was based in the United States and had come online several weeks before it began the assault.

As it turns out, the July attack may have been a dress rehearsal for an all-out cyberwar once the shooting started between Georgia and [Russia](#). According to Internet technical experts, it was the first time a known cyberattack had coincided with a shooting war.

But it will likely not be the last, said Bill Woodcock, the research director of the Packet Clearing House, a nonprofit organization that tracks Internet traffic. He said cyberattacks are so inexpensive and easy to mount, with few fingerprints, they will almost certainly remain a feature of modern warfare.

“It costs about 4 cents per machine,” Mr. Woodcock said. “You could fund an entire cyberwarfare campaign for the cost of replacing a tank tread, so you would be foolish not to.”

Exactly who was behind the cyberattack is not known. The Georgian government blamed Russia for the attacks, but the Russian government said it was not involved. In the end, Georgia, with a population of just 4.6 million and a relative latecomer to the Internet, saw little effect beyond inaccessibility to many of its government Web sites, which limited the government’s ability to spread its message online and to connect with sympathizers around the world during the fighting with Russia.

It ranks 74th out of 234 nations in terms of Internet addresses, behind Nigeria, Bangladesh, Bolivia and El Salvador. Cyberattacks have far less impact on such a country than they might on a more Internet-dependent nation, like Israel, Estonia or the United States, where vital services like transportation, power and banking are tied to the Internet.

In Georgia, media, communications and transportation companies were also attacked, according to security

researchers. Shadowserver saw the attack against Georgia spread to computers throughout the government after Russian troops entered the Georgian province of [South Ossetia](#). The National Bank of Georgia's Web site was defaced at one point. Images of 20th-century dictators as well as an image of Georgia's president, Mr. Saakashvili, were placed on the site. "Could this somehow be indirect Russian action? Yes, but considering Russia is past playing nice and uses real bombs, they could have attacked more strategic targets or eliminated the infrastructure kinetically," said Gadi Evron, an Israeli network security expert. "The nature of what's going on isn't clear," he said.

The phrase "a wilderness of mirrors" usually describes the murky world surrounding opposing intelligence agencies. It also neatly summarizes the array of conflicting facts and accusations encompassing the cyberwar now taking place in tandem with the Russian fighting in Georgia.

In addition to D.D.O.S. attacks that crippled Georgia's limited Internet infrastructure, researchers said there was evidence of redirection of Internet traffic through Russian telecommunications firms beginning last weekend. The attacks continued on Tuesday, controlled by software programs that were located in hosting centers controlled by a Russian telecommunications firms. A Russian-language Web site, [stopgeorgia.ru](#), also continued to operate and offer software for download used for D.D.O.S. attacks.

Over the weekend a number of American computer security researchers tracking malicious programs known as botnets, which were blasting streams of useless data at Georgian computers, said they saw clear evidence of a shadowy St. Petersburg-based criminal gang known as the Russian Business Network, or R.B.N.

"The attackers are using the same tools and the same attack commands that have been used by the R.B.N. and in some cases the attacks are being launched from computers they are known to control," said Don Jackson, director of threat intelligence for SecureWorks, a computer security firm based in Atlanta.

He noted that in the run-up to the start of the war over the weekend, computer researchers had watched as botnets were "staged" in preparation for the attack, and then activated shortly before Russian air strikes began on Saturday.

The evidence on R.B.N. and whether it is controlled by, or coordinating with the Russian government remains unclear. The group has been linked to online criminal activities including [child pornography](#), malware, identity theft, phishing and spam. Other computer researchers said that R.B.N.'s role is ambiguous at best. "We are simply seeing the attacks coming from known hosting services," said Paul Ferguson, an advanced threat researcher at Trend Micro, an Internet security company based in Cupertino, Calif. A Russian government spokesman said that it was possible that individuals in Russia or elsewhere had taken it upon themselves to start the attacks.

"I cannot exclude this possibility," Yevgeniy Khorishko, a spokesman for the Russian Embassy in Washington, said. "There are people who don't agree with something and they try to express themselves. You have people like this in your country."

"Jumping to conclusions is premature," said Mr. Evron, who founded the Israeli Computer Emergency Response Team.

[Copyright 2008 The New York Times Company](#)

[Privacy Policy](#) | [Search](#) | [Corrections](#) | [RSS](#) | [First Look](#) | [Help](#) | [Contact Us](#) | [Work for Us](#) | [Site Map](#)

---