

August 13, 2008

Cyberspace Barrage Preceded Russian Invasion of Georgia

By **JOHN MARKOFF**

Weeks before physical 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+Russia.

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 certain Georgian servers.

The Georgian government blamed [Russia](#) for the attacks, but the Russian government said it was not involved.

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. The researchers said the command and control server that directed the attack, which was based in the United States, 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 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 that tracks Internet traffic. He said cyberattacks are so inexpensive and easy to mount, with few fingerprints, that 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."

Shadowserver saw the attack against Georgia spread to computers throughout the government after Russian troops invaded the Georgian province of [South Ossetia](#) on Sunday.

Georgina media, communications and transportation companies were also targeted, according to security researchers.

"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 who assisted in pushing back a cyber attack on Estonia's

Internet infrastructure last May. "The nature of what's going on isn't clear."

A Russian government spokesman said that the government was not involved, but 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. "There are people who don't agree with something and they try to express themselves. You have people like this in your country."

Mr. Nazario said the attacks appeared to be politically motivated. They were continuing on Monday against Georgian news sites, according to Mr. Nazario. "I'm watching attacks against [apsny.ge](#) and [news.ge](#) right now," he said.

The attacks were controlled from a server based at a telecommunications firm in Moscow, he said. In contrast, the attacks last month came from a control computer that was based in the United States. That system was later disabled.

Denial of service attacks, aimed at making a Web site unreachable, began in 2001 and have been refined in terms of power and sophistication since then. They are usually performed by hundreds or thousands of commandeered personal computers, making it difficult or impossible to determine who is behind a particular attack.

The Web site of the president of Georgia was moved to an Internet operation in the United States run by a Georgian native over the weekend. The company, Tulip Systems Inc., based in Atlanta, is run by Nino Doijashvili, who was in Georgia at the time of the attack. Two Web sites, [president.gov.ge](#) and [rustavi2.com](#), the Web site of a prominent Georgian TV station, were moved to Atlanta. Computer security executives said the new sites had also come under attack.

On Monday, Renesys executives said that most Georgian networks were unaffected, although individual Web sites might be under attack. Networks appeared and disappeared as power was cut off and restored as a result of the war, they said

A company researcher noted that Georgia was dependent on both Russia and Turkey for connections to the Internet. As a result of the interference the Georgian government began posting news dispatches to a [Google-run](#) blogging Web site, [georgiamfa.blogspot.com](#). Separately, there were reports that Estonia was sending technical assistance to the Georgian government.

There were indications that both sides in the conflict — or sympathizers — were engaged in attacks aimed at blocking access to Web sites. On Friday, the Russian language Web site Lenta.ru reported that there had been D.D.O.S. attacks targeted at the official Web site of the government of South Ossetia as well as attacks against the RIA Novosti, a Russian news agency.

Internet researchers at Sophos, a computer security firm based in Britain, said that 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.

Internet technical experts said that the Georgian Internet presence was relatively small compared with

other former Soviet states. The country has about a quarter the number of Internet addresses as Estonia or Latvia, according to Mr. Woodcock, the research director of the Packet Clearing House.

With support from the United States, Georgia is in the process of completing a 1,400-kilometer fiber optic network link under the Black Sea connecting its port city of Poti to Varna, Bulgaria. That connection is scheduled for completion in September. The link will give the country added redundancy and make it less reliant on Russian companies for its data communication needs.

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

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