Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar

By Kim Hart
Washington Post Staff Writer
Thursday, August 14, 2008; D01

As the violence unfolded between Russia and Georgia during the past week, hackers waged war on another front: the Internet.

The Georgian government accused Russia of engaging in cyberwarfare by disabling many government Web sites, making it difficult to inform citizens quickly of important updates. Russia said that it was not involved and that its own media and official Web sites had suffered similar attacks. Although a cease-fire has been ordered, major Georgian servers are still down, hindering communication in the country.

Some Georgian officials, bloggers and citizens were able to work around the disruptions, sending text messages to friends in other countries using Web sites hosted by servers in the United States, Poland and Estonia that are less likely to fall victim to a cyberattack.

Concerted online attacks have been a threat for years. But security experts say the "cyberwar" between Russia and Georgia underscores the havoc that can spread on a digital battlefield. It also highlights how vulnerable Web-reliant countries are to assaults that could cripple military communications or a national banking industry.

The attacks against Georgia's Internet infrastructure began nearly two months before the first shots were fired, according to security researchers who track Internet traffic into and out of the countries. Such attacks, known as "denial of service" attacks, are triggered when computers in a network are simultaneously ordered to bombard a site with millions of requests, which overloads a server and causes it to shut down.

"In terms of the scope and international dimension of this attack, it's a landmark," said Ronald J. Deibert, director of the University of Toronto's Citizen Lab, which has nearly 100 researchers mapping Web traffic through several countries, including Russia and Georgia. He said small-scale attacks have occurred between the countries since June. "International laws are very poorly developed, so it really crosses a line into murky territory . . . Is an information blockade an act of war?"

Cyberattacks can be launched cheaply and easily, with a few hundred computers and a couple of skilled hackers. Simpler tactics are even easier to mount by hacking into a server and deleting files, reconfiguring settings and altering photos. Compared with expensive military attacks, cyberwar tactics "seems like the kind of thing that a sophisticated military would want to experiment with," said Ben Edelman, assistant professor at Harvard Business School who has studied cyberattacks.

"Imagine how devastating it would be to a military commander to lose access to a server that tells him..."
where his troops are stationed and where he has resources," he said, adding that "this is the first time we've had such strong evidence of cyberwarfare."

Instructions on how to mount such attacks are readily available on blogs, making it easy for a grass-roots effort to quickly escalate into a crippling assault, said Evgeny Morozov, a technology consultant based in Berlin who has tracked blogs in Georgia and Russia.

Figuring out who is behind the attacks has been difficult, Deibert said, because of complex routing methods and a multitude of connection exchanges. The Internet's infrastructure is a maze of lines laid by different service providers traversing many countries, masking how information is traveling -- or blocked.

"It's an ongoing battle in documenting where it's coming from and helping people get around it," he said.

In Georgia, which is not as dependent on the Internet as other nations, the cyberattack mainly hindered the government's ability to communicate with its citizens and others during the fighting. The Georgian Foreign Ministry's Web site, for example, was disabled except for a collage that compared Georgian President Mikheil Saakashvili to Adolf Hitler.

"Battles today are as much about ideas and images as they are territories," Deibert said. "If you're a military and intelligence agency, you're going to take down information that is in opposition and control the message."

To get around the blockade, Georgian officials relocated national Web sites to addresses hosted by Google's Blogspot, whose U.S. servers are more immune to attack. Citizens used blogging platforms such as LiveJournal -- the dominant platform in Russia and Georgia -- to post their own reactions during the fighting.

For example, a Georgian refugee from Abkhazia who blogs under the name Cyxymu on LiveJournal posted photos of Russian troops entering the Georgian town of Gori. The blogger said the photos were taken after Russia had announced its withdrawal, proving, he said, that fighting continued.

Morozov said only a few hundred Georgians used blogs to communicate with people outside the country. Even that tool was threatened, he said, when a group of Russian bloggers sent a letter asking Sup, the Russian company that owns and manages LiveJournal, to censor posts with pro-Georgian sentiment. Sup did not comply.

Givi Bitsadze, in Tbilisi, used microblogging site Twitter to share updates about the fighting in English and Russian.

"Tbilisi is still safe, but other cities are under attack, bombs kinda stopped, but Russian soldiers are breaking in a houses," one post read yesterday. He also noted an Olympic victory: "Georgia beats Russia in beach volleyball."

The cyberwar will most likely serve as a Web security wake-up call, Morozov said.

"Georgia was completely unprepared to the fact that all this information was on the Internet," he said. "I think it taught them -- and a lot of people -- a lesson."