

FREE EVENT  **Google's Universal Search for Business Webcast**
Learn how your business can benefit from Google's universal search capabilities.
Wednesday, August 13, 2008 | 2:00 PM Eastern/11:00 AM Pacific

Sponsored by
Google **COMPUTERWORLD**

REGISTER NOW

COMPUTERWORLD Security

 Print Article  Close Window

Update: Estonia, Poland help Georgia fight cyberattacks

Jeremy Kirk

August 12, 2008 ([IDG News Service](#)) In an intriguing cyberalliance, two Estonian computer experts are

scheduled to arrive in Georgia by evening to keep the country's networks running amid an intense military confrontation with Russia.

And Poland has lent space on its president's Web page for Georgia to post updates on its ongoing conflict with Russia, which launched a military campaign on Friday to eject Georgian troops from South Ossetia and Abkhazia, two renegade areas with strong ties to Russia.

The cooperation between the former Iron Curtain allies is aimed at blunting pro-Russian computer hackers, who have been blamed over the last few years for cyberattacks against Estonia, Lithuania and Georgia in incidents linked to political friction between those nations and Russia.

Two of the four experts that staff Estonia's Computer Emergency Response Team (CERT) were waiting Tuesday morning in Yerevan, the capital of Armenia, seeking permission to drive into Georgia, said Katrin Pärasmäe, communication manager for the Estonian Informatics Center. The two officials are also bringing humanitarian aid, she said.

Estonia is also now hosting Georgia's Ministry of Foreign Affairs Web site, which has been under sustained attack over the last few days.

"Let's just say we moved it," Pärasmäe said. "I know that there are interested parties who read media so it's not good to say exactly where the hosting is."

The Web site for Georgia's president, Mikheil Saakashvili, remained up on Tuesday morning. That site was knocked offline around mid-July after a DDOS attack from a botnet, network experts said.

The botnet was based on the "MachBot" code, which communicates to other compromised PCs over HTTP, the same protocol used for transmitting Web pages. MachBot code has been known to be used by Russian bot herders, according to the Shadowserver Foundation, which tracks malicious Internet activity.

Shadowserver said Monday that hackers had at one point defaced the Web site for Georgia's parliament. "The attackers have inserted a large image made up of several smaller side-by-side images of pictures of



Sun
microsystems

Leave it to Sun to get
the most from Intel.

60-DAY FREE TRIAL
[CLICK HERE FOR DETAILS >](#)

solaris  Windows 

both the Georgian president and Adolf Hitler," the group wrote.

Georgia is now also hosting some sites in the U.S., a logical move to better defend the sites against attacks, Pärngmäe said. Shadowserver wrote that the presidential site appeared to have been moved to an IP address belonging to Tulip Systems Inc., an ISP in Atlanta.

The country is also looking to other ways to keep information flowing. A Georgian news site was also up, but the site warned it was under "permanent DDOS attack." That Web site has set up a group in [Google's](#) Groups service, where subscribers can get the news stories it regularly posts.

Georgia's banking sites also suffered attacks that caused them to shut down their online systems, said David Tabatadze, a security officer with the Georgia Research and Educational Networking Association and Georgia's CERT. Some of those systems are still down, he said.

Tabatadze said that the majority of Georgia's Internet traffic is routed through Turkey, with some of it going through Russia. Although some news reports indicated Georgia's Internet traffic may have been shifted through Russia, Tabatadze said that's not the case.

"We have checked the traffic route on Ripe.net...and we did not see any traffic re-routing via Russia," Tabatadze said.

It appears that large groups of hackers are working together to take down the Web sites, but the attacks have been so intense that it will take a while to analyze, Tabatadze said.

Other CERTs around the world have been helping to provide information on the attacks, Tabatadze said.

The last few days have been a nerve-racking time for Georgians, said Tabatadze, who said he heard explosions on Sunday when Russian planes bombed air-traffic control stations near Tbilisi, Georgia's capital.

"You can't even imagine the situation," Tabatadze said. "This is a terrible end for Georgia."

On Tuesday morning, Russia announced it would stop military operations in South Ossetia and Abkhazia, saying the safety of its peacekeepers in the region had been secured.

On Tuesday morning, Russia announced it would stop military operations in South Ossetia and Abkhazia, saying the safety of its peacekeepers in the region had been secured.