

# **Russian Invasion of Georgia**

## **Russian Cyberwar on Georgia**

**10 November 2008**

Regular updates can be found on the Georgia Update website:

<http://georgiaupdate.gov.ge/>

The Russian invasion of Georgia was preceded by intensive cyberattacks designed to disrupt, deface or bring down critical Georgian governmental and civilian online infrastructure.

These attacks, which became a massive assault on the eve of the invasion, mark a new phase in the history of warfare. They are the first recorded case in which a land-sea-air-invasion was coordinated with an orchestrated cyber-offensive.

Cyberattacks are becoming an increasingly established form of warfare. The pioneer in this form of warfare has been the Russian Federation, widely suspected of having played a leading role in the first large scale cyberattacks on a NATO member state when, in spring 2007, Estonian servers came under massive Distributed Denial-Of-Service (DDoS) assaults. That attack succeeded in disabling much of Estonia's online infrastructure, with serious consequences for its banks and airports. Following that attack, NATO at its April 2008 Bucharest summit decided to set up the Cyber Defence Centre of Excellence in Tallinn.

In July and August 2008, attacks originating from the Russian Federation resumed, this time directed against Georgia. On 20 July, the website of the President of Georgia, Mikheil Saakashvili, came under an intensive DDoS attack and was disabled for over 24 hours. This attack, it later turned out, appeared to be a rehearsal for the much larger attacks that were to come.

The full-scale attack started late on Thursday, 7 August, a day before Russia claims it first entered Georgia. A large number of Georgian servers and much of Georgia's Internet traffic were seized and placed under external control. For the first few days of the war, most Georgian government and media sites were either unavailable or defaced. An infamous example was the composite picture portraying President Saakashvili as Hitler which replaced the web site of the Ministry of Foreign Affairs.

This made it near-impossible for Georgia to communicate with the world, and afforded Russia its initial propaganda victories: global media outlets had no choice but to rely almost exclusively on Russian websites carrying Russian claims about the cause, scope and running of the war.

DDoS attacks of varying intensity continued after the Kremlin announced that it had ceased hostilities on 12 August. Thanks to the efforts of numerous specialists and volunteers, normal traffic was resumed within a week. Most critical websites were hosted outside of Georgia.

US-based Tulip Systems is one of the firms that took over the hosting of Georgian government websites during the conflict. In a recent interview, Tulip Systems executive Tom Burling said its experts had worked frantically to curtail the damage from the hackers, remarking that "they have been attacking Georgia from a cyber standpoint since July". Bill Woodcock, the research director at Packet Clearing House, a California-based nonprofit group that tracks Internet security trends, told Newsweek that the attacks bear the markings of a "trained and centrally coordinated cadre of professionals."

While we do not yet know who wrote the malware that was used to cause Georgian servers to crash, it proliferated on Russian Web sites. Gary Warner, a cybercrime expert at the University of Alabama, told Newsweek that he found "copies of the attack script" posted in the reader comments section at the bottom of virtually every story in the Russian media that covered the Georgian conflict, complete with instructions on how the script could be used to attack a specific list of Web sites. For example, the target list advertised on stopgeorgia.ru ran to 36 entries, including the US and UK embassies in Tbilisi, the Georgian Parliament, the Georgian Supreme Court, the Ministry of Foreign Affairs, various news agencies and other media resources, and the Central Election Commission.

An example of Russian efforts to shut the mouse of Georgian media is the story of the Georgian news agency GHN. The first attack against the agency's website occurred in August 2008. Another wave of cyber attacks started on 8 September. As a result, the GHN news agency website had been paralyzed for 2 weeks. Another Georgian media website that came under consistent cyber attacks after the end of the armed conflict is [www.apsny.ge](http://www.apsny.ge) – website of the Georgia-Online news agency. It is interesting to note that Russian efforts to prevent Georgian Internet media resources from disseminating information continued even after the war.

While the attack on Estonia was the first to come to the world's attention, and the one on Georgia the first to be coordinated with a land assault, it was not the first time Russia had tested this tool. Back in 2006, State Duma deputy and member of the Duma Security Committee Nikolai Kuryanovich drafted a formal parliamentary letter of appreciation to hackers who had taken down several Israeli web sites, stating "In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers. This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces."

Cyberattacks are easy to organize, cheap to implement, and difficult to defend against. They disable a country's infrastructure and help an invading enemy win initial propaganda battles. The recent events have graphically illustrated the importance of NATO's efforts to defend its member states against this new form of warfare.