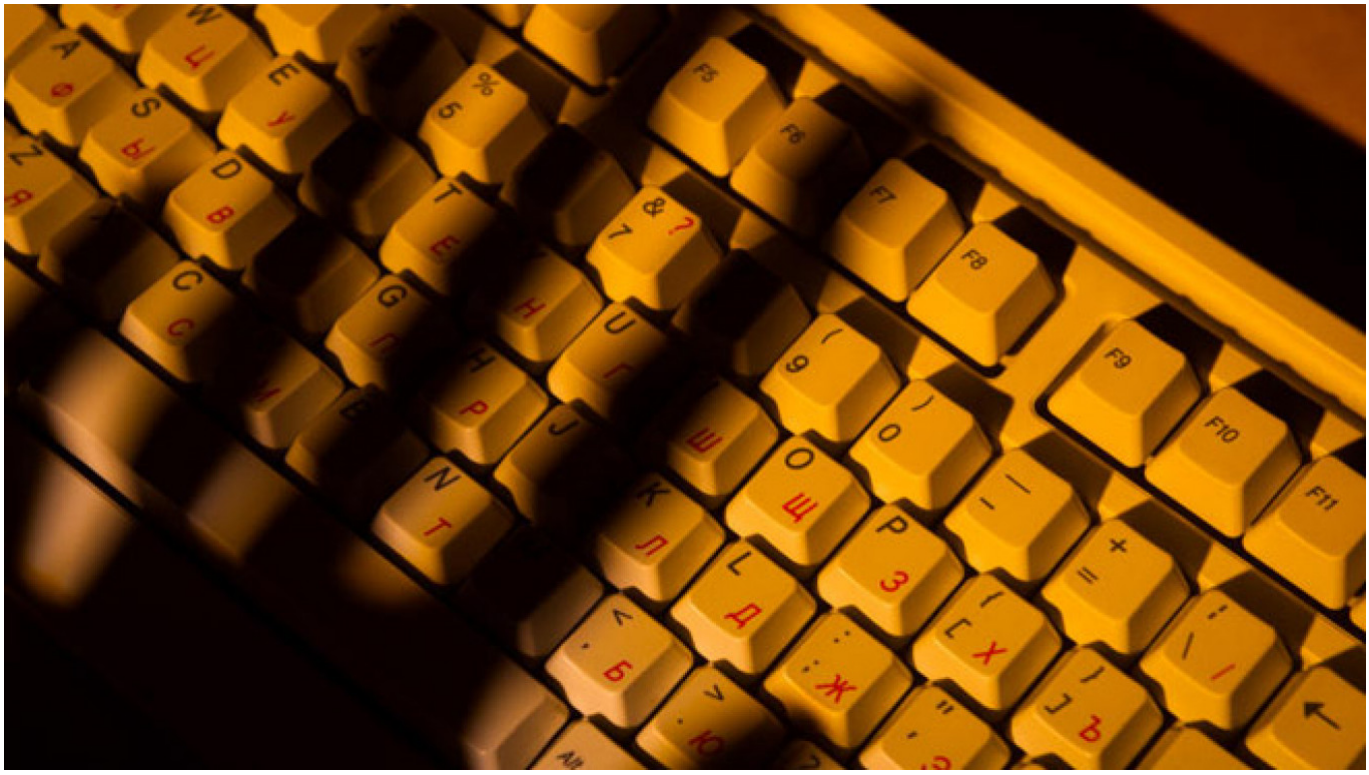
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Is Russia's Cyberwar Heating Up Amid New Cold War?

By Alexey Eremenko

November 26, 2014



Russia's own capabilities for cyber-warfare and -espionage remain very much an unknown, but have not been shown to be very impressive so far.

A recent influx of reports about Russian electronic espionage activity has prompted fresh concerns that the Kremlin may be gunning for a cyberwar with the West.

Not everyone is convinced: Russian IT analysts interviewed by The Moscow Times were more inclined to blame the spike in attack reports on media hype and cybersecurity companies exploiting clients' fears.

But Russia's leading expert on domestic security services, Andrei Soldatov, said the pattern of the attacks indicated that the Russian government may be mounting a covert Internet offensive.

Experts could not say, however, whether heavy guns with the FSB electronic espionage

agencies have been deployed.

"All government-linked attacks so far have been carried out by people on the market: the cyber-mercenaries," Soldatov, editor-in-chief of the Agentura.ru website, said Wednesday.

From NATO to Webcams

The most recent reports emerged last week, when the head of the German domestic intelligence service spoke about an increase in hacker assaults on German targets, including governmental ones.

Russian and Chinese hackers accounted for most of the spike, Hans-Georg Maassen was cited by Reuters as saying.

In late October, U.S. IT security firm FireEye said that Russian-speaking hackers were likely behind the theft of confidential data from NATO and Georgian networks, and that the alleged hacker group, known as APT28, is "most likely sponsored by the Russian government."

Kremlin spokesman Dmitry Peskov dismissed the report, the Bloomberg news agency said.

In mid-October, U.S. company iSight Partners said Russian hackers had exploited a Microsoft Windows bug to access computers belonging to NATO, the EU, Ukraine and certain energy and telecom firms.

British tabloid The Daily Mail last week reported that Russian hackers had gained access to hundreds of home webcams in the U.K., though the Russian government was not implicated in that story.

Earlier this year it was alleged that the Kremlin could have been behind the attack on bank JPMorgan Chase, but last month the FBI said there was no evidence that the hacking had been carried out in revenge for U.S. sanctions on Russia, as previously claimed.

Hacking as Usual

Russia and the Western powers entered what many have dubbed the "new Cold War" after Moscow annexed Ukraine's Crimea Peninsula at gunpoint in March and was accused of backing pro-Russian separatists in eastern Ukraine this summer, an allegation denied by the Kremlin.

Rumors of the Kremlin's cyber-warfare have been swirling since 2007, when it was implicated in DDoS attacks on government websites in Estonia, then an opponent in a fierce political spat.

The attacks have been traced to hacktivists on Russian territory, but never to the Kremlin.

Cybercrime in the ex-Soviet space is robust: Russia was the world's No. 1 source of cyber-attacks as of last month with 2.7 million launched, according to statistics by Deutsche Telecom. The runner-up, Germany, lagged significantly with 1.4 million, followed by the U.S. (1.2 million) and China (1 million).

But most of those attacks have nothing to do with politics, like the hackers themselves, said Karen Kazaryan, chief analyst for the Russian Association of Electronic Communications.

Cybersecurity companies are simply trying to capitalize on the new Russian scare by touting activity by "Russian hackers," said Ilya Sachkov, head of cybersecurity firm Group-IB, which has offices in Moscow and New York.

Soldatov of Agentura.ru disagreed, pointing out that while Russia's standoff with the West over Ukraine began in March, the reports about attacks only spiked in recent weeks.

"Nothing can be proven, but it definitely benefits the Russian authorities," he said, while admitting that media hype about any perceived Russian threats also played a role.

The Russian government staged a major cyber-wargame in July, testing the "defense capabilities of the Russian segment of the Internet." Experts surmised that that experiment may have been a jumping-off point for the current wave of attacks.

Mercenaries or the FSB?

Russia's own capabilities for cyber-warfare and -espionage remain very much an unknown, but have not been shown to be very impressive so far.

The absolute majority of government-linked attacks are believed to have been perpetrated by independent hackers contracted by the government, Kazaryan said.

This was likely the case in Estonia in 2007, among other things, he said.

Sachkov of Group-IB said the hackers in 2007 may have been motivated by patriotic indignation rather than financial gain, but also agreed they were likely independent contractors, not security service staff.

Last year, Russia's Defense Minister Sergei Shoigu announced a "hunt" for programmer graduates of Russian universities to serve in the "Russian cyber army."

But a year is not much time to build a full-fledged cyberforce capable of major, complex attacks such as the famous Stuxnet malware, which took out the computers of Iran's nuclear program in 2010. U.S. and Israeli security services are believed by experts to have worked on Stuxnet for several years.

Meanwhile, Russia has a functioning electronic espionage corps in what was previously known as the Federal Agency of Government Communications and Information, Russia's analogue to the U.S. National Security Agency.

The agency, which was merged into the FSB in 2003, is capable of pulling off acts of intricate cyber-espionage beyond the skills of contract hackers, Soldatov said.

But there is not enough information concerning the recent attacks to say whether the FSB corps was behind it, or whether ordinary hackers could have pulled it off, he said.

"They've been lying low recently, and rarely get involved in politics, so it's hard to say if they

are in the game now," Soldatov said.

"But Russia has the technical capabilities for high-profile cyber-attacks," he said.

The FSB did not return a request for comment.

Contact the author at a.eremenko@imedia.ru

Original url:
https://www.themoscowtimes.com/2014/11/26/is-russias-cyberwar-heating-up-amid-new-cold-war-a41756