



## U.S. and Russian officials talk cyberissues

[Angela Moscaritolo](#)

December 14 2009

In a notable policy shift, American and Russian officials have met to discuss cybersecurity issues, such as collaboration among law enforcement bodies and the use of cyberweapons, the *New York Times* reported in its Saturday editions.

Under the Bush administration, U.S. officials simply “refused to engage” with the Russians on cyberissues, James Lewis, director of technology and public policy at the Center for Strategic International Studies, told SCMagazineUS.com on Monday.

But in mid-November, Gen. Vladislav Sherstyuk, deputy secretary of the Russian Security Council, along with other Russian officials, including the former leader of the Russian equivalent of the National Security Agency, met in Washington with representatives of the National Security Council and the State, Defense and Homeland Security departments, the *Times* [reported](#) on Saturday.

The U.S. and Russian officials have different goals with respect to cybersecurity, Lewis said.

The Russians have proposed a treaty between the two nations that would ban the use of offensive cyberweapons, Lewis said. The agreement comes in light of news earlier this year that the U.S. military [is developing and testing](#) several new offensive and defense cyberdevices, including a system that would enable nonexpert military personnel to launch a cyberattack.

Meanwhile, the United States has maintained that a treaty relating to the use of cyberweapons is not needed, and instead, cooperation on law enforcement and information sharing is enough, Lewis said.

The United States could propose a counter-draft, Lewis said.

“Not signing the current [disarmament treaty] draft is a good idea,” Lewis said. “It was written by the Russians to hamper U.S. operations.”

Government agency and White House representatives could not be reached for comment on Monday.

Cybersecurity has received considerable attention within government this year. In April, President Obama [declared](#) the U.S. digital infrastructure a “strategic national asset” and announced a new five-part protection plan for the country, along with the creation of a federal cyber coordinator position, which remains unfilled to date.

The number of cyberattacks against U.S. government networks has been rising steadily in recent years and is expected to increase 60 percent in 2009 compared to last year, according to a report prepared for Congress by the U.S.-China Economic and Security Review Commission.

The military [spent more than \\$100 million](#) in the first six months of 2009 alone repairing damage to its networks caused by cyberattacks -- many of which are attributed to China or Russia.

In one incident late last year, foreign government spies, believed to be from China or Russia, broke into a classified Department of Defense network and remained there for several days, Lewis said.