U.S. and Russia Differ on a Treaty for Cyberspace

By JOHN MARKOFF and ANDREW E. KRAMER

The United States and Russia are locked in a fundamental dispute over how to counter the growing threat of cyberwar attacks that could wreak havoc on computer systems and the Internet.

Both nations agree that cyberspace is an emerging battleground. The two sides are expected to address the subject when President Obama visits Russia next week and at the General Assembly of the United Nations in November, according to a senior State Department official.

But there the agreement ends.

Russia favors an international treaty along the lines of those negotiated for chemical weapons and has pushed for that approach at a series of meetings this year and in public statements by a high-ranking official.

The United States argues that a treaty is unnecessary. It instead advocates improved cooperation among international law enforcement groups. If these groups cooperate to make cyberspace more secure against criminal intrusions, their work will also make cyberspace more secure against military campaigns, American officials say.

“We really believe it’s defense, defense, defense,” said the State Department official, who asked not to be identified because authorization had not been given to speak on the record. “They want to constrain offense. We needed to be able to criminalize these horrible 50,000 attacks we were getting a day.”

Any agreement on cyberspace presents special difficulties because the matter touches on issues like censorship of the Internet, sovereignty and rogue actors who might not be subject to a treaty.
United States officials say the disagreement over approach has hindered international law enforcement cooperation, particularly given that a significant proportion of the attacks against American government targets are coming from China and Russia.

And from the Russian perspective, the absence of a treaty is permitting a kind of arms race with potentially dangerous consequences.

Officials around the world recognize the need to deal with the growing threat of cyberwar. Many countries, including the United States, are developing weapons for it, like “logic bombs” that can be hidden in computers to halt them at crucial times or damage circuitry; “botnets” that can disable or spy on Web sites and networks; or microwave radiation devices that can burn out computer circuits miles away.

The Pentagon is planning to create a military command to prepare for both defense and offensive computer warfare. And last month, President Obama released his cybersecurity strategy and said he would appoint a “cybersecurity coordinator” to lead efforts to protect government computers, the air traffic control system and other essential systems. The administration also emphasizes the benefits of building international cooperation.

The Russian and American approaches — a treaty and a law enforcement agreement — are not necessarily incompatible. But they represent different philosophical approaches.

In a speech on March 18, Vladislav P. Sherstyuk, a deputy secretary of the Russian Security Council, a powerful body advising the president on national security, laid out what he described as Russia’s bedrock positions on disarmament in cyberspace. Russia’s proposed treaty would ban a country from secretly embedding malicious codes or circuitry that could be later activated from afar in the event of war.

Other Russian proposals include the application of humanitarian laws banning attacks on noncombatants and a ban on deception in operations in cyberspace — an attempt to deal with the challenge of anonymous attacks. The Russians have also called for broader international government oversight of the Internet.

But American officials are particularly resistant to agreements that would allow governments to censor the Internet, saying they would provide cover for totalitarian regimes. These officials also worry that a treaty would be ineffective because it can be almost impossible to determine if an Internet attack originated from a government, a hacker loyal to that government, or a rogue acting independently.
The unique challenge of cyberspace is that governments can carry out deceptive attacks to which they cannot be linked, said Herbert Lin, director of a study by the National Research Council, a private, nonprofit organization, on the development of cyberweapons.

This challenge became apparent in 2001, after a Navy P-3 surveillance plane collided with a Chinese fighter plane, said Linton Wells II, a former high-ranking Pentagon official who now teaches at the National Defense University. The collision was followed by a huge increase in attacks on United States government computer targets from sources that could not be identified, he said.

Similarly, after computer attacks in Estonia in April 2007 and in the nation of Georgia last August, the Russian government denied involvement and independent observers said the attacks could have been carried out by nationalist sympathizers or by criminal gangs.

The United States is trying to improve cybersecurity by building relationships among international law enforcement agencies. State Department officials hold out as a model the Council of Europe Convention on Cybercrime, which took effect in 2004 and has been signed by 22 nations, including the United States but not Russia or China.

But Russia objects that the European convention on cybercrime allows the police to open an investigation of suspected online crime originating in another country without first informing local authorities, infringing on traditional ideas of sovereignty. Vladimir V. Sokolov, deputy director of the Institute for Information Security Issues, a policy organization, noted that Russian authorities routinely cooperated with foreign police organizations when they were approached.

This is not the first time the issue of arms control for cyberspace has been raised.

In 1996, at the dawn of commercial cyberspace, American and Russian military delegations met secretly in Moscow to discuss the subject. The American delegation was led by an academic military strategist, and the Russian delegation by a four-star admiral. No agreement emerged from the meeting, which has not previously been reported.

Later, the Russian government repeatedly introduced resolutions calling for cyberspace disarmament treaties before the United Nations. The United States consistently opposed the idea.

In late April, Russian military representatives indicated an interest in renewed negotiations at a Russian-sponsored meeting on computer security in Garmisch, Germany.
John Arquilla, an expert in military strategy at the Naval Postgraduate School in Monterey, Calif., who led the American delegation at the 1996 talks, said he had received almost no interest from within the American military after those initial meetings. “It was a great opportunity lost,” he said.

Unlike American officials who favor tightening law enforcement relationships, Mr. Arquilla continues to believe in cyberspace weapons negotiations, he said. He noted that the treaties on chemical weapons had persuaded many nations not to make or stockpile such weapons.

The United States and China have not held high-level talks on cyberwar issues, specialists say. But there is some evidence that the Chinese are being courted by Russia for support of an arms control treaty for cyberspace.

“China has consistently attached extreme importance to matters of information security, and has always actively supported and participated in efforts by the international community dedicated to maintaining Internet safety and cracking down on criminal cyber-activity,” Qin Gang, spokesman for the Foreign Ministry, said in a statement.

Whether the American or Russian approach prevails, arms control experts said, major governments are reaching a point of no return in heading off a cyberwar arms race.

*John Markoff reported from New York, and Andrew E. Kramer from Moscow. Edward Wong and Xiyun Yang contributed reporting from Beijing.*