CISSM Center for International and Security Studies at Maryland
School of Public Policy, University of Maryland

Policy Brief **April 2013**

Cybersecurity in Russian-U.S. Relations

By Pasha Sharikov

Executive Summary

Threats to cyberspace and to information security are emerging as central elements of Russian-U.S. security relations. As much as U.S. officials have expressed concerns about Russian-sponsored cyber-activities, Russia is equally concerned about U.S. military intentions in the cyber domain. Differing definitions of what activities pose a threat complicates relations on this issue. While the United States is concerned primarily with threats to technology and economic well-being, Russia is also concerned about activities that threaten interference in Russian sovereign affairs. Russian concerns have been heightened by repeated U.S. rebuffs on draft U.N. resolutions to address some threats. U.S. and NATO pronouncements about the need for collective defense against cyberattacks have raised similar concerns. Ongoing Russian-U.S. cooperation at the highest level demonstrates that the states recognize the common interests at stake, but officials will have to work on a mutually beneficial basis to make any level of cooperation work.

Introduction and context

Securing information infrastructure has become a significant national security priority for developed countries. Internet technologies are widely spread around the world and are accessible to most of the population, opening almost unlimited opportunities for states and non-state actors to share, access, and manipulate information without the consent of the entity on the other end of the interaction. This represents a dynamic shift the system of international relations. As transnational corporations, nongovernmental organizations, intergovernmental organizations, social groups, and other actors gain more powerful information potential—a form of power based on information resources—than traditional governments, they sometimes possess more instruments of international influence than states, creating a polycentric system of international relations.[1]

[1] Joseph S. Nye, Jr., "Cyber Power" in *The Future of Power in the 21st Century* (New York: Public Affairs Press, 2011).

The participation of some actors in this system does not necessarily coincide with the national interests of all of the world's powers, including the United States and Russia. Nations and nongovernmental actors have already clashed—see, for example, the 2010 conflict between China and Google, which aptly demonstrates the affects of non-state actors. In addition, several states (the United States, China, Great Britain, Germany, Russia, Japan and some others) have demonstrated a willingness to use their "cyberpowers" to influence international affairs.

Defining the problem

Russian and American experts take different approaches on the problems associated with cyberspace. American notions of "cybersecurity" and "cyberspace" imply technological understanding; the primary goal of cybersecurity is to keep technologies safe from disruption, unauthorized access, or other kinds of interference. According to the U.S. International Strategy for Cyberspace, the challenges come in a variety of forms:

> Natural disasters, accidents, or sabotage can disrupt cables, servers, and wireless networks on U.S. soil and beyond. Technical challenges can be equally disruptive, as one country's method for blocking a website can cascade into a much larger, international network disruption. Extortion, fraud, identity theft, and child exploitation can threaten users' confidence in online commerce, social networks and even their personal safety. The theft of intellectual property threatens national competitiveness and the innovation that drives it. . . . Cybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace."[2]

The Russian position on information security is outlined in recent Russian foreign policy documents:

> "Russia will act according to its national interests in providing national and international information security, preventing political, economic and social security threats emerging in cyberspace, to fight terrorist and other criminal kinds of criminal activity. Russia opposes military-political use of information technologies that contradict international law, including actions aimed at interference in domestic affairs, as well as that kind of using IT that pose threat to international peace, security and stability."[3]

For Russians, the more common terms, "information security" and "information space," also have philosophical and spiritual meanings. For instance, the term "noosphere" was introduced almost 100 years ago by the famous Russian philosopher Vladimir Vernadsky to explain the

[2] U.S. officials, "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World," released by the White House in May 2011, p. 4.

[3] "The Foreign Policy Concept of the Russian Federation," approved by the President of the Russian Federation Vladimir Putin, February 12, 2013. The concept is available at http://mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/c32577ca0017434944257b160051bf7f

sphere of knowledge and information that exists on Earth along with the biosphere and the geosphere. Technology is one of many elements of Russians' understanding of information security, and not necessarily the most important one. For Russia, "information security" also aims to keep the nation's knowledge and culture safe.

Indeed, Russia's 2000 "Doctrine of Information Security of the Russian Federation" does not even contain the word internet. According to the doctrine, information security refers to the maintenance of national security interests, but those interests include the interests of citizens, society, and the government. According to this definition, information security includes the free flow of information that promotes civil society and all kinds of spiritual and educational development and the maintenance of social and moral stability. It also necessitates government engagement in IT development to provide for and protect the constitutional rights of the population.

The official Russian position on information security continues to evolve. Russian Presidents Dimitry Medvedev and Vladimir Putin have repeatedly declared that the development of information technologies is a national priority. In a 2008 document, "Information Society in Russian Federation Development Strategy," Russian government officials stated that they want to make Russia one of the top 20 information societies in the world before 2015.

The potential for cooperation

The United States has a special role in cyberspace. Due to historical circumstances, the United States leads in the majority of relevant production indicators (global share of patents, technology education, consulting services, etc.) and in the export of information goods and services. It also controls many of the mechanisms for governing the global cyber domain. The importance of the United States in cyberspace is one of the reasons why Russian interests in this area are strongly interconnected with bilateral Russian-U.S. relations, as well as with American global foreign strategy.

According to Russian officials, the United States has long conducted military R & D programs in cyberspace that have raised serious concerns for other international actors, including Russia.[4] Since the beginning of the twenty-first century, Russia has repeatedly tried to initiate a resolution in the U.N. General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," aimed at addressing these concerns. The resolution would create an international legal framework, based on the principles of non-use of force, non-interference in domestic affairs, and respect for human rights and

[4] "Interview with Sergey Ryabkov, Deputy Minister of Foreign Affairs," VPK-News, March 14-20, 2012. Available at http://vpk-news.ru/sites/default/files/pdf/VPK_10_427.pdf .

fundamental freedoms, and would aim to prevent the use of information and telecommunications in violation of the U.N. Charter. The U.S. has consistently opposed the resolution in part because of "a lack of shared understanding regarding international norms pertaining to State behavior in cyberspace." This lack of understanding, the U.S. believes, "argues for the elaboration of measures designed to enhance cooperation and build confidence, reduce risk or enhance transparency and stability."[5]

Since President Barack Obama took office, cybersecurity has remained a national security priority, but Washington has ceased to strive for global information dominance, whereby the United States would pursue both qualitative and quantitative superiority of cyber capabilities, and the ability to govern global technological development. Indeed, the Obama administration's adoption of an "International Strategy for Cyberspace," and of multiple bilateral and multilateral initiatives demonstrates Obama's different approach.

Among the administration's initiatives is the bilateral Russian-American Agreement on Information Security that is being prepared jointly by high-level U.S. and Russian national security officials.[6] The very fact that such a document is being discussed on such a high level means that Russia and the United States recognize that they share common interests in cyberspace. Yet, U.S. contributions to the agreement do not address potential military cybersecurity issues. Given the development of U.S. cyber capabilities, Russia is concerned that U.S. officials consider Russia a primary source of cyberthreat. Supporting this notion are comments by U.S. officials. In 2012, Director of National Intelligence James Clapper assessed the cyber threat to the United States, saying, "Among state actors, China and Russia are of particular concern."[7]

Implications of conflicting definitions

Shortly after the conflict between Google and China mentioned above, U.S. Secretary of State Hillary Clinton gave a speech on internet freedom that made clear some of the implications of differing ideas about cybersecurity. In her speech, Clinton said: "Those who disrupt the free flow of information in our society or any other pose a threat to our economy, our government, and our civil society. Countries or individuals that engage in cyberattacks should face consequences and international condemnation. In an internet-connected world, an attack on one nation's networks

[5] United Nations, "Developments in the Field of Information and Telecommunications in the Context of International Security," Blue Book Study Series, No. 33, 2001, p. 38.

[6] A 2011 joint statement by U.S. cybersecurity coordinator Howard Schmidt and Russian National Security Council Deputy Secretary Nikolay Klimashin outlines some of the work of the group. Joint Statement, " U.S. and Russian Delegations Meet to Discuss Confidence Building Measures in Cyberspace," June 21-23, 2011. Statement available at http://www.whitehouse.gov/sites/default/files/uploads/2011_klimashin_schmidt_cyber_joint_statement.pdf.

[7] James R. Clapper, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community," Senate Select Intelligence Committee," January 31, 2012.

can be an attack on all. And by reinforcing that message, we can create norms of behavior among states and encourage respect for the global networked commons."[8]

Clinton's language, particularly the phrase "an attack on one nation's networks can be an attack on all," raises the specter of Article V of the North Atlantic Treaty. This holds the potential to undermine the multilateral cooperation that is vital on issues related to international information security. If cybersecurity is a global issue, then states should not attempt to address it in the context of a regional organization such as NATO. Indeed, NATO's cybersecurity programs have already raised Russian concerns. These programs were born out of the concerns of NATO members who accused Russia of being complicit in cyberattacks on their critical infrastructures—even though later investigations proved that Russian officials had nothing to do with the attacks.

In response to NATO's actions, Russia has led efforts to adopt collective cybersecurity measures in both the Shanghai Cooperation Organization and Collective Security Treaty Organization. Russia has also initiated a discussion about a "Convention on International Information Security," which would formulate the basic threats to international information security and confirm a "triad" of military, terrorist, and criminal threats. To counter these threats, the convention would advocate universally recognized principles and existing international law, as well as confidence building measures.[9] Among the measures that the convention advocates is that all states party to the convention "take all necessary steps to prevent any destructive information action originating from their own territory or using the information infrastructure under their jurisdiction, as well as cooperate to locate the source of computer attacks carried out with the use of their territory, to repel these attacks and to eliminate their consequence," and that they "refrain from using information and communications technology to interfere with the internal affairs of another state."

Russia's cyberspace interests and the resources it possesses to pursue and defend those interests, in addition to the Russian-American "reset" of relations, provide ample opportunity for Russian-U.S. cooperation in cyberspace. To work, this cooperation must be mutually beneficial and contribute to the common interest of a secure global cyberspace. It might also require engaging other cyberspace actors as necessary.

[8] Secretary of State Hillary Rodham Clinton, "Remarks on Internet Freedom," January 21, 2010. Available at http://www.state.gov/secretary/rm/2010/01/135519.htm .

[9] The Convention is translated in English and available at the website of Russian Ministry of Foreign Affairs: http://mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/6912ce36aa5f1e92c32579250035bebd!OpenDocument.

A way forward?

One possible way for Russia and the United States to cooperate in cybersecurity would be in establishing international norms that would effectively deter other actors from engaging in disruptive, destructive, or illegal behavior in cyberspace. Russian and American decision-makers together face the challenge of adapting to the ever-evolving nature of international politics. Ensuring national security and maintaining international stability are increasingly defined by factors such as the role of information technologies.

Attempts by the United States and Russia to work together to deter cyber attacks would be complicated by several circumstances:

- information resources cannot be fully controlled by the governments; in other words, the unauthorized use of cyberweapons is very likely;
- the potential for nonstate actors' to engage in information warfare can exceed that of states; and
- the lack of regulation containing the military exploration of cyberspace has the potential to turn efforts aimed at protecting economic competitiveness into a cyberarms race.

Still, Russia and the United States should continue developing their bilateral relations in this area. Establishing reliable cooperation is the only way to counter criminal and terrorist threats in cyberspace, as well as those posed by states.

About the Author

Pavel Sharikov is the head of the Center for Applied Research at the Institute for U.S. and Canada Studies, Russian Academy of Sciences.