Russia, The United States, And Cyber Diplomacy

Opening the Doors

By Franz-Stefan Gady and Greg Austin

EastWest Institute
Forging Collective Action for a Safer and Better World

www.ewi.info

About the Authors

Franz-Stefan Gady is an associate at the EastWest Institute. He has previously worked as an adjunct research assistant at the Institute for National Strategies Studies of the National Defense University in Washington, D.C., focusing on regional security issues. He was also an analyst for the Project on National Security Reform, a congressionally funded nonprofit organization founded to reform the national security structure of the United States. He holds an M.A. in Strategic Studies/International Economics from the School of Advanced International Studies, Johns Hopkins University, and has served in the Austrian Army and the Austrian Foreign Ministry, working on various security issues. To contact him, write to: fgady@ewi.info.

Greg Austin is Vice President of Program Development and Rapid Response at the EastWest Institute. Greg's career in international affairs spans thirty years and includes senior posts in academia and government. He writes a weekly column in the newspaper New Europe. He has also held senior posts at the International Crisis Group and the Foreign Policy Centre in London. Greg is the author of several well-reviewed books on international security, especially on Asia. His books include The Armed Forces of Russia, co-authored with Alexei Muraviev. He has several postgraduate qualifications in international relations, including a Ph.D. His main specializations have included Soviet and Russian security policy.

Russia, The United States, And Cyber Diplomacy

Opening the Doors

Franz-Stefan Gady and Greg Austin

EastWest Institute
Forging Collective Action for a Safer and Better World

www.ewi.info

The EastWest Institute is an international, non-partisan, not-for-profit policy organization focused solely on confronting critical challenges that endanger peace. EWI was established in 1980 as a catalyst to build trust, develop leadership, and promote collaboration for positive change. The institute has offices in New York, Brussels, and Moscow.

For more information about the EastWest Institute or this paper, please contact:

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010
U.S.A. 1-212-824-4100
communications@ewi.info

Cover photo: President Barack Obama and Russian President Dmitry Medvedev walk through Lafayette Park from the White House to a attend a meeting at the U.S. Chamber of Commerce in Washington, Thursday, June 24, 2010. (AP Photo/J. Scott Applewhite)

Printed in the United States.

Contents

Acknowledgments

The findings of this paper are based on consultations in Moscow, Washington, and Brussels over the course of one year. Franz Stefan Gady conducted interviews in Moscow in March 2010 with leading Russian specialists on cybersecurity from both the public and private sector. The authors would like to thank Dr. Valery Yaschenko, First Deputy Director of the Moscow State University Institute of Information Security; Dmitry Griegoriev, Political Advisor to the Director of the Institute of Information Security; Vladimir Denezhkin, CEO, Trafica; Leonid Zhukov, Technical Director, Trafica; Pasha Sharikov, Fellow, Institute for U.S. & Canadian Studies; Vladimir V. Sokolov, Associate Professor, Lomonosov Moscow State University; Alexey Salnikov, Vice Director, MSU Institute of Information Security. The authors would like to thank Liza Kurukulasuriya, Vladimir Ivanov, Galina Kulikova, Benjamin Barber, Pablo Rodriguez, and Sem Jean Weemaels from the EastWest Institute for their participation in interviews, their comments, and their research support.

Executive Summary

Russia and the United States have been unable to establish a common understanding in their bilateral diplomacy on most aspects of cybersecurity. In spite of a 1998 declaration of their interest in joint leadership of global responses to cybersecurity challenges, the two countries have acted more often than not like enemies guarding sensitive national security secrets rather than as allies committed to protecting common interests in the global digital economy and the socially networked world.

There are compelling historical precedents to suggest that reservations in Russia and the United States that are rooted in national security sensitivities can be overcome. For example, in preparing for Y2K, there was a potential global threat and most countries cooperated despite national security sensitivities. Russia and the United States adopted very intrusive measures for joint monitoring of the most sensitive launch and warning procedures for ballistic missiles. More recently, the United States and Russia agreed on new joint encryption arrangements for the forty-year-old hotline between the Kremlin and the White House. Moreover, American and Russian banks already cooperate in secure digital communications for international transfers of staggeringly large sums of money.

The United States and Russia approach the problem of cybersecurity from two different angles: the United States focuses on a law enforcement approach at the domestic level with voluntary international collaboration, while Russia focuses on developing binding international regimes. There are also quite different philosophies at work: Russia favors social control of the Internet as a medium, while the United States, for the most part, does not.

Despite these differences, the United States and Russia agreed in December 2009 at a meeting of the U.N. Committee on Disarmament and International Security to begin talks on strengthening Internet security and limiting military use of cyberspace. After rejecting Russia's cybersecurity overtures for a number of years, the United States has clearly decided on a major policy shift. In announcing its cybersecurity goals on May 29, 2009, the Obama administration showed its determination to elevate the issue of cybersecurity to a new level. Consequently, new agreements between the United States and Russia may be within reach.

This paper outlines the arguments for pushing for more rapid progress in U.S.-Russian cooperation on cybersecurity—or, as the Russians prefer to call it, information security. It urges the two sides to make good on their public announcement in December 2009 that they would begin new consultations on cybersecurity in the framework of a United Nations General Assembly resolution. To examine the obstacles and ways to overcome them, the paper discusses four possible areas of cooperation: public key infrastructure; rapid response to cyber crime; deliberation by the Organization for Security and Co-operation in Europe (OSCE) on laws of cyber war; and NATO-Russia cybersecurity cooperation.

Recommendations

The recommendations listed below have been crafted by taking the avowed declaration of both sides to work together and applying it to leadership of change in each of the four areas. The paper is urging the two governments to jointly propose each initiative in an appropriate international forum (for example, the International Telecommunication Union), to chair the necessary working groups, and to involve other stakeholders in the debate in order to build trust for deeper cooperation. This should be followed by concrete bilateral discussions on specific aspects of cooperation that are too sensitive to be discussed in an international forum.

1. Public Key Infrastructure: Russia and the United States should champion in the International Telecommunication Union (ITU) the idea of a binding multilateral agreement on Public Key Infrastructure (PKI) to promote internationally an "ecosystem" of trusted identities. This could be based on a "joint policy assessment" (JPA) by Russian and American experts.
2. Cyber crime emergency response: Russia and the United States should expand the existing infrastructure of around-the-clock Network of Contacts for High-Tech Crime under the umbrella of the G8 and jointly champion a global framework of 24/7 points of contact, including support for a global program of capacity building in law enforcement and cyber investigation for all countries connected to the Internet.
3. International cyber law: Russia and the United States should undertake joint policy assessments of legal aspects of regulating cyber warfare offensive and defensive activities, especially in the area of critical infrastructure and "rules of engagement." Choice of forum for this is problematic, but the best of a series of poor choices may be the OSCE.
4. NATO-Russia cyber military exercises and exchanges: At a political level, NATO and Russia should commit to completing a joint assessment within a given time frame (say, two years) of what constitutes global cybersecurity and how it can be achieved. In the framework of NATO-Russia scientific cooperation, Russia and the United States should engage in reciprocal observation of and participation in simulations of cyber attacks. Along with the NATO partners, both countries should develop methodologies and standards for vulnerability assessments and ranking of critical facilities.

From Espionage and Cyber War to Cyber Diplomacy

We face a clear and present danger in the digital world. Information from classified sources on the scale and scope of these threats gives far more cause for concern than the already troubling public record. This is not a case of scaremongering. If anything, the reverse is true. Public perceptions of the danger lag behind the reality.

In announcing a new cybersecurity policy on May 29, 2009, President Barack Obama showed how far behind the United States feels it is in mounting its defenses. He said that "we're not as prepared as we should be" and that "we've failed to invest in the security of our digital infrastructure."[1] In a December 2008 report, a commission organized by the Center for Strategic and International Studies (CSIS) in Washington, D.C., called cyber war the "hidden battle," similar to those in signals intelligence in World War II. The commission concluded that "America's failure to protect cyberspace is one of the most urgent national security problems."[2]

In 2000, Russia's President Vladimir Putin signed an "Information Security Doctrine," which concluded, among other things, that:

- There is a deteriorating situation with "the security of data that constitute state secrets";
- The most qualified specialists had left the field in Russia;
- The lag of national information technologies "forces the government to purchase foreign equipment which increases the likelihood of unsanctioned access";
- Russia's dependence on foreign computer and telecommunication hardware and software manufacturers is growing;
- Threats of the use of the "information weapon" against Russia have increased;
- There is "insufficient coordination and poor budget financing" when it comes to the national response to these threats;
- "Not enough attention is being given to the development of space reconnaissance and electronic warfare systems."[3]

The vulnerabilities are immense for everyone, ranging from personal information, banking records, and controls on sensitive medical equipment, to the controls on nuclear power plants and nuclear missiles. And in all these domains, we can find horror stories occurring over the last decade. One attacker reportedly reached and downloaded the highly classified designs of one of America's newest military aircraft.

To protect data and information networks, the United States and Russia, as well as other countries, have adopted what resemble fortress strategies, emphasizing physical defenses. This is an approach more worthy of the medieval age than of the cyber age, but an understandable one. Russia and the United States are still locked in intense intelligence collection efforts against each other; each wants to conceal weapons technology development from the other; and both also undertake offensive cyber operations against each other. Cybersecurity has to beseen as a matter of good defense. Firewalls serve as the equivalent of physical defenses, and they will continue to play this role. . We are in an era of military confrontation—or at least clashes—in a domain where there is almost no regulation. The traditional domains of land, sea, and air, and even outer space, have far more rules for safe "international navigation" than does cyberspace.

Because of the high levels of cross-border connectivity in the cyber world, new approaches for cybersecurity must factor in the international dimension. Thus, instead of exclusively focusing on cyber defense or cyber war, it is also important to begin to develop cyber diplomacy. Few governments have even thought about the diplomatic dimension of cybersecurity, and they certainly haven't developed diplomatic strategies commensurate with the threats. Most governments do little beyond asserting the need for diplomacy in this new area; even if some officials try to do more, they find it difficult to overcome the domestic sensitivities associated with national security.

The paper is a response in part to declared U.S. and Russian interest in joint leadership to overcome global challenges in the field of information and network security. In 1998, the presidents of Russia and the United States made a joint statement on "Common Security Challenges at the Threshold of the Twenty-First Century," in which

1 "President Obama's Remarks on Securing U.S. Cyber Infrastructure," May 29, 2009, http://www.america.gov/st/texttrans-english/2009/May/20090529161700eaifas0.1335871.html.

2 James A. Lewis et al., *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, Washington, D.C., CSIS, December 2008, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

3 Russian Federation, *Information Security Doctrine of the Russian Federation*, September 2000, http://www.mid.ru/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b?OpenDocument.

they noted the "importance of promoting the positive aspects and mitigating the negative aspects of the information technology revolution now taking place, which is a serious challenge to ensuring the future strategic security interests of our two countries." They specifically committed to working together on the Y2K problem and made a general commitment on "consistently mobilizing the efforts of the entire international community" and using all available resources to do so. They said they would "continue to play a leadership role bilaterally and multilaterally to advance common objectives in the area of security."[4]

A good start has been made in efforts to prevent cyber crime. But the first international treaty in this area was the Council of Europe's Convention on Cybercrime, which opened for signature on November 23, 2001. It is designed to address several categories of crimes committed via the Internet and other computer networks."[5] The United States is a signatory and has ratified the treaty, but Russia is not a signatory. (Only twenty-nine countries have ratified the treaty, which entered into force in 2004. The United Kingdom has not signed the treaty, either.)[6] Russia does cooperate in international criminal investigations with positive results, but does not devote as many resources to this as the United States does.[7]

In 2006, during its chairmanship of the G8, Russia advanced an initiative for public-private partnerships to counter terrorism and organized crime, and cybersecurity was one of three priority areas (alongside critical energy infrastructure protection and cross-border movement of people, goods, and money, which also included cybersecurity aspects).[8] The United States and leading American corporations participated in this initiative but with few tangible results.

Beyond cyber crime, the international system needs to develop a concept of what constitutes cyber peace and a code of conduct on what is reasonable behavior and what is not.[9] In the military domain, diplomats will need to frame ideas on deterrence, arms control, and confidence-building especially appropriate for cyberspace. They will need to devise a cyber hotline to allow quick communications between information and communication technology (ICT) specialists in cases of presumed cyber attack by one country on another.

There are important examples within the field of cybersecurity where international cooperation and trust levels are very high. One need go no further than the international system of bank settlements. Other examples include cyber crime and international standards development. Yet governments, especially those charged with cybersecurity, seem to have little confidence that the traditional tools of diplomacy can provide even part of the solution for the threat. American leaders regularly identify Russia as one of the main sources of threat. For many in Russia, the United States' quest for "information dominance"—the term is used in its military strategy—makes it the main source of threat.

The Obama review completed in May 2009 calls for the United States to "develop a strategy designed to shape the international environment" for cybersecurity. This will mean new alliances with the more technologically advanced countries (including Russia, China, and India) against the emerging threats from nonstate actors and rogue states. We should expect some reflection of this in NATO's new security concept, due to be published in November 2010.

For its part, Russia has for more than a decade led an effort in the framework of the United Nations to establish some rules of the game. In 1998, in the U.N. General Assembly, Russia took the lead on the adoption of a resolution (without a vote) on "Developments in the Field of Information and Telecommunications in the Context of International Security."[10] The resolution:

1. *Calls upon* Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security;

4 Joint Statement on Common Security Challenges at the Threshold of the Twenty-First Century, September 2, 1998. See Weekly Compilation of Presidential Documents (http://www.gpoaccess.gov/wcomp/) with text available at http://frwebgate1.access.gpo.gov/cgi-bin/TEXTgate.cgi?WAISdocID=648262514085+15+1+0&WAISaction=retrieve.

5 Kristin Archick, "Cybercrime: The Council of Europe Convention," CRS Report, 2004, http://fpc.state.gov/documents/organization/36076.pdf.

6 "Convention on Cybersecurity," Council of Europe, (CETS No.: 185) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=05/04/2010&CL=ENG.

7 Marina Volkova, "Cybercrime should be stamped out by entire world," *Voice of Russia*, March 22, 2010, http://english.ruvr.ru/2010/03/22/5520499.html.

8 "Working Meetings: Summit 2006," G8 Summit 2006, Moscow, November 28-30, http://en.g8russia.ru/page_work/32.html. "G8 Initiative For Public-Private Partnerships To Counter Terrorism: Private Sector Action Beyond 2006," (EastWest Institute, November 2006. The EastWest Institute supported the Russian government's initiative by convening preparatory meetings and helping to mobilize private sector participation), http://www.ewi.info/public-private-partnerships-combat-terrorism.

9 Sergei Komov, Sergei Korotkov, and Igor Dylevski, "Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law," (Disarmament Forum, 2007, No. 3), http://www.unidir.ch/pdf/articles/pdf-art2645.pdf.

10 "Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations General Assembly, A/Res/53/70, January 12, 1999, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement.

2. *Invites* all Member States to inform the Secretary-General of their views and assessments on the following questions:
   a. General appreciation of the issues of information security;
   b. Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources;
   c. Advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality.

By 2009, the General Assembly had followed more than a decade of international diplomatic activity in the sphere with consideration of a draft on the creation of a global culture of cybersecurity.[11] Landmark undertakings have included the World Summit on the Information Society, the establishment by the International Telecommunication Union (ITU) of a High Level Expert Group (HLEG) on Information Security, and nongovernmental work by organizations such as the Permanent Monitoring Panel on Information Security of the World Federation of Scientists and IMPACT (International Multilateral Partnership Against Cyber Threats). Russian and American specialists and officials participated in most of these multilateral consultations, but neither has signed up as a "partner" with IMPACT, even though it now carries a mantle of global authority as the repository of the ITU's Global Cybersecurity Agenda.[12]

In spite of the two countries' participation in such multilateral initiatives, there have been few exclusively bilateral contacts.

By the end of 2009, the original 1998 U.N. resolution introduced by Russia had been strengthened in important ways to address U.S. concerns. As a result, that year the resolution approved by the General Assembly[13] was supported by the United States. It:

1. *Calls* upon Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information;
2. *Considers* that the purpose of such measures could be served through the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;
3. *Invites* all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:
   a. Possible measures that could be taken by the international community to strengthen information security at the global level;
4. *Requests* the Secretary-General, with the assistance of the group of governmental experts, established in 2009 . . . to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as the concepts referred to in paragraph 2 above, and to submit a report on the results of this study to the Assembly at its sixty-fifth session;
5. *Notes with satisfaction* the holding, in Geneva in November 2009, of the first session of the group of governmental experts established by the Secretary-General and the intention of the group to convene three more sessions in 2010 in order to fulfill its mandate as specified in resolution 63/37.[14]

The work between Russia and the United States on mutually acceptable language on the U.N. resolution helped effect a thaw in their bilateral cyber diplomacy. By July 2010, there had been further discussions at the official level, including a high-profile visit by the U.S. assistant secretary of commerce for communications and information, Lawrence E. Strickling, and the coordinator for international communications and information policy, Ambassador Philip Verveer. They attended the second meeting of the Russia/U.S. ICT Forum in May (the first meeting was held in 2004). The second forum

11 "UN Information Department, Report on the Plenary of the 64th General Assembly," GA/10907, December 21, 2009, http://www.un.org/News/Press/docs/2009/ga10907.doc.htm: "The Assembly invited Member States to use the voluntary self-assessment tools, as listed in the draft's annex, to protect critical information infrastructures and strengthen cybersecurity to aid national efforts and highlight areas for further action."

12 "On 3 September 2008, IMPACT and the ITU formally entered into a Memorandum of Understanding (MoU) in which IMPACT's state-of-the-art Global HQ in Cyberjaya, Malaysia, effectively became the physical and operational home of the GCA. Under this landmark collaboration, IMPACT provides the ITU's 191 Member States with the expertise, facilities and resources to effectively address the world's most serious cyber threats." http://www.impact-alliance.org/about_collaboration.html.

13 A similar resolution had been approved each year by the General Assembly since 1998 without a vote but with the explicit disapproval of the United States.

14 "Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations General Assembly, A/RES/64/25, December 2, 2009.

was meant to spur dialogue on a broad range of topics, including cybersecurity. Among the other subjects: broadband, Internet governance, spectrum management, the analog to digital TV transition, and "coordination of positions for upcoming meetings at the International Telecommunication Union."[15] The U.S. delegation met with industry representatives and took part in the first Russian Internet Governance Forum and the U.S.-Russia Business Council's first Strategic Infrastructure Forum. American officials linked the forum to the Bilateral Presidential Commission, though ICT is not one of the formally constituted working groups of that commission.

There is a set of compelling historical precedents suggesting that existing reservations in Russia and the United States about the significant national security sensitivities of cooperation in cybersecurity can be overcome. In civil aviation, there was once total objection to allowing the aircraft of one country to overfly the major cities of the other. The 1963 Kennedy-Khrushchev hotline is another example. The cooperation involved in forming the International Maritime Satellite Organization, INMARSAT—originally a not-for-profit organization, established at the behest of the International Maritime Organization with the goal of creating a satellite communications network for the maritime community—is also illustrative. There were sensitive issues of technology transfer, private sector interests were prominently involved, and a new mechanism (institution) was created to meet the need. In preparing for Y2K, there was a global threat and most countries cooperated despite national security sensitivities. Russia and the United States adopted very intrusive measures for joint monitoring of the most sensitive launch and warning procedures for ballistic missiles. There is little public awareness of the value of such precedents, or even of their existence, and how they might help overcome resistance to cooperative action on cybersecurity.

It is important for both the United States and Russia to recognize that cybersecurity is a global problem, transcending national boundaries. Traditional concepts of national power based on conventional economic, political, and military factors are of little consequence in the cyber world. The asymmetric nature of cyber threats makes any policy formulation very difficult. As a recent report notes, "Comprehensive protection of the entire critical infrastructure against all threats and risks is impossible, not only for technical and practical reasons, but also because of costs."[16] Cybersecurity poses similar problems to policymakers as terrorism. The global nature of information networks means that attacks can be launched from anywhere in the world. As the CSIS Commission on Cyberspace states: "We recommend that the United States advocate measures to secure cyberspace in every multilateral initiative where it is appropriate, just as we have advocated measures to advance nonproliferation or to combat terrorism."[17]

Yet unlike acts of terrorism, cyber attacks can be hard to detect and discovering the origins of the attack (the so-called "attribution problem") is particularly difficult. There are neither battlefields nor front lines and often victims of a single cyber attack can be spread over five continents and dozens of nations. Single states and law enforcement agencies are frequently powerless in the face of new these transnational threats.

The United States and the Russian Federation have much to gain from mutual cooperation on cybersecurity. As a Russian government representative pointed out in front of the United Nations General Assembly:

> The Information Revolution is a global phenomenon that influences all aspects in society, such as international attitudes, the policy, the economy, the financial sector, science and culture. Information resources have become one of the most valuable national and international assets. At the same time there is a deep concern about the potential threats this progress can have on the international peace, stability, and security. Therefore, it is important to limit potential international confrontations within the IT sphere.[18]

15 Office of the Spokesman, "Roundtable on U.S.-Russia Information, Technology: Dialogue on a range of topics including broadband and Internet governance," U.S. Department of State, May 10, 2010, http://www.america.gov/st/texttrans-english/2010/May/20100510144916xjsnommis0.4230245.html.

16 Myriam Dunn Cavelty, "Critical Information Infrastructure: Vulnerabilities, Threats and Responses," *Disarmament Forum*, no. 3, September 2007.

17 James A. Lewis et al., *Securing Cyberspace for the 44th Presidency*, p. 34.

18 Jan Softa, *Threats Against Russia's Information Society* (Charleston, S.C.: BookSurge, 2008), p. 22.

Two Contrasting Approaches to Cybersecurity

The Russian government's policy approach to cybersecurity is focused on different priorities from those of the United States. According to Russian experts, the U.S. terms *cybersecurity* and *cyberspace* are primarily technological, whereas the Russian terms for "information security" and "information space" are seen as having broader philosophical and political meanings. The technology is perceived as only one of many components in Russia's understanding of information security and is not considered to be the most important one. The Information Security Doctrine of the Russian Federation, for example, does not even once mention the word *Internet*. Russia's stated aims for its information concept are protecting the nation's knowledge and culture, and guaranteeing the free flow of information. Of course, the latter claim is hotly disputed by the Kremlin's critics at home and abroad, who believe its information concept is really designed to silence certain antigovernment critics. This political aspect complicates the decision-making for U.S. officials who fear domestic censure for working with Russia to improve cybersecurity collaboration. The main priorities for U.S. cybersecurity policy are to safeguard domestic technologies from disruptions, unauthorized access, or any other kind of interference, thus emphasizing the technological aspects of cybersecurity.

Overall, the United States focuses much more on a domestic law enforcement approach, while Russia prefers to add on an additional goal of establishing international regimes. There is room for both approaches since they complement each other. A report of the CSIS Commission on Cyberspace comments on the nature of the global digital environment: "The Internet is part town square (where people engage in politics and speech), part Main Street (where people shop), part dark alleys (where crime occurs), part secret corridors (where spies engage in economic and military espionage), and part battlefield."[19] Misunderstandings between actors are therefore inevitable, and these can only be addressed through dialogue and compromise.

19 Lewis et al., *Securing Cyberspace for the 44th Presidency*, p. 23.

Russia

Russia began pushing early for a serious focus on the political implications of information security. The subject was already heatedly debated at the then newly established Russian Security Council in 1992.[20] The organizations responsible for cybersecurity are the Security Council, the Federal Security Service (FSB, from its name in Russian),[21] the Federal Guard Service, the Federal Technical and Export Control Service, and the Ministry of Information Technologies and Communications.[22]

The nominal separation of responsibilities when it comes to cyber-related activities in the Russian government is as follows. The Ministry of Internal Affairs (known by its Russian acronym MVD) is responsible for countering cyber crime, the Ministry of Defense is responsible for cyber warfare, and the FSB is responsible for cyber terrorism and other aspects of internal security and state control. This division is in accordance with the Russian government's emphasis on three basic areas: criminal, terrorist, and military-political threats in cyberspace. The Russian policy is coordinated through an intergovernmental committee in the Security Council, chaired by Vladislav Sherstyuk, an assistant secretary in the council, and Boris Miroshnikov, head of the Bureau for Counteracting High-Tech Crimes, of the Ministry for Internal Affairs.

The Russian Information Security Doctrine, which was adopted in September 2000, characterizes information security as the "protection of its [Russia's] national interests in the information sphere defined by the totality of balanced interests of the individual, society, and the state." It further deals with a wide range of issues ranging from data protection, personal privacy, and hacking to state secrets and access to information.[23]

According to a recent publication, the main purpose of Russia's information policy is to contribute to the stability of social and political developments within Russia and guarantee public support of official state policies.[24] In 2010 the Russian government identified four central objectives of its state information policy:

20 Softa, *Threats Against Russia's Information Society*, p. 23.

21 *Federal'naya sluzhba bezopasnosti.*

22 Elgin Brunner and Manuel Suter, "Russia—Critical Sectors," in *An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*, ed. Andreas Wenger, Victor Mauer, and Myriam Dunn (Zurich: Center for Security Studies, ETH Zurich, 2008), p. 347.

23 Ibid, p. 342.

24 A. A. Streltsov, *Gosudarstvennaya informatsionnaya politika: osnovy teorii*, State Information Policy: The Basis of the Theory, (Moscow, 2010), p. 77.

- Developing a system of values for Russian society;
- Securing support of state activities from national and international public opinion (public support of state policy);
- Countering destructive ideologies, religious extremism, and disinformation of national and international constituencies on state policies (political information aspects);
- Countering disruptions of stability and safety and the functioning of national information infrastructure (including military, technological, and political aspects).[25]

Due to its perceived inferiority in communications technology,[26] Russia envisions an international convention that would ban or constrain the development or use of a wide range of military and civilian information technologies. As the Russians see it, this convention should specifically address the threat of cyber attacks and prevent a digital "arms race." This convention should also contain definitions recognized by the world community for aggression in cyberspace and for information weapons. According to a recent report on Russia's critical infrastructure, the rationale for promoting such a treaty is national interest:

> Russia's international cooperation in ensuring information security has two distinctive features: International competition for technological and information resources and for dominance in the markets has increased, and the world's leading economies have achieved a growing technological lead that allows them to build up their potential for information warfare. Russia views this development with concern, as it could lead to a new arms race in the information sphere and raises the threat of foreign intelligence services penetrating Russia through technical means, such as a global information infrastructure.[27]

Consequently, Russia vehemently wants to restrict offensive cyber weapons. Its proposed treaty would ban "offensive weapons" such as embedded malicious software codes that could be activated remotely in a war.28 The Russian proposals also introduce the idea of extending to governments the right to constrain or ban information transmitted into national territory from outside their borders should it be deemed disruptive politically, socially, and culturally.

To advance its cybersecurity agenda, Russia, in accordance with U.N. General Assembly Resolution No. 58/32, chaired a U.N. working group of government experts on cybersecurity in 2003 and continued to play a leading role in similar expert groups into 2010. Also, the Russian Federation has established special partnerships on information security with the members of the Shanghai Cooperation Organization as well as with the Collective Security Treaty Organization.[29]

For Russia, the "most significant" development—in the view of a leading Russian official—has been the adoption in 2009 by the Shanghai Cooperation Organization of a treaty on information security. The treaty is intended to "to create the political, legal and organizational foundations for strengthening confidence and developing cooperation among the parties and relevant national agencies."[30]

United States

In 2009, the Obama administration appointed a cybersecurity coordinator as part of the National Security Staff to coordinate national strategy in this area. The new office is tasked with producing a coherent national policy on strengthening and improving the electronic defense of critical infrastructure, as well as with coordinating activities of the federal government in information security.[31] In the past there have been a number of initiatives and policies in the field of cybersecurity, such as the 2002 National Strategy to Secure Cyberspace, the 2006 National Infrastructure Protection Plan, and the 2007 National Strategy for Information Sharing.[32] In January 2008, the Bush administration prepared the Comprehensive National Cybersecurity Initiative (CNCI) in order to make

25 Ibid.

26 Ibid, p. 342. For example, in 2001 the "*Electronic Russia*" program was launched. Its main purpose is to increase the efficiency of the Russian economy, improve management in the public sector, and enhance self-government by applying information and communication technologies.

27 Ibid, p. 345.

28 John Markoff and Andrew E. Kramer, "U.S. and Russia Differ on a Treaty for Cybersecurity," *New York Times*, June 27, 2009, p. A1.

29 Brunner and Suter, "*Russia—Critical Sectors*," p. 346.

30 S. Shestakov, Representative of the Russian Federation, "Joint meeting of the OSCE Forum for Security Co-operation and the OSCE Permanent Council," (June 12, 2010), http://www.osce.org/documents/fsc/2010/06/44705_en.pdf.

31 White House Blog, "Introducing the New Cybersecurity Coordinator," http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator (posted December 22, 2009).

32 Brunner and Suter, "Russia—Critical Sectors," pp. 635–37.

the United States more secure against cyber threats. The directives establishing this initiative are classified.[33]

Within the federal government the most important agencies and organizations that deal with cybersecurity issues are the Department of Homeland Security, Department of State, Department of Defense, the Office of Cybersecurity and Communications, the National Infrastructure Protection Center, and the Computer Crime and Intellectual Property Section of the Department of Justice.[34]

The United States favors a defensive approach in which improved cooperation among international law enforcement is the central element. Furthermore, the United States believes that the goal of cybersecurity can best be achieved by a state-centric approach, where states acting nationally and cooperating internationally enhance the security of their own critical information infrastructures. For example, according to a U.S. position paper on the 2003 World Summit on the Information Society (WSIS) Action Plan, the United States supports the idea that each state establish a national program that:

- educates and strengthens awareness of best practices in information network and infrastructure security;
- effectively criminalizes misuse of information technology;
- fosters a partnership between government and industry to provide incentives to ensure the security of their national systems;
- establishes a national incident warning and response capability and procedures for sharing information both nationally and internationally.[35]

On the subject of international norms and cooperation, the cyberspace policy review of the current U.S. administration states:

> International norms are critical to establishing a secure and thriving digital infrastructure. In addition, differing national and regional laws and practices—such as laws concerning the investigation and prosecution of cybercrime; data preservation, protection, and privacy; and approaches for network defense and response to cyber attacks—present serious challenges to achieving a safe, secure, and resilient digital environment. Only by working with international partners can the United States best address these challenges, enhance cybersecurity, and reap the full benefits of the digital age.[36]

As the quote above illustrates, the United States, like Russia, believes that the key threat to cybersecurity originates in cyber attacks by organized criminals, individual hackers, and nonstate actors, including terrorists. This is further emphasized by the WSIS position paper:

> . . . the benefits of cyberspace can best be protected by focusing both on the effective criminalization by States of the misuse of information technology and on the systematic national implementation of measures designed to prevent damage to critical information infrastructures no matter the source of the threat, what the U.S. calls the creation of a global culture of cybersecurity.[37]

The United States is vehemently opposed to the establishment of "cyberspace borders" (an approach favored by Russia) and sees it as a direct challenge to democratic principles that could easily be used by governments to justify restrictions on the free flow of information and the peaceful use of information technology. In a number of statements on cybersecurity, U.S. officials have emphasized the freedom of individuals to seek, receive, and communicate information and ideas, as set forth in Article 19 of the Universal Declaration of the Human Rights.[38]

Despite current and past efforts on these cyber issues, a recent report on the United States' international engagement in cybersecurity finds that "the international aspects of cybersecurity have been among the least developed elements of U.S. policy. Given the multinational and global aspects of network security, this must be remedied, as energetic engagement could produce real benefits in promoting U.S. objectives and reducing risk."[39]

Experts have warned against fomenting "cyber angst" by hyping cyber threats, but there's no doubt that the

33 John Rollins and Anna C. Henning, "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations," *Congressional Research Service Report for Congress*, March 10, 2009, p. 3.

34 Brunner and Suter, "Russia—Critical Sectors," pp. 635–37.

35 "United States Views on Information Network and Infrastructure Security in the WSIS Action Plan," position paper presented at the South East European Cooperation Conference, (Sofia, Bulgaria, September 8–9, 2003).

36 White House, Executive Office of the President, *Cyberspace Policy Review—Assuring a Trusted and Resilient Information and Communications Infrastructure* (May 29, 2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

37 Ibid.

38 Ibid.

39 Lewis et al., *Securing Cyberspace for the 44th Presidency*, p. 23.

increasing number of cyber attacks and their increased sophistication demand new policy approaches. The former director of national intelligence Mike McConnell stated that the "time is not too far off when the level of sophistication reaches a point that there could be strategic damage to the United States."40

The United States, however, remains skeptical toward Russian ideas such as an international agreement, since it could provide cover for totalitarian regimes to censor the Internet. The United States also worries that a treaty would be ineffective because it is now almost impossible to determine if an Internet attack originated from a government, a hacker loyal to that government, or a rogue acting independently.[41]

Nevertheless, the United States recently agreed to begin talks in the U.N. Committee on Disarmament and International Security on strengthening Internet security and limiting military use of cyberspace.[42] This represents a major policy shift by the United States after rejecting Russia's overtures on this initiative for a number of years. The appointment of a cybersecurity coordinator and advisor by the president in late 2009 shows the commitment of the Obama administration to taking the issue of cybersecurity seriously. Consequently, an agreement on the proposals put forward by the Russian government on international protocols restricting the use of cyber warfare is not out of the question. Early talks are to be held between the Russian National Security Council, the FSB, and the George C. Marshall European Center for Security Studies on the American side.[43]

What to Expect

Russia and the United States may be routinely engaged in cyber "attacks" or cyber "probes" on the security infrastructure of others. But over time, as technology advances and as civil nuclear proliferation gathers pace, countries like the United States and Russia will not be seen as enemies in cyber war, but rather as important partners, and they may even become active allies.

This may take ten or more years, but the long-term trend is clear. There is an important precedent with Russia. As senior U.S. defense officials have noted, Russia and the United States cooperated smoothly in the Y2K Center for Strategic Stability in Colorado Springs, Colorado, at the time of the millennium rollover.[44] This led to a shared early warning effort with Russia on ballistic missile launches worldwide, albeit an effort somewhat short-lived and limited in scope.

The first outputs will be intangible but nonetheless crucial to the bilateral relationship. As framed by EWI Distinguished Fellow Karl Rauscher, they will include "guiding the two countries towards progressive confidence building, encouraging transparency where appropriate, and sharing a sense of the mutual benefits and starting points for discussion. We should not put too much faith in trust beyond seeing it as a joint commitment that cooperation is possible and that problems will be addressed through negotiation. A key to success can be the discipline of framing and conducting of bilateral dialogue with a focus on the intrinsic vulnerabilities of the cyber domain, rather than on specific threats, which are often more sensitive."

The longer-term value proposition could include tangible commercial benefits:

- Better quality of existing communications (improved security, faster, more resilient);
- New capabilities jointly developed, for mutual benefit;
- Cost avoidance (e.g., from crime, re-directed investment, or infrastructure failure).

We suggest that the broad agenda of the two countries on cybersecurity address the following issues:[45]

- *Trusted identities:* Develop a bilateral private-public forum to discuss issues concerning certificates, authentication and other aspects of civilian security infrastructure.
- *Emergency warning networks:* What is the best approach for countries to develop emergency warning networks regarding cyber vulnerabilities, threats, and incidents?
- *Awareness raising:* What is the best approach for raising awareness to facilitate stakeholders' understanding of the nature and extent of their critical

40 Rollins and Henning, "Comprehensive National Cybersecurity Initiative," p. 3.

41 Markoff and Kramer, "U.S. and Russia Differ on a Treaty for Cybersecurity."

42 John Markoff and Andrew E. Kramer, "In Shift, U.S. Talks to Russia on Internet Security," *New York Times*, December 12, 2009, p. A1.

43 Bruce Jones, "Moscow and Washington Seek Cyber Security Regulations," *Jane's Defence Weekly*, January 6, 2010, p. 6.

44 Private meeting, April 24, 2009.

45 This list is a modified version of topics identified during preparatory meetings organized by EWI for Russia's G8 initiative in 2006 on public-private partnerships to counter terrorism.

information infrastructures, and what is the role each must play in protecting them?

- *Threat assessment:* Do interdependencies exist among infrastructures; and how can the protection of infrastructures be enhanced?
- *Private-public partnerships:* What is the best approach for promoting partnership among stakeholders, both private and public, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage or attacks on such infrastructures?
- *Crisis communication networks:* What is the best approach for creating and maintaining crisis communication networks and to test them to ensure that they will remain secure and stable in emergency situations?
- *Tracing attacks:* What is the best approach for tracing attacks on critical information infrastructures? How can we best facilitate the disclosure of tracing information among countries?
- *Circulation of illegal or dangerous information:* Websites are ideal tools for disseminating information and disinformation on a global scale. Terrorist groups increasingly use the Internet for their propaganda as well as recruitment. Electronic mail has become one of the most important forms of communication in the world. Terrorists can take advantage of the anonymity and accessibility of cyberspace. How can the private and public sectors cooperate to prevent the use of the Internet for terrorist purposes?

Four Breakthrough Measures

This section of the paper outlines the arguments for more rapid progress in U.S.-Russia diplomacy in the area of information security (as the Russians prefer to call it) or cybersecurity (as many Americans prefer). The paper lays out some general considerations for promoting cooperative approaches to the problem, building on the two countries' public announcement in December 2009 that they would begin new consultations on cybersecurity in the framework of the United Nations. The paper discusses four possible areas of cooperation: public key infrastructure, rapid response for cyber crime, an OSCE cyber treaty, and NATO/Russia cooperation on cybersecurity.

The proposed four areas of U.S.-Russia cooperation are merely meant to be ideas for policymakers and do not go into any technical details or organizational processes to execute them. This approach entails the initial willingness by both Russia and the United States to jointly propose the initiative in an international forum (e.g., ITU), to chair working groups, and involve other stakeholders in the debate. This should be followed by bilateral discussions on specific aspects of cooperation too sensitive to be discussed in an international forum.

Public Key Infrastructure Technology

Russia wants a new approach here. As one specialist put it, "We need a 'center of trust' in order to deal with the attribution problem. Without it any progress on Public Key Infrastructure will be impossible."[46] The increasing sophistication of cyber crime/cyber terrorism and low entry barriers for cyber criminals, who are exploiting the Web's anonymity, point to the need for action in this field by both the United States and Russia. One irony here, according to a Russian specialist, is that as trust grows, so does cyber crime: "There is a clear correlation between the increase of trust in online sources and an increase in cyber crime. There were more than 17,000 cases of reported cyber crime in Russia alone in 2009."[47] A recent policy paper released by the U.S. government identified the need to create a "trust ecosystem," one part of which relates to PKI.[48] The paper concentrated on a national ecosystem, and did not even address the international aspects, and tried to finesse this illogical oversight by saying that there was probably a fine distinction to be drawn between the two.[49] The point is that in globally interdependent cyberspace, there can be no exclusively "national" eco-system of trust.

---

46 EWI Interview, Franz-Stefan Gady and Liza Kurukulasuriya, Moscow, March 2010. One of the most challenging aspects in the field of cybersecurity is the problem of attribution, i.e., tracing back an action in the cyber sphere to its originator, be it an individual, an organization, or a state. Public Key Infrastructure is used for encryption of data, electronic signatures (i.e., non-repudiation), and authentication of users.

47 Interview, Moscow, March 2010.

48 "National Strategy for Trusted Identities in Cyberspace," pp. 13–14, June 25, 2010, http://www.dhs.gov/xlibrary/assets/ns_tic.pdf.

49 Ibid, p.29. The document had a very short section on international cooperation: "The Federal Government will prioritize and appropriately staff existing international efforts associated with trusted digital identities. As discussed previously, standards development and adoption at the international level is a cornerstone of global commerce and information exchange. To avoid localized standards development and adoption, domestic efforts should endeavor to adopt international standards whenever they are consistent with domestic goals."

The Public Key Infrastructure (PKI) concept was introduced in the mid-1970s as a new development in cryptography.[50] It allows parties to exchange encrypted data without communicating a shared secret key in advance. An important feature of public key cryptography is a "digital electronic signature," which, like a handwritten signature, can be used to verify the integrity of data or the authenticity of the sender of data.[51]

PKI has been recognized as one of the vital strategies in combating cyber crime (e.g., identity theft) since it is one of the simplest ways to lift the veil of anonymity (the "attribution problem") in the digital sphere. But it is one of the most difficult issues to resolve in combating cyber crime and cyber terrorism because of the differing concerns of the United States and Russia.[52]

A CSIS report on cybersecurity flatly states: "Creating the ability to know reliably what person or device is sending a particular data stream in cyberspace must be part of an effective cybersecurity strategy."[53] The U.S. Department of Defense's PKI is one of the largest in the world and one of the most widely exposed to cyber attacks. Most of these attacks are impossible to trace back, due to the lack of a coherent attribution methodology.[54] Nevertheless, the frequency of cyber attacks fell by 50 percent once the department decided to introduce a new identification system (Common Access Card) and tackle the problem of attribution in 2008.[55]

In a paper that examines the top cybersecurity problems of the world, the World Federation of Scientists Permanent Monitoring Panel on Information Security mentions the "attribution problem" several times. Its recommendations to enhance cybersecurity in this specific area include the following:

- Enable information management at the data structure level, in particular, data structures that represent identity information to ensure the identification, authentication, and authorization of communications to allow seamless, secure information management on a secure basis beyond the limits of current public key infrastructure.
- Improve the ability to track and trace cyber communications to enable source identification (accountability) and use of digital assets by technical means, reducing the reliance on cooperation between Internet Service Providers, while safeguarding privacy.
- Develop tools that protect privacy and enable audits of activity in environments that involve data mining, digital surveillance and profiling for personalized services, and in the protection of personal and business data.
- Develop digital identification mechanisms to protect and advance the interconnection of devices, information, and networks. Develop an identification framework that identifies personal users in its use of networked devices.
- Place higher emphasis on cryptography, especially by developing cryptologic algorithms that will withstand future challenges, including those identified with quantum computing.[56]

Despite these recommendations, there is very little cooperation in the field of Public Key Infrastructure between the United States and Russia apart from some private sector cooperation in the finance and electronic logistic service sector.[57] Whereas Russia has pushed for closer cooperation in this field for some time, the United States has been cautious, fearing that progress in this field might be used by Russian authorities to clamp down on regime critics and dissidents.[58]

Nonetheless, some U.S, officials have appeared to endorse an approach similar to Russia's. In July 2009,

50 According to searchsecurity.com: "A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on. The public key infrastructure assumes the use of *public key cryptography*, which is the most common method on the Internet for authenticating a message sender or encrypting a message." http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214299,00.html.

51 *Report on Background and Issues of Cryptography Policy,* Directorate for Science, Technology and Industry, Organisation for Economic Co-operation and Development, 1997, http://www.oecd.org/document/36/0,3343,en_2649_34255_1814820_1_1_1_1,00.html.

52 *Global Cybersecurity Agenda: Framework For International Cooperation in Cybersecurity,* International Telecommunication Union, 2007, p. 8.

53 Lewis et al., *Securing Cyberspace for the 44th Presidency*, p. 49.

54 Kelly Jackson Higgins, "DoD Official Says U.S. Needs Separate Cyberczar For Online Identity," *DarkReading.com*, July 30, 2009, http://www.darkreading.com/security/government/showArticle.jhtml?articleID=218900177.

55 Lewis et al., *Securing Cyberspace for the 44th Presidency*, p. 49.

56 *Top Cyber Security Problems that Need Resolution—The Planetary Emergency Regarding the InSecurity of Global Communications*, World Federation of Scientists, Permanent Monitoring Panel on Information Security, January 11, 2010.

57 Valerie Abend et al., "Cyber Security for the Banking and Private Sector," in *Wiley Handbook of Science and Technology for Homeland Security*, ed. John G. Voeller (New York: Wiley, 2008); Elena G. Efimova and Maria K. Tsenzharig, "Electronic Logistics Services in Russia: The Bridge to United Europe," *Electronic Publications of Pan-European Institute,* March 2009, http://www.tse.fi/FI/yksikot/erillislaitokset/pei/Documents/Julkaisut/Efimova%20and%20Tsenzharik%200309%20web.pdf.

58 Markoff and Kramer, "U.S. and Russia Differ on a Treaty for Cybersecurity."

Robert Lentz, deputy assistant secretary of defense for cyber, identity, and information assurance, argued that identity theft and anonymity are at the heart of securing the Internet. He also called for the establishment of a cyber czar just for identity and emphasized that reducing anonymity is crucial to ensuring security and resiliency on the Net. The United States subsequently published a white paper titled "National Strategy for Trusted Identities in Cyberspace" on this.[59]

The Federal Security Service (FSB) of the Russian Federation is the leading Russian agency to deal with cryptology, digital authentication, and Public Key Infrastructure protection. The FSB commission on imports and exports has to approve any foreign cryptology technology that is imported into or any domestic technology that is exported from Russia. Any discussion on international PKI cooperation will have to start there. For example, the U.S. Federal Bureau of Investigation (FBI) and FSB could hold initial discussions on PKI, focusing on ways to achieve some sort of interoperability between the Russian block cipher and the United States' DES system (Data Encryption Standards), in order to identify weaknesses that third parties such as cyber criminals or cyber terrorists can exploit.

In Russia, the Russian Association of Networks and Services (RANS) is responsible for developing norms and legal documents for the implementation and use of secure IT infrastructure. It was established through an initiative of the Russian Ministry for Information Technologies and Communications in 1994. At present, RANS has more than 110 members from all over Russia, including universities, scientific institutions, and ministries.[60] RANS has several committees and working groups on topics like Internet, security, privacy, and wireless communications. In terms of information security, RANS deals with the creation and development of the PKI and information security concept in Russia, the preparation of draft laws on electronic signatures, and the integration of Russian information and telecommunication systems into European and world infrastructure.[61]

Since the private sector is critical in the development of cryptographic products such as electronic signatures, private-public partnership will be especially important. Most Public Key Infrastructures—in energy, communications, transport, and financial services—in both countries are in private hands. One possibility could be to create incentives for private-private sector cooperation on encryption technologies, with an American company providing the more difficult to develop hardware and a Russian company providing software. There is a considerable choice of cryptographic products and methods to meet the requirements put forth by a joint U.S.-Russia effort in that field. A neutral multilateral entity (a "Center of Trust," as a Russian expert put it recently) could provide nonpartisan technical and policy advice to both governments and other leading cyber nations.

The International Telecommunication Union (ITU) has the most responsibility for these practical aspects and applications of international cybersecurity, and it would be the most suitable organization to initiate a first joint technical U.S.-Russia initiative on Public Key Infrastructure. The ITU has developed an international standard for PKI (labeled ITU x.509, but also known as ISO 9594-8).[62] Both the United States and Russia have supported the establishment of the Global Cybersecurity Agenda (GCA) launched by the ITU in May 2007 as a framework for international cooperation to promote cybersecurity and enhance confidence and security in the information society.[63] In addition to this, the ITU's Study Group 17 has been active in promoting cybersecurity initiatives, including how to apply trace-back and digital forensics mechanisms. The ITU is not ideal as an international platform to deal with these sensitive issues because of its large worldwide membership and consensus-based decision-making, yet through its smaller working groups it can serve as a means to build trust for bilateral discussions.

Recommendation: Russia and the United States should champion in the International Telecommunication Union the idea of a binding multilateral agreement on Public Key Infrastructure.

59 "...The Strategy defines and promotes an Identity Ecosystem that supports trusted online environments. The Identity Ecosystem is an online environment where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their digital identities.... privacy protection and voluntary participation are pillars of the Identity Ecosystem. The Identity Ecosystem protects anonymous parties by keeping their identity a secret and sharing only the information necessary to complete the transaction." *National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy*, Draft Paper, (Washington DC, June 25 2010,) http://www.nstic.ideascale.com/.

60 Russian Association of Networks and Services, http://www.rans.ru/eng/about/.

61 Ibid.

62 International Telecommunications Union, *X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*, http://www.itu.int/rec/T-REC-X.509.

63 Stein Schjølberg, *Report of the Chairman of High Level Experts Group (HLEG)*, ITU Global Cybersecurity Agenda, September 2008, http://www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf.

This could be based on a "joint policy assessment" by Russian and U.S. experts, which would serve to refine the problem statement more clearly and foreshadow possible solutions to be adopted through multilateral agreements.

A binding multilateral agreement on PKI will help reduce the "attribution problem" and the vulnerabilities of critical infrastructure in both countries. A free exchange of information under the auspices of the ITU will invite other countries to contribute to the discussion, paving the way for further international cooperation. It would create an impetus for further collaboration between the United States and Russia on a number of other policy issues, such as missile defense, Afghanistan, and combating international terrorism.

A common U.S.-Russian approach should start by identifying the required or desired exchange of information. This should be followed by a joint risk assessment of particular sectors, indicating where closer cooperation would be beneficial to both sides. This could be tied to national critical infrastructure plans from both countries. The risk assessment then would outline specific measures to be taken—for example, the need for encryption and authentication in specific sectors.

There is an inherent tension between common security and the right to privacy in this discussion. A report on Russia from 2002 emphasizes:

> Privacy is a relatively new concept in the Russian legislative process . . . [A]lthough the Russian legislature is trying to address the protection of personal data in cyberspace, the balance between the right of the individual and the right of various government layers continues to be skewed in favor of the latter. . . . [T]hrough a variety of legislative measures, the Russian security services have obtained the right to monitor all forms of electronic correspondence. . . .[64]

The privacy versus security debate would be a contentious issue domestically in the United States as well and might cause a political backlash from political activists and human rights groups. A CSIS report finds: "For authentication systems to be widely adopted, privacy concerns must be addressed. A new initiative can do this by making authentication requirements proportional to risk—high-risk situations require strong authentication, while the lowest-risk situations require no authentication. The goal is to avoid a one-size fits all approach to credentialing."[65] Any dialogue between Russia and the United States should take this into account.

Finally, Russia is a participant in the Wassenaar Arrangement, which restricts the export of cryptographic hardware and software.[66] Thus any technical cooperation would first have to overcome this legal obstacle.

Cyber Crime Cooperation/G8

The most common day-to-day threats to the integrity of the global information infrastructure usually originate from cyber criminal activity rather than military attacks by states against one another. The major problem with responding to cyber crime cooperation is that it can be the most transnational of all crimes yet law enforcement agencies have to respect borders.

Cooperation between the United States and Russia on cyber crime has been sporadic at best in the past. A much-publicized recent crackdown on cyber crime in Russia, preceded by close cooperation between America's FBI and Russia's FSB, has been hailed as a new breakthrough in cooperation between the two countries.[67] However, the potential of this new cooperation is still to be tested. According to a Russian specialist, "There is no real reason why Russia and United States should not have joint investigations into cyber crimes. However, Interpol is a controversial organization in Russia and cooperating with them will be difficult."[68] So other international channels are needed.

The most prominent multilateral attempt to contain cyber crime is the Council of Europe's Convention on Cybercrime, which entered into force in July 2004.[69] As of January 2010, twenty-three of the forty-seven member states of the Council of Europe had ratified the convention. Five member states have not yet signed it. Those five include Russia, which maintains that its sovereignty would

64 Dependability Development Support Initiative, RAND Europe, *National Dependability Policy Environments: Russian Federation,* November 2002, 11. http://www.ddsi.org/htdocs/Documents/final%20docs/DDSI_Country_Reports_Final_Russia.pdf.

65 Lewis et al., *Securing Cyberspace for the 44th Presidency*, p. 64.

66 For further information on the cryptography agreement in the Wassenaar framework, see http://www.international.gc.ca/controls-controles/about-a_propos/expor/Wassenaar_crypto.aspx?lang=eng.

67 Joseph Menn, "Moscow cracks down on cybercrime," CNN, March 25, 2010, http://www.cnn.com/2010/BUSINESS/03/22/moscow.cybercrime.ft/index.html.

68 EWI Interview, Moscow, March 2010.

69 Council of Europe, Convention on Cybercrime, (Budapest 23.XI.2001) http://conventions.coe.int/treaty/en/treaties/html/185.htm.

be threatened by the treaty.[70] Turkey has also not signed it. Some sixteen states that did sign the treaty have not ratified it, and these include the United Kingdom, Sweden, Georgia, and Belgium.[71] As a Russian specialist explains, "Russia is prepared to sign the European Convention on Cybercrime if the sovereignty clause is eliminated. Putin actually ordered the ratification two years ago, but the Ministry of Foreign Affairs blocked him out of political expediency."[72]

The Council of Europe describes the convention as "the only binding international treaty on the subject to have been effectuated to date."[73] It is unique in several respects. For the first time, a convention addresses illegal activities and practices that crop up across a broad spectrum of cybersecurity threats. Second, it is the first attempt to establish common standards and procedures in cyberspace that are legally binding on its signatories. Third, the convention is open to Council of Europe member states and others, which means it could become an international instrument accepted by more than one group of countries. (For example, the United States has signed and ratified it.) Finally and most controversially, the convention introduces requirements for data handling and access, which have given rise to concerns over privacy rights and civil liberties, and, as in the case of Russia, questions about state sovereignty.[74]

In addition to the Council of Europe's work on legal regimes in this area, the OSCE, the Organisation for Economic Co-operation and Development (OECD), and the United Nations have initiated a number of multilateral cyber initiatives. But as a report by the Economic Crime Division of the Council of Europe concludes, none of these really represents a foundation for effective implementation or international cooperation.[75] Since Russia is not a member of the OECD and has refused to join the Convention on Cybercrime, the main vehicle for cooperation between the United States and Russia has been the G8 Sub-Group on High-Tech Crime, which both countries have chaired during their respective chairmanships of the G8.

The Sub-Group on High-Tech Crime, founded as a subgroup of the 1996 Lyon Group to combat transnational organized crime, has created a Network of Contacts for High-Tech Crime, operating 24/7, as well as an international Critical Information Infrastructure Protection (CIIP) Directory. It has also published best-practice documents and guides for computer and network security threat assessments, along with organizing international training conferences for cyber crime agencies. Russian and U.S. representatives have participated in these conferences and helped draft some of the best-practices documents. They are both represented in the subgroup by multidisciplinary delegations that include cyber crime investigators and prosecutors, and experts on legal systems, forensic analysis, and international cooperation agreements.[76]

The Network of Contacts for High-Tech Crime is the first of its kind in the world and has been joined by more than twenty countries. Contacts within these countries are available at all hours to receive information and/or requests for cooperation involving cyber crimes. The contact point for the G8's Network of Contacts in the United States is the Computer Crime and Intellectual Property Section of the Department of Justice. It is responsible for implementing the department's national strategies in combating computer and intellectual property crimes worldwide.[77] On the Russian side the point of contact is the FSB.

Recommendation: Russia and the United States should expand the existing infrastructure of the Network of Contacts for High-Tech Crime under the umbrella of the G8 and jointly champion a global framework of 24/7 points of contact, including support for a global program of capacity building in law enforcement and cyber investigation for all countries connected to the Internet.

Mechanisms should be put in place to:

1. Promote partnership among stakeholders, both private and public, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures;

70 "Putin Defies Convention On Cybercrime", Computer Crime Research Center, March 28, 2008, http://www.crime-research.org/news/28.03.2008/3277/.

71 Council of Europe, *Convention on Cybercrime CETS NO.: 185,* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

72 EWI Interview, March 2010.

73 Pedro Verdelho, "The Effectiveness of International Co-operation against Cybercrime: Examples of Good Practice," Discussion Paper (Draft), Project on Cybercrime, Council of Europe, March 12, 2008, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/DOC-567study4-Version7_en.PDF.

74 Ibid.

75 For a list of examples of good practices, see ibid.

76 "Meeting of G8 Justice and Home Affairs Ministers," (Sea Island, GA. 2004) http://www.justice.gov/criminal/cybercrime/g82004/g8_background.html.

77 Ibid.

2. Establish emergency warning networks to provide alerts on cyber vulnerabilities, threats, and incidents;
3. Engage in international cooperation and secure critical information infrastructure, especially through coordinating investigations of attacks on such infrastructures, in accordance with domestic laws.[78]

Such an international network for emergency response would indirectly address the problem of cyber conflict by faster identification of threats and their sources, thereby enabling the swifter resolution of legal issues such as the jurisdiction of a cyber crime lawsuit.[79] Additionally, by reducing cyber crime through increased cooperation, networks and critical infrastructures will be made safer. As a U.S. analyst states, "The security of cyberspace needs to be considered like an ecosystem. Cyber crime is making the Internet a messy place today. If we were to clean up crime in cyberspace, it would be easier for governments to attribute attacks to their actual sources."[80] Creating this international network, in combination with new mechanisms such as authentication processes, would be a major step in addressing the "attribution problem," thereby deterring cyber attacks and cyber crime.

Setting up a global network of contact points would be just the first step in U.S.-Russia cooperation to combat cyber crime and cyber terrorism. Harmonizing legislation across countries and dealing with the legal aspects of the attribution problem would be just as important. As Jeffrey Carr points out in his book *Inside Cyberwarfare,* states are caught in a bind because of lack of a standardized approach that makes attribution easier and because efforts to identify an attacker are extremely time-consuming and complex. He calls this a "response crisis": "More than anything else, the attribution requirement perpetuates the response crisis."[81]

Without clear legal frameworks, this assistance by the state of origin will not come easily, even if technical cooperation on tracing back attacks will be substantially improved by setting up a global 24/7 network of contacts. Consequently, this will need to be followed by much broader legal initiatives.

78 "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures," United Nationas General Assembly, 58th Session, A/Res/58/199, (January 30, 2004) http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.

79 *Virtuality Here: The Age of Cyber Warfare,* McAfee, Inc. December 2009, http://resources.mcafee.com/content/NACriminologyReport2009NF.

80 Ibid.

81 Jeffry Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Seattle: O'Reilly Media, 2009), p. 47.

Cyber Warfare Law/OSCE

Cyber warfare remains a legal and strategic gray zone. Recent policy debates on the subject have yielded very little in the way of concrete international agreement.[82] The lack of progress surrounding the cyber warfare debate is especially troublesome considering the recent surge of cyber attacks thought to be state-sponsored. A treaty on cyber warfare would establish protocols on what is acceptable and unacceptable behavior in cyberspace. Provisions could be made to exclude civilian infrastructure from cyber attacks in any future conflict between states and to assert that a disregard of the provisions would justify retribution. Many legal experts have argued that substantial updating of the laws of armed conflict may be necessary.[83] In particular, the justification for using force against another nation—*jus ad bellum*—needs clearer definitions.

A report issued by the National Research Council on the technological, legal, ethical, and policy implications for the potential acquisitions and use of cyber attack capabilities states: "There will be uncertainties in how [laws of armed conflict] and UN Charter law might apply in a given instant."[84] A new treaty would address this issue and clearly outline what is permissible and what is not. History has shown that having clearly defined laws in the realm of warfare is always better than having ambiguous rules, or none at all.

A treaty on cyber warfare is a delicate matter in the international arena. Most intelligence agencies are using cyber technology to hack into other countries' critical infrastructure. This has been part of most countries' intelligence gathering for decades now. In reality, the methods used by spies, cyber criminals, or cyber terrorists do not substantially differ. A treaty specifically outlawing these kinds of activities would receive little support from any of the major world powers and would be impossible to enforce.

Another challenge that the United States and Russia would face in trying to adopt an effective cyber protocol is the very slow pace of negotiations on a multilateral basis under the auspices of an international organization. By the time the treaty is drafted and implemented, the technology might already have made large sections of such a treaty obsolete. More importantly, a treaty negotiated between states does not apply to nonstate actors.

82 McAfee, *Virtuality Here.*

83 Ibid.

84 Ibid.

One of the first dilemmas in trying to advance the regulation of cyber war under international law is choosing the most effective forum to do so. There are several options: the International Legal Commission, the U.N. Security Council and General Assembly, or the International Telecommunication Union. Left to their own devices, all of these forums would inevitably lead to a protracted process possibly lasting decades. Therefore, it makes sense to choose a strategy for forcing the pace at the same time as a forum is chosen.

The Russian Federation first introduced the idea of a treaty on "information warfare" in 1995. In 1998, it submitted a draft resolution to the U.N. secretary general outlining its ideas to impose a ban on "information weapons."[85] During the Fifty-fourth Session of the General Assembly, the Russian Federation proposed a new draft resolution, where for the first time the *military potential* of cyber technology was mentioned.[86] In 2000, the Russian Federation submitted to the U.N. Secretariat another set of draft principles concerning international information security.

The United States objected to the establishment of a treaty because it felt it was premature to discuss negotiations on an international agreement on information warfare. The United States instead argued for a more concentrated focus on international cooperation to combat cyber crime and cyber terrorism, a position that changed very little until recently. With respect to military applications of information technology, the United States considers such an international convention to be unnecessary. As the U.S. WSIS position paper states: "The law of armed conflict and its principles of necessity, proportionality, limitation of collateral damage, already govern the use of such technologies."[87]

Recommendation: Russia and the United States should undertake joint policy assessments of legal aspects of regulating cyber warfare, including both offensive and defensive activities, especially in the area of critical infrastructure and "rules of engagement." The assessment should make recommendations on the best forum to advance multilateral moves toward regulation.

The strategy for change might include a group of "driver" countries, possibly the United States and Russia, but possibly also a regional organization that includes both of them.

The Organization for Security and Co-operation in Europe (OSCE) has taken a growing interest in the challenge of cybersecurity. During the last two years, it has also played an increasingly prominent role, particularly after the war in Georgia in August 2008. After a long period in which the OSCE looked marginalized, the Georgia events catapulted the organization back into the international limelight, similar to Cold War times. Consequently, it may be beneficial for the United States and Russia to try to push any initiative on cyber warfare through OSCE channels, taking advantage of the organization's recent prominence. Russia remains skeptical and even antagonistic toward the OSCE.

Before the 2007 cyber attacks on Estonia and the war in Georgia, the OSCE had done very little on cyber warfare. In December 2004, the Ministerial Council (composed of the foreign ministers of OSCE participating states) resolved to address "the extent of use of the Internet by terrorist organizations,"[88] including a range of activities such as terrorist recruiting, fund-raising, organization, and propaganda. While Estonia held the OSCE presidency in 2008, it proposed that the OSCE adopt a comprehensive approach to the issue of cybersecurity.[89] An OSCE workshop on a comprehensive OSCE approach to cybersecurity was held in 2009 and its recommendations for further cooperation were adopted by the Ministerial Council.[90] Russia and the United States both participated in this workshop.

Many people advise against using the OSCE as a vehicle for advancing international law on cybersecurity. Of course, it is likely that the OSCE would not quickly or easily come to final agreement on a treaty in this field. But if the OSCE provides a more manageable platform at least for debate and refinement of the issues than the United Nations does, then it may be the better option. The adoption of principles within the OSCE would not

85 "Treaty on Cyberwarfare—Is one needed?" Space and Telecom Law Faculty, University of Nebraska, PowerPoint presentation, available in PDF form at http://spaceandtelecomlaw.unl.edu/c/document_library/get_file?folderId=1790400&name=DLFE-19052.pdf.

86 A. A. Streltsov, "International Information Security: Description and Legal Aspects," *International Disarmament Forum*, no. 3, 2007, http://www.unidir.org/pdf/articles/pdf-art2642.pdf.

87 "United States Views on Information Network and Infrastructure Security in the WSIS Action Plan." World Summit on the Information Society, www.cybersecuritycooperation.org/.../WSIS-SecurityPositionPaper-Handout_Version.doc.

88 Triin Parts, "2009—A New Beginning for The OSCE?," in *Estonian Ministry of Foreign Affairs Yearbook 2008/2009*, p. 42, http://web-static.vm.ee/static/failid/003/Triin_Parts.pdf.

89 Ibid., p. 42.

90 Ministerial Council Decision No. 2/09, *Further OSCE Efforts to Address Transnational Threats and Challenges to Security and Instability*, December 2, 2009, http://www.osce.org/documents/cio/2009/12/41869_en.pdf.

preclude agreement on future protocols adopted within the framework of the U.N.

NATO/Russia

Russky Newsweek, the Russian-language edition of *Newsweek*, ran a cover story in its November 23, 2009, issue on cyber crime that pointed a very big finger at Russian hackers working from home and abroad. It used terms like the "Evil Cyber Empire" and the "Cold Cyber War." At the same time, NATO is trying to understand how it should deal with cybersecurity issues. Does a cyber attack on a NATO member state trigger the Article V commitment of the mutual defense treaty?

Geopolitics during the Cold War was about borders and defending them. Cyber diplomacy in the twenty-first century is about managing a world that is not just borderless but can function best when connectivity is almost seamless. This world—so dependent on stable financial transactions and global trading—cannot function at all if cyber connectivity is successfully attacked. So how does NATO, a geographically defined alliance trying to redefine its relationship with Russia, understand its role in promoting cyber diplomacy and cyber peace? What should the institutional structure and strategic profile of NATO look like if the biggest security threats to it in the next ten years are from terrorists or states with advanced cyber offensive capabilities?

One big change will be in espionage. It will continue but its fundamental character will change. Russia will change its intelligence-gathering priorities in NATO countries, and the United States will change its espionage priorities in Russia. All parties will become more interested in protecting at least some of the others' secrets than in stealing them, because to do so will buttress their own economic security.

For NATO, the time has definitely arrived for it to elevate cybersecurity to the top rank of issues to be dealt with in its official relations with Russia; the two sides have a shared interest in seeking common solutions, not simply looking at each other as potential threats.

A low-profile speech by the vice chairman of the U.S. Joint Chiefs of Staff, General James E. Cartwright, in June 2009 gave a glimpse of an emerging strategic concept in the world's only military superpower—something he dubbed "global strike."[91] He said that the low-end capability for global strike "is probably [the ability to be] any place on the face of the earth in an hour," while the "high end is any place on the face of the earth in about 300 milliseconds—that's cyber." This view was expressed during a discussion of the forthcoming quadrennial review of the country's military planning and capability. It flowed from Cartwright's vision of what deterrence looks like in the twenty-first century.

Citing the proliferation of ballistic missiles, Cartwright observed that a new attack—potentially nuclear—"could be over in minutes." This circumstance would require, he said, "something that deters that conflict and it has to be more than nuclear." For him, part of the argument is that his country's military bases are located "where we fought the Indians, the Japanese and the Germans." He suggested that current basing realities might not address the needs of deterring or responding to new threats.

The U.S. Cyber Presence in Europe

The United States response to the emerging security threats has been to move its forces and bases in Europe, small as they are, either to the east or the south, closer to the trouble spots of the Middle East and the Horn of Africa. In 2004, the United States began planning the closure of almost half of its 589 military bases in Europe as a result of its Global Posture Review Thus, the United States is now more interested in "cooperative security locations" (CSLs) than classic military bases. And the United States has singled out Black Sea countries, such as Romania and Bulgaria, as prime targets for this reorientation of the U.S. "presence" and establishment of CSLs.

This confirms that, in terms of addressing existing and prospective ballistic missile or nuclear threats from countries in the Middle East, the United States—and, therefore, NATO—is attaching increasing importance to the Black Sea region. This means that cyber warfare capabilities, along with associated intelligence collection and covert operation needs, are likely to be built up there. This new overlay may well drive the way in which the United States shapes its relations with the countries of the Black Sea: Russia, Ukraine, Georgia (including Abkhazia), Romania, Bulgaria, and Turkey.

---

91 Vice Chairman for the Joint Chiefs of Staff General James Cartwright, "Whither the Forward-Basing of U.S. Forces?" *Quadrennial Defense Review*, United States Department of Defense, Presentation at the Center for International and Strategic Studies, June 4, 2009. http://www.defense.gov/qdr/transcripts_cartwright_20090604.html.

Cyber Military Exercises and Exchange

NATO-Russia relations received a sharp setback in the aftermath of Russia's war against Georgia in August 2008. Some commentators even drew comparisons to the pre-Reykjavik times of the Cold War.[92] Relations had already cooled shortly before the war when Georgia and the Ukraine applied for membership in NATO. Prime Minister Vladimir Putin went so far as to argue that a Ukraine NATO membership "may bring into question Ukraine's existence as a sovereign state."[93] The likely involvement of the Russian government in cyber attacks on Georgian critical infrastructure during the Russia-Georgia conflict remains especially controversial and debated. Project Grey Goose, a U.S.-based nongovernmental organization, stated in its key finding in October 2008, "We assess with high confidence that the Russian government will likely continue its practice of distancing itself from the Russian nationalistic hacker thus gaining deniability while passively supporting and enjoying the strategic benefits of their actions."[94] The Russian government has vehemently and repeatedly denied any involvement. NATO-Russia relations are slowly improving yet suspicions remain on both sides especially in the sphere of cybersecurity. NATO is currently discussing and drafting its new Strategic Concept, with two of the key questions being the future of NATO-Russia relations and the role of cybersecurity in NATO's future security planning.

The NATO-Russia Council is the key body for formal engagement between NATO and the Russian Federation. It was established in 2002 in the wake of the terrorist attacks of September 11, 2001, and was meant to emphasize the need for coordinated action to respond to common threats such as terrorism. The council functions through twenty-seven committees and working groups responsible for different areas of policy. One of these working groups is the NATO-Russia scientific cooperation forum, which among other mandates is a means for collaboration in the field of cybersecurity.

NATO has also set up a "Center of Excellence" for cyber defense in Estonia to study cyber attacks and determine under what circumstances such an attack should trigger NATO's common defense principle that an "attack on one is an attack on all." Its other main mission is to improve the capabilities, cooperation, and information sharing among NATO states through lessons learned. The center was established in 2008 and membership is open to all NATO countries.

Recommendation: At a political level, NATO and Russia should commit to completing a joint assessment within a given time frame (e.g., two years) of what constitutes global cybersecurity and how it can be achieved. In the framework of NATO-Russia scientific cooperation, Russia and the United States should engage in reciprocal observation of and participation in simulations of cyber attacks. Along with the NATO partners, both countries should develop methodologies and standards for vulnerability assessments and ranking of critical facilities.

However unrealistic this recommendation seems, participation in cyber military exercises should not be dismissed as impossible in the current political climate. Just as the United States military has done, the Russian armed forces have developed a robust cyber warfare doctrine, which is designed to act as a force multiplier. As a recent report notes,[95] it includes the capability to disrupt the information infrastructure of Russia's enemies and disrupt financial markets and civilian and military communications capabilities. The sensitivity and secrecy of these capabilities have so far precluded any form of cooperation. One reason for that are the activities of both countries' intelligence agencies in the field of cyber espionage. The Cold War ended only twenty years ago, and mutual suspicions are difficult to overcome. But experts agree that the methods used by cyber warriors do not differ from those used by cyber criminals and cyber terrorists, which both countries agree are the main threats to their critical infrastructure. Mutual exchanges of information during joint exercises would increase the resilience of both nations as they try to protect themselves against such threats. From a technical point of view, it is important to note that there is no "forced entry" in cyberspace.[96] Every intruder enters through pathways produced by the system itself. It is only a modest exaggeration to say that organizations, ministries, and states are vulnerable to cyber attack only

92 Daniel Korski, "*Shaping a New NATO-Russia Partnership*," SAIS Center for Transatlantic Relations, http://transatlantic.sais-jhu.edu/bin/q/s/korski_Shaping_a_New_NATO-Russia_Partnership.pdf.

93 Quoted in Anders Aslund and Andrew Kuchins, "Pressing the 'Reset Button' on US-Russia Relations," *CSIS Policy Brief*, March 2009.

94 See Project Grey Goose, "Russia—Georgia Cyber War: Findings and Analysis," Phase 1, 2008, p. 3. Project Grey Goose, an NGO, was a forerunner to the for-profit firm Grey Logic, both set up by Jeffrey Carr. , http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report

95 Arie J. Schaap, "Cyber warfare operations: Development and use under international law," Air Force Law Review, December 22, 2009, http://findarticles.com/p/articles/mi_m6007/is_64/ai_n42124173/?tag=content;col1.

96 Martin C. Libicki, "Cyberdeterrence and Cyberwar," RAND, Project Air Force, 2009, http://www.rand.org/pubs/monographs/2009/RAND_MG877.sum.pdf.

to the extent they allow themselves to be.[97] Cooperation in this field is thus mutually beneficial.

A dialogue with the private sector, particularly defense industries, could also be started under the umbrella of the NATO-Russia Council. Specialists in each country have difficulty understanding how the government structure and the private sector function in the other country. Since the role of government is central to almost all spheres of cybersecurity, and since much of the burden of implementing preventive strategies falls on the private sector, improved familiarity with organizational responsibilities and practical experiences would be of benefit to many specialists in both countries, despite obvious structural differences in the setup of the U.S. and Russian defense sectors in terms of government ownership.

NATO countries and Russia differ on the importance of the NATO-Russia Council in managing the mutual relationship. For Russia, the council was always intended to be the main platform to discuss NATO-Russia relations, whereas major NATO countries never saw it as a substantive forum.[98] Consequently, the political importance of the council has not lived up to expectations, and it has failed to remove or redress major disputes and grievances between NATO and Russia. Some analysts argue that the only reason why Russia remains engaged in the council at the moment is pure political expediency: it wants to sideline the OSCE, which has had a prominent role in Russia in monitoring elections and in the postconflict situation in Georgia.[99]

Considering the secrecy with which both countries are guarding their cyber capabilities, it's hardly surprising that there is considerable reluctance to engage in military cooperation in this field. Initial exchanges could be limited to unclassified information in the framework of the NATO-Russia Council, to be followed by more concrete bilateral exchanges on specific mutual threat scenarios such as safeguarding critical infrastructure (e.g., nuclear plants) from cyber attacks during times of war. Transparency on all aspects of information warfare capabilities is not required, nor is there a need to exchange classified information on the inner workings of both governments.

97 Ibid.

98 Daniel Korski, "Shaping a New NATO-Russia Partnership."

99 Ibid.

Other Lines of Action

The four concrete examples of cooperation outlined above should be supported by other initiatives and projects such as joint threat assessments and the development of joint terminology (e.g., cybersecurity versus information security). The Lomonosov Moscow State University's Institute of Information Security Issues (IISI) has been officially appointed by the Security Council of the Russian Federation as the leading scientific organization in Russia to deal with information security issues and international cooperation. Contacts between IISI and the U.S. National Defense University are already in place but should be intensified in all spheres, especially on the sensitive subject of cyber warfare. Joint research projects may enhance the capability to deal with global cyber-related problems. For example, one American cybersecurity expert suggested the construction of a Cyber Early Warning Network.[100] This idea could be jointly put forward by Russian and U.S. experts in an international forum such as the ITU. Expanding other international contacts and cooperation between Russian and American universities, think tanks, and the private sector will also prove helpful in overcoming the all-important trust deficit.

Russian experts have called for the establishment of a "Global Center for Monitoring, Identification and Assessment of Threats in the Information Sphere" and the founding of an international mechanism for consultation on the most difficult problems of ensuring international information security. This has received scant attention internationally. U.S. government officials have been more cautious and inward oriented. Nonetheless, the U.S. House of Representatives passed the Cybersecurity Act in March 2010, with the chairman of the of the House Science and Technology Committee, Bart Gordon, observing that "improving cybersecurity will require a collaborative effort both domestically and internationally."[101]

100 Carr, *Inside Cyber Warfare*, pp. 179–89.

101 Roy Mark, "House Passes Cybersecurity Act," *Eweek.com*, March 2, 2010, http://www.eweek.com/c/a/Government-IT/House-Passes-Cybersecurity-Act-682741.

Conclusion

It remains to be seen whether genuine and effective bilateral cooperation between Russia and the United States on cybersecurity will be possible. There is no shortage of political leaders and security specialists in both countries who see the relationship as essentially confrontational: their offensive threat, our defensive countermeasures. For these people, the idea of "common security" in the cyber domain does not have much appeal. Yet the common vulnerabilities are immense: from personal information, banking records, and controls on sensitive medical equipment to the controls on nuclear power plants and nuclear missiles. Consequently, old policy paradigms will have to change. Outdated concepts such as deterrence through mutual assured destruction make no sense in cyberspace. If Russia and the United States can begin to open the doors of their cyber homes a little more widely, this will be a major step toward building trust, safeguarding information infrastructure, and promoting an open information society at the global level.

EWI Board of Directors

EastWest Institute

Forging Collective Action for a Safer and Better World

OFFICE OF THE CHAIRMAN

Francis Finlay (U.K.)
EWI Chairman
Former Chairman,
Clay Finlay LLC

Armen Sarkissian (Armenia)
EWI Vice-Chairman
Eurasia House International
Former Prime Minister of Armenia

OFFICERS

John Edwin Mroz (U.S.)
President and CEO
EastWest Institute

Mark Maletz (U.S.)
Chair of the Executive Committee of EWI Board of Directors
Senior Fellow, Harvard Business School

R. William Ide III (U.S.)
Counsel and Secretary
Partner, McKenna Long & Aldridge LLP

Leo Schenker (U.S.)
EWI Treasurer
Senior Executive Vice President, Central National-Gottesmann, Inc.

MEMBERS

Martti Ahtisaari (Finland)
Former President of Finland

Jerald T. Baldridge (U.S.)
Chairman
Republic Energy Inc.

Thor Bjorgolfsson (Iceland)
Chairman
Novator

Peter Castenfelt (U.K.)
Chairman
Archipelago Enterprises, Ltd.

Maria Livanos Cattaui (Switzerland)
Former Secretary-General
International Chamber of Commerce

Mark Chandler (U.S.)
Chairman and CEO
Biophysical

Joel Cowan (U.S.)
Professor
Georgia Institute of Technology

Rohit Desai (U.S.)
President
Desai Capital

Addison Fischer (U.S.)
Chairman and Co-Founder
Planet Heritage Foundation

Melissa Hathaway (U.S.)
President
Hathaway Global Strategies, LLC;
Former Acting Senior Director for Cyberspace
U.S. National Security Council

Stephen B. Heintz (U.S.)
President
Rockefeller Brothers Fund

Emil Hubinak (Slovak Republic)
Chairman and CEO
Logomotion

Wolfgang Ischinger (Germany)
Chairman
Munich Security Conference

Haifa Al Kaylani (U.K.)
Founder & Chairperson
Arab International Women's Forum

Donald Kendall, Jr. (U.S.)
Chief Executive Officer
High Country Passage L.P.

Sigrid RVC Kendall (U.S.)
Managing Partner
Kendall-Verwaltungs-GmbH

James A. Lash (U.S.)
Chairman
Manchester Principal LLC

Christine Loh (China)
Chief Executive Officer
Civic Exchange, Hong Kong

Ma Zhengang (China)
President
China Institute of
International Studies

Michael Maples (U.S.)
Former Executive Vice President
Microsoft Corporation

Peter Maurer (Switzerland)
Ambassador
Permanent Mission of Switzerland
to the United Nations

Thomas J. Meredith (U.S.)
Co-Founder and Principal
Meritage Capital, L.P.

Francis Najafi (U.S.)
Chief Executive Officer
Pivotal Group

Frank Neuman (U.S.)
President
AM-TAK International

Yousef Al Otaiba (U.A.E.)
Ambassador
Embassy of the United Arab
Emirates in Washington D.C.

Ross Perot, Jr. (U.S.)
Chairman
Hillwood;
Member of Board of Directors
Dell, Inc.

Louise Richardson (U.S.)
Principal
University of St Andrews

John R. Robinson (U.S.)
Co-Founder
Natural Resources Defense Council

George F. Russell, Jr. (U.S.)
Chairman Emeritus
Russell Investment Group;
Founder, Russell 20-20

Ramzi H. Sanbar (U.K.)
Chairman
Sanbar Development Corporation, S.A.

Ikram Sehgal (Pakistan)
Chairman
Security and Management Services

Kanwal Sibal (India)
Former Foreign Secretary of India

Henry J. Smith (U.S.)
Chief Executive Officer
Bud Smith Organization, Inc.

Hilton Smith, Jr. (U.S.)
President and CEO
East Bay Co., Ltd.

Henrik Torgersen (Norway)
Retired Executive Vice President
Telenor ASA

William Ury (U.S.)
Director
Global Negotiation Project
at Harvard Law School

Pierre Vimont (France)
Ambassador
Embassy of the Republic of
France in the United States

Alexander Voloshin (Russia)
Chairman of the Board of Directors
OJSC MMC Norilsk Nickel

Charles F. Wald (U.S.)
Former Deputy Commander
U.S. European Command

Bengt Westergren (Sweden)
Senior Vice President for Corporate &
Government Affairs, Europe and C.I.S.
AIG Companies

Igor Yurgens (Russia)
Chairman
Institute for Contemporary
Development

Zhang Deguang (China)
President
China Foundation for
International Studies

Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Marshall Bennett (U.S.)
President
Marshall Bennett Enterprises

John A. Roberts, Jr. (U.S.)
President and CEO
Chilmark Enterprises L.L.C.

J. Dickson Rogers (U.S.)
President
Dickson Partners, L.L.C.

Laurent Roux (U.S.)
President
Gallatin Wealth Management, LLC

George Sheer (U.S.)
President (retired)
Salamander USA & Canada
Founder & CEO
International Consulting Group, USA

CHAIRMEN EMERITI

Berthold Beitz (Germany)
President
Alfried Krupp von Bohlen und
Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California
at Los Angeles

Hans-Dietrich Genscher (Germany)
Former Vice Chancellor and Minister of Foreign Affairs of Germany

Donald M. Kendall (U.S.)
Former Chairman & CEO
PepsiCo., Inc.

Whitney MacMillan (U.S.)
Former Chairman & CEO
Cargill, Inc.

Ira D. Wallach* (U.S.)
EWI Co-Founder

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
Chief Executive Officer
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
Institute for Regional Cooperation
and Conflict Prevention
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

John W. Kluge (U.S.)
Chairman of the Board
Metromedia International Group

Maria-Pia Kothbauer (Liechtenstein)
Ambassador
Embassy of Liechtenstein
to Austria, the OSCE and the
United Nations in Vienna

William E. Murray* (U.S.)
Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International
Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates, Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg (Norway)
Former Minister of Foreign
Affairs of Norway

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead (U.S.)
Former Co-Chairman of Goldman Sachs
Former U.S. Deputy Secretary of State

* Deceased

EastWest Institute

Forging Collective Action for a Safer and Better World

Founded in 1980, the EastWest Institute is a global, action-oriented, think-and-do tank. EWI tackles the toughest international problems by:

Convening for discreet conversations representatives of institutions and nations that do not normally cooperate. EWI serves as a trusted global hub for back-channel "Track 2" diplomacy, and also organizes public forums to address peace and security issues.

Reframing issues to look for win-win solutions. Based on our special relations with Russia, China, the United States, Europe, and other powers, EWI brings together disparate viewpoints to promote collaboration for positive change.

Mobilizing networks of key individuals from both the public and private sectors. EWI leverages its access to intellectual entrepreneurs and business and policy leaders around the world to defuse current conflicts and prevent future flare-ups.

The EastWest Institute is a non-partisan, 501(c)(3) non-profit organization with offices in New York, Brussels and Moscow. Our fiercely-guarded independence is ensured by the diversity of our international board of directors and our supporters.

EWI Brussels Center
59-61 Rue de Trèves
Brussels 1040
Belgium
32-2-743-4610

EWI Moscow Center
7/5 Bolshaya Dmitrovka Str.
Bldg. 1, 6th Floor
Moscow 125009
Russia, 7-495-691-0449

EWI New York Center
11 East 26th Street
20th Floor
New York, NY 10010
U.S.A. 1-212-824-4100

www.ewi.info