Toward U.S.-Russia Bilateral Cooperation in the Sphere of Cybersecurity

THOMAS REMINGTON, CHRIS SPIRITO, ELENA CHERNENKO,
OLEG DEMIDOV & VITALY KABERNIK

Working Group Paper 7

MAY 2016

us-russiafuture.org

WORKING GROUP ON THE FUTURE OF U.S.- RUSSIA RELATIONS
РАБОЧАЯ ГРУППА ПО БУДУЩЕМУ РОССИЙСКО-АМЕРИКАНСКИХ ОТНОШЕНИЙ

Toward U.S.-Russia Bilateral Cooperation in the Sphere of Cybersecurity

THOMAS REMINGTON, CHRIS SPIRITO, ELENA CHERNENKO,
OLEG DEMIDOV & VITALY KABERNIK

Working Group Paper 7

MAY 2016

us-russiafuture.org

WORKING GROUP ON THE FUTURE OF U.S.- RUSSIA RELATIONS
РАБОЧАЯ ГРУППА ПО БУДУЩЕМУ РОССИЙСКО-АМЕРИКАНСКИХ ОТНОШЕНИЙ

Working Group on the Future of U.S.-Russia Relations

The Working Group on the Future of U.S.-Russia Relations convenes rising experts from leading American and Russian institutions to tackle the thorniest issues in the bilateral relationship. By engaging the latest generation of scholars in face-to-face discussion and debate, we aim to generate innovative analysis and policy recommendations that better reflect the common ground between the United States and Russia that is so often obscured by mistrust. We believe our unique, truly bilateral approach offers the best potential for breakthroughs in mutual understanding and reconciliation between our countries.

The Working Group is a project of the Davis Center for Russian and Eurasian Studies at Harvard University on the U.S. side and of the National Research University–Higher School of Economics in Russia.

The Working Group on the Future of U.S.-Russia Relations gratefully acknowledges the support of Carnegie Corporation of New York, and Mr. John Cogan toward the costs of Working Group activities, including production of this report.

The statements made and views expressed in this publication are solely the responsibility of the authors.

© 2016 Thomas Remington, Chris Spirito, Elena Chernenko, Oleg Demidov, and Vitaly Kabernik

Please direct inquiries to:

Working Group on the Future of U.S.-Russia Relations
c/o Kathryn W. and Shelby Cullom Davis Center for Russian and Eurasian Studies
Harvard University
1730 Cambridge Street, Suite S301
Cambridge, MA 02138
Phone: 617.496.5684
Fax: 617.495.8319
http://us-russiafuture.org

The full text of this report can be accessed at http://us-russiafuture.org/publications. Limited print copies are also available. To request a copy, send an email to info@us-russiafuture.org.

Contents

Executive summary

In recent years, the dynamics of international cooperation and conflict in the cyber domain have become the focus of intense interest on the part of national governments and expert communities around the world. Russia and the United States have often been at odds even in defining the nature of the problem: Russia emphasizes "international information security," whereas the United States believes that cybercrime, cyberespionage, and cyberterrorism are the main threats in this domain and so prefers the term "cybersecurity" and a focus on the protection of computer networks and resources. It is encouraging, therefore, that the two countries reached agreement in June 2013 on the need for cooperation over "threats to or in the use of ICTs [Information-Communications Technologies] in the context of international security." Subsequent events have inhibited further progress toward cooperation. In this working paper, we seek to outline some of the challenges as well as the opportunities for bilateral U.S.-Russia cooperation in the sphere of cybersecurity.

Cybersecurity poses certain unique difficulties where cooperation is concerned. Theories of strategic conflict and security drawn from the nuclear arms race do not carry over readily into the cyber domain. Some experts, for example, question whether doctrines of deterrence and verification of compliance with agreements are applicable to the cyber domain. The problem of attributing an attack to its source is far greater. An attack can be nearly instantaneous and without warning.

Moreover, the Russian and U.S. sides tend to approach the problem of cybersecurity from different perspectives. The Russian government generally emphasizes the principle of sovereign control over the entire information and communications domain. Russia regards cyberweapons as inherently first-strike weapons, useless if they are not used in the early stages of a conflict. The United States, in contrast, rejects "information security" as a foundational principle and champions the idea that the Internet should be "open, secure, interoperable, and reliable." The United States distinguishes between legitimate and illegitimate operations in the cyber domain; forms it considers illegitimate include espionage by governments and corporations to obtain commercial secrets and efforts by criminal (including terrorist) organizations to damage ICT infrastructure. It accepts that governments will conduct espionage in the interest of national security as well as operations to influence public opinion in target countries, even to the point of attempting to overthrow those countries' regimes. The United States, which favors international cooperation to prevent and defend against criminal attacks on critical ICT infrastructure and to ban commercially motivated espionage, has found common ground with Russia and other states in reaching agreements in these areas.

Both countries recognize the potential danger posed by cyberattacks to national infrastructure, such as electric power grids, dams, water supply, sanitation, oil and gas extraction equipment, and telecommunications networks. The dangers of a large-scale and effective attack on critical infrastructure are thus extremely severe. For this reason, the cyber domain is not entirely virtual; it includes the physical and human infrastructure linked to it.

The Russian government is also concerned about the possibility that the U.S. government could interfere with the management of the core infrastructure of the Internet, even to the point of disrupting Russia's access to it. Although the reform of the ICANN (Internet Corporation for Assigned Names and Numbers) to take effect in mid-2016 will move ICANN's technical functions away from the U.S. government's stewardship and to a self-regulating, independent international body, Russia's concerns about the governance of the Internet may not be entirely allayed.

We believe that these characteristics of the cyber domain should be addressed both bilaterally and multilaterally. We offer six recommendations for bilateral U.S.-Russia cooperation in the sphere of cybersecurity:

a. agreement on an explicit definition of the thresholds for attacks on critical infrastructure such that an attack would trigger a counterattack using either cyber or other types of weapons;

b. agreement on the types of information that would be shared in the event of a cyberattack, for example along the lines of a response to a bio-weapons attack;

c. prohibition of automatic retaliation in cases of cyberattacks;

d. prohibition of attacks on elements of another nation's core Internet infrastructure;

e. joint evaluation of the Internet Core Governance (UIS, IANA, DNS RZM) infrastructure to assess whether stakeholders feel that their interests and contributions are being given adequate consideration following the reform of ICANN's governance; and

f. broader international discussion of cybersecurity beyond the bilateral U.S.-Russia framework, for example under the auspices of the UN Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE).

For the longer-term future, we believe a formal, binding international treaty is needed to ensure full compliance with these norms. The bilateral norms we propose can serve as a model for such a multilateral agreement.

Historical Background

In recent years, the dynamics of international cooperation and conflict in the cyber domain have become the focus of intense interest on the part of national governments and expert communities around the world. Cybersecurity is one of the subjects on which Russia and the United States have held extensive negotiations—some frustrating, others fruitful. The disagreements between the United States and Russia start at the conceptual level. The United States and its allies believe that cybercrime, cyberespionage, and cyberterrorism are the main threats in this domain, so they use the term "cybersecurity" and focus on the protection of computer networks and resources. Russia is concerned with these threats as well, but also very much with content issues: Moscow is worried about the use of new technologies to wage information warfare and destabilize regimes. Therefore Russia, like some other countries (China among them), stresses sovereignty over the information domain so as to deny a potential adversary the ability to conduct offensive operations inside the country. Consequently Russia usually speaks of "international information security" and puts an emphasis on political and ideological confrontation in cyberspace.[1] The difference in approaches blocked agreement on the very definition of the problem.[2]

Cybersecurity is one of the subjects on which Russia and the United States have held extensive negotiations—some frustrating, others fruitful.

Nonetheless, notwithstanding these differences, Russia and the United States finally reached agreement on terminology that permitted them to sign on June 17, 2013, a major agreement at the G-8 summit meeting in Northern Ireland that covered "issues of threats to or in the use of ICTs in the context of international security."[3] The two countries agreed to:

a. establish a direct, secure voice communications link between Moscow and Washington to be used in case of security threats involving ICTs; in effect, this authorized direct contact between Russia's Federal Security Bureau (FSB) and the U.S. Central Intelligence Agency (CIA) over cyberthreats;

b. allow the nuclear "hotline" (the U.S.-Russia Nuclear Risk Reduction Centers) to be used for communications about cyberthreats, including warnings about upcoming cyberexercises or ongoing cyberattacks; and

c. envision coordination between the two countries' Cyber Emergency Response Teams (CERTs)—that is, the teams of specialists who investigate and address attacks on critical ICT infrastructure.

---

[1] The Russian Foreign Ministry's concept paper for a convention on international information security may be found at http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument.

[2] We provide a glossary of cyber-related terminology in Appendix A.

[3] Oleg Demidov, "U.S.-Russian CBMS in the Use of ICTS: A Breakthrough with an Unclear Future," *Security Index*, vol. 20 nos. 3–4 (108–9) (2014), pp. 69–80.

Shortly after this agreement was signed, the revelations about massive U.S. surveillance of telephone and Internet communications of citizens and governments around the world began to be released by Edward Snowden, formerly an employee of a contractor working with the U.S. National Security Agency. Shortly after the United States indicted Snowden, the Russian government granted him asylum. Both developments dampened interest on the part of the U.S. and Russian governments in further cooperation in the cyber area.

Further exacerbating the relationship, after the overthrow of the Russian-backed Yanukovych government in Ukraine in early 2014, the Russian government acted to make Crimea a Russian federal subject and to begin providing support for separatist rebels fighting the Ukrainian government in Ukraine's eastern *oblasts*. The United States and its allies responded by imposing economic and financial sanctions against Russia. U.S.-Russia relations fell to their lowest level in decades. The United States suspended discussions with Russia over cybersecurity-related issues. Neither side, however, sought to abrogate the 2013 agreement.

The term "cyberwarfare" covers multiple forms of potential conflict—an interstate war fought in cyberspace, an interstate war employing cyberweapons in addition to other types of weapons, and malicious attacks in the cyber domain falling short of outright war.

Despite the obvious obstacles to cooperation in the cybersecurity domain, the members of this working group believe that here, as in other areas that we have identified in past years, both countries can benefit from agreeing on certain basic rules. We believe it is possible and desirable to build on the 2013 agreement and reestablish cooperative relations with a view toward preventing catastrophic damage to the national ICT infrastructures of the two countries. We recognize, of course, that each side fears that sharing information about vulnerabilities in its ICT infrastructure may allow an adversary to exploit such a vulnerability for an offensive operation. Therefore meaningful cooperation will require agreement on the nature of the information to be shared before and after suspected attacks.

Can we learn any useful lessons from the experience of bilateral cooperation in controlling and reducing the nuclear arms race? The nuclear arms race has been curbed by a series of agreements beginning with the Test Ban Treaty signed by Soviet leader Nikita Khrushchev and President John F. Kennedy in 1963 and continuing through the ABM, SALT, and START agreements. These agreements are associated with commitments that are verifiable through "national-technical means"—particularly satellite imagery—and via onsite inspections. Verification of compliance rather than trust underpins observance of these treaties by the two sides. As in the Prisoner's Dilemma, it is in the interest of each side to cooperate so long as there is a means to ensure that the other side is also cooperating. Of course, each side recognizes its self-interest in avoiding the risk of a military confrontation that could result in a nuclear conflict. Therefore the capacity to launch a crippling second strike reinforces mutual deterrence through the reality of mutual assured destruction. The combination of mutual deterrence and verification of commitments helps to maintain stability in the nuclear arms competition. Since the 1970s, both sides have recognized strategic stability in the nuclear realm as a desirable outcome.

Many observers, however, emphasize the differences between security in the cybersphere and security in the area of nuclear weapons. First, the term "cyberwarfare" covers multiple forms of potential conflict—an interstate war fought in cyberspace, an interstate war

employing cyberweapons in addition to other types of weapons, and malicious attacks in the cyber domain falling short of outright war. In this report, we treat espionage as falling short of warfare.

Some experts argue that in the sphere of cybersecurity, unlike that of conventional or nuclear weapons, neither verification of compliance with agreements nor deterrence is possible.[4] Verification of compliance with agreements over cybersecurity is impeded by the extreme difficulty of tracing the source of an attack. Some argue that accurate and timely attribution of responsibility for a cyberattack is impossible or next to impossible, and certainly impossible in real time. For example, even if an attack can be traced to a particular IP address, it may be difficult to identify which computer was using the IP address, let alone the operator of the computer. This basic fact raises the concern that states may respond to a perceived cyberattack with a counterattack in another form. That is, a country under cyberattack might respond with conventional or nuclear force. Increasingly, military planners on both sides regard cyberwar as a likely element of a "hybrid war" involving clandestine and guerrilla elements and deniable attacks on the enemy's communications networks.[5] Because the United States and Russia have reserved the right to respond to cyberattacks as if they were conventional acts of aggression, a cyberattack, whether as a standalone event or an element of a hybrid war, could have catastrophic consequences through escalation.

Moreover, it is far from inconceivable that a malicious hacker representing a criminal, terrorist, or national entity might attack critical infrastructure of the United States by capturing servers in a third country. If the United States were under attack from servers based in Russia, would the United States consider it likely that the Russian government had sponsored the attack? How would the United States respond? The successful use of the Stuxnet worm against Iranian nuclear centrifuges demonstrates that cyberweapons exist, are used, are effective, and are hard to attribute to a source. If governments were to agree to the "responsibility rule" proposed by Eneken Tikk, which states that "the fact that a cyber attack has been launched from an information system located in a state's territory is evidence that the act is attributable to that state," countries would be held responsible both legally and militarily for attacks emanating from their territories. This norm would in turn place pressure on the state hosting the attack to assist in stopping it and apprehending those responsible.[6]

While many believe that verification of compliance in cyberspace is not possible, tactics, techniques, and procedures exist that allow an organization to approach this problem. Indicators that are collected have multidimensional pivot points that create classifiable sets of actor-attributed behaviors. This works in two ways. First, it allows cyberdefenders to create threat actor sets and tag to them exclusive or shared behaviors. Second, it allows threat actors working within internationally accepted norms of behavior (such as nation states' conducting computer network exploitation and intelligence collection) to embed in

---

[4] Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Forum* 77, 2015, pp. 8–15.

[5] On the way military planners in Russia and the United States understand—and frequently misuse—the concept of "hybrid warfare," see Samuel Charap, "The Ghost of Hybrid War," *Survival* 57:6 (December 2015–January 2016), pp. 51–58.

[6] Eneken Tikk, "10 Rules for Cyber Security," *Survival* 53:3 (June–July 2011), pp. 119–32.

their indicators a set of shared attributes that mitigate the potential for conflict over hostile attacks in cyberspace. This technical scheme for "watermarking" was described by Dave Aitel in his CyberSecPolitics post as follows:

> Significant intrusions get analyzed by teams of experts when they are discovered. But of course, signs of intrusions are being looked for by automated systems all the time. Our goal is to create a system that is detectable by a team of experts, but not by an automated system. An extremely robust system will be detectable just from an incident response report, without any access to the raw intrusion data at all, which has some political advantages.[7]

This approach would allow verification of compliance with an agreement that any activities will be appropriately watermarked or tagged. Of course, many will argue that threat actors have no incentive to be honest all the time, a fact that makes compliance verification unlikely. This, we would argue, is to be expected, as the development of trust takes time. We would also expect that any agreement which ultimately produces no indicators of attack or compromise would be an indicator that an actor generating a threat is indeed acting outside of the compliance agreement.

Given the uncertainty over the effectiveness of a deterrence-based regime, more and more national governments recognize the value of establishing certain rules of behavior that could reduce the onset, escalation, and destructiveness of cyberwarfare and that would deepen cooperation in protecting the Internet from criminal or terrorist attacks. These considerations helped to motivate the UNGGE to produce a consensus report to the UN Secretary-General on June 26, 2015. The UNGGE, comprising senior ICT specialists of twenty national governments, including Russia and the United States, agreed unanimously on several points, among them[8]:

a. states should cooperate to prevent harmful use of ICTs;

b. states should prevent the use of their territories for such purposes;

c. states should exchange information about the use of ICTs for criminal activity and terrorism;

d. the use of ICTs to attack critical Internet infrastructure (CI) is extremely dangerous, not only for the country attacked but also for the entire world because of the global integration of the Internet;

e. ICT attacks can be very rapid and are hard to attribute; and

f. countries whose own Internet infrastructure is poorly protected pose a threat to the entire global community.

---

[7] http://cybersecpolitics.blogspot.com/2016/03/a-technical-scheme-for-watermarking.html.

[8] "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations General Assembly, A/70/174. The text may be accessed at http://www.csistech.org/blog/2015/8/27/un-publishes-latest-report-of-the-group-of-government-experts.

Agreement on these points at the fourth round of negotiations by the UNGGE represented a signal success. For the first time, the group was able to produce a strong consensus report that outlined the need for drawing up norms of responsible behavior of states in cyberspace. A notable principle of the agreement is the idea that the law of armed conflict (LOAC) applies to the realm of cybersecurity.[9] The practical suggestions of the report include norms to ensure the protection of critical infrastructure, the protection of cyberincident response teams, and cooperation between states in responding to appropriate requests in mitigating malicious cyberactivity emanating from their territories. For example, in the event of an attack against a U.S. or Russian system originating from a site in the other country, an appropriate response would be for the victim (through its national Computer Emergency Response Team [CERT]) to contact its counterpart in the other country to request a detailed response, for example: *"We believe a cyber attack on System X originated from System Y (IP address: aa.bb.cc.dd), which is within your IP space. Would you please tell us if you have any evidence of this attack that we could analyze together?"* Under the agreement, each side would then exercise the right to narrowly penetrate the ICT space of the presumed attacker to attempt to neutralize the attack. A test of agreement robustness would be whether the two actors jointly conducted the probe (analysis) and neutralization of the cyberthreat. Finally, consistent with the extension of the Wassenaar Arrangement (an international effort to prevent the export of "dual use" technologies) into the cyber domain, another recommended norm would call on states to prevent the proliferation of cyberweapons that could be used for egregiously malicious and nefarious purposes.

The 2013 bilateral agreement between Russia and the United States and the 2015 UNGGE agreement indicate that the United States and Russia, together with other leading countries, recognize the dangers posed by threats to cybersecurity and the benefit of establishing agreed-upon norms and practices to reduce the risk of unwanted conflict. This suggests that, as in other areas of national security, the cyber domain is one wherein certain rules can be agreed on to govern the behavior of sovereign states in ways that benefit their own national interests.

The United States and Russia, together with other leading countries, recognize the dangers posed by threats to cybersecurity and the benefit of establishing agreed-upon norms and practices to reduce the risk of unwanted conflict.

[9] The way LOAC applies to the cyber domain is so far best described in the "Tallinn Manual" published by the NATO Cooperative Cyber Defence Centre of Excellence in 2013 (although this is not an official NATO document). The product of a three-year project by twenty renowned international law scholars and practitioners, the "Tallinn Manual" identifies the international law applicable to cyberwarfare and sets out ninety-five "black-letter rules" governing such conflicts. It addresses topics including sovereignty, state responsibility, the *jus ad bellum*, international humanitarian law, and the law of neutrality. Russian experts have voiced criticism of many points of the manual but have so far not produced an alternative view on the subject.

Assessing the Prospects for U.S.-Russia Cooperation

The Russian government generally emphasizes the principle of sovereign control over the entire information/ communications domain.

Both the 2013 bilateral agreement and the 2015 UNGGE agreement required the establishment of depoliticized norms that could apply to all states. Yet, although both represent significant steps forward in international cooperation in cyberspace, the fact that these norms are voluntary and declarative—lacking enforcement mechanisms—mitigates their effectiveness. They are statements of principle, but they lack binding means of ensuring compliance. We believe that effective agreements in the cybersecurity field must be enforced by the combination of mutual verification of compliance plus mutual deterrence that has operated for more than fifty years in the area of nuclear weapons. Agreements on general principles are necessary but not sufficient to this end. Therefore we believe that a formal agreement is preferable to soft law or flexible norms. We are convinced, however, that narrowly delineated measures to enhance cybersecurity are possible. We identify six such areas of possible agreement that would be applicable during peacetime:

a. agreement on definitions and thresholds of critical infrastructure such that an attack would trigger a counterattack using either cyber or other types of weapons;

b. agreement on the types of information to be shared in the event of a cyberattack;

c. agreement on a ban on automatic retaliation in the event on a cyberattack;

d. agreement on a norm to refrain from attacks on the core Internet infrastructure of another nation;

e. greater transparency and verification of the management of the Internet's core infrastructure; and

f. agreement on the desirability of international discussion of cybersecurity issues, for example under the auspices of the UNGGE.

Below we discuss these potential points of agreement in more detail. First, however, we must consider the differences in the ways in which Russia and the United States approach cybersecurity.

The Russian government generally emphasizes the principle of sovereign control over the entire information/communications domain. This concern is reflected in the agreement between Russia and China signed on May 8, 2015.[10] The two sides agreed that the foundational principle for cooperation is information security, which refers to the defense of each state against attacks on its social, political, economic, and cultural stability. The agreement defined "information security" as protection of individuals, society, and the state from threats and destructive influences in its "information space." It also included a provision prohibiting either side from using "information resources" to attack the other, amounting to a cyber "non-aggression pact."[11] The agreement also calls for cooperation through the exchange of information and research findings.

Formally, at least, the United States rejects the concept of "information security" as a foundational principle. Rather, the U.S. government's concept (as reflected in the 2015 Defense Department statement on cybersecurity) is that "the United States is committed to an open, secure, interoperable, and reliable Internet that enables prosperity, public safety, and the free flow of commerce and ideas."[12] Similarly, a recent Council on Foreign Relations (CFR) report laid out a set of principles that are broadly accepted by the U.S. political establishment. The report proceeds from the premise that the Internet should be "open, global, secure, and resilient."[13] "Openness" refers to maximum public access to the Internet and minimal censorship and interference by government; "global" implies opposition to the fragmentation of the Internet into multiple national intranets; "security" refers to states' ability to defend against attacks; and "resilience" means the capacity of communications networks to survive malfunctions, breakdowns, and attacks. The U.S. view, reflected again in the CFR report, is that governance of the Internet should be carried by both governments and private companies in a "multi-stakeholder" conception of shared interest. The report cited the danger that efforts by governments to defend the security of their national domains against real or perceived threats from abroad could end in the imposition of draconian content controls, localization laws, and even the hiving off of national domains into separate self-contained Internets. The United States regards it as important to maintain the self-regulating, decentralized, distributed character of the Internet. Of course, as experts now recognize, it was the priority of those principles over security that resulted in the vulnerabilities to disruption that have now been so clearly revealed.[14]

The United States regards it as important to maintain the self-regulating, decentralized, distributed character of the Internet.

---

[10] http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html. The Russian text of the agreement may be found at http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf.

[11] http://blogs.cfr.org/cyber/2015/08/20/the-next-level-for-russia-china-cyberspace-cooperation/.

[12] The U.S. Defense Department issued a cyberstrategy doctrine in April 2015: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, p. 1 (henceforth referred to as DOD Cyber Strategy).

[13] Council on Foreign Relations, "Defending an Open, Global, Secure and Resilient Internet," Independent Task Force Report No. 70, 2013.

[14] An important example is the risk that Internet traffic can be hijacked by manipulating the Border Gateway Protocols (BGP) that operate as decentralized dispatchers of data across the Internet. Their effectiveness relies on the willingness of all interlinked networks to share information about the availability of data links. An accidental or deliberate disruption to the BGPs could allow all Internet traffic to flow to one particular national network, either overwhelming it and shutting it down or enabling a hostile government or organization to disrupt traffic across the entire system. See the series of investigative reports by Craig Timberg, "Net of Insecurity," in the *Washington Post* from May 30 to November 5, 2015.

Is the U.S. position contradicted by its behavior in the cyber domain? Documented U.S. actions include large-scale monitoring of domestic and international communications to gather intelligence,[15] covert operations to influence populations (such as the Zun Zuneo social media network run by USAID in Cuba[16]), and influence over U.S. telecommunications and social media operators to further U.S. policy goals (as when the United States asked Twitter not to take its network down for maintenance during Iran's "Green Revolution"[17]). The United States distinguishes between legitimate and illegitimate operations in the cyber domain; forms it considers illegitimate include espionage by governments and corporations to obtain commercial secrets and efforts by criminal (including terrorist) organizations to damage ICT infrastructure. It accepts that governments will conduct espionage in the interest of national security as well as operations to influence public opinion in target countries, even to the point of attempting to overthrow their regimes. The United States favors international cooperation to prevent and defend against criminal attacks on critical ICT infrastructure and to ban commercially motivated espionage, and it has found common ground with Russia and other states in reaching agreements in these areas.

As noted above, the divergence in approaches between Russia and the United States accounts for the fact that it took the two countries a year and a half to reach agreement on compromise wording for the very subject of a bilateral agreement whose substance had already been accepted. The same divergence of perspectives also has blocked agreement over the role of the International Telecommunications Union (ITU) with respect to Internet governance. At the ITU world conference in December 2012, the United States opposed granting the ITU the power to regulate the Internet. Some eighty-nine countries—Russia among them—signed the agreement giving the ITU such power; fifty-four countries joined the United States in opposing it. This was not surprising given that the ITU asked Kaspersky Lab (a Russian cybersecurity company) to provide it with an analysis of Flame (a non-attributed U.S. malware suite), thus supporting the U.S. view that giving ITU a governance role could be problematic for the United States in years to come.[18] The result is that one set of international telecommunications regulations binds the United States and those supporting its position, while another set of regulations applies to Russia and the others.

On the other hand, although the United States opposes granting the ITU regulatory powers over the Internet, it does support multilateral practical cooperation in fighting the abuse of Internet technology for criminal purposes. The United States is a signatory to the Council of Europe's Convention on Cybercrime, known as the Budapest Convention (signed in 2001). The Budapest Convention obliges countries to investigate and prosecute computer-mediated crimes, which the Convention defines as criminal activity. The Convention has been ratified by thirty-nine countries—many outside Europe—but not by Russia or China.

---

[15] http://www.politico.com/story/2015/05/nsa-phone-data-collection-illegal-court-ruling-117725.

[16] http://www.slate.com/blogs/the_world_/2014/04/03/zunzuneo_the_u_s_government_s_bizarre_and_ill_advised_plan_to_build_a_fake.html?wpisrc=burger_bar.

[17] http://www.washingtonpost.com/wp-dyn/content/article/2009/06/16/AR2009061603391.html.

[18] http://www.cyberdialogue.ca/2012/05/cyber-intrigue-the-flame-malware-international-politics.

Both governments regard cooperation in fighting cybercrime as threatening a potential loss of sovereignty, because it allows transborder access to stored computer data without the authorization of another party. Russian accession to the Budapest Convention might allay suspicions that the government tacitly condones cyberattacks on other countries conducted from its territory (as in the case of the wave of concerted attacks on Estonian ICT infrastructure in April 2007).

Cyberattacks, Cyberweapons, and Cyberwarfare

The prospect of cyberwar and of the use of cyberspace for military purposes is relatively new to both Russian and U.S. military planning. The armed forces of both countries have established doctrines governing offensive and defensive operations in cyberspace, recognizing the cyber domain as forming part of a larger set of potentially militarized domains in which armed conflict can occur, including land, sea, and air.[19] A significant point of debate in both countries is how comprehensive national cybersecurity responsibility should be. Whether the government should be required to defend private companies against attacks from foreign sources is a question that has become acute in the United States owing to multiple attacks on financial institutions and business corporations (such as Sony Pictures). These attacks can be extremely costly: Kaspersky Lab estimates that over a two-year period, a criminal gang stole $1 billion from financial institutions worldwide.[20]

Both countries' militaries also recognize the potential danger posed by cyberattacks on national infrastructure, such as electric power grids, dams, water supply, sanitation, oil and gas extraction equipment, and telecommunications networks. Even if these systems are not directly connected to the Internet, the Supervisory Control and Data Acquisition (SCADA) devices that are used to control them remotely by secure communications links could be compromised by an attack on the facilities using them. The dangers of a large-scale and effective attack on critical infrastructure are thus very real. For this reason, the cyber domain is not entirely virtual; it includes the physical and human infrastructure linked to it.

Above we observed that both similarities and differences exist between the nuclear arms race and the threat of cyberwar. One difference is that proliferation of cyberweapons is far easier than the proliferation of nuclear weapons. Measures to check nuclear proliferation have, so far, had some success in slowing the spread of nuclear weapons technologies and materials and represent an area in which Russia and the United States have had some successful cooperation. Another difference lies in the relative advantage of first-strike capability. In the nuclear arms race, the threat that one side could deliver an incapacitating counterforce first strike was always offset by the prospect that some second-strike capability would be used by the attacked side. This doctrine underlay the efforts by both sides to harden their land-based missile sites and to diversify their weapons across land, sea, and air. In the cyber domain, some believe, a first strike could be both faster than a nuclear first

---

[19] DOD Cyber Strategy. Russia first enunciated an information security strategy in 2000 and has since updated and supplemented it several times. In 2013 Russia adopted the "Foundations of State Policy of the Russian Federation in the Sphere of International Information Security through 2020." See http://www.scrf.gov.ru/documents/6/114.html. This has been further updated with documents in 2014 and 2015. These may be found at https://ccdcoe.org/cyber-security-strategy-documents.html.

[20] http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide.

strike and more lethal to the target's own capacity to respond. In this view, the temptation to strike first introduces a destabilizing element into the strategic balance. These experts believe, therefore, that the posture of mutual assured destruction does not apply to the cyberwarfare realm.

On the other hand, recent events, such as the theft of sensitive personnel files for more than 22 million people from the U.S. Office of Personnel Management, which the U.S. government traced to China, reflect a long-term effort to gather intelligence on U.S. government and military personnel rather than a crippling first strike.[21] Such espionage may yield a larger cumulative advantage for an adversary than would an overt effort to disrupt or destroy the adversary's ICT networks.

Regardless of the relative seriousness of the threat of a successful cyber first strike, as opposed to multiyear efforts to probe and exploit vulnerabilities in a target's ICT domain, experts on both sides agree that the weight of strategy should shift to improving defensive capabilities—the ability to prevent crippling attacks—and strengthening the resilience of core capabilities in the event of an attack. Taken to its logical extreme, this means that military planners might separate their national Internet domains from the global Internet in the face of an anticipated or real-time cyberattack. This would mean creating a separate Domain Name System (DNS) Root Zone Management capability—in effect, a separate national Internet or national intranet. In popular parlance, this would enable Russia to "turn off" the Runet in case of an emergency and use a backup system disconnected from the global Internet.[22] Experts indicate that Russia is exploring the possibility of cooperation with other BRICS members in creating such a parallel capability.

Reinforcing Russia's fear that it might be subject to an attempt to gain control over the Runet for hostile purposes—for example, to foment a revolution or to deny Russia access to its own ICT resources—is the fact that the U.S. government, through the Department of Commerce's National Telecommunications and Information Administration (NTIA),[23] remains a party to the agreement with the Internet Corporation for Assigned Names and Numbers (ICANN) to maintain the databases that are crucial to the operation of the global Internet. Although the U.S. government ceded control of ICANN in 2009, the Commerce Department continues to be a party to the agreement with ICANN to manage the IANA (Internet Assigned Names Authority) through a series of short-term extensions to the original contract. The Russian fear is that the U.S. government could, in case of emergency, order ICANN, or the private commercial operator Verisign, which performs crucial technical functions for the DNS Root Zone, to acquire control over the Runet.

---

[21] Ellen Nakashima, "Officials: Chinese Had Access to U.S. Security Clearance Data for One Year," *Washington Post*, June 18, 2015.

[22] Alexandra Kulikova, "Top 8 Major Trends on the Russian Internet in 2014," *Russia Direct*, December 24, 2014, http://www.russia-direct.org/analysis/top-8-major-trends-about-russian-Internet.

[23] NTIA is the Executive Branch agency that is principally responsible for advising the President on telecommunications and information policy issues. NTIA's programs and policymaking focus largely on expanding broadband Internet access and adoption in America, expanding the use of spectrum by all users, and ensuring that the Internet remains an engine for continued innovation and economic growth. Source: NTIA Mission at NTIA website https://www.ntia.doc.gov.

The 2015 U.S. Defense Department statement on cyberdefense appears tacitly to assume that attribution problems can be solved using advanced forensics. It calls for the development of a deterrence capability based on the ability to respond to an attack, to defend successfully against an attack, and to survive an attack. The document does not explicitly state—indeed, it would foolish to do so—that the United States currently has the ability "to reduce anonymity in cyberspace and increase confidence in attribution."[24] The document instead says that the United States "requires" such capabilities and that it has "invested significantly" in them.

According to the U.S. Defense Department statement, the U.S. military has three principal missions in cybersecurity: defending its own systems, defending the country against significant cyberattacks, and providing support for U.S. military operations (including use of cyberweapons).[25]

Controlling the proliferation of cyberweapons is extremely difficult, but it is a worthwhile objective.

For Russia, the conception of cyberspace as a domain of warfare operates with a somewhat more expansive view of the mission. Cyberspace is viewed as a domain of all cybernetic devices, including both hardware and software, and their respective operators. The Russian military accordingly sees the hardware and infrastructure used to perform operations in cyberspace as a part of cyberspace. Likewise, the people who are servicing, operating, or otherwise involved with the operations performed in cyberspace are part of the cyber domain. Thus, significantly, the cyber domain is not viewed as completely virtual. It has physical and targetable entry points. Data centers, operators, and communication infrastructure are all viewed as legitimate targets to control cyberspace.

Therefore, linked telecommunications networks (e.g., the Internet) and cyberspace are not the same. Guidance and management systems like the fly-by-wire complex implemented in the fighter jet—including the pilot—are all viewed as parts of cyberspace, even if only on its margin. These systems are not connected to the Internet and will never be because of incompatibility of protocols. The same assumption works for SCADA systems physically disconnected from the Internet and possibly using a non–TCP/IP infrastructure. This multitude of devices, control systems, separate networks, and so on are all parts of cyberspace in the Russian view.

Moreover, the Russian military treats cyberspace as part of a seamlessly integrated and complex battle space. This battle space includes land, sea, and airspace, now with cyberoperations included. Incorporating cyberspace into the integrated field of war follows a straightforward logic. If one side lacks an advantage in one domain of the battle space, it will seek to exploit its advantage in another. In effect this means that the side that is losing in cyberspace may and will resort to other domains of warfare.

The models of escalation developed for Russian armed forces proceed from the assumption that the side which initiates offense in cyberspace will win the upper hand early on and that it will be difficult for an adversary to overcome such an attack. Passive defense will not suffice. Therefore the only effective means of deterrence and denial would be an early

[24] DOD Cyber Strategy, p. 11.

[25] DOD Cyber Strategy, pp. 4–5.

move to seize the initiave with a proactive and offensive move. If this assumption is valid, the escalation of a conflict involving cyberwarfare will be far faster compared with that of conventional warfare, and the time in which it will be possible to freeze or deescalate the conflict will be very limited.

Accordingly, in the Russian view, cyberweapons are explicitly created as first-strike weapons. If they are not used in early stages of conflict escalation, they will become essentially useless when the conflict evolves into classical warfare. In other words, cyberweapons are usable only for full-scale global warfare between similarly powerful states for the few first hours of engagement, until the communication networks are either disrupted or destroyed. Global reach and nearly instant reaction time are the primary characteristics for cyberweapons. These characteristics align cyberweapons with other types of strategic weapons.

Thus by this logic, even as states work to improve their defenses against rogue attacks, they are creating militarized cyberweapons capabilities in a process that is almost impossible to stop—much like the nuclear arms race. Controlling the proliferation of cyberweapons is extremely difficult, but it is a worthwhile objective. So, too, is the effort to define thresholds of damage that would trigger a military response. The U.S. Department of Defense Cyber Strategy Statement refers to the need to "defend the United States and its interests against cyberattacks of significant consequence." The president would make the final determination of what constitutes "significant consequence," but, according to the statement, it would include "loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States."[26] In the case of the attack on Sony Pictures attributed to North Korea in late 2014, the United States responded with what President Barack Obama termed "proportionate force." Proportionality of response is one of the laws of armed conflict that are accepted by the UNGGE. In this case, the United States publicly imposed further sanctions on several North Korean government officials and may have clandestinely but temporarily disrupted North Korea's access to the Internet.[27]

The Sony–North Korea incident raises two issues directly relevant to the question of international cooperation in cybersecurity: What is the threshold of damage to a country's national interests from a cyberattack at which a government is warranted in responding with military means, and how certain must a national government be about attributing the attack to a specific source before it retaliates against that government or organization? Some observers expressed doubts on both scores about the United States' actions in the Sony case, questioning both whether the attack on Sony represented a significant threat to vital U.S. national interests and whether the evidence that North Korea was the sponsor of the attack was firm enough to justify targeting it in response. The U.S. government held that the intelligence information on which it based its attribution determination was too sensitive to be released publicly, so the expert community cannot assess the government's claims. The United States and Russia might wish to apply to cyberwarfare a test derived from doctrines of escalation in kinetic warfare: that the threshold to using an offensive cyberweapon in response to a cyberattack must be very high.

---

[26] DOD Cyber Strategy, p. 5.

[27] https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html, http://www.wsj.com/articles/u-s-penalizes-north-korea-in-retaliation-for-sony-hack-1420225942.

Although we do not offer a judgment on either the threshold or attribution issue, we believe that the case helps to clarify the issues at stake. Bilateral and multilateral discussions on what constitutes vital national interests in the area of cybersecurity may help increase transparency in decision making about the use of cyberweapons. We believe that both Russia and the United States can agree that the core elements of the infrastructure of the Internet itself should be off-limits to cyberattacks and should be the subject of shared multistakeholder governance. Such an agreement should be a central element of a follow-up U.S.-Russia cybersecurity agreement.

A norm on sharing information about attacks should be a second core element of a follow-on agreement. Here a different model might be pertinent: Rather than compare cyberattacks to nuclear war, we might consider them as something more closely resembling a suspected bio-weapons attack. Following an outbreak of a suspected act of warfare or terrorism by a biological weapon, different elements of government typically respond in different ways. Law-enforcement agencies immediately seek to collect evidence for a criminal prosecution, classifying and withholding relevant information about the attack in order to prevent panic and deny the enemy any advantage from revealing vulnerabilities. Public-health authorities, on the other hand, seek as much openness as possible, sharing information in order to mitigate the consequences of the attack as much as they can. Their priority is not prosecution and punishment as much as it is containment and neutralization of an outbreak. Only once the outbreak has been stopped would it be appropriate to determine the source of the attack and to respond as needed. Public-health officials emphasize the need for a wider exchange of information about the spread of a deadly disease rather than its concealment.

Sharing sensitive information about vulnerabilities exposed by a cyberattack will require a certain level of trust. As in confidence-building measures in the realm of conventional and nuclear arms competitions, so confidence-building in the cyber domain may be based on regular exchanges of information among government and nongovernment specialists in rival countries. Mutual confidence may accumulate through the experience of exchanging accurate information about cyber activities over time. Track Two (i.e., unofficial) discussions among experts may play a useful role in this regard in complementing diplomatic channels.

In a similar way, if deterrence in the domain of cybersecurity cannot be firmly grounded in certain attribution of responsibility for attacks, nor in the threat of effective retaliation (because of the first-mover advantage),[28] then denial of strategic advantage to an attacker through investment in defense and resilience is more likely to be effective than deterrence through the threat of a counterstrike. This, therefore, prompts our third recommendation: that the two sides recognize that a "launch-on-warning" hair-trigger or automatic retaliation posture should be ruled out by both sides, in favor of a posture of denial through defense and resilience. Edward Snowden revealed one such program being developed by the United States called MonsterMind.[29] We oppose the use of such mechanisms for the reasons identified above. First, a cyberattack is likely to be disguised by being routed through third-party machines, such as an unwittingly infected botnet or third-party private or

[28] The first-mover advantage in game theory refers to the advantage accruing to the actor who makes the first move in the game.

[29] http://www.wired.com/2014/08/nsa-monstermind-cyberwarfare/.

public servers. An automatic response could therefore lead to military conflict with nations where such servers are located. Second, a counterstrike could well inadvertently visit collateral damage on bystander systems, such as critical civilian infrastructure. The concept of automatic retaliation therefore suffers from the same fundamental flaws as did the doomsday machine in *Dr. Strangelove*.

We therefore recommend that the two sides agree to share information about an attack rather than to conceal it.

Governance of the Internet's Global Infrastructure

"One of the major risks is purposeful disconnenction of Russia from the global Internet."

The fourth area of recommended agreement concerns the issue of governance of the technical infrastructure underlying the global Internet. Because ensuring the resilience of the Internet is a shared interest of Russia and the United States, the two countries recognize the importance of the stability, security, and resiliency (SSR) of the Internet's Unique Identifiers System (UIS) and management of critical business processes related to its operation.

These issues have never been the part of the cybersecurity agenda in its usual understanding, nor they are part of the U.S.-Russia bilateral security track at the moment. However, both countries have a significant stake in this field. Moreover, without constructive dialogue, potential developments in this area might affect both ordinary operations of the Internet for core communications and economic needs and even the integrity of the global Internet.

As noted above, the United States historically has had a unique relationship with the technical bodies that are responsible for operation of this infrastructure on a global level, including ICANN and its technical department IANA. International and domestic U.S. debate on the U.S. government's role in oversight of the functions of these technical bodies has significantly intensified over the past several years, especially after Edward Snowden's revelations, though they were not related directly to the Internet's global infrastructure. In March 2014, the IANA Oversight Transition Process was launched, the purpose being to enable passing over the oversight of certain critical functions in this field from the U.S. government to the global multistakeholder community. ICANN will essentially become self-governing.[30] The new model was approved at the March 2016 meeting of ICANN in Marrakech and is due to take effect by fall 2016.

From Russia's standpoint, beginning in 2014 the issue of ensuring stability and security of the national segment of the Internet's infrastructure has moved to the forefront of its national security agenda for a number of reasons. In July 2014 the first truly large-scale cybertraining was conducted by the Russian ICT Ministry with the participation of the Federal Security Service; the Federal Protective Service; the Ministry of Defense; the Ministry of Internal Affairs; Russia's largest ISP, Rostelekom; RU/.РФ registry CCTLD; and Russia's largest Internet Exchange Point (IXP),[31] MSK-IX. This cybertraining was a milestone, first, because of its scale and the range of federal bodies involved, but also because of the models of threats that were tested over its course. Some of the threat models

[30] "We the Networks," *Economist*, March 5, 2016.

[31] IXPs are the physical points through which networks exchange information.

were not typical for the international—namely, Western—cybertraining practices. According to an interview with Igor Shchegolev, an aide to President Putin, to the Expert Center of the E-Government online portal, dated October 17, 2014, one of the models of threats at the cybertraining implied disruption of the operation of the Russian segment of the Internet's global infrastructure as a result of "hostile external actions." This wording actually might be used for cyberattack on the Runet's infrastructure, such as DDoS attacks on the DNS servers, DNS amplification attacks, DNS servers cache poisoning[32], disrupting routing between networks through information injection, and the like.

Public discussion of the cybertraining and the interview with the president's aide had a very clear and strong focus on vulnerability of the Russian segment of the Internet's infrastructure as a consequence of the fact that the global Internet's infrastructure is *de facto* managed by foreign nation-states, namely the United States. "Hostile external actions" from this viewpoint might be something very different from cyberattacks on infrastructure. As Shchegolev put it, "One of the major risks is deliberate disconnection of Russia from the global Internet." In the next sentence he stressed that on a global level the Internet is still managed by the United States.

In October 2014, Russia's Security Council held a closed session dedicated to ensuring stability, security, and resiliency of the Runet in light of the cybertraining held in July. After the session, the head of the Russian ICT Ministry, Nikolay Nikiforov, stated that Russia will seek collaboration with its BRICS partners, for the sake of developing, installing, and overprovisioning some reserve critical infrastructure for Russia's national segment of the Internet. In later publications and expert discussions in the Russian media it was suggested by some experts that the prime goal of these arrangements should be to ensure backup technical capacities for the Russian segment of DNS in order to enable its autonomous operation in case of a major crisis.

This agenda has also triggered further activities carried out by the Ministry of Communications and Mass Media and other Russian governmental regulators. In March 2015, major Russian media disseminated the news that Minister Nikiforov was going to present to the government a confidential report containing a set of proposals aimed at strengthening resiliency and ensuring sovereignty of the Russian segment of the Internet. Most of these proposals were reported to be focused on tightening governmental control over certain segments of the Runet's critical infrastructure, including major IXPs' enabling transborder exchange of the traffic of Russian operators. Among those, one IXP—MSK-IX—plays a particularly important role in enabling transborder exchange of a major share of the Runet's traffic. Alongside MSK-IX, two other entities were reported to have crucial roles for resiliency and robustness of the Russian Internet's segment: Coordination Center for TLDs .RU/.РФ (administrator of the Russian TLDs [Top Level Domains]) and the Technical Center of the Internet (TCI), a technical body providing backbone services to the registries and running the domain registration services of Russia's national domains, closely related to the Coordination Center. Notably, the major motivation for focusing the state's

[32] I.e., contamination with malware.

efforts on achieving these aims was claimed to be "protection of the Runet from external attacks and hostile impacts." However, no public updates on the status of the report and its presentation have been made since then.

Most recently, in October 2015 the head of a Russian Internet provider, ER-Telecom, told the media about an experiment reportedly conducted by the Ministry of Communications and Roskomnadzor in April 2015 and aimed at modeling a cutoff of Russia from the global Internet as a result of some "external actions." According to the media, Russian providers blocked traffic streamed to major channels connecting the Runet with the global network, following the instructions from the Ministry and using Deep Packet Inspection (DPI) equipment. However, the experiment failed because of minor Russian providers: Because they lacked installed DPI equipment and used diversified channels, including satellites, the transborder traffic was still flowing through their networks, maintaining the Runet's connection with the global Internet. It should be added that information about the experiment was denied by Russian federal bodies and described as a "total misinterpretation" of their real activities.

In spring 2015, at a *Track 2* international meeting on information security, a high-level Russian official made a surprising statement. According to the official, if the United States does not make steps toward internationalization of the global Internet governance mechanism, Russia could hypothetically launch with its allies certain forms of collaboration that might result in the development of an autonomous transnational network that would be independent of the global Internet on key infrastructure layers. Ultimately, that would mean fragmentation of the global Internet, which, as the speaker admitted, would have a large negative impact on transborder Internet-enabled services, business processes, and the global digital economy. However, the speaker also stressed that such a move in theory could create massive benefits in terms of security, stability, and protection against cyberattacks and electronic surveillance for those states that would switch to the new autonomous network. Moreover, today's cybersecurity concerns together with the drawbacks of current Internet governance architecture could make this scenario an "inevitable evil." In effect, that was a manifesto of what is usually called fragmentation of the Internet—architectural decomposition of the global net into several (or many) half or fully autonomous and independent segments.

Historically, the development of the Internet, the Internet governance mechanisms, and the Internet's infrastructure resulted in a unique model of the Internet's Unique Identifiers System (UIS).[33] On a global level, secure, stable, and resilient operation of UI system is the responsibility of a technical structure—the Internet Assigned Numbers Authority (IANA). IANA is not even a legal entity but a technical department of another structure—ICANN. ICANN, which is a noncommercial corporation registered in the state of California, is a party to the contract for IANA functions operation. To date, the other side of the contract is the U.S. government, represented by NTIA. The contract in fact reaffirms and fixes the longstanding status quo when IANA runs a number of critical business processes enabling the Internet's UIS operation under the U.S. government's oversight.

---

[33] A more detailed discussion of the Internet's Unique Identifiers System (IUS) may be found in Appendix B. Appendix C is a schematic organizational chart of Internet governance.

One of the most important business processes is the DNS Root Zone Management process (RZM). The DNS Root Zone Management is a critical process for the stability, security, and resiliency of the UI system, and for the moment, it involves several responsible parties:

a. IANA functions operator, currently represented by ICANN. The operator receives, reviews, and processes Root Zone file change requests, performs technical checks, notifies operators of completion of requests, and implements changes to the Root WHOIS database.

b. An administrator, currently (before the NTIA stewardship completion) represented by NTIA. The administrator verifies the process, procedures, and policies followed by the IANA functions operator, authorizes the maintainer to implement Root Zone file changes requested by TLD operators, and authorizes the IANA functions operator to implement WHOIS database changes.

c. Root Zone maintainer, currently represented by Verisign. The Root Zone maintainer implements changes to the Root Zone File/conducts generation of updated Root Zone file and also conducts its distribution to the DNS authoritative Root Servers operators.

The Root Zone management process includes several stages, such as sending the change request by a TLD operator to IANA, processing the request by IANA and sending it for review and approval to NTIA, and approval of the request by NTIA and sending it to the Root Zone maintainer: Verisign. The RZ maintainer performs technical operations within the framework of the business process: Verisign generates the updated Root Zone file on its hidden primary master server, and then it distributes the generated RZF to the thirteen secondary authoritative root servers named in Latin from A to M. These servers together constitute the infrastructure of the DNS Root Zone, the highest global level of the DNS hierarchy.

The RZF contains information on all TLDs and IP resources related to them. Changing this data in the RZF would result in changes in the global domain name space. In the context of the cybertraining in Russia in 2014 and the model of threats analyzed, one of them in theory might include deletion of the information on TLDs .RU/.РФ from the RZF. After the cache on the DNS Root servers expires, resources in these TLDs would become unavailable for users both in Russia and the world over. The only way to access these resources would be by their IP addresses, which would certainly be extremely inconvenient for every category of users.

What are the problems with the institutional mechanism of the DNS Root Zone management that have been fueling Russian concerns and that came into focus with the cybertraining of 2014 and the following session of the Russian Security Council?

First, they are not about technical parameters of the system as such. Even tough opponents of the IANA and the U.S. government–supported model of the Internet's global infrastructure operation admit that the infrastructure of the DNS Root Zone and Number Resource system is distributed, overprovisioned, and resilient enough to withstand even the most sophisticated and massive attacks. Today, almost every DNS root server is mirrored in

multiples copies over the world—for example, ICANN-operated root J has more than 150 mirrors on all continents except Antarctica. The infrastructure of the global IP allocation system is also distributed among five Regional Internet Registries (RIRs), each of which is responsible for its region (including Antarctica)—and there are actually RIRs, not IANA, that control the assignment of IPs and Autonomous System Numbers (ASNs)[34] to ISPs and other entities. Some RIRs also develop and enforce usage policies.. Finally, the track record proves that, except for some incidents in 2002, there have been no cases of malicious actions such as cyberattacks causing massive disruption to the operation of the DNS or the Number Resources infrastructure. Of course, there are certain flaws with the DNS protection against DDoS (or use of the DNS itself for leveraging DDoS traffic through amplified DNS responses); there are serious flaws with security of the global routing system that is based upon the Border Gateway Protocol (BGP),[35] a protocol in which security was not an integral part of its design. In the final equation, however, everyone, including Russia, China, and other nation-states, accepts that the Internet's UIS is very resilient and robust.

From the standpoint of national security and strategic stability, the U.S. government has legal powers that hypothetically might be used to disrupt Russia's access to the global Internet—or to isolate the Runet segment from the global Internet.

So, from Russia's standpoint, the fundamental problem with the current governance system has not been not technical perfection of the Internet's UIS but rather a deep-rooted mistrust in the business processes run by the operators of the critical technical business processes. A real threat to the Russian national segment of the Internet in the eyes of the Russian Security Council and other national security bodies are not hackers breaking into DNS Root Servers and erasing data on Russian TLDs (.RU/.РФ) from the Root Zone file copies but NTIA and the U.S. Federal Court twisting ICANN's arms through governmental directives and orders and making IANA do so. This threat scenario is based on the perception that IANA as well as other operators of global Internet infrastructure under certain circumstances might not be able to remain unbiased and independent from the U.S. government. For example, in case of a political crisis, like an early stage of transition to war, the U.S. government might directly—formally or informally—order ICANN or Verisign to implement certain technical operations in order to attempt to disrupt Russia's connectivity to the global Internet.

For the moment, no information is available about precedents that would indicate when the NTIA would ever disapprove ICANN's request for an update of the RZF. Likewise, no precedents are known for the U.S. government's proactively demanding that ICANN submit any changes to the Root Zone functions. From a formal standpoint, the IANA Functions Contract does not grant the U.S. government such functions. Also, ICANN, IANA, RIRs, and Verisign have repeatedly stressed that they perform clearly identified and standardized technical functions and are never going to engage in political issues.

The problem is that security, stability, and resiliency of the national segments of the Internet's global infrastructure have become a critical and sensitive national security issue for nation-states, including cyberpowers such as Russia. Taking into account the economic impact of the Internet-dependent businesses and other activities on national economy, stability and security of this infrastructure certainly counts among vital, core national

[34] An ASN is an identifier for a collection of IP networks and routers under the control of one entity.

[35] Protocols that handle the exchange of routing information among autonomous systems.

interests of a national government. When the stakes are so high, as in the field of strategic stability, decisions are made based not on the current intentions of one's counterpart but on the counterpart's potential, capacities, and capabilities.

However unfounded in terms of actual incidents of this kind, Russian concerns over U.S. government intervention into the operation of the Internet's UIS rely upon a certain logic—the logic of strategic stability which demands that a decision maker assess all possible ways in which a potential counterpart might inflict strategic damage regardless of collateral damage and the counterpart's own costs. From the standpoint of national security and strategic stability, the U.S. government has legal powers that hypothetically might be used to disrupt Russia's access to the global Internet—or to isolate the Runet segment from the global Internet. In case of further escalation of a political crisis—not even necessarily a military one—these powers might hypothetically be used to maintain pressure on Russia by limiting its access to the Internet. This is the perception of the Security Council of Russia, as far as can be derived from public comments on the issue.

When the stakes are so high, as in the field of strategic stability, decisions are made based not on the current intentions of one's counterpart but on the counterpart's potential, capacities, and capabilities.

Therefore, from Russia's standpoint, there is a problem. Moreover, if it is not addressed, it might ultimately result in policies that could trigger fragmentation of the Internet on a global scale. This would affect not only Russia; because of the distributed nature of the networks, it would affect the entire system.

What are potentially available solutions that might meet Russian concerns and benefit the United States and the global stakeholder community? There are at least two possible ways, as far as the Russian side is concerned.

The first one is increasing transparency and accountability of the business processes ensuring operation of the Internet's UIS. This closely parallels the declared goals of the IANA Oversight Transition process. The proposed reform of ICANN's governance is intended to achieve this. The reform will create a quasi-government, with a board, a set of by-laws, an independent review process with binding powers, and a set of supporting organizations and advisory committees. The board will be required to consider advice from the government advisory council, but only if that council has achieved "full consensus."[36] Conservatives in the U.S. and national governments, including that of Russia, criticize the reform on the grounds that national governments have too little say under the reform. Moreover, it remains unclear how the reform will affect certain technical functions.

The IANA Functions contract with the U.S. government expired on September 30, 2015. At that time the U.S. Department of Commerce used one of its options for extension of the IANA Functions contract until September 30, 2016. Debate over reform of ICANN governance continued at the ICANN meetings in June 2015 (Buenos Aires) and March 2016 (Marrakech).[37] The Buenos Aires meeting launched a three-phase process to reform the IANA Oversight Transition. As noted above, the process is scheduled to be complete by fall 2016. According to the responses to the IANA Stewardship Transition Coordination Group (ICG) from the three communities (IETF community, Numbers community, and

[36] "We the Networks," p. 2.

[37] https://www.icann.org/news/announcement-2016-03-10-en.

Naming community), the transition should encompass major IANA functions related to the Internet's global infrastructure, including IANA's role in the DNS Root Zone management. However, that does not include general oversight over other stages of the DNS RZM business process. Moreover, because Verisign as the Root Zone technical maintainer has its separate contract with NTIA and is not a party to the NTIA-ICANN contract, its functions remain beyond the scope of the IANA Oversight Transition process. At the ICANN meeting in Buenos Aires, there were certain rumors that Verisign's technical maintainer's functions will also be subject to transition in parallel with the IANA Transition, but no public confirmation has been made so far.

If the window of opportunities for increasing transparency and accountability of the Internet's UIS operation and its operators through IANA Transition process faces certain limitations or delays, Russia might choose to look for other options.

One probable answer is providing guarantees to the beneficiaries of these business processes. In the case of the Internet's UIS, the beneficiaries are all nation-states. Because the prime concern in this field has been expressed by Russia, the guarantees might be discussed and negotiated among a limited number of actors, including of course Russia and the United States. Participation of other major cyberpowers such as China and the European Union might be beneficial for such a mechanism of guarantees. Such guarantees do not need to be overcomplicated. A single mutually agreed-upon norm might be a useful foundation upon which further consensus on related issues could be set—for example, under the auspices of the UNGGE.

Such a norm might simply be the non-intervention of governments into the operation of the Internet's UIS. Specifically, this would include two elements:

a. a ban on state-sponsored attacks on the global level components of the Internet's UIS infrastructure (DNS RS and Number Resources installations operated by IANA and RIRs); and

b. a ban on politically driven intervention through judicial or administrative leverage into the operation of IANA, Verisign, RIRs, and other technical structures running the business processes related to the Internet's UIS. This would satisfy an interest of Russia and does not contradict the basic goals of the U.S. government with regard to the NTIA Stewardship Transition process.

Recommendations and Next Steps

In sum, we offer six recommendations for bilateral agreements in the cybersecurity realm:

a. an explicit definition of the thresholds for attacks on critical infrastructure such that an attack would trigger a counterattack using either cyber- or other types of weapons;

b. an agreement on the types of information that are to be shared in the event of a cyberattack, for example along the lines of a response to a bio-weapons attack;

c. prohibition of automatic retaliation in cases of cyberattacks;

d. prohibition of attacks on elements of another nation's core Internet infrastructure;

e. joint evaluation of the Internet Core Governance (UIS, IANA, DNS RZM) infrastructure to assess whether stakeholders feel that their interests and contributions are being given adequate consideration following the reform of ICANN's governance; and

f. broad international discussion of this issue beyond the bilateral U.S.-Russia framework. To this end, the UNGGE might be a relevant and fruitful framework. The idea of a non-attack (or a more broadly defined "non-interference") consensus with regard to the Internet's global and vital infrastructure could easily become another point in the list of the nonbinding voluntary policy norms proposed in its report of June 2015. Even if nonbinding and loosely defined, such a policy norm would advance considerably the international diplomatic debate on this issue as a result of the established status of the UNGGE and its widely shared approach, both earned to a significant degree by Russia's persistent long-term efforts. Therefore, elaborating a loose nonbinding consensus within the UNGGE framework would help Russia and the United States as two important contributors to the group's activities develop a common understanding on this issue and might serve as a prologue or a blueprint framework to the future bilateral agreement on preserving stability, security, and resiliency of the Internet's global infrastructure. If there is political will and understanding of its importance, this work might be started even as soon as 2016, when the fifth UNGGE resumes work. In the longer-term future, however, we think that a formal binding international treaty is needed to require full compliance with the norms. The bilateral norms we propose can serve as a model for such a multilateral agreement.

Appendix A: Glossary of Terms

As mentioned in the paper, the path to a common understanding between the United States and Russia on key definitions related to cyber/information security has been difficult and is still not complete. Some terms were defined in 2013 by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. However, one of the most successful attempts at defining key terms in this field was made through a joint effort between by The East-West Institute (United States) and Moscow State University's Institute of Problems of Information Security (Russia). In 2014 experts from both think tanks published the first forty consensus definitions around key cluster areas of cybersecurity terminology: (https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf).

The glossary below is based on their list, with minor editorial changes. More detailed explanations as well as other definitions can be found in the report published by the two institutes.

critical cyberinfrastructure: the electronic infrastructure that is essential to vital services for public safety, economic stability, national security, international stability, and the sustainability and restoration of critical cyberspace.

cyberattack: an offensive use of a cyberweapon intended to harm a designated target.

cyberconflict: a situation between or among nation-states or organized groups whereon hostile cyberattacks result in retaliation.

cyberdefense: organized capabilities to protect against, mitigate against, and rapidly recover from the effects of cyberattack.

cyberespionage: a cyberoperation to obtain unauthorized access to sensitive information through covert means.

cybersecurity: a property of cyberspace that allows individuals or organizations to protect digital assets from being compromised or having their underlying functions exploited. This includes the ability to detect, react, respond to, recover from, and deter cyberattacks.

cyberspace: an electronic medium through which information is created, transmitted, received, stored, processed, and deleted.

cyberthreat: a danger, whether communicated or detected, that can target a cyber vulnerability.

cyberwar: an escalated state of cyberconflict between or among states in which cyberattacks are carried out by state actors against cyberinfrastructure as part of a formal or *de facto* military campaign, either one that is formally declared by an authority of one of the parties or one conducted without a formal declaration.

cyberwarfare: an organized set of cyberattacks that are authorized by state actors against cyberinfrastructure as part of a militarized conflict.

cyberweapon: software, firmware, or hardware designed to deliver a damaging digital effect through the cyber domain.

information space: any medium through which information is created, transmitted, received, stored, processed, or deleted.

information war: an escalated state of information conflict between or among states in which information operations are carried out by state actors for politico-military purposes.

Appendix B: Internet Infrastructure

In order to understand the technological context of this issue, one should have a basic idea of what the Internet's global infrastructure is, how it functions and how it is controlled and operated, and, finally, how in theory a nation-state might be disconnected from the global Internet. It is therefore necessary to highlight some basic facts about the Internet's Unique Identifiers System (the Internet's UIS).

In a decentralized global Internet with its inherent scalability, distributed network architecture, and extreme resiliency, there is only one global centralized and hierarchical infrastructure complex. This is the Internet's Unique Identifiers System, which is the core and the heart of the Internet itself. It enables operation of the Internet on a global scale. Without the Internet's UIS there is no Internet as such, and this is the only system with regard to which this sentence is true. It includes three large infrastructure subsystems:

- The Global Domain Name System (DNS), a set of protocols and global hierarchical distributed database that are designed to provide translation from human-friendly domain names to data in other formats, including translation from domain names of IPv4 addresses and of IPv6 addresses. At the same time, as pointed out by Internet Society, today DNS is used in the Internet for much more than that and now acts as a form of "directory assistance operator" for both human-to-machine as well as machine-to-machine interactions. In addition to IP addresses, the DNS is used to look up mail servers, cryptographic keys, latitude and longitude values, and other diverse types of data. The majority of uses of the Internet are critically dependent on the performance of the DNS and the SSR of its operation. Though the DNS is not essential for operation of the Internet itself, it is absolutely vital for end users and businesses, despite the assertion that advanced search engines would make it obsolete quite soon.

- The Internet's Number Resource allocation system, which is composed of the IP address allocation system, and the Autonomous Systems Number allocation system.

    - The IP addressing system is the core component of the Internet's global infrastructure. As RFC 770 (January 1980) says, IP address is "a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication." The two major functions of IP include host or network interface identification and location addressing. The uniqueness of Internet Protocol numbers (IPs) is a fundamental technological requirement that enables communication and exchange of traffic between networks on the Internet. Uniqueness of IPs guarantees that the data packets will ultimately be able to reach the addressee wherever it is located. If IP

uniqueness criteria are not met in any aspect—for example, if different nodes on the Internet announce and use the same IPs—a collision would take place in the routing system that would result in disrupted access to some or all of such nodes on the network.

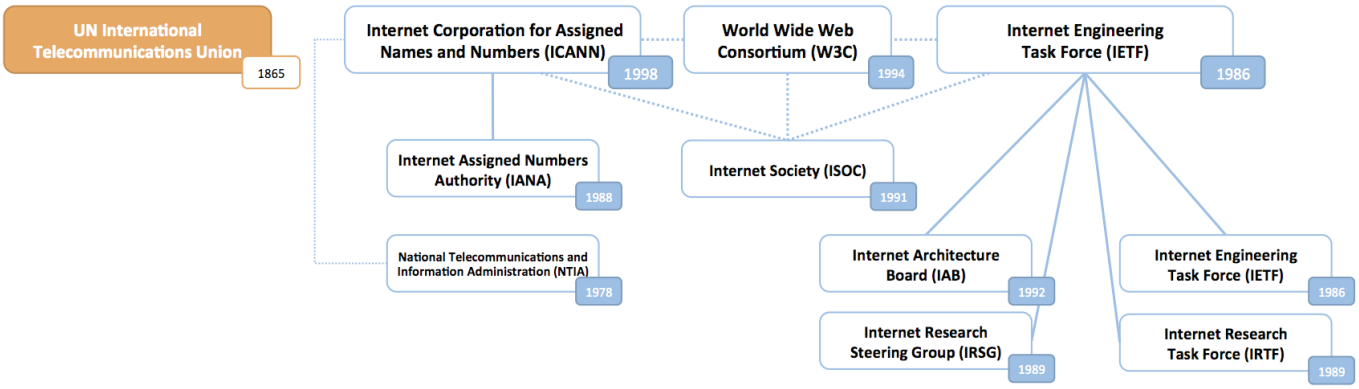
- Autonomous Systems (ASes) and Autonomous Systems Numbers (ASNs). An AS is a set of networks under a single administrative routing policy. The very concept of ASes emerged as a kind of superstructure over the IP level, which allows aggregating billions of IPs into limited and manageable amount of larger but still unique entities on the Internet. The need behind such aggregation is rooted in the limitations of the interdomain routing system. Currently, this system generally uses the BGP-4 protocol to build routing paths between ASes that roughly amount to 75,000 on the Internet today. The number of available routes directly or indirectly depends on the total number of available ASes, and this is important for the path calculation process conducted by BGP routers. The number of available routes on the Internet and their combination define the size of so-called routing tables maintained by routers. So without the "aggregation" of the internetwork routing to the AS level, the routing would have been based on sending data packets directly between nodes with different IPs. Even for IPv4 with its global pool of just 4.25 billion unique addresses it would make routing tables unreasonably huge, and the routing path–building process extremely resource-consuming. As for IPv6 with its global pool of 2^{128} unique addresses, global routing on the Internet would become impossible because of limitations of calculating capacity of the routing equipment. So, the ASes in essence are just a necessary way to simplify things with regard to interdomain routing.

So, together with the Autonomous Systems Numbers, DNS, and the global routing system, the IP address resources constitute the Internet's UIS, which was initially described in RFC 791: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."

- Finally, there are also parameters of the Internet protocols and numbers of the protocols' ports. Parameters of protocols and the number of protocols' port that are used for internetwork communication on the Internet are prescribed characteristics that constitute the third and final component of the Internet's UIS. Coordinated use of port numbers by multiple network operators does not require a resourceful and global system of servers, as DNS does. In fact, both parameters of protocols and port number are an open database, managed by a responsible structure, but published and available globally to every network operator on the Internet.

In fact, physical infrastructure is present only for the DNS and Number Resource allocation system. The Internet protocols and their ports are not physical objects; they are implemented standards that enable interoperability of networks across the global Internet. It is not possible to corrupt their infrastructure because no such infrastructure actually exists.

Appendix C: Internet Governance Organization Chart



About the Authors

Thomas Remington is Goodrich C. White Professor of Political Science at Emory University. He is also Senior Research Associate of the International Center for the Study of Institutions and Development of the Higher School of Economics in Moscow, Russia, and an Associate of the Davis Center for Russian and East European Studies at Harvard University. He received his Ph.D. in political science from Yale University in 1978 and an M.A. in Russia and East European Studies from Yale in 1974. He is author of a number of books and articles on Russian and postcommunist politics. Among his publications are *Presidential Decrees in Russia: A Comparative Perspective* (Cambridge University Press, 2014); *The Politics of Inequality in Russia* (Cambridge University Press, 2011); *The Russian Parliament: Institutional Evolution in a Transitional Regime, 1989–1999* (Yale University Press, 2001); and *The Politics of Institutional Choice: Formation of the Russian State Duma* (co-written with Steven S. Smith) (Princeton University Press, 2001). Other books include *Politics in Russia* (7th edition, Longman, 2011); *Parliaments in Transition* (Westview Press, 1994); and *The Truth of Authority: Ideology and Communication in the Soviet Union* (University of Pittsburgh Press, 1988). He is currently conducting research on inequality and social policy in Russia and China.

Chris Spirito is a Nuclear–Cyber Security Consultant with the the Department of Energy–Idaho National Laboratory. His focus is on protecting and defending critical infrastructure from cyberattacks and developing improved models for the education and training of control system security professionals. Prior to joining INL Chris was the International Cyber Lead within the National Security Engineering Center at the MITRE Corporation. Chris joined MITRE in 1998 in its Information Warfare group and has spent the majority of his career supporting cybersecurity initiatives within the Department of Defense (DoD) and the intelligence community. Chris's areas of focus at MITRE included the intersection of cyber- and nuclear security, foreign language cyberanalysis, cybereducation and training, and the development of international cybernorms and confidence-building measures. Chris is a Visiting Lecturer at the University of Tartu Faculty of Law and co-author of a book released by the International Institute of Strategic Studies, *Evolution of the Cyber Domain: The Implications for National and Global Security*.

Elena Chernenko is head of the foreign desk of the *Kommersant* newspaper (Moscow) and member of the press pool of the Russian Ministry of Foreign Affairs. Her areas of expertise are cybersecurity, Russia's foreign policy, and its relations with Western and post-Soviet countries. She is a participant of the MSC Munich Young Leaders Program–2015; member of the Board of the PIR Center; member of the Council for Foreign and Defense Policy; and member of the Working Group on the Future of U.S.-Russia Relations.

Oleg Demidov is Consultant and Advisory Board Member at the PIR Center, a leading Russian non-governmental think tank conducting research in the field of global security. Oleg graduated from the PIR Center's International School on Global Security in 2012. Since 2014, Oleg has been a member of the Research Advisory Network (RAN) under the Global Commission on Internet Governance (GCIG). He is also member of the Internet Governance Committee under Coordination Center for TLDs .RU/.РФ. Oleg's field of expertise includes global cyber governance and Internet governance, management of the Internet's global infrastructure and CII protection. Since 2011, Oleg has been contributing to the global technical and expert debate on these issues within such fora as ICANN Meetings, IGF, NETmundial summit, EuroDIG, Russian IGF, CSCAP, and UNIDIR expert meetings.

Vitaly Kabernik is Senior Expert for the Center of Strategic Studies at MGIMO University, a widely known institution forging the backbone of Russian diplomatic service. He is also a member of the PIR Center Working Group for Cybersecurity and Internet Governance. Vitaly is the author of a number of publications studying the transformations in military doctrines that arise with introduction of novel concepts such as the revolution in military affairs, cyberwar, hybrid conflicts, unrestricted warfare, etc. His area of expertise includes non-proliferation studies, public diplomacy, strategic intelligence, PSYOPs, cyberweapons, applied encryption algorithms, and critical IT infrastructure protection.

Working Group on the Future of U.S.-Russia Relations

U.S. members

Rawi Abdelal, Herbert F. Johnson Professor of International Management, Harvard Business School; Director, Davis Center for Russian and Eurasian Studies, Harvard University

Samuel Charap, Senior Fellow for Russia and Eurasia, International Institute for Strategic Studies

Timothy Colton, Morris and Anna Feldberg Professor of Government and Russian Studies, and Chair, Department of Government, Harvard University

Alexander Cooley, Director, Harriman Institute; Professor of Political Science, Barnard College, Columbia University

Keith Darden, Associate Professor, School of International Service, American University

Henry Hale, Professor of Political Science and International Affairs, George Washington University

Yoshiko Herrera, Professor, Department of Political Science; Co-Director, International Institute; Faculty Director, UW-Nazarbayev University Project, University of Wisconsin-Madison

Sarah Hummel, Assistant Profesor, Department of Political Science, University of Illinois at Urbana-Champaign

Pauline Jones Luong, Professor of Political Science and Director of International Institute, University of Michigan

Jeffrey Mankoff, Deputy Director and Fellow, Russia and Eurasia Program, Center for Strategic and International Studies (CSIS)

Thomas Remington, Goodrich C. White Professor of Political Science, Emory University

Kevin Ryan, Director, Defense and Intelligence Project, Belfer Center for Science and International Affairs, Harvard Kennedy School of Government

Randall Stone, Professor of Political Science, and Director of the Skalny Center for Polish and Central European Studies, University of Rochester

Alexandra Vacroux, Executive Director, Davis Center for Russian and Eurasian Studies, Harvard University

Cory Welt, Associate Director, Institute for European, Russian and Eurasian Studies, GW Elliott School of International Affairs, and Adjunct Fellow, Center for American Progress

Russian members

Pavel Andreev, Head of International Projects, RIA Novosti

Oleg Barabanov, Head, Department of EU Politics, European Studies Institute at MGIMO University; Professor, School of World Economics and Politics, National Research University—Higher School of Economics

Timofei Bordachev, Director, Center for Comprehensive European and International Studies, National Research University—Higher School of Economics; Director on Research, Council on Foreign and Defense Policy

Elena Chernenko, Special Correspondent, *Kommersant*

Oleg Demidov, Consultant, PIR Center

Alexandr Gabuev, Senior Associate and Chair of the Russia in the Asia-Pacific Program, Carnegie Moscow Center

Vitaly Kabernik, Senior Expert, MGIMO Center for Military and Political Studies; Working Group on Cybersecurity Member, PIR Center

Sergei Karaganov, Dean, School of International Economics and Foreign Affairs, National Research University—Higher School of Economics; Chairman, Presidium of the Council on Foreign and Defense Policy

Vasiliy Kashin, Research Fellow, Center for Analysis of Strategies and Technologies

Ekaterina Koldunova, Deputy Dean, School of Political Affairs and Associate Professor, Department of Asian and African Studies, MGIMO

Valery Konyshev, Professor, Department of the Theory and History of International Relations, St. Petersburg State University

Vasiliy Kuznetsov, Assistant Professor, Moscow State University; Director, Center for Political Systems and Cultures

Fyodor Lukyanov, Editor-in-Chief, *Russia in Global Affairs*; Chairman of the Presidium, Council on Foreign and Defense Policy

Boris Mezhuev, Associate Professor, Moscow State University; Co-Editor, *Terra America* portal

Gevorg Mirzayan, Research Fellow, Institute for the USA and Canada Studies, Russian Academy of Science

Natalia Stapran, Associated Professor, Department of Oriental Studies, MGIMO

Andrey Sushentsov, Associate Professor, Applied Analyses of International Problems Department, MGIMO

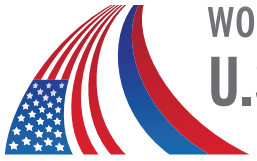
Dmitry Suslov, Deputy Director, Center for Comprehensive European and International Studies, National Research University—Higher School of Economics; Deputy Director of Research Programs, Council on Foreign and Defense Policy

Mikhail Troitskiy, Associate Professor of International Relations and Russian Foreign Policy, MGIMO University

Sergey Veselovsky, Associate Professor, World Politics Department, MGIMO

Igor Zevelev, Director, Moscow Office, MacArthur Foundation

The Working Group on the Future of U.S.-Russia Relations convenes rising experts from leading American and Russian institutions to tackle the thorniest issues in the bilateral relationship. By engaging the latest generation of scholars in face-to-face discussion and debate, we aim to generate innovative analysis and policy recommendations that better reflect the common ground between the United States and Russia that is so often obscured by mistrust. We believe our unique, truly bilateral approach offers the best potential for breakthroughs in mutual understanding and reconciliation between our countries.



WORKING GROUP ON THE FUTURE OF
U.S.- RUSSIA RELATIONS