CISSM | CENTER FOR INTERNATIONAL & SECURITY STUDIES AT MARYLAND

Alternative Approaches to Information-Age Dilemmas Drive U.S. and Russian Arguments about Interference in Domestic Political Affairs

By Pavel Sharikov

September 23, 2020

This paper was made possible by generous support from the Carnegie Corporation of New York.

Center for International
and Security Studies at Maryland
4113 Van Munching Hall,
School of Public Policy, University of Maryland
College Park, MD 20742
(301) 405-7601

Abstract

This paper investigates differences in Russian and American approaches to challenges of the information age, and explores some destabilizing effects on bilateral relations. The governments and societies in Russia and the United States base political and economic decisions about the development and use of information technology on different principles; in a globalized, interconnected world Russia's collectivistic approach clashes with American individualistic approach. This exacerbates numerous problems in Russia-U.S. relations, including reciprocal allegations of information attacks as a form of interference in domestic affairs. Alternative approaches to information-age dilemmas make Russia and the United States particularly sensitive to different ways of using information technology to impact electoral processes and domestic politics, with little understanding of each other's narratives and national priorities.

Introduction

Relations between the United States and Russia have deteriorated to their lowest level since the worst times of the Cold War. The current Russia-Western standoff, which intensified in 2014 over the events in Ukraine, has become a major feature of the new international system. The same level of courage and creativity that helped stabilize and end the U.S.-Soviet Cold War is needed today.

The current situation differs enough from the earlier Cold War to be called the "Cold War 2.0." It does not involve the same ideological premises; the parties are not peer competitors; and they are not locked in a zero-sum competition for world dominance. Cold War 2.0 also has a new feature: the widespread use of cyber and information technologies (IT) for strategic advantage through espionage, disruptive cyber-attacks, and interference in domestic politics.

Just as Cold War security experts worried that the superpowers' nuclear competition could lead to a disastrous war that neither desired, some are now starting to recognize that unconstrained cyber competition could have a similar result. For example, some current security experts have become increasingly concerned that as mistrust grows, exploitative cyber operations intended to collect information about a potential adversary's military capabilities for defensive reasons could be misperceived as a prelude to disruptive cyber-attack, eliciting a pre-emptive reaction that escalates out of control. Russian offensive cyber capabilities are perceived as serious security risks and have not yet became subject to international regulation.[1]

Differences between U.S. and Russian ideas about legitimate versus hostile use of IT in the political sphere have received little attention as a form of misperception that could lead to miscalculation and dangerous escalation. Yet, they have already contributed to one of the most serious problems in current Russian-American relations: mutual accusations of unacceptable interference in domestic political affairs. Russians assert that the United States employed IT to advance color revolutions in neighboring countries and in Russia itself. Americans are convinced that Russia meddled in numerous European elections and "weaponized" stolen data and social messaging to help President Donald Trump win the 2016 election.

[1] https://carnegieendowment.org/files/Kuhn_Baltics_INT_final_WEB.pdf

Leaders of both countries vehemently deny that they did anything wrong. This precludes a constructive conversation about what uses of IT that impact the other's internal politics are considered legitimate by both countries, and are tolerated as a normal part of rough-and-tumble competition, and which uses are viewed as unacceptably threatening. Inability to move forward on this issue is impeding the two countries' ability to work together on anything else. Yet, neither side knows what to do besides accuse the other and defend itself.

The purpose of this paper is not to endorse either side's accusations or defenses. Instead, it is to facilitate a more constructive conversation about highly sensitive issues by helping each side develop a more nuanced understanding of the other's choices and concerns in order to reduce the likelihood that one or both countries will continue to use IT in ways that threaten the foundations of the other's political system.

This paper argues that differences between the political culture and political economy of the United States and Russia have led to diametrically opposed policies for the management of information and communication technologies (ICT). These policies exacerbate different types of internal political vulnerabilities about which leaders are very sensitive. Other countries could be tempted to leverage these vulnerabilities for strategic advantage without realizing that the target state and other countries with similar ICT policies could view such uses of IT as political acts of war.

Because the United States and Russia have nearly opposite narratives about how to understand and address the challenges of the information era, they have chosen different ways to use information as a foreign policy instrument, defend their own information security, and seek advantage in the information ecosystem. They remain far apart on key questions about global governance of ICTs, such as whether the internet should be managed by a multi-stakeholder group as a global public utility fostering the free flow of information or if it should be controlled by sovereign states that can stop unwanted information from entering their territories.

This article starts by describing key political challenges posed by the information revolution. The first section considers how security functions of governments have evolved in the information age, how individual empowerment by IT alters the domestic political environment, and how countries that adopt individualist versus collectivist national IT policies have tried to shape international governance arrangements. The more individualistic political culture of the West helps explain why the U.S. government defines "cybersecurity" in terms of ensuring that everybody has fast, reliable access to the internet and other types of critical IT infrastructure; that free speech and freedom of information are protected; and that nobody has unauthorized access to data, devices, and networks. The more collectivist political culture in Russia leads it to define "information security" in terms of the government's ability to control both the content of information and the means of its production, dissemination, and storage. Differences between individualistic and collectivist political culture also create disagreements in international political fora, including debates about internet governance and disputes about how international law applies in cyberspace.

The second section suggests that while the United States has managed and adapted to the information revolution relatively successfully, some aspects of U.S. political culture and economy create vulnerabilities that are becoming increasingly clear. Allegations of Russian interference in

U.S. domestic politics have drawn attention to some of these vulnerabilities, but are only one of the reasons for growing concern.

The third section looks in more depth at continuity and change in Russian information policies since the end of the Cold War. It argues that choices made to preserve the power of the Russian political and economic elite have contributed to Russia's relatively weak international position in the information age, and exacerbated internal problems that may undermine the government's efforts at control. The Russian government fails to create a hospitable environment for technological innovations, so the country cannot compete with the leaders of the information age.

The fourth section explores mutual accusations about the use of IT to interfere in domestic politics. It concludes that the two countries misjudge each other's concerns and reactions because of their nearly opposite approaches to information policy. Divergent perceptions of the political role of information lead to different ideas about which state-sponsored activities are illegitimate forms of interference in other countries' internal politics. This explains why the United States considers its use of ICTs to empower civil society and promote democracy in countries around the world to be laudable while the Russian government deems it despicable. Russian authorities think that tightly controlling political information not only protects their own power, but also preserves social cohesion in ways that benefit society as a whole. They see what appears to be a free-for-all in the American marketplace of ideas during political campaigns and the so-called culture wars. Yet, Americans view alleged Russian action during the 2016 election, including the targeted release of sensitive information stolen from Democratic officials and the troll farms that spread false messages on social media, as an assault on a sacred national institution.

The final section offers some recommendations to reduce the negative effects that differences in information policies are having on U.S.-Russian relations. Russia and the United States have a record of reaching agreements on cybersecurity in the United Nations and other multilateral fora on some basic principles, norms, and confidence-building measures for ICTs. However, these understandings are so new and abstract that it is unclear how countries will interpret them and what, if any, impact they will actually have on behavior.

Political challenges for all national governments in the information age

One of the most basic government functions is to ensure security against internal disorder and external threats. In the information age, though, governments have limited technical capability to control their citizens' consumption and production of information, let alone what information flows across their borders. As information grows more valuable, becoming, in some cases, a critical resource, governments have become more concerned about the security of IT infrastructure and the confidentiality, integrity, and accessibility of data.[2] They must confront basic questions about how much and what type of control over information is important for sovereignty in the twenty-first century.[3]

[2] https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf p. 15
[3] Lawrence Lessig, Code. P.3 http://codev2.cc/download+remix/Lessig-Codev2.pdf

Defining and maintaining the proper balance between governmental control and individual freedom has become more challenging as access to IT leads to individual empowerment in political and economic terms, which enhances social and political transformations. John Micklethwait and Adrian Wooldridge observed that "web-based collaboration is allowing people to do for themselves what government used to do for them,"[4] at least in some regards.

Some governments worry that IT could shift too much power from the state to society. They seek greater control by developing laws and technologies that restrict what information is publicly available, and that expand government access to personal or corporate information.[5] Yet, excessive government control violates individual freedoms, and imposes different limitations on economic growth, and general individual and national development.

The choices that governments make about managing the two main information resources—infrastructure and content—reflect their national political traditions. Governments in countries with more individualistic political traditions, such as the United States, generally encourage information production and consumption by private citizens and companies. They also create opportunities to maximize every citizen's potential, and allow citizens to take advantage of the global nature of information space. Governments in countries with more collectivist traditions, like Russia, try to exert more control over the production and consumption of information. Both approaches have merits, challenges, and drawbacks. Countries' national IT policies can fall anywhere along the individualist-to-collectivist spectrum and can shift over time.

In Western countries, information policies reflect the strong commitment to the rule of law based on individual rights and restraints on government power. The government is expected to respect and protect information resources belonging to individual citizens, private companies, and civil society groups with political guarantees similar to those given to industrial assets (e.g. property rights). Western governments ensure information security by using tools such as copyright regulations (which originated in Britain in the 17th century) to protect the creator or owner of information. Major information security challenges include privacy and confidentiality guarantees, infrastructure construction and support, government and commercial secrecy, reputation losses, intellectual property rights, and many other facets of information resources. Western governments tend to encourage information communication, and prioritize freedom of information communication in security and national sovereignty.

Countries with more authoritarian political traditions tend to adopt collectivist rather than individualistic information policies. These governments perceive information as a state asset, so they tend to nationalize information by introducing limitations on domestic and foreign information exchange, traffic control, and other similar measures. Mechanisms for the control and distribution of goods in such political systems are much more likely to benefit the government class than to promote equal opportunities. When information becomes a resource subject to government redistribution, both the government and civil society can benefit where their goals coincide—but if governments try to strictly control the individual consumption and production of information rather than encourage individual empowerment, citizens enjoy fewer benefits.

[4] Micklethwait J., Wooldridge A. The Fourth Revolution. Penguin Press. 2014. p. 209-210
[5] https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf

Information sovereignty implies government control and the introduction of an information nonproliferation regime. In this context, citizens or interest groups may be unaware of the ideas of privacy and confidentiality. They may also be subject to government surveillance and propaganda.

A second major challenge for national governments is how IT shapes international politics, both as a power resource in cooperation and as an arena for competition.[6] Differences between individualistic and collectivist political traditions have led to long-standing disagreements about internet governance and more recent debates about what principles should govern other aspects of interstate relations in the field of ICT.

Some analysts have argued that Western governments want global governance arrangements to maintain a safe and reliable IT infrastructure, including the global internet and the devices and networks used by individuals, firms, and organizations; while non-democratic governments are most concerned about controlling content that could threaten their domestic political control or their national security.[7] The reality is more complex. Authoritarian governments have some concerns about IT infrastructure security, such as disruption, intrusion, or hacking. Likewise, democratic governments have certain concerns about content. They want to protect some content, such as classified and proprietary information, credit card and personnel records, and messages posted on social media. They also prohibit certain types of content, including child pornography and some speech that incites violence.

Since cyberspace is global, international cooperation is needed. Not surprisingly, though, individualistic and collectivist political traditions lead to very different ideas about what forms would be beneficial. Internet governance is a case in point.

International disputes over internet governance stem from the manner in which IT evolved in the late 1990s.[8] The internet was designed as a global network of networks to facilitate sharing information around the world. It promoted globalization, created new global markets, and expanded access to intellectual capital. The more national governments, companies, and citizens benefitted from using the internet, the more important access, speed, and reliability became to them. At the same time, some governments grew concerned that domestic dissidents, criminals, violent non-state actors, economic competitors, or hostile governments would harm their interests by disrupting their access to the internet, stealing information as it moved through the network or spreading subversive information.

When the internet became open to mass audiences, most of it physically belonged to and was managed by the United States. The general supervision of the network was executed by the Commerce Department. In 1998, the United States decided to create a special nonprofit organization responsible for assigning names and numbers—a basic function for internet governance—called the Internet Corporation for Assigned Names and Numbers (ICANN).

---

[6] http://www3.weforum.org/docs/GCR2018/05FullReport/TheGlobalCompetitivenessReport2018.pdf World Economic Forum Global competitiveness report.

[7] Sergey Guriev and Daniel Treisman developed an informational theory of modern autocracies. They argue that modern dictators survive not by means of force or ideology but because they convince the public of their competency. Guriev, Sergei and Treisman, Daniel, A Theory of Informational Autocracy (April 3, 2019). Available at SSRN: https://ssrn.com/abstract=3426238 or http://dx.doi.org/10.2139/ssrn.3426238

[8] http://www.pircenter.org/media/content/files/13/14340274400.pdf p. 17

Russia perceived this step as an attempt to establish U.S. control over cyberspace and possibly start building a military offensive cyber capability. In 1999, the Russian delegation introduced a resolution A/RES/53/70, "Developments in the Field of Information and Telecommunications in the Context of International Security,"[9] to the United Nations demanding international control over the internet. Russia insisted that the internet was a global asset and thus should be run by an international body, not a corporation or a single country. Every year for 20 years, Russia's resolutions were supported by many countries but not the United States or Europe. This is very clear evidence that differences over information policies existed long before the Cold War 2.0. These differences do not represent contemporary political contradictions between Russia and the United States but constitute a much deeper controversy between Western democracies and other countries with authoritarian political traditions.

Governments choose from the different forms of IT-enabled aggression. However, this aggression is most likely nonviolent—hence its use cannot be defined as an act of war. At the same time, if governments use information resources as a means of nonviolent aggression against another country, their actions are hardly peaceful. The different roles of government in the information age result in different conceptions of key international terms: national sovereignty, international aggression, conflict, war and peace, weapons. Attempts to develop formal and informal rules for international interactions in cyberspace similar to those for physical domains have made little progress for many of the same reasons it has proven difficult for national governments to develop internal governance mechanisms—particularly the challenge of balancing government control and individual freedoms.

Yet the difficulty does not diminish the need. As scholars Nancy Gallagher and Theresa Hitchens note, "[t]here is near-unanimous agreement on the need for more international cooperation to increase stability and security in cyberspace," yet "[s]tates disagree about fundamental issues such as freedom of access to information versus state control of political content, the limits of sovereignty in the cybersphere, and management of the internet."[10] Russia and the United States may represent the two most opposed views, which becomes a source of tension in bilateral relations. Russian initiatives in the United Nations gain the support of many countries that adhere to the collectivist approach of information policies. American resolutions are supported by Western democracies that adopt an individualist approach to regulating information. These contradictions also bring additional problems to bilateral relations.

The U.S. Government's Role in the Information Age

In the United States, the government's role is relatively narrow. Many responsibilities are left to the private sector, civil society, or individual citizens. Moreover, the U.S. government has made choices about its role in the information age that have stimulated the growth of the high-tech sector, supported private industry, and increased public access. By many measures, these choices have been very successful. However, there are some unresolved tensions. One of the most serious problems related to finding the proper balance between government and individuals involves

[9] https://undocs.org/A/RES/53/70

ensuring privacy and confidentiality of information. Excessive government control is as harmful as unregulated individual freedom.

The American political system has not handled the transition to the information age perfectly, but it has done better than many countries. U.S. research and development (R&D) policies have been favorable for cultivating knowledge and relatively good at expanding public access to IT (and the fruits of an IT-centric economy.)[11] Due to the collapse of the Soviet Union, the need to develop secret sophisticated technologies against a peer enemy seemed unnecessary, so some former military technologies were commercialized. That included GPS and the internet. The development of these technologies was driven not only by government procurement, but increasingly also by consumer demand. The ubiquitous spread of internet and information technologies resulted in significant changes to the U.S. political economy, and encouraged the rapid development of a technology sector benefiting the whole national economy.

Obviously, these processes required careful political decisions. There are unresolved tensions in the U.S. political approach, particularly as it relates to the balance between individual freedom and government control over infrastructure and content. For example, because of its reliance on private entities in the IT services market, the U.S. government has to choose whether to assert a specific role for itself in regulating commercial actors or to defer to commercial prerogatives.

While IT provide individuals with many different opportunities, the ability of the government to guarantee equality in these opportunities decreases. The debate over net neutrality illustrates the quandary for U.S. policy makers. As a concept, net neutrality is meant to provide all internet users equal opportunity to produce and consume information online and to protect their information from political or economic influence. While some policy makers are reticent to insist on this type of regulation, the alternative—where internet service providers (ISPs) slow the transmission of some information or exercise other forms of control, either for political reasons or for commercial profit—is unappealing as well.[12]

Debates about privacy in the United States tend to involve questions about government access to content stored on or communicated over IT.[13] These types of public debates have intensified as the amount of information traversing these networks has grown and as access to this information has come to be seen as an important tool of both domestic and international security. For instance, there has been intense debate around antiterrorist legislation and tactics where some political actors have insisted that the collection of personal information of American citizens is necessary to prevent and respond to terrorist attacks, while critics argue that preserving privacy and the confidentiality of personal information should be a higher priority. This approach has certain benefits but also creates vulnerabilities. Foreign and domestic actors may interfere with open information communications, influence public opinion, and possibly alter electoral outcomes.

Prioritizing individual freedom of self-expression in domestic information policies has implications for foreign policy. In her 2010 remarks on internet freedom after a conflict between Google and the Chinese government, Secretary of State Hillary Clinton said that “in an internet-

[11] https://www.oecd.org/naec/THE-KNOWLEDGE-ECONOMY.pdf
[12] https://www.nap.edu/read/10235/chapter/8#175
[13] https://www.brookings.edu/wp-content/uploads/2016/06/0401_databuse_wittes.pdf

connected world, an attack on one nation's networks can be an attack on all."[14] Within this paradigm, the United States considers freedom of information to be a universal value. Foreign government policies that impede the free flow of information worldwide become a challenge for U.S. diplomats. Americans also see them as a commercial risk, because they restrict US companies' access to foreign markets.

Nearly unregulated consumption of internet content resulted in the spread of social internet networks. The United States leads the world in the number of Facebook and other social network users. In 2020, the United States had 89.8 percent internet penetration, 90.1 percent of which were Facebook registered users. Russia had 79.7 percent internet penetration and only 5.7 percent Facebook-registered users.[15] As social networks became efficient political instruments, the global nature of the internet created the opportunity for international actors to influence public opinion. At first, social media platforms were considered to be just a vehicle for information sharing, and the most popular of them stayed away from politics. However, social media's ubiquity and increased demand has led it to be a political instrument. Indeed, the most popular social networks—Facebook and Twitter—have evolved beyond being vehicles for communication, becoming independent political actors in their own right.

In this context, every measure that potentially interferes with the freedom of speech provokes a new wave of public discussions. For example, shortly after Twitter labeled Donald Trump's tweets as requiring "fact-checking," the president issued an executive order addressing online censorship.[16] The order empowered the Federal Trade Commission (FTC) to "consider taking action, as appropriate and consistent with applicable law, to prohibit unfair or deceptive acts or practices." The order prompted concerns about freedom of speech, further highlighting the independent political role of social media.

The Russian Government's Role in the Information Age

The Russian government defines its responsibilities in the information sphere much more broadly than the U.S. government does. Russia's collectivist political culture and resource-based political economy have encouraged the government to make choices that have hurt Russian global competitiveness, both in the technology sector and more generally. Moreover, Russian government concerns about internal disorder and external interference have led to a series of doctrinal and legal changes that give the government greater control. This is partly an illusion, though, because the rules are hard to enforce, and technical workarounds exist. There is a growing gap between segments of society that acquiesce to government controls over information and those that find ways to become empowered through IT. The debate over the proper balance between government controls and individual freedoms in Russia has become part of the political struggle between the current government and opposition. Russia's collectivist political culture and its embodiment in Russian information policy may have also contributed to Russia becoming a political boogeyman in the United States and other individualistic, information-age-oriented Western countries.

[14] https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm
[15] https://www.internetworldstats.com
[16] https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/

The Russian government has had difficulty adapting to the global economy in the information-age. Russia's collectivist political traditions and its powerful industrial sectors are in tension with the technological, political, and economic trends that drive the information age economy and empower individuals. The Russian government has favored policies that preserve the traditional natural resources industries, because they are integrated into existing political institutions. These policies disadvantage high-tech industries within Russia's domestic market and make them less competitive on a global level. This means that Russian IT companies have less economic and political clout than American companies do. It also means that the Russian government has less compunction about exerting political controls that further erode the growth and global competitiveness of its IT sector.

Despite all their disadvantages, Soviet R&D policies made the USSR competitive geopolitically with the United States at a time when the global economy was primarily based on natural resources and manufacturing. The U.S. Central Intelligence Agency (CIA) estimated that Soviet R&D expenditures were comparable to American expenditures during the Cold War, but Russian R&D expenditures are much smaller than U.S. expenditures now.[17] Moreover, R&D during the Cold War was primarily directed toward industrial sectors of economy in both countries. While the United States now focuses on R&D in technology and information-related sectors, contemporary Russia still focuses on traditional industries and invests less heavily in R&D than the Soviet government did.

Russia still relies heavily on Soviet-style planned economic policies that inhibit the innovation, experimentation, and competition needed to keep advancing in the information age. Central planning weakened after the collapse of the Soviet Union, but it strengthened again under President Vladimir Putin. An economy driven by government procurement is uncompetitive compared to a market-driven one. In a controlled economy, producers are not motivated to compete because their income depends on fixed government redistribution. Under these circumstances, economic growth relies on exporting natural resources and raw materials.

Russia's R&D spending is extremely low—1.1% of GDP or about $40 million (compared to 2.7% in the U.S.—almost $500 million)[18]. According to the 2015 United Nations Educational, Scientific and Cultural Organization Science Report (see table below), the government remains the main source of R&D spending in Russia. The private sector has very little interest in funding high-tech research in Russia because most companies are connected with the government and don't produce genuinely high-tech products.

[17] https://www.cia.gov/library/readingroom/docs/DOC_0000309798.pdf. Most of the statistics that could prove these points remain classified.
[18] http://uis.unesco.org/apps/visualisations/research-and-development-spending/

Table: 2013 R&D expenditure by source and sector of performance in USA and Russia

	Source of funds %		Sector of performance %	
	USA	Russia	USA	Russia
Business enterprise	59.13	28.16	69.83	60.60
Government	30.79	67.64	11.93	30.26
Higher education	2.98	1.04	14.03	9.01
Private non-profit	3.30	0.12	4.48	0.13
Abroad	3.80	3.03	-	-

Source: https://unesdoc.unesco.org/ark:/48223/pf0000235406

Because Russia's economy favors natural resources and manufacturing over high-tech industries, and under-invests in R&D, a significant portion of its highly educated workers are underemployed. More than 50 percent[19] of Russian workers have advanced degrees, yet only one-third of them are employed in a field related to their degree. A quarter have jobs that do not require an advanced degree.[20] This wastes human capital and threatens to intensify Russia's "brain drain." In some public opinion polls, 40 percent of Russians express a desire to emigrate.[21] More than half of these Russians are aged 25 to 39 years old. The desire to leave Russia is greater among people with higher education (36 percent) than for less educated people (14 percent).

Russia's collectivist information policies have exacerbated these problems by seeking to impose a "digital iron curtain" on internet availability—restricting and controlling access to information by citizens. These policies have evolved considerably since the end of the Cold War, but a more collectivist approach has always dominated.

In the early post-Cold War period, the Russian government let the information sphere develop with minimal government interference, involvement, and oversight. This leniency was more a consequence of the weak and chaotic condition of the Russian state during that period rather than a deliberate policy decision by the government. Academician Evgeniy Primakov estimated that the Russian economy suffered bigger losses in the 1990s than during World War II.[22] A number of independent, high-tech companies emerged during this period. The most prominent of these are Yandex (a Russian search engine, similar to Google), VKontakte (a Russian analogue to Facebook), Kaspersky Lab, Mail.ru, and a number of others. During the late 1990s and early 2000s, these companies were not considered targets for nationalization, and government control had little effect on them.

While the Soviet government exercised extensive official control over the news media, prohibiting views oppositional to the government, until the period of "glasnost," the 1993 Russian constitution recognized citizens' freedom of speech and freedom of the press, even if the government retained significant *informal* influence over the media. As a consequence, during the 1990s, a number of non-governmental media were started by oppositional oligarchs. By the turn of the millennium,

[19] http://www.ilo.org/ilostat/faces/oracle/webcenter/portalapp/pagehierarchy/Page3.jspx
[20] Russians with advanced educational degrees: where do they work and what do they do. http://www.demoscope.ru/weekly/2017/0713/tema06.php
[21] https://www.levada.ru/2019/02/04/emigratsionnye-nastroeniya-3/
[22] Evgeniy Primakov. Russia in modern world. 2009. p. 17

some of these oligarchs were expelled from Russia and the others were forced to cooperate with authorities—limiting access to alternative points of view. Today, TV and radio stations are either state-owned or closely controlled by the government.

Russia's first official information security doctrine was adopted in 2000. Because it was still trying to modernize its economy and develop a more democratic political system along the lines of Western countries, this doctrine prioritized individual interests over state interests in several notable ways. It authorized some government regulation of the news media to promote favorable coverage, but in a less heavy-handed way than had happened under communism. The doctrine did not contain the word "internet." Most of the provisions were devoted to fostering the spiritual development of Russian people by guaranteeing basic human rights, prohibiting censorship and agitation that encourages hatred and bigotry, and ensuring freedom of speech.

During recent years, Russia's government passed a number of laws that significantly increased the level of state responsibility for information security. It also issued a major revision to its information security doctrine in 2016,[23] most likely in response to the deterioration of relations with the Western hemisphere after the annexation of Crimea. The new information security doctrine, along with many other decisions, was meant to counter Western criticism of Russia's foreign policies. That criticism both came as a surprise and did not leave Russian authorities much time to prepare. President Putin's decision to revise this foundational document (among others) was motivated by what he perceived as an increasingly hostile strategic environment after the 2014 conflict in Ukraine. Russian leadership saw a threat in the penetration of foreign, primarily Western information into Russia's cyberspace because liberal Western ideas were inconsistent with Russia's conservative values.

In general, the new doctrine matches the new strategic position of the government. It continues to address information security issues on three levels: individual, societal, and governmental. However, if the 2000 doctrine prioritized individual interests, the 2016 vision is completely focused on national interests in the field of information. The new document contains almost no provisions referring to international development and international peace. Most of the conclusions of the doctrine devoted to international cooperation are aimed at preventing conflicts and defending from foreign interventions in the Russian information field.

According to the document, one of the most serious threats to national security is "increased information influence on the population of Russia, mainly on the young generation, aimed at erosion of traditional Russian spiritual and moral values." The doctrine prioritizes "proper" content more than technological security and perceives individual empowerment as a threat. In other words, given the opportunities for individual empowerment provided by IT, the Russian government is trying to limit individual consumption and production of information.

Another important part of the 2016 strategy is external relations. Russia considers providing a foreign audience with proper and authentic information about Russian foreign policy as one of its national interests.

[23] http://kremlin.ru/acts/bank/41460

Russian domestic regulation of information

In recent years, the Russian government has also passed domestic laws that significantly increase its authority to punish the production and dissemination of information contrary to official policies. These new laws are meant to contain simmering domestic political turmoil. For instance, legislation adopted in 2014 criminalizes those who "call for extreme actions aimed against the government authorities or sovereignty," or those who "raise hate and hostilities or perform humiliation against human dignity." As a result, the number of people charged with violating these laws increased fourfold.[24] Another piece of legislation introduced in early 2019 was nicknamed the "Fake News Act" because it authorizes the government to fine the source of and block any website that publishes "fake" information without any judicial recourse.[25,26] However, traditional (state-owned or -controlled) media are not considered potential sources of fake news. This measure was intended to improve the credibility of government-sponsored information, mostly broadcasted through TV and Radio, and to make the internet sources "untrustworthy."

The 2016 doctrine and other recent legislation also impose new controls over Russian IT infrastructure. Although the term "internet" is introduced in the new strategy, it continues the trend towards the fragmentation of the Russian segment of the internet and enhances national information sovereignty. It suspends Russia's integration into the global Internet, and promotes the development of a national system of internet management.

A 2014 law requires all ISPs to store their data on hard drives physically located within the territory of Russia.[27] This move blocked access to many foreign internet services, but provoked little public reaction. Some human rights activists outwardly opposed it, but the more common response has simply been to circumvent it; software that lets individuals and businesses access prohibited sites is easily available. Even some government officials continue to use services that have been formally prohibited in Russia (such as LinkedIn).

Another law requires ISPs to gather most users' personal data, store it for six months, and share it with Russian intelligence agencies without any special judiciary procedure.[28] The law was passed in 2016 despite multiple warnings from representatives of the business sector.[29] Changes in laws governing official access to private information also allow government security agencies to request personal data from Russian social networks (most notably, Vkontakte). Vkontakte officials have denied cooperating with the government,[30] but judicial documents prove that such cooperation has taken place without any legal procedure.[31]

---

[24] https://www.kommersant.ru/doc/3607022
[25] http://sozd.duma.gov.ru/bill/606593-7
[26] https://www.theguardian.com/world/2019/mar/06/russian-parliament-outlaws-online-disrespect
[27] Kozlov, V. 2015. "Russian personal data law set to come into force despite fears". *Computer Weekly*, October. http://www.computerweekly.com/feature/Russian-personal-data-law-set-to-come-into-force-despite-fears
[28] Borshchevskaya, A. 2016. "'Brave New World': Russia's New Anti-Terrorism Legislation". *The Forbes*, July 8. https://www.forbes.com/sites/annaborshchevskaya/2016/07/08/brave-new-world-russias-new-anti-terrorism-legislation/#5383bdf83d55 Last accessed June 6, 2018
[29] AEC (Association for Electronic Communications) 2016. *Official position of the Association for Electronic Communications on the Yarovaya law*. http://old.raec.ru/times/detail/5225/ Last accessed June 6, 2018
[30] https://vk.com/wall6492_7183
[31] https://echo.msk.ru/blog/echomsk/2261270-echo/

Legislation called "Russia's Sovereign Internet Act" places nearly all telecommunications infrastructure under government control by proscribing the "proper" hardware for telecommunications companies to use and by authorizing the creation of a separate information network apart from the internet.[32] The sponsors of the legislation claim that it is intended to increase the resilience of the Russian internet in case of foreign attack, yet critics fear that it will cut the Russian part of cyberspace from the global internet. Despite 15,000-person demonstrations around hearings for the legislation in the spring of 2019, the legislation was adopted on May 1, 2019.

Together, these laws, doctrines, and other regulations enhance the Russian government's control over the data of Russian individuals and entities, and increase the fragmentation of Russia's piece of cyberspace.

Russian Public Opinion on Domestic Internet Regulations

Debates about how effective and reasonable these information policies are do occur in Russia. The sum of these efforts will likely constrain Russia's economy by further hampering its transition from the industrial age to the information age. Some Russian economic associations issued public reports predicting negative consequences if all of these new laws took effect and anticipated they would further hamper the country's transition from the industrial age to the new information age. The experts of the Society to Defend the Internet, a non-profit organization that supports free internet in Russia, argued that all interest groups are resistant to antiterrorist legislation, including representatives of the government and the opposition.[33] They argue that the adoption of the antiterrorist legislative package would require excessive spending on infrastructure from IT companies, which would negatively affect the overall digital market.

In addition to directly affecting the Russian economy, these information policies are likely to exacerbate political divisions over time. So far, the public response to changes in Russian information policies has been relatively muted. Street protests against recent legislation have gathered no more than 15,000 to 20,000 people, which is relatively small compared with the estimated 60,000 who participated in an anti-corruption protest in March 2016 and the 200,000 people who joined protests against pension reform in the summer of 2018. Yet, serious domestic economic instability could provoke political discontent, particularly among young Russians.

Younger generations of Russians tend to get their information from multiple sources, but their largest source is the internet (see Table 3). These generations tend to support the Russian government less than the average Russian, and have become more favorable toward the West in recent years. While older generations tend to be more conservative and rely on traditional Russian media, younger generations, who never lived in the Soviet Union, are more likely to access foreign media.

[32] http://sozd.duma.gov.ru/bill/608767-7 and https://www.themoscowtimes.com/2019/03/10/point-of-no-return-russias-libertarians-lead-protest-against-sovereign-internet-a64758
[33] https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws

Table 3: Public opinion poll: What are the primary sources of political news? (%)

August 2018	Total	18-24 yrs	25-39 yrs	40-54 yrs	55+ yrs
Television	73	49	59	75	89
Radio	15	13	14	14	18
Newspapers	13	8	6	13	19
Friends, relatives, neighbors	18	19	21	19	16
Internet (websites)	37	54	51	41	18
Internet (Social networks)	28	48	42	31	9

Table 4: Public opinion poll: What sources of information are most trustworthy? (%)

August 2018	Total	18-24 yrs	25-39 yrs	40-54 yrs.	55+ yrs.
Television	49	41	36	47	65
Radio	10	13	7	7	12
Newspapers	7	5	4	7	11
Friends, relatives, neighbors	13	16	12	14	11
Internet (websites)	24	36	34	27	9
Internet (Social networks)	15	30	24	17	2

Source: https://www.levada.ru/cp/wp-content/uploads/2018/09/Doverie-novostyam_tab..pdf

The growing gap between those who enjoy the benefits of the information age and those who do not may undermine government efforts to promote a cohesive Russian national identity. A 2018 Levada public opinion poll finds that the general attitude of Russians towards the United States is starting to become more positive, especially among younger Russians who prefer the internet to traditional media.[34] Those Russians who can access alternative sources of information are likely to continue to run up against the so-called patriotic majority. Given that the Russian government has not yet cut off all citizens from the internet, this conflict is likely to only grow stronger and further destabilize the domestic political environment and exacerbate relations between Russia and the West.

In sum, the Russian government has been adopting policies that are increasingly inconsistent with the best practices of the global information age. Russia clearly has ambitions to join the club of major economic and political powers in the 21st century, but its information policies do not promote the type of economic development that would allow it to ascend to this level on its own terms. Russia remains one of the most powerful industrial powers in the world, particularly in political terms, but this is increasingly a liability, not an asset. The domination of industrial sectors makes it hard for Russian high-tech industries to develop domestically and compete abroad. Moreover, Russian foreign policies aimed at preserving the status quo ante of the industrial-age international order are inherently in conflict with Western views of the future global order.

The government's information policies and internet regulations discourage individual empowerment, scare off foreign investors, and pose challenges to small high-tech companies. They also deepen the generation gap and intensify anti-government sentiment among younger

[34] https://www.levada.ru/2018/12/06/kak-budet-menyatsya-otnoshenie-rossiyan-k-ssha/

generations. The latter have very limited opportunity to legally influence the decision making on this matter, which leaves them no option besides going into the streets to protest. The protests consist mostly of younger people who lack notable representation in the government where most general decisions are made by Soviet-type managers. Instead of acknowledging the protestors' domestic economic and political grievances, the government blames foreign interference for the unrest, and the protester's demands remained ignored.

Different Approaches to Information Policy Lead to Different Concerns about Interference with Domestic Politics

All countries agree that interference into domestic political affairs threatens national sovereignty and security, albeit in a very different way than a military invasion or a terrorist attack does. Chapter One of the Charter of the United Nations starts with two basic premises: preserving international peace and security and promoting friendly relations among nations based on respect for "the principle of equal rights and self-determination of peoples." It includes the principle that "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[35] Numerous U.N. Security Council decisions have reaffirmed these principle and "reiterated the importance of good-neighborliness and non-interference by States in the internal affairs of others."[36]

While accusations of domestic political interference are a central component of the current Russian-Western standoff, they are not a unique feature of the Cold War 2.0. Well before the advent of the internet, the Soviet and American governments accused each other of conducting propaganda and disinformation campaigns with more traditional information dissemination technologies, including human agents and radio broadcasts. The internet, and networked communications in general, have made it much faster and easier to steal or disseminate information without having to physically infiltrate another country first. The growing reliance on digital information and communication technologies makes it possible to affect another country's domestic politics in other ways, too. For example, they can disrupt or facilitate citizens' communications with each other; alter images and audio to discredit political figures; use fictitious social media accounts to influence public opinion; compromise election-related data or machinery; and potentially even falsify electoral results.

Different American and Russian ideas about how governments should interact with private companies, civil society organizations, and individual citizens to manage the benefits and risks of IT lead to different views about what types of digital activities are appropriate during election campaigns and other domestic political processes, what types are unsavory but tolerable, and what are unacceptable or illegal.

The U.S. political system sees vigorous competition between opposing candidates and their supporters as a hallmark of healthy democracy in ways that go well beyond what is traditional, or

[35] Charter of the United Nations, Article 2 (4)
[36] Purposes and principles of the Charter of the United Nations https://www.un.org/en/sc/repertoire/2010-2011/Part%20III/2010-2011_Part%20III.pdf

even acceptable, in the Russian political system. Strong political opposition and competitiveness are common for the American bipartisan system. By contrast, in Russia's current system, political competition does not exist. All major political forces either side with the president and his United Russia party, or their activities are considered illegal. In the United States, political candidates are expected to participate in debates, answer questions about their policy positions posed by public interest groups, and undergo intensive media scrutiny. President Putin, who has been functionally in charge of Russia since 2000, has never participated in such strenuous political competition. Even during electoral campaigns, he does not participate in debates, and avoids direct communication with the media.

In the United States, the Bill of Rights protects free speech and prohibits government limitations on expression of political opinions by citizens and non-citizens, including very radical statements that would be illegal in Russia. Public criticism of incumbent politicians is common in the United States, but unwelcomed in Russia, and sometimes illegal. The Russian political system can be characterized as an "imitational democracy." Russia formally holds all vital democratic procedures, including elections, but not once during president Putin's presidency has any oppositional candidate been allowed to run. Opposition politicians are cut off from the public political process, so there is no such thing as oppositional candidates.

The U.S. government has a long history of trying to manage foreign influences on domestic politics. The 1938 Foreign Agents Registration Act (FARA) allows foreign entities to lobby U.S. government officials if they register and meet disclosure requirements, but the 1995 Lobbying Disclosure Act created various exemptions.[37] Under Federal Election Commission rules, foreign individuals and entities cannot make financial contributions to political candidates or political action committees.[38]

During the early post-Cold War years of Russia's transition to democracy, Russian officials welcomed some forms of foreign election assistance from U.S. and European governments, intergovernmental bodies such as the Organization for Security and Cooperation in Europe (OSCE), and civil society groups. For example, the U.S. Agency for International Development (USAID) funded many projects in Russia related to electoral politics and civic engagement with the knowledge and support of Russian officials.[39] According to U.S. officials: "Democratization aid has included technical advice to parties and electoral boards, grants to [non-governmental organizations (NGOs)], advice on legal and judicial reforms (such as creating trial by jury and revising criminal codes), training for journalists, advice on local governance, and exchanges and training that familiarize Russian civilian and military officials and others about democratic institutions and processes."[40]

---

[37] Kai Berner-Chen, "Lobbying Disclosure Exemption Allows for Continued Foreign Influence in U.S. Politics," Center for American Progress, December 13, 2019, at: https://www.americanprogress.org/issues/democracy/news/2019/12/13/478745/lobbying-disclosure-exemption-allows-continued-foreign-influence-u-s-politics/

[38] https://www.fec.gov/help-candidates-and-committees/taking-receipts-pac/who-can-and-cant-contribute-nonconnected-pac/

[39] https://www.usaid.gov/news-information/fact-sheets/usaid-russia

[40] https://fas.org/sgp/crs/row/RL32662.pdf

Perhaps the most overt example of U.S. involvement in Russian electoral politics occurred during President Boris Yeltsin's re-election campaign in 1996. A *Time* magazine article described in detail how Yeltsin asked for U.S. help when defeat looked likely, and how American political consultants used sophisticated messaging and data analysis technologies to turn the race around.[41] Newly declassified information indicates that Yeltsin personally asked President Bill Clinton for financial aid that he needed to win the elections in 1996.[42] At the time, Russian society seemed unperturbed by American consultants helping Yeltsin win re-election,[43] because the political technologies used were new to the Russian people during the transition from an authoritarian regime.

The Russian government's attitude toward foreign assistance with elections and financial aid to certain civil society organizations began to shift in the late 1990s for a mix of economic, political, and geostrategic reasons. Russia faced serious social-economic problems in the 1990s, related to rapid transition from a controlled (planned) economy towards a market-driven economy, which were partly addressed with aid from Washington. By the end of the 1990s, Russian authorities decided that Russia had recovered from the shocks of the post-communist transition, and further reception of American aid made Moscow dependent on the United States at a time when Russian leaders had grown wary of U.S. motives.

The pivotal moment was in March 1999, when prime-minister of Russia Yevgeny Primakov canceled his official visit to Washington and made a U-turn on a plane while flying over the Atlantic Ocean. The "Primakov's loop" incident was motivated by the North Atlantic Treaty Organization's decision to start bombing Yugoslavia during the Kosovo war without Security Council approval and over Russian and Chinese objections.

As Russia's official position towards the United States started to change, American support for cultural, educational, and research activities with Russian partners was increasingly seen as a hostile use of soft power to make Russian society oppositional to the government. By the early 2000s, Russian authorities were particularly concerned about foreign-funded NGOs and foreign entities using IT to empower political dissidents. These concerns were exacerbated by the color revolutions in Ukraine and Georgia in 2004-2006 and the Arab Spring in the early 2010s. As a result, the Russian government suspended democracy USAID promotion projects in 2012.[44] In 2012, Vladimir Putin's decision to become president for a third term provoked many protests in Russia. His election that year was followed by allegations of U.S. interference and of attempts to prevent him from retaking power.[45]

---

[41] Rescuing Boris: The Secret Story of How Four U.S. Advisers Used Polls, Focus Groups, Negative Ads and All the Other Techniques of American Campaigning to Help Boris Yeltsin Win. By Michael Kramer/Moscow Monday, July 15, 1996. Time. http://content.time.com/time/magazine/article/0,9171,984833,00.html

[42] https://nsarchive2.gwu.edu//dc.html?doc=4950566-Document-07-Memorandum-of-Telephone-Conversation

[43] https://www.nytimes.com/1996/07/09/world/moscow-journal-the-americans-who-saved-yeltsin-or-did-they.html

[44] https://www.mid.ru/web/guest/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/142978?p_p_id=101_INSTANCE_cKNonkJE02Bw&_101_INSTANCE_cKNonkJE02Bw_languageId=en_GB

[45] https://www.washingtonpost.com/news/democracy-post/wp/2017/07/21/did-the-united-states-interfere-in-russian-elections/

Russia's Foreign Agents Law was initially enacted in 2012 and continually amended until 2016. It does not completely prohibit foreign funding but does require full transparency and imposes many limitations on political activities. Laws requiring registration of organizations who lobby the local government on behalf of a foreign government exist in many countries, including the United States. However, Alexandra Orlova, an associate professor from Reyrson University, sees this law "reflecting contemporary Russian political rhetoric that views Western governments and their agents, including NGOs, as attempting to undermine Russia's ruling regime and threatening national security."[46] Orlova compares Russia's Foreign Agents legislation and the American FARA (Foreign Agents Registration Act) and concludes that "the scope of the regulated activity under FARA is much narrower than the Russian Foreign Agents Law, for FARA is mostly concerned with lobbying, consultancy, and advertising. Most actions of Russian NGOs that are captured under the Russian Foreign Agents Law would not be captured under FARA."

A February 2018 report by the temporary commission of the Russian Federation Council on defending government sovereignty and preventing interference into domestic affairs asserts that U.S. interference in Russian domestic affairs intensified as Russia became less deferential to the United States and more assertive internationally. The official reason for this report was concern about potential U.S. interference in the Russia's presidential election the next month, but it can also be read as a retort to U.S. accusations of Russian interference in the 2016 presidential election. The report is a rare example of a publicly available official government vision of Russia's newest historical period. The authors claim that the United States is the main source of the attempts to interfere with Russia's domestic affairs and that the number of these attempts have increased dramatically along with the restoration of Russia's true independence and enhancing international influence after 2007.

The authors assert that during the Cold War, the United States used military aggression and secret CIA operations to interfere in the domestic politics of countries in Africa, Asia, and Latin America, but after the collapse of the Soviet Union—especially in the twenty-first century—they used "hard political diplomatic artillery."[47] The report outlines 10 major forms of foreign interference in Russian domestic affairs, including: NGOs; education; media; compromising the Russian Orthodox Church; encouraging protest activities, especially among younger generations; and defamation of Russia's political and economic developments internationally.[48] The authors were especially concerned about episodes of soft power interference via educational programs, and media, details of which were described in the classified version of the report.

Members of the Duma special foreign interference committee depict the protest activity described above as foreign-supported attempts to start an "orange revolution." For example, they mentioned having "evidences [sic] that prove intentional preparation of mass civil disorder in Moscow, which coincide with the interests of an American company that acts as a U.S. government proxy" prior to the protests in the summer of 2019 about elections to Moscow Duma.[49]

---

[46] Alexandra V. Orlova, "Foreign Agents," Sovereignty, and Political Pluralism: How the Russian Foreign Agents Law is Shaping Civil Society, 7 Penn. St. J.L. & Int'l Aff. 382 (2019). Available at: https://elibrary.law.psu.edu/jlia/vol7/iss2/2

[47] http://council.gov.ru/media/files/G6hNGZ3VbQNiMdZki1BKbrsrvuRxPwim.pdf p. 51

[48] https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf

[49] https://rg.ru/2019/10/08/klimov-v-sf-est-dokazatelstva-podgotovki-massovyh-besporiadkov-v-moskve.html

The Commission on Foreign Interference has published two other volumes of the report. Both volumes described the United States as the main (and sometimes only) foreign country willing to violate Russian sovereignty. In the spirit of Russian doctrines, the alleged cases of interference included either critical media coverage of the Russian elections, or possible contacts with the political opposition. The second volume described alleged U.S. involvement in the Russian presidential and regional elections in 2018,[50] as well as U.S. interference in voting for constitutional amendments in July 2020.[51] There were no known attempts to resolve these problems with embassies or the Ministry of Foreign Affairs.

When Americans make claims about foreign use of IT to interfere in U.S. domestic politics, they are primarily talking about very different types of activities than those described in the Federation Council commission report. The alleged Russian interference in the 2016 U.S. presidential election included multiple components: the hacking of the Democratic National Committee (DNC) server, publication of stolen emails through Wikileaks, Russia Today's (RT) biased coverage of the presidential campaign, and targeted political advertisements that violated U.S. campaign finance laws. The first and fourth episodes garnered most of the attention from the U.S. political system and led to sanctions against Russian entities and the indictments of Russian citizens.

Over time, much of the U.S. focus on Russian meddling has shifted from the DNC hack and Wikileaks, to troll factory activities that were widespread by the summer of 2016 and that have continued in various forms ever since. A troll factory is an operation that maintains fake social network accounts that publish offensive commentaries on political posts in order to create an image of popular discontent with certain politicians or policies. These activities are very similar to methods the Russian government uses at home to shape public opinion about domestic affairs. Troll factories are usually associated with the Internet Research Agency (IRA), a company which was allegedly created and funded by Evgeny Progizhin, a Russian oligarch and close associate of president Putin. While Progizhin's official business is a monopoly on catering services for government organizations, he is also reported to be the head of the IRA. The Russian government controls nearly all the traditional media, but most protest activities happen on the internet, which the government cannot monopolize. Russian opposition forces claim that the IRA has engaged in disinformation activities on social media in Russia for many years and is responsible for similar information attacks on U.S. social media. The *New York Times* reports that "when the troll factory was formed in 2013, its basic task was to flood social media with articles and comments that painted Russia under Mr. Putin as stable and comfortable compared to the chaotic, morally corrupt West."[52] The IRA does not exist anymore, but evidence indicates that Prigozhin is still involved in trolling activities domestically and abroad.

The IRA's activities gained public attention in the United States when former U.S. Department of Justice special counsel Robert Mueller published the indictment and launched a trial against Mr. Prigozhin. The indictment did not involve the content of information published on Facebook, because the U.S. government has no right to limit self-expression. Instead, it claimed that these individuals faked their identities to post political advertisements on American social networks.

[50] http://council.gov.ru/media/files/LIkgU7Df0m31nfswAg80N5d4TKFhy8UG.pdf
[51] http://council.gov.ru/media/files/x6oigY4UFWahyXMJCK9Ah1RAhzrYx4z9.pdf
[52] https://www.nytimes.com/2018/02/16/world/europe/prigozhin-russia-indictment-mueller.html

Because the American legislation prohibits any foreign sponsored political advertisement, the trolls had to steal the identities of American citizens to spread such content, which is a criminal act.

Neither the Mueller report nor any other official document has publicly provided hard evidence of Russian top-level officials authorizing and/or running the information campaign. If the interference was a state-sponsored attack, though, it could be viewed either as an act of war or an act of aggression below the threshold of armed conflict. Both interpretations raise difficult questions about what would constitute an effective and appropriate response that would make such interference less likely in the future, minimize the risk of escalation, and have bipartisan support in the United States.

President Barack Obama used a secure White House-Kremlin communication channel in September 2016 to tell Putin that there would be "serious consequences" if Russia did not "cut it out."[53] Similar messages had been sent on ministerial, ambassadorial levels and through the head of the CIA; the Senate Intelligence Committee Report characterized Obama's call as "a final warning" that activated the "cyber hotline" for the first time.[54] The United States has imposed several rounds of sanctions on Russia related to election interference. The Trump administration also reportedly used offensive cyber operations to take the IRA off-line on the day of the 2018 mid-term elections.[55]

Attempts to repair the damage done to the U.S.-Russia relationship by mutual accusations of election meddling have made little progress since neither side will admit that it has done anything wrong. In a conversation with then-CIA Director John Brennan, the director of Russian Federal Security Service Alexander Bortnikov both "denied that Russia was doing anything to influence the election and also accused Washington of conducting similar activities against elections in Russia."[56] Americans are quick to dismiss such statements as posturing, but Bortnikov basically admitted perception of interference into domestic affairs and hinted that the problem should be addressed on a principle of parity. That is difficult, though, when Americans not only believe that their involvement in other countries' domestic politics is qualitatively different from and morally superior to what Russia has allegedly been doing, but also fail to understand that Russians see both countries competing for strategic advantage.

Trump and Putin did agree on the margins of a G20 meeting in 2017 that their countries would work toward an agreement not to meddle in each other's elections or use cyberattacks for political subversion.[57] The working group charged with this task, however, was never created.

Special Representative of the Russian President for international cooperation in the field of information security Andrey Krutskikh suggested releasing transcripts of pre-election contacts between Moscow and Washington about U.S. "concerns over the intrusion into its electronic

[53] https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume3.pdf
[54] Ibid.
[55] https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html
[56] https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume3.pdf
[57] https://www.usatoday.com/story/news/politics/2017/07/07/trump-putin-g-20/458210001/

infrastructure."[58] Ambassador Krutskikh thought that making public transcripts which contained no evidence of Russia's participation in the cyberattacks would prove Russia's innocence and change American attitudes. The United States rejected this suggestion; President Trump accepts Putin's reassurance that Russia did nothing inappropriate to help him win the election. The proposal was repeated by the Russia's foreign minister Sergey Lavrov during his visit to Washington in December 2019. Obviously, the Russian government is trying to do damage control and repair Russia's image, but they have not been successful.

During the Helsinki summit in 2018, President Putin suggested another idea that the United States quickly dismissed. He invited American special services to observe the Russian interrogation of the servicemen who had been indicted by Mueller, but only after a formal request by the U.S. Justice Department.[59] This was a tacit acknowledgment that indicted individuals actually exist and may be related to Russia's offensive cyber capabilities. In a move reminiscent of the Cold War, though, president Putin conditioned this offer on reciprocity—that Russian representatives be allowed to watch questioning of American citizens accused by Russia of interference into its political affairs. Russia was particularly interested in hearing an interrogation of William Brauder—the person who allegedly funded the anticorruption investigations conducted by Sergei Magnitsky, whose death led Congress to impose sanctions in 2012 through the Magnitsky Act.

It is notable that British intelligence came to similar conclusions about Russian online activities during the Brexit referendum.[60] British intelligence went a step further and also considered Russian state-controlled media to be a part of an interference campaign.

Interference into domestic affairs is a very ambiguous phenomenon in domestic politics as well as international affairs. In Russia and in the United States different understandings of interference dominate, even though both countries accuse each other of using means of cyber and information aggression. Mutual accusations of interference escalate the existing conflict between Russia and the United States and do not have any perspective for improvement.

Conclusions and Recommendations

The deterioration of U.S.-Russia relations that began in the late 1990s has been accompanied by increasingly acrimonious accusations about the misuse of IT to gain unfair advantages in the gray zone between peace and war. These activities include sophisticated cyber espionage, lucrative cybercrime, and disruptive cyberattacks. Yet, governments and citizens are especially sensitive to perceived use of IT to increase social and political divisions or to alter political preferences and electoral processes, because these activities strike at the very heart of a country's sovereignty and self-determination.

[58] https://www.washingtonpost.com/opinions/moscow-shouldnt-misjudge-the-mueller-moment/2019/03/27/5b6544e6-50fb-11e9-8d28-f5149e5a2fda_story.html?utm_term=.b890974f5fc7

[59] http://kremlin.ru/events/president/news/58017

[60] https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl

The Trump administration sees cyber aggression by Russia, China, Iran, and other hostile states as a hallmark of great power competition in the twenty-first century. In response to their "continuous operations and activities against our allies and us in campaigns short of open warfare to achieve competitive advantage and impair U.S. interests,"[61] the new U.S. cyber doctrine maintains that the only way for the United States to regain and maintain a position of strategic dominance is to beat its adversaries at this game.

This doctrinal shift takes Cold War 2.0 to a more dangerous level. Jason Healey argues that "if adversaries do not reduce their attacks, for any reason, the theory offers little advice other [than] to defend forward harder. If the strategy isn't succeeding, then U.S. cyber forces must still have too many restraints, or are not causing enough friction, or not holding targets at risk for deterrent attacks."[62] Obviously, persistent engagement raises the probability of an open conflict on a new level. While the Russian policies are becoming less and less transparent this creates a significant chance for a misperception and may lead to catastrophe. Moreover, Russian state media is considered not only to be "toxic," but also a tool for interference.

The problem of interference into domestic affairs is a complex issue. On the one hand, the specific accusations could be resolved by diplomatic and legal instruments. The problem, however, is much broader. Its roots are in a general mistrust between the countries, which, in turn, results from two different paths of political development in the information age.

During the first Cold War and in the decades since, strategic dialogue was seen as a first step toward reducing misperceptions and increasing crisis stability. This tactic is not in use today in part because the United States and Europe suspended many venues for strategic dialogue to protest Russia's annexation of Crimea. None of the U.S. reports on Russian meddling recommend engaging in a dialogue with Russia about where each side draws the line between acceptable influence and assistance, and unacceptable interference in internal politics. The reports on U.S. interference prepared by the members of the upper and lower chambers of the Russian parliament also fail to recommend dialogue with the United States.

Part of the problem is that at least some politicians on both sides make accusations about foreign interference for their own political benefits. Russian lawmakers are convinced that foreign powers are interfering with Russian domestic politics and come up with new versions with every new political crisis. In 2019, they claimed that foreign powers conduct virtual exercises with Russian opposition leaders.[63] U.S. officials keep accusing Russia of interfering in its electoral process.[64] These fears are sometimes exaggerated, and sometimes completely made up, so repeating them further damages U.S.-Russian relations.

Russian anti-Americanism and American anti-Russian sentiments are very different by nature. The modern American legal system is based on principles of freedom, equality, and non-

[61] U.S. Cyber Command. Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command. 23 March 2018. https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf

[62] Jason Healey, The implications of persistent (and permanent) engagement in cyberspace, *Journal of Cybersecurity*, Volume 5, Issue 1, 2019, tyz008, https://doi.org/10.1093/cybsec/tyz008

[63] https://www.kommersant.ru/doc/4163659

[64] https://www.theatlantic.com/magazine/archive/2020/06/putin-american-democracy/610570/

discrimination, not government-sponsored systemic xenophobia against Russians, Chinese, Arabs or any ethnic or racial minority. Moreover, there are a lot of Russian immigrants in the United States. While they are not as connected through diaspora organizations as other ethnic groups, they have integrated into American society quite successfully. Critical arguments against Russian politicians do not flow from a fear of all things Russian. Average Americans do not project their criticism of Russian politicians onto Russian citizens. Russian anti-Americanism is different. Russian government-controlled media mischaracterizes American criticism towards Russian politicians as Russophobia. It tries to turn Russia's public opinion against the people, as well as the government, of the United States. In this way, it seems that Russian domestic and foreign policy is more ideologically motivated compared to the United States.

There are U.S. and Russian security experts who would like to find ways to reduce risks of misperception, escalation, and inadvertent conflict. Yet, most either refuse to discuss future cooperation until the other side admits past wrong-doing and makes restitution, or they believe that talking about election interference, the status of Crimea, and other particularly sensitive topics will prevent constructive conversations about arms control and other forms of cooperative nuclear risk reduction.

As a result, the United States and Russia are unable or unwilling to resolve even relatively minor arms control compliance disputes, let alone any of the bigger problems in their relationship. Thus, they are ending key arms control and confidence-building agreements at the same time as they are ramping up competition across the military spectrum and into cyberspace.

Under these circumstances, a real or imagined use of IT to interfere with domestic politics could trigger a military response. In 2017, the United States designated election infrastructure to be a type of critical infrastructure deserving priority protection,[65] and the 2018 Nuclear Posture Review specified that the Trump administration would consider using nuclear weapons in response to a "significant non-nuclear strategic attack on…U.S., allied, or partner civilian population or infrastructure…"[66] Russia's nuclear deterrence posture published in June 2020 envisions the use of nuclear weapons under a much more limited set of circumstances, including "an attack with nuclear weapons, or attack that threatens the sovereignty and integrity of the country."[67] The document does not provide any further details. Such statements raise concerns, though, given that many Russian officials claim that the United States threatens Russian sovereignty and integrity through information policies.

Officials on both sides have opportunities to reduce tensions. To start, Americans and Russians can find ways to have constructive conversations about which uses of IT to affect political attitudes and processes are laudable, which are tolerable, and which are deeply threatening or intolerable. These conversations can happen in person or online; among students, curious citizens, independent experts, or government officials; in dedicated sessions, as part of existing fora like the U.N. Group of Government Experts and the OSCE meetings on IT and cybersecurity, or on the margins of meetings about other topics.

---

[65] https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical
[66] https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF (p. 21) Information Security Doctrine 2000.
[67] http://static.kremlin.ru/media/events/files/ru/IluTKhAiabLzOBjIfBSvu4q3bcl7AXd7.pdf p.4

As part of these interactions, both sides need to acknowledge that they each have good reasons for being concerned about social cohesion, political legitimacy, and trust in government. They also need to accept that each believes the other has used IT in ways that make those problems worse. Such acknowledgments are neither admissions of guilt nor claims of moral equivalence. Rather, they indicate a willingness to take each other's concerns seriously, which is a prerequisite for constructive conversations about how to reduce those concerns.

Another useful step would be for the two sides to use terminology that clarifies meaningful distinctions instead of conflating very disparate ways in which IT can be used to influence political opinions, operations, and outcomes, For example, much of what American media refers to as Russian cyberattacks on U.S. elections is better understood as social media propaganda, influence operations, or information warfare since the perpetrator gained access openly, if sometimes dishonestly, rather than by hacking into an information system. Within this realm, some actions are clearly illegal under U.S. law, such as foreign entities paying for political advertisements, while many others are currently legal, if not completely honorable.

Similar distinctions could be made among different kinds of election-related hacking. Both countries routinely use cyber espionage to collect information about leading political candidates for important positions, including about their campaign committees, donors, and potential voters. If that is a normal part of tradecraft, though, strategically releasing real or falsified stolen information to help or hurt particular candidates is more clearly out of bounds. Various disruptive cyberattack scenarios, such as altering voter registration records, interfering with election-day operations at numerous polling locations in a critical jurisdiction, or changing electronic voting results would be considered, by Americans at least, an even more outrageous assault on democracy.

The more Russian and Americans understand about each other's sensitivities and concerns regarding the impact of IT on internal politics, the less likely they are to take actions without first considering how that will be perceived by the other side. Likewise, the more Americans and Russians know about each other's policies and practices regarding IT, the less likely they are to assume that the other side is deliberately trying to gain an unfair advantage when their officials, companies, or non-governmental organizations do something objectionable with IT. Increased awareness could reduce misperceptions and misjudgments. It might also lead to tacit reciprocal restraint.

If U.S. and Russian leaders want a joint agreement not to meddle in each other's elections or use cyberattacks for political subversion, then they need a much better understanding than they currently have about what that would actually mean. The two countries have very different approaches to internal regulation of information, speech, social media, IT infrastructure, elections, and domestic politics writ large, so they will naturally have very different ideas about this question. In each country, the relevant laws and regulations governing IT use by public officials, private companies, civil society, and individual citizens are changing rapidly. In some instances these laws are ambiguous or non-existent. Accordingly, there is bound to be confusion about what outsiders can and cannot do. It should be possible, though, to get agreement on some behaviors that one or both sides consider unacceptable. The rules do not have to be exactly the same for each country

given how different the internal political systems are, but they should be viewed by both sides as roughly equitable. Questions about how to verify compliance with the rules, and what to do if rules are broken would naturally depend on what, if any, rules could be agreed.

Along with these steps to address the misuse of IT to interfere with domestic politics, Russia and the United States could take additional steps to reduce the risk of competition in cyberspace leading to an unwanted war.

It is critical to increase transparency. The Russian political system is more closed than the American political system, but even during the Cold War leaders would sometimes share sensitive information to verify compliance with arms control treaties, to de-escalate crises, and to build confidence in each other. Complete transparency regarding information and cyber resources seems impossible, but more modest transparency is not. For example, the governments could agree to exchange information about their postures and their rules of engagement for cyber offensive technologies. Such doctrines may include the pathways of escalation, definition of red lines, explanation of intentions, confidence-building measures.

Both countries share a common approach against cybercrime and have adopted similar measures in countering cybercriminals. The relatively large role of the private sector in the United States complicates the agreement between Russia and the United States, because it is hardly imaginable that the United States would take similar government responsibility as in Russia. The Russian private IT sector in its turn participates much less in these negotiations and in international relations in general. It is also critical to understand that any bilateral agreement will only be able address aspects of cybersecurity and information policy that are considered the government's responsibility in both countries, which means that the terms will be largely set by the smaller scope of U.S. government involvement than the much broader Russian conception of the government's role in cyber-policy making.

Author Biography

Pavel Sharikov graduated from the University for Humanitarian Studies in 2005 holding a degree of specialist in international relations. Prior to his academic career he worked as a reporter in major Russian information agencies.

Sharikov has worked as a research fellow in the Institute for USA and Canada Studies of Russian Academy of Sciences since 2002, where he studies American politics in general and cybersecurity issues in particular. In 2009 he defended a dissertation devoted to American cybersecurity policies. In 2012 he majored in legal informatics from the Department of Law at Higher School of Economics. In 2015 he authored a book "Information security in a multipolar world."

From 2011 to 2019, Sharikov ran the Center for Applied Research in the Institute for USA and Canadian Studies of Russian Academy of Sciences, and taught at Moscow State University. In 2019-2020 he was a visiting assistant research scholar at the Center for International and Security Studies at University of Maryland.