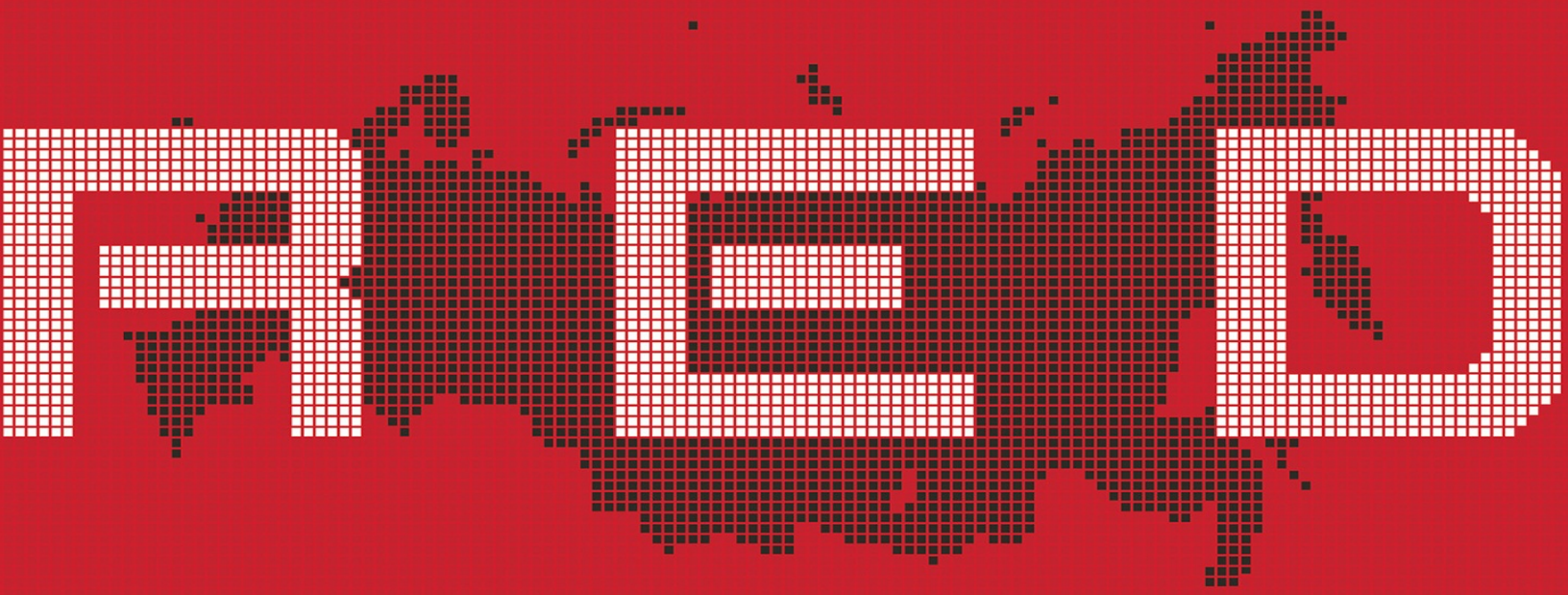
THE RED WEB

THE STRUGGLE BETWEEN RUSSIA'S DIGITAL DICTATORS *and* THE NEW ONLINE REVOLUTIONARIES



ANDREI SOLDATOV *and* IRINA BOROGAN

THE RED WEB

THE STRUGGLE BETWEEN RUSSIA'S DIGITAL DICTATORS *and* THE NEW ONLINE REVOLUTIONARIES

ANDREI SOLDATOV *and*
IRINA BOROGAN

PUBLICAFFAIRS
New York

Published in the United States by PublicAffairs™, a Member of the Perseus Books Group

Book Design by Cynthia Young

Library of Congress Cataloging-in-Publication Data
Soldatov, Andrei
The red web : the struggle between Russia's digital dictators and the new online revolutionaries / Andrei Soldatov and Irina Borogan.
—First Edition.
pages cm
Includes bibliographical references and index.
ISBN 97811-61039157418 (electronic)
1. Internet—Political aspects—Russia (Federation) 2. Information society—Political aspects—Russia (Federation) 3. Internet—Access control—Russia (Federation) 4. Electronic surveillance—Russia (Federation) 5. Freedom of information—Russia (Federation) 6. Russia (Federation)—Politics and government—1991–
I. Borogan, I. (Irina) II. Title.
JN6695.A55A859 2015
303.48'330947—dc23
2015015850

First Edition

10 9 8 7 6 5 4 3 2 1

“Information wants to be free.”

—Futurist Stewart Brand

“This is not a phone conversation.”

—a Russian expression meaning a wish to discuss something in person because somebody else might be listening

Chapter 11. Putin's Overseas Offensive

Vladimir Putin was certain that all things in the world—including the Internet—existed with a hierarchical, vertical structure. He was also certain that the Internet must have someone controlling it at the top. He viewed the United States with suspicion, thinking the Americans ruled the web and that it was a CIA project. Putin wanted to end that supremacy. Just as he attempted to change the rules inside Russia, so too did he attempt to change them for the world. The goal was to make other countries, especially the United States, accept Russia's right to control the Internet within its borders, to censor or suppress it completely if the information circulated online in any way threatened Putin's hold on power.

Andrey Krutskikh devoted his entire career in the Russian Foreign Ministry to arms control. He joined the diplomatic service in 1973, right after university, and served in the ministry for the final eighteen years of the Soviet Union's existence. He admired the diplomatic style of the stolid and uncompromising foreign minister, Andrei Gromyko, known informally in the West as Mr. Nyet. Krutskikh often called Gromyko "great."

From the very beginning of his service Krutskikh's work centered on disarmament, nuclear weapons, and the so-called main adversaries, the United States and Canada. When he was twenty-four years old, in 1975, he was sent to Salt Lake City as a member of the Soviet delegation to negotiate strategic nuclear arms control. Krutskikh's experience at the negotiations in Salt Lake City left a strong impression on him. It was a time when Soviet diplomats had stature; they decided the fate of the world and spoke on equal terms with the Americans. After the Soviet collapse and into the late 1990s Krutskikh continued to focus on arms-control issues and rose through the ranks of the ministry. He was not a smooth or

slick diplomat; he had a rather agitated manner—expressive, his hands always in motion. Krutskikh soon wondered whether arms control could be useful in the emerging realm of cyber conflict.

Among a particular group of Russian generals who represented FAPSI, the powerful electronic intelligence agency that had grown out of the KGB, a similar mindset was developing. The agency's headquarters was located in a stark, modern terraced building with giant antenna globes on the roof not far from the KGB headquarters. Like the US NSA, FAPSI was responsible for information security, signals, and electronic intelligence. For many years their generals watched the growth of the Internet with suspicion, thinking it was a threat to Russia's national security, because in the early days the Russian Internet was built with Western technology, and they were obsessed with the fear that it would be thoroughly penetrated by the Americans.

The leader of this group of suspicious generals was Vladislav Sherstyuk, a colonel-general in the intelligence wing of the agency and a KGB officer since 1966. By the 1990s he became head of the very mysterious and powerful Third Department of FAPSI, in charge of spying on foreign telecommunications. All Russian centers of electronic espionage abroad were subordinated to this department, including the radio interception center at Lourdes in Cuba, which was in charge of monitoring and intercepting radio communications from the United States. Sherstyuk was a spymaster, determined to exploit communications to steal US secrets and protect Russia against espionage of the same kind. This naturally made him wary of the Internet, where so much was beyond his control.

When the war in Chechnya began, Sherstyuk was put in charge of FAPSI's group there, and he organized the interception of Chechens' communications. In December 1998 he was appointed director of FAPSI, a mighty intelligence service in its own right that competed head-to-head with the FSB. Among other things, they had a very special role in controlling the government's most sensitive communications networks.

Krutskikh and the FAPSI generals spoke the same language of suspicion—a language of threats posed by the Internet. In early 1999 Krutskikh was helping to draft a resolution for the UN General Assembly that reflected these views and

warned that information—the Internet—could be misused for "criminal or terrorist purposes" and could undermine "the security of States." In other words, information technologies had to be controlled because they could be dangerous. The resolution was adopted without a vote.[1]

Krutskikh and the generals viewed the Internet as a battleground for information warfare. (This term should not be mixed with cyberwarfare, which is mostly about protecting a nation's critical digital networks from hackers.) For Krutskikh and the generals, information warfare encompasses something political and menacing, including "disinformation and tendentious information" that is spread to incite psychological warfare, used for altering how people make decisions and how societies see the world.[2] In contrast to those who celebrate free media and the Internet as a glorious information superhighway that opens limitless possibilities for discovery, Krutskikh and the generals worried that it could become the front lines of conflict between nations and hostile groups.

In December 1999 Sherstyuk moved out of FAPSI to the Russian Security Council, an advisory group to the president on security. Once there, he supervised a department for information security, which included the Internet, and brought his ideas with him. The Security Council normally is made up of top officials, including the president, and meets periodically, but it also has an influential staff, which Sherstyuk joined. In 2000 his team composed the "Doctrine of the Information Security of the Russian Federation," which included an unusually broad list of threats, ranging from "compromising of keys and cryptographic protection of information" to "devaluation of spiritual values," "reduction of spiritual, moral and creative potential of the Russian population," as well as "manipulation of information (disinformation, concealment or misrepresentation)." Quite ominously, it identified one source of the threats as "the desire of some countries to dominate and infringe the interests of Russia in the global information space."[3] Putin approved the doctrine on December 9, 2000.

In 2003 FAPSI was disbanded, but not the ideas of the suspicious generals. Sherstyuk remained at the Security Council, and some of his views were reinforced when a like-minded top official from the FSB, Nikolai Klimashin, was moved to the Security Council. Sherstyuk founded and headed the Information

Security Institute at Moscow State University, which he built into a major think tank to define Russian foreign policy on information security. Meanwhile, Krutskikh rose to become deputy chief of the Department for Security and Disarmament Issues at the ministry.

For years at international meetings Krutskikh had been driving home that Russia wanted to govern its own space on the Internet. Whereas others, including the United States, saw the Internet as a wide-open expanse of freedom for the whole world, Krutskikh insisted that Russia should be able to control what was said online within its borders. He expressed fear that, without such control, hostile forces might use the Internet to harm Russia and its people. "If through the Internet we would be forced to forget our mighty great Russian language, and speak only using curse words, we should not agree with that," he told us, echoing Putin's deep suspicions about the Internet and who was behind it. Krutskikh repeatedly proposed some kind of international agreement or treaty that would give Russia the control it sought over the Internet. Influenced by his own career in arms-control negotiations, he was convinced that such an agreement must be between Russia and the United States. He wasn't anti-American, but he grew emotionally attached to the idea that the two former Cold War superpowers could somehow make a pact that would give Russia control over its digital space. The United States, however, never warmed to the idea—the US government never attempted to control content on the Internet, and many of the first Internet pioneers in America were very open about the Internet as a symbol of how information should roam free—but what Krutskikh wanted most was to be taken seriously and to have his views treated with respect, as they were during the Cold War.

But he didn't get much respect. At a bilateral meeting in March 2009 in Vienna, Krutskikh delivered a long monologue arguing that Russia and the United States—and perhaps other nations—should collaborate to regulate the Internet as nations and governments. He expressed fear that the Internet was building beyond their control, that there could be an arms race in cyber space, and it was time for governments to take charge.

Russian generals felt they were losing the global cyber arms race and wanted to put some limits on the United States' offensive capabilities. But

Krutskikh's speech fell on deaf ears. An American diplomat cabled back an account of the meeting, saying, "There was little change, if any, between U.S. and Russian long-held views" on the subject. Krutskikh desperately wanted some sort of joint statement with the United States, but the US administration was reluctant to sign anything.[4]

But he didn't give up. In 2010 Kaspersky Lab investigated Stuxnet, the US-Israeli worm that wrecked nearly a thousand Iranian centrifuges.[5] Krutskikh seized on the incident—with its destructive malware, designed in part by the United States—as a justification for a ban on cyber weapons.[6] In 2011 Kaspersky, who was highly regarded in Russia as an Internet entrepreneur, added his voice to the idea of a ban on cyber weapons, and in November he wrote on his blog, "Considering the fact that peace and world stability strongly relies on the internet, an international organization needs to be created in order to control cyber-weapons. A kind of International Atomic Energy Agency but dedicated to the cyberspace."[7]

In the Bavarian Alps a small mountain resort town, Garmisch-Partenkirchen, is famous for its spectacular views and NATO's Marshall Center for Security Studies, which is based there. Nearby is a pretty hotel, Atlas, with a traditional Bavarian three-story lodge that is a twenty-minute walk from the Marshall Center. Founded in the early sixteenth century as a tavern, the hotel proudly lists among its previous guests Duke Ludwig from Bavaria, the Prince of Wales, and the King of Jordan. Every April, for almost a week, the hotel hangs a Russian flag from its balcony, hung personally by Sherstyuk, who, since 2007, has been bringing to the lodge a group of Russian and American generals and high-placed officials to talk quietly about information security and cyber conflict. The first two days are always reserved for general discussions, mostly on cyber security and what kind of research is required. Russians gathered in one part of the hotel, and non-Russians gathered in another, partly because many Russians didn't speak English, and most Americans didn't speak Russian. The third day was devoted to

individual meetings. The real business was conducted in closed rooms with only a few participants. Klimashin was among the guests, as well as Krutskikh, who never tired of making speeches and arguing for agreement on "terms and definitions" in cyberspace and for greater UN involvement in Internet governance. He favored the United Nations because it was filled with governments, not companies, and many of them were sympathetic to Russia's desire to control the Internet within their borders.[8]

The US government took the gatherings in Garmisch very seriously every year. High-level officials were sent; in 2010 the US delegation included Christopher Painter, the second-ranking White House official on cyber security, and Judith Strotz, the director of the State Department's Office of Cyber Affairs.[9]

Russian officials in charge of information security often spoke bitterly of US domination of the Internet, believing all the tools and mechanisms for technical control were in US hands. Their main target was the Internet Corporation for Assigned Names and Numbers, known as ICANN, a nonprofit organization headquartered in California. In 1997 President Clinton directed the secretary of commerce to privatize the management of the domain name system, a critical part of the Internet that serves as a giant warehouse of web addresses looked up every time a user wants to go somewhere online. The Defense Advanced Research Projects Agency, the National Science Foundation, and other US research agencies had previously performed this task. On September 18, 1998, ICANN was created and given a contract with the US Department of Commerce to oversee a number of Internet-related tasks, but the most important among them was to manage the distribution of domain names worldwide. In the 2000s other nations campaigned to have a greater role in ICANN, but the Kremlin's idea was more radical: to strip ICANN of its powers.

The president of ICANN, Paul Twomey, hastened to the second gathering in Garmisch in 2008. He and other high-ranking ICANN representatives tried to keep open channels of communications with the Russians. One of the top US ICANN representatives who made sure always to attend was George Sadowsky. Looking always professorial, he taught mathematics at Harvard and was a technical adviser to the United Nations in the 1970s. In 2001 Sadowsky became executive

director of the Global Internet Policy Initiative, which promoted Internet freedoms in the former Soviet Union and Central Asia. In 2009 he was selected to the board of directors of ICANN. Sadowsky had a great deal of experience in dealing with Russian officials. He found the endless discussions to be frustrating, as both sides saw the world differently and had trouble even agreeing to a common language about the Internet; there were very basic divisions over definitions regarding the Internet. "Is it a communications service or is it an information service?" he recalled. "And this went on, and on, and on."[10] In Garmisch both Russians and Americans tried to be pleasant and friendly, but they were at a stalemate. And with each passing year the discussions became increasingly difficult—after the conference in 2010 Sadowsky admitted, "The Russians have a dramatically different definition of information security than we do; it's a broader notion, and they really mean state security."[11]

When the Russian officials failed to get an agreement with the United States about ICANN, they shifted strategy, looking for a new way to assert more sovereignty over the Internet. This new approach led them to the International Telecommunications Union, or ITU. With headquarters in Geneva, the organization was originally established in 1895 to regulate the telephone and telegraph. It is a specialized UN agency, and as such, it is dependent on the member states.

The ITU was not involved in Internet governance until late 2006, when Hamadoun I. Touré was elected its secretary general. Touré made the Internet a central issue for the ITU from the start of his tenure. A citizen of Mali, he speaks fluent Russian and studied at the Communications Institute in Leningrad, the same institute where Boris Goldstein, one of the main Russian experts on SORM, studied and has been working for decades. Touré was well known in and maintained close ties with Russia—he was first elected and then, in 2010, reelected with the full support of Russia. As secretary general of ITU, he became very critical of ICANN, and in August 2010 he even refused Rod Beckstrom, then chief executive and president of ICANN, permission to attend an ITU conference.

Krutskikh spotted all this jockeying and, frustrated by the failures to change ICANN, moved to promote a larger role for the ITU. This was a surprising development for Sadowsky. When he met Krutskikh at a Moscow conference in 2008, the Russian official was pleasant and restrained. But it was another story two years later when they met again at the same conference. Sadowsky said something unfavorable about the ITU, and Krutskikh responded emotionally and forcefully, interrupting the American midremarks.

For Sadowsky, it seemed like Krutskikh—and Russia—had wagered a big bet on the ITU.

The tumultuous uprisings of the Arab Spring that threw out long-serving authoritarian leaders—uprisings that Internet communications accelerated—suddenly made the issue of Internet governance more urgent for Putin. In June 2011 Putin went to Geneva to talk to Touré. They met at the large hall at the UN Office, and Putin reminded Touré that Russia cofounded the ITU and went on to say that Russia intended to actively participate in "establishing international control over the internet" by using the capabilities of the ITU.[12] It was an audacious idea: to control the Internet using a century-old UN agency.

Krutskikh, in preparation for the new effort, moved in August 2011 to another department inside the Foreign Ministry. The department was closely tied to the security services and had once been supervised by a former first deputy director of the FSB. Then in March of the following year he was made a special coordinator for issues regarding political use of information and telecommunication technologies—the Internet—and given a rank of ambassador. He was to be Putin's point man on a campaign to wrest more control of the Internet from the United States.

The next major ITU conference was scheduled for December 2012 in Dubai. The top ITU officials intended to use the gathering to change the rules for the Internet globally through a review of an existing global treaty, which was last updated in 1988, before the digital era. The ITU intended to amend the treaty to

include the Internet and, thus, make it subject to ITU regulation. And the Kremlin decided to make the conference in Dubai the launch pad for a general offensive against US domination of the Internet.

Krutskikh went to work recruiting other countries to support Russia. He won nods of agreement from China, where the Internet is rigidly and widely censored, and from Central Asian nations that were former Soviet republics and also largely authoritarian. In May 2012 Krutskikh won backing directly from the Kremlin. The former minister of communications Igor Shchegolev moved to the administration as Putin's adviser on the Internet, and he fully shared Krutskikh's ideas about the ITU and ICANN. Shchegolev had accompanied Putin in June 2011 to Geneva and took part in the meeting with Touré.[13] The new communications minister, Nikolai Nikiforov, twenty-nine, was technically savvy but inexperienced. He was appointed to his position from Kazan, Tatarstan, where he had served as Tatarstan's minister of communications. He was far from being an independent political figure.

Krutskikh plotted his strategy for the Dubai meeting in an office near the foreign ministry's twenty-seven-story tower in central Moscow. His office building next door looked like a giant, seven-story cube with an oblique angle. From there, on the fourth floor, with an Andreevsky Flag (two blue stripes crossed diagonally on white, the insignia of the Russian fleet) on the wall and a spaceship model on his desk, with his papers always carefully sorted, Krutskikh laid out the battle plan, drafting dozens of proposals for the ITU summit.

Google launched a campaign against the Russian offensive. In May 2012 Vint Cerf, "chief Internet evangelist" at Google and widely recognized as one of the fathers of the Internet, published an op-ed in the *New York Times* headlined "Keep the Internet Open."[14] He referred to Putin's remark at the meeting with Touré in 2011 and criticized a proposal submitted by China, Russia, Tajikistan, and Uzbekistan to the UN General Assembly that sought to establish government-led "international norms and rules" in cyberspace. Cerf proclaimed, "The decisions taken in Dubai in December have the potential to put government handcuffs on the Net." He appealed for action against it.

But Russia was undeterred, and preparations became more intense. In June

the first draft of the Russian proposals to the ITU conference were leaked to the press. They were couched in jargon, but the point was crystal clear: Russia proposed to give countries the right to control the Internet in cases in which it was used "for the purpose of interfering in the internal affairs or undermining the sovereignty, national security, territorial integrity and public safety of other states, or to divulge information of a sensitive nature." This would give nations the right to censor on the slimmest of pretexts.[15] Then, just two weeks before the conference started in Dubai, there was another leak of Russian proposals, and then another one. The direction of the drafts was the same, giving nations "the sovereign right . . . to regulate the national Internet segment."[16]

The two-week ITU conference started on Monday, December 3, at the Dubai World Trade Center, a thirty-nine-story rectangular tower built in 1978 at the city's Trade Centre Roundabout. More than nineteen hundred participants from 193 countries attended.[17] Krutskikh hoped this would be his triumphal moment.

The Russian delegation was led by the minister of communications, Nikiforov, with Krutskikh as a member of his team. Touré at once appointed Nikiforov one of the vice chairs of the conference. Russia's hopes looked promising: the Russian team had already secured private pledges of support from China and eighty-seven other countries for the draft proposals, and Krutskikh was determined to win over other countries.

Throughout the first week of the conference the participants debated the leaked Russian drafts in the corridors and meeting rooms as they waited anxiously for the official Russian proposal to come.[18] Tensions were high, as the United States opposed talking about Internet regulation at the ITU conference at all. On Thursday, December 6, the head of the US delegation, Ambassador Terry Kramer, convened a special briefing. Kramer was not a career diplomat but rather a top company manager with a twenty-five-year career in the private sector and telecommunications, mostly at Vodafone, and was specifically appointed by President Obama to head the delegation. Kramer didn't hesitate to use strong

words. “Fundamentally, the conference, to us, should not be dealing with the internet sector,” he declared. “That carries significant implications that could open the doors to things such as content censorship.” He dismissed the Russian proposals out of hand. “What can happen is what are seemingly harmless proposals can open the door to censorship, because people can then say, listen, as part of internet security, we see traffic and content that we don’t like.”[19]

On Friday, December 7, a twenty-two-page document was passed to the conference’s organizer, the ITU. It was headed, “Russia, UAE, China, Saudi Arabia, Algeria, Sudan, and Egypt. PROPOSALS FOR THE WORK OF THE CONFERENCE.” The document had the insignia of the ITU globe at the top and was dated December 5, 2012. Although the document was written in English, it had been edited by someone with a computer in Cyrillic. Some of the editing changes were made by Maria Ivankovich, an expert at the Radio Research and Development Institute within the Russian Ministry of Communications, one of three major research centers involved in developing SORM, the Russian system of communications interception.

A day later, on December 8, the website wcitleaks.org made a splash in the media by publishing a link to the latest Russian proposal, which declared that member states have “the sovereign right to establish and implement public policy, including international policy, on matters of Internet governance.”[20] The proposal drew condemnation from around the world, and Krutskikh’s dream began to fall apart; the Egyptian delegation announced that despite the fact that its name was on it, it “never supported the document.” On December 10, without explanation, the Russian delegation withdrew it. It was reported that Touré talked personally to Nikiforov to persuade Russia to withdraw the proposal following American threats to walk out of the conference if the document was formally submitted.[21] Touré feared that the proposal could break up the conference completely, and he wanted the new treaty to be signed.

The Russian initiative failed spectacularly—strongly opposed by the United States and other Western governments.

At the last day of the conference, on Friday, December 14, a new treaty was offered for signing, and eighty-nine countries endorsed the document, including

Russia. Much of the language of the earlier drafts had been taken out, but the final document still contained Article 5B, which stated, "Member states should endeavour to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services."

It sounded rather unobjectionable. But the Western delegations were certain that this clause was intended, among other things, to support actions by governments that want to control content on the Internet, as Russia was striving to do. Kramer said the treaty was "seeking to insert governmental control over Internet governance" and, in a dramatic moment, walked out of the hall, destroying any prospects for a treaty.[22] On the whole, fifty-five countries refused to sign the new treaty, including Western European and Anglo-Saxon nations, and their refusal to sign the new treaty meant that the document simply could not be implemented.

Krutskikh was the only Russian official in Dubai willing to comment. "The Americans are the fathers and mothers of the Internet, and we have to appreciate that," he said with bitterness. "But words like 'Internet' and 'security' should not be treated like curse words. They have been treated like curse words by some delegations at this conference."[23]

The Kremlin had sought to recruit nations from around the world to change the rules of the Internet to give authoritarian countries the ability to censor it. But it didn't work. The nations involved in building the Internet, chiefly the United States, were dead set against it.

Krutskikh's dream slipped away.

A few months after the ITU disaster Krutskikh took part in a conference on information security in Russia. He spoke at length about the threats to Russia on the Internet, and when he finished, Irina approached him and asked for a comment about what had happened in Dubai. He was both angry and passionate, stating that the Russian initiative didn't fail because it was never officially on the table. Then he exclaimed, "We have not lost! Eighty-nine countries support us!" He vowed that Russia would continue to promote its model of global Internet regulation in every possible forum.

Snowden's revelations of mass surveillance of Internet and telephone metadata in 2013 prompted other countries to start thinking in terms of "national sovereignty" on the Internet, and the United States faced widespread condemnation and criticism. Brazil's communications minister said that local ISPs could be required to store data on servers within the country, saying local control over data was a "matter of national sovereignty." Later, Germany's Deutsche Telekom declared that it wanted to create a national Internet to protect Germany from privacy infringements. In February 2014 German chancellor Angela Merkel, furious at the disclosure that the NSA had monitored her cell phone, raised the prospect with French president François Hollande to build a European network so as to avoid data passing through US servers.

In June 2013 Presidents Obama and Putin agreed to establish a new working group within the US-Russia Bilateral Presidential Commission as part of a cyber security confidence-building measure between the two countries. To chair the group from the Russian side Putin appointed deputy secretary of the Security Council Klimashin, and Krutskikh was made the group's cocoordinator.[24] Putin clearly still trusted Krutskikh and his generals. The new working group gathered for the first time in November in Washington; the participants, our sources told us, consciously left Snowden's name out of the talks.

Krutskikh got a second chance. In February 2014 Putin appointed him his special representative for international negotiations on Internet regulation. On April 23–24, in São Paulo, Brazil, a conference was held, NETmundial. Provoked by Edward Snowden's revelations, it was a two-day global meeting on the topic of Internet governance. Nikiforov, the Russian minister of communications, noted that the conference delivered a standing ovation after a speaker expressed words of gratitude to Snowden. Nikiforov delivered welcoming remarks prepared by Krutskikh, and they had all his usual hallmarks—attacks on ICANN and calls to hand over all powers to the ITU. But against Nikiforov's expectations, the speech didn't go over well—the participants simply ignored Russia's proposals.

The very next day in Moscow Putin declared that the Internet was a "CIA

project" and that Russia needed to be protected from it.[25] His remarks were reported far and wide, overshadowing the Russian presentation at the conference, and Nikiforov's speech was omitted from the documents of NETmundial. The Russian ministry was outraged and published a protest on its site.[26]

Many countries were unhappy with the way the Internet was governed, but it didn't mean they would march in lockstep with Russia. They could be very critical of US dominance on the Internet or the way their citizens' personal data was circulated, but they were not ready to turn the global network into a collection of local Internets under the control of national governments.

The Kremlin's attempt to change the global rules of the Internet fell flat. But there were other ways Putin could experiment with digital sovereignty—for example, in a small, beautiful town on the Black Sea.

Chapter 12. Watch Your Back

In the center of Toronto, on Bloor Street, on a cold day in March 2013 we walked up the steps of a two-story English-style mansion with a tall round tower attached to it. During World War II the building was used to train pilots to identify weather patterns, but now it is part of the University of Toronto. Inside we found a bunch of geeks and researchers who worked to identify surveillance and filtering equipment on communications around the world.

We were met by Professor Ron Deibert, forty-nine years old, who, as a scholar, was deeply interested in the impact of the Internet on world politics. In the mid-1990s he moved to the University of Toronto because it had been the home of Canadian communications theorists Harold Innis and Marshall McLuhan. In 2001 the Ford Foundation offered him a $250,000 grant to conduct research on the Internet and international security, giving rise to a research center known as the Citizen Lab.[1] Deibert recruited ex-hackers, programmers, and researchers in an effort to discover hidden surveillance and content filtering on global networks.

In a few years Citizen Lab emerged as a primary source of data on repressive regimes' Internet intrusions and attacks on their critics and opponents. In 2009 they identified a massive intrusion into the computers of the Tibetan leader, the Dalai Lama, and on computers in 103 countries. The intrusion was called "GhostNet" and was believed to have emanated from China. Citizen Lab also revealed malware campaigns against Syrian activists and exposed how a remote intrusion and surveillance software called FinFisher was used against protesters in Bahrain and political dissidents in Malaysia and Ethiopia.

We met that day in the tower on Bloor Street. The group also included Masashi Nishihata and Sarah McKune from Citizen Lab as well as Eric King of Privacy International, the British organization concerned with privacy issues. Deibert showed us into the turret room under the ceiling of the tower, known to the staff as the Jedi Council. We joined the group to plan an investigation into Russian surveillance in the upcoming Olympic Games, scheduled for February 2014 at

Sochi on the Black Sea.

The games were a showcase for Vladimir Putin. In 2007 he had personally presented, in English, Russia's bid to the International Olympic Committee, and Russia won. In the years before the games Putin put the FSB in charge of providing security for the Olympics. In 2010 an FSB general, Oleg Syromolotov, was appointed as the chairman of the Russian group that would oversee security at the games. We described to the others at the meeting how Syromolotov, inside the FSB, was not in charge of counterterrorism operations, as might be expected; rather, he was a top counterintelligence officer at Lubyanka since 2000. He spent his entire career in the KGB and then the FSB, and for thirteen years he had directed FSB efforts to hunt down foreign spies. Now he was put in charge of providing security for a major international gathering that would host athletes, journalists, and political leaders from around the world. We told the group that Syromolotov's appointment was significant. It could mean that Russia viewed the games as an opportunity to collect intelligence.

We obtained a PowerPoint presentation about security at the games that was primarily concerned with the communications challenges, and we found something revealing on its final pages, which we shared with our colleagues. The slides revealed how SORM—the black boxes of the FSB that were placed on all kind of communications connections—were being deployed to Sochi to cover all communications at the games. The next to last slide gave a list of the black boxes' basic requirements, including that they should be able to "intercept all segments of the network," that the fact of SORM's presence there should be completely secret, that there should be an iron-clad system to avoid anyone discovering that they were being intercepted, and that they should be hidden from the personnel of phone companies and ISPs. We suggested to our colleagues that Russia was preparing to use surveillance of the same intensity that China had in the 2008 Summer Games in Beijing.

King, of Privacy International and a world-renowned expert in spotting the presence of surveillance equipment suppliers, had made it his passion to attend every expo on surveillance throughout the globe. He knew what SORM was about —he had come across this technology in Central Asia. He asked us, "What does it

mean that it is being upgraded for the Olympics? Does that mean that SORM will be combined with deep packet inspection [the system of infiltrating the content of communications]? If they were used together, would that transform the targeted surveillance into mass surveillance? In other words, would it help to identify and track, say, activists by words they use?"

We just didn't know. We thought there might be clues if we could find out what hardware and equipment was being used, but that would take some digging.

One thing we did know was that the FSB and Interior Ministry officials spoke openly and increasingly about their experiences in the 1980 Moscow Olympics more than three decades earlier. Officials had learned certain lessons about both surveillance and physical security of the Games. The lesson for surveillance was to monitor as much as possible; the lesson for physical security was to isolate the Games as much as possible.

In 1980 the Olympic Games were secured in a way that was only possible in the totalitarian Soviet state—Moscow was ruthlessly cleansed of any possible troublemakers, who were sent out of the capital, and the city stood empty for the two weeks of the competitions, surrounded by troops and with KGB officers at every corner. When some of the sporting events were underattended, the authorities just sent troops to fill the stands. The Moscow Olympics was surrounded by paranoia; the KGB prepared dozens of reports of foreign intelligence services' "hostile intentions" to undermine the games.

We underscored to the group in Toronto that the appointment of Syromolotov, a top counterintelligence officer in the FSB, seemed to echo this Soviet-style approach. It was clear that in Sochi the authorities wanted to combine the KGB's traditional methods with cutting-edge surveillance technologies.

Those who gathered in Citizen Lab's tower that day knew how quickly the pace of electronic surveillance was growing in Russia. The FSB's supervision of the Olympics security meant that all measures were to be carried out under a veil of secrecy. For years it had been impossible to obtain comments from the FSB; the press office was effectively shut off from journalists' requests. Not only officials but also companies contracted by the authorities to provide security solutions were reluctant to talk.

Under the turret that day we acknowledged with the others that there were many unknowns. We felt that Russia was preparing something large and menacing in surveillance, but we didn't know how it would be actually used, how it would work, and what was the goal for the FSB: to gather intelligence using interception and surveillance, to stop protesters from reaching the site of the games, or maybe to use the surveillance measures as a big stick to intimidate and frighten possible troublemakers?

We also wondered about the future of SORM and what the Russian authorities wanted to do after the games ended. Was Sochi intended to be a laboratory to be replicated all over the country? After all, many security measures, first tested in Moscow in 1980, were then introduced on the national level. Even the antiriot police units known as OMON, which had beaten protesters during the demonstrations in 2011–2012, were formed because of the Moscow Olympics. What kind of legacy would Sochi leave in terms of surveillance and control of information?

The information games were afoot.

Once we got back to Moscow we decided to make a point of examining all kinds of open sources, including technical documents published on the government's procurement agency website, zakupki.gov.ru; Russian law requires all government agencies, including the secret services, to buy their equipment through this site. We also scrutinized presentations and public statements made by government officials and top managers of firms involved with the Olympics and security for the city of Sochi. We reviewed public records of government oversight agencies such as the telecoms watchdog Roskomnadzor. Soon we found out that our suspicions about upgrading SORM were correct.

The Russian Supreme Court keeps statistics about court orders issued for interception, but they are held deeply inside the court's filing system and are not in the open. For years finding such information was impossible; members of parliament told us they could not get it. Then a lawyer gave us a hint on how to

mine the data out of the computers. We followed the lawyer's advice and discovered what we were looking for—the court's statistics. We found that in six years Russia's use of SORM had skyrocketed: the number of intercepted phone conversations and e-mail messages doubled in six years, from 265,937 in 2007 to 539,864 in 2012. These figures do not include counterintelligence eavesdropping on Russian citizens and foreigners, the area of Syromolotov's department.

It was hard to find specific details about SORM deployment in Sochi, so we turned to the data of Roskomnadzor, the communications watchdog that was very busy making sure SORM equipment was properly installed in the Sochi region. We discovered that several local ISPs were fined for having failed to install Omega, the SORM black box recommended by the FSB. One document from Roskomnadzor showed that in November 2012 the ISP Sochi-Online was officially warned for "failing to introduce the required technical equipment to ensure the functioning of SORM."

Our suspicions about SORM deepened on April 8 when Gus Hosein, director of Privacy International, forwarded us a US State Department warning for Americans wanting to attend the Olympics in Sochi. The document, issued by the department's Bureau of Diplomatic Security, carried the title, "Russian SORM Factsheet, Winter Olympics; Surveillance; Cyber," and it warned that when traveling to Russia, people "should be aware that their telephone and electronic communications may be subject to surveillance, potentially compromising sensitive information." The warning then went into details describing SORM, stating that the system "permits the monitoring, retention and analysis of all data that traverses Russian communications networks." The document warned people heading to Sochi to be extremely careful:

> Consider traveling with "clean" electronic devices—if you do not need the device, do not take it. Otherwise, essential devices should have all personal identifying information and sensitive files removed or "sanitized." Devices with wireless connection capabilities should have the Wi-Fi turned off at all times. Do not check business or personal electronic devices with your luggage at the airport. . . . Do not connect to local ISPs at cafes, coffee shops, hotels, airports, or other local venues. . . . Change all your passwords before and after your trip. . . . Be sure to

> remove the battery from your Smartphone when not in use. Technology is commercially available that can geo-track your location and activate the microphone on your phone. Assume any electronic device you take can be exploited. . . . If you must utilize a phone during travel consider using a "burn phone" that uses a SIM card purchased locally with cash. Sanitize sensitive conversations as necessary.[2]

When we read this, we wondered what the Americans knew about SORM that we didn't.

A year before, in August 2012, the Americans were the most numerous spectators at the London Olympics, with over sixty-six thousand Americans attending the games.[3] It was clear that Americans would come by the thousands to Russia in February 2014.

Although we worried about the use of surveillance and interception in Sochi, it had a legitimate purpose in fighting terrorism. The threat and the reality of terrorism cast a long shadow over Sochi, and then it happened.

On April 15, 2013, Boston hosted its annual marathon, and 23,000 runners took part. About two hours after the winner crossed the finish line but with more than 5,700 runners yet to finish, two bombs detonated on Boylston Street. Three people were killed and more than 250 injured. The same day, using surveillance cameras, police identified two brothers as suspects, Tamerlan and Dzhokhar Tsarnaev. After a manhunt, the older brother, Tamerlan, was killed, and Dzhokhar captured. It was soon discovered that over a decade before the attack, their parents, ethnic Chechens, had moved the family to the United States from Dagestan, a Russian internal republic in the North Caucasus.

The terrorist attack had a lasting impact on the way the terrorist threat to the Sochi Olympics was viewed in the United States and around the world. It was long assumed that the militants in the North Caucasus were not interested in attacking Western targets. Since the 1990s the Chechen movement shifted from a nationalist agenda to make Chechnya independent, to one embracing radical Islam.

The Chechen's top commander, Dokku Umarov, proclaimed an Islamic state in the North Caucasus, the Caucasus Emirate, in October 2007, and since then militants spread across the republics of the North Caucasus, but primarily in Dagestan. They continued to attack Russians—developing a clear terrorist strategy, attacking civilians on the Russian mainland, including in Moscow, and killing law enforcement personnel in the North Caucasus. But foreigners were not in their crosshairs.

The Boston bombing raised questions about whether that had changed. To make things worse, in a few months thousands of Americans would fly close to the Islamists' stronghold; Sochi, one of the most beautiful places in South Russia, on the coast of the Black Sea, is geographically located at the foot of the Caucasus Mountains.

Soon it became known that the Russian FSB had sent messages in 2011 to the FBI and CIA about Tamerlan Tsarnaev.[4] Though these letters were not real warnings—rather, the FSB asked for information on Tsarnaev, fearing he could join the militants in Dagestan—this information inflamed public opinion in the United States, and there were calls for more cooperation between Russian and American security services. Putin and Obama spoke twice by phone in the wake of the marathon bombing.[5] A White House statement said Obama praised the "close cooperation" Washington received on counterterrorism from Moscow, stating, "Both sides underlined their interest in deepening the close cooperation of the Russian and US special services in the fight against international terrorism."[6] On May 11 British prime minister David Cameron said that the Russian and British security services would cooperate in the build-up to the Winter Olympics in Sochi after his talks with Putin, adding that Britain would be providing "limited" security support at the Olympic Games. "We both want the Sochi Games to be a safe and secure Games," he said.[7]

This was a bad time to be asking questions about surveillance at the Olympics. The bombings in Boston made many people more tolerant of surveillance because of tangible fears of terrorism.

Six months before the Olympics were to open, on August 19, 2013, Putin signed executive order, No. 686, that effectively turned the Olympics venue into a fortress.[8] It banned the entry of all vehicles and cars apart from those specially registered to Sochi from January 7 to March 21, 2014. Putin's order also prohibited any protests in the area of the Games during this period. But some of the fortress wasn't visible.

All those who wanted to visit the Olympics were required to pass through advance screening by the security services. The Russian authorities introduced a new security measure, a spectator pass that all visitors of the Games would need to have. To get it, a visitor was required to post his or her passport data and photo on a special website and wait for the FSB to check their information. If there were no suspicions, an applicant could receive a spectator pass, which bore his or her photo and name. Only with the spectator pass in hand could a visitor buy tickets to the Olympic competitions. The procedure was clearly aimed at gathering data on tens of thousands of people from across the globe.

In August 2013 Irina decided to get a spectator pass, so she went on the official Olympic website. Because the procedure required taking a photo, Irina clicked the function to do this. Her computer then warned her that the site "is requesting access to your camera and microphone. If you click 'Allow,' you may be recorded." This seemed suspicious, so we asked Citizen Lab's researcher Byron Sonne to look at the site more closely. "This image, where the Flash entity on the site is asking for access to your camera and microphone, does indeed appear pretty intrusive and downright creepy," he responded. We wondered whether this procedure was intended to collect legitimate information or to send a message that everybody was being watched.

We analyzed dozens of open-source technical documents published on the government procurement agency website as well as public records of government oversight agencies and presentations of companies contracted by the government. We confirmed that SORM had been greatly strengthened in Sochi for the Olympics.

In November 2012 it was announced that there would be free WiFi access at all the competition venues "for the first time in Olympic history" as well as in the

media centers and media hotels. But all users were required to login and provide their spectator pass details—the FSB wanted to make sure nobody went unrecognized.

Conventional security measures would be high at Sochi, with more than forty thousand police on duty and more than five thousand surveillance cameras installed across the city. To gather data from cameras, in 2009–2011 Sochi had a federal program called "Safe Sochi," and a centralized command and control center was built in the city. The cost of the program was more than 1.5 billion rubles (over $48 million), and 1.2 billion of that was provided by MegaFon, one of three national mobile operators. We also discovered that Sochi was to be the first Olympics that would use surveillance drones, with both the FSB and the Interior Ministry acquiring drones. The FSB also purchased sonar systems to detect submarines so as to prevent a sea-launched terror attack.

We wanted our investigation to come out before the Olympics, as we hoped that the international and national media attention to Sochi could help prompt the conversation about out-of-control surveillance throughout Russia. But where could we publish the story? When dealing with sensitive stories, Russian media preferred not to be the initial source. In our investigation project "Russia's Surveillance State," most of our stories were first published in *Wired* and only then translated and picked up by Russian media.

The *Guardian* seemed to us the obvious choice. The British newspaper put a great deal of effort into covering surveillance issues. In these months the *Guardian* had been running Snowden's revelations almost on a weekly basis, and the *Guardian*'s Luke Harding had been our friend since his days as a Moscow correspondent.

We wrote to Luke in early September, describing what we had. "Sochi is a terrific story," he answered. He forwarded our e-mail to the *Guardian*'s foreign editor and put us in touch with their new Moscow correspondent, Shaun Walker, whom we met at a Moscow café to discuss the story and possible repercussions. It

was a very sensitive story, and we didn't know how the Kremlin might react to such an account in a Western newspaper; the Games were Putin's personal project, guarded by the FSB. The decision was not easy for Shaun either; though he had been living for years in Moscow, it was his very first week as the *Guardian* Moscow's correspondent, and the FSB had expelled his predecessor, Luke Harding, from Russia two years before.

We spent three weeks editing and repackaging our investigation. Meanwhile Shaun worked on getting comments. But it was slow and painful. Finally Shaun said that the *Guardian* had decided to run the story on October 1. Then it was delayed. And then, a surprising development: on the morning of October 2 the authorities announced that there was to be a press conference about security measures at the Olympics, that day at 2:00 p.m. Shaun rushed to the RIA Novosti building, where the press conference was to take place. FSB official Alexey Lavrishchev was listed among the participants and stated, "No, the city of Sochi will not be like a concentration camp." He then recalled the London Olympics: "Video surveillance cameras were mounted everywhere, even, excuse me, in the toilets. None of this will happen in Sochi!" He stressed that security in Sochi will be "invisible and unnoticeable."[9] Shaun sent us a quick message, "Amazing press conference! He read off a sheet of paper for 15 minutes, then they had questions, but only Russian outlets." He added, "He scuttled off like a crab at the end."

The *Guardian* ran our investigation on Sunday, October 6, placing it on the front page and headlined, "Russia to Monitor 'All Communications' at Winter Olympics in Sochi." It added, "Exclusive: Investigation Uncovers FSB Surveillance System—Branded 'PRISM on Steroids'—to Listen to all Athletes and Visitors." The term "PRISM on Steroids" was coined by Ron Deibert, with PRISM referring to the especially intrusive NSA program designed to intercept communications without the knowledge of communications services providers, exposed by Snowden.

Three days after the *Guardian* piece was published, the major English-language Russian government propaganda outlet, the *Voice of Russia*, ran an interview with a pro-Kremlin expert about the story, full of personal attacks against us and Shaun Walker.[10] We had expected as much. But the next day the

position was changed: the same *Voice of Russia* published a story that seemed to come clean about what we were reporting. We were stunned at the admissions, particularly the headline that admitted that the authorities were tapping the phones. "Don't Be Scared of Phone Tapping During Sochi-2014, It's for Your Own Safety —Experts."[11] We were further surprised when these experts talked openly about the equipment installed. They admitted that "technological equipment of special services provides for eavesdropping on telephone conversations, as well as for analyzing social network and e-mail correspondence" and said that "this kind of control is the best way to spot terrorist activity and nip the problem in the bud."[12]

We began to wonder: Why was this being acknowledged so openly? Were all these sophisticated technologies going to be actually used at Sochi, or was it something else? Was it just the threat of surveillance being used to intimidate and deter? What really puzzled us was that the story was not met with the usual denials and silence; instead, the authorities were talking about it.

Even as the acknowledgment of the surveillance plans surprised us, we did a double-take on November 8, 2013, when Prime Minister Dmitry Medvedev signed an instruction listing all the parties who would be subject to FSB surveillance, including the organizers of the Games, all the athletes from around the world, judges for the competitions, and the thousands of journalists who would converge on Sochi.[13] The decree provided for the creation of a database for the users of all types of communication, including Internet services at public WiFi locations "in a volume equal to the volume of information contained in the Olympic and Paralympic identity and accreditation cards"; that is, the database contained not only each subscriber's full name but also detailed information guaranteed to establish his or her identity. The database contained "data on payments for communications services rendered, including connections, traffic, and subscriber payment," meaning it contained all information on who called whom or sent messages during the Games as well as the location of each call. In the language of intelligence agencies this is called "gathering metadata," the same

kind of data-harvesting that the US NSA carried out and Snowden exposed.

It was the openness of Medvedev's instruction that shocked us—it was posted on the government's website. What's more, it seemed to us that the authorities were trying, somehow, to signal that at the Olympics, watch your back, because we are watching you.

Medvedev's instruction required the government to store the data collected during the Games for three years and said the FSB must be provided "round-the-clock remote access to the subscriber database." That means the FSB, operating from a remote location, will have three years to explore by whom, when, and how often athletes, judges, and journalists attending the Games were contacted.

On November 13 three members of the European parliament tabled written questions that raised concerns about surveillance at the Sochi Olympics, referring in particular to our investigation. "Given that everybody seems to be spying on everyone else these days, it seems legitimate to ask questions not only about the EU and the United States but about Russia as well," said Sophie in 't Veld, a Dutch member of the European parliament and the author of the questions. "Russia is a particular problem because of the Olympics, which it is using as a pretext for stepping up surveillance, with no court oversight." She added, "I hope this will act as a wake-up call."[14]

On December 29, at 12:45 a.m., a suicide bomber walked in the hall of the railway station in Volgograd, about six hundred miles from the venue of the Olympics, and blew himself up. Eighteen people were killed. The next day around 8:30 a.m., a trolleybus that connects a suburb to Volgograd's downtown area was hit by a suicide bomber, killing sixteen people. Volgograd is a large city located in the South Federal District of Russia, the same district as Sochi. Militants from Dagestan organized the bombings, which raised fears that the Russian authorities would be unable to secure the Games and that the "ring of steel" Putin had declared was built around Sochi would not stop terrorists. The stakes were high, and Western leaders hastened to offer Putin more help in providing security.

Privacy concerns were set aside.

On Sunday, January 19, the Islamic militants in Dagestan claimed responsibility for the bombings. They also delivered a direct threat to the Olympics. In a video posted online two men addressed Putin, "If you hold these Olympics, we will give you a present for the innocent Muslim blood being spilled all around the world: in Afghanistan, in Somalia, in Syria." One of them added, "For the tourists who come, there will be a present, too."[15]

A few days before the video was posted, Dokku Umarov, a leader of Islamist extremists on the North Caucasus, was reported to have been killed by Russian forces, but it didn't eliminate the threat. The Olympics presented a tempting target for militants. In the 2000s strong censorship in the Russian media had deprived the militants of attention, and the movement was in decline. But for the Olympics the eyes of all major global news organizations were to be focused on Sochi.

At the time journalists spotted wanted posters with the images of three women who were suspected suicide bombers, so-called black widows, at the airport and in the Sochi hotels. Police launched an urgent search for possible suicide bombers and distributed the posters further. For months the Russian media had been under pressure to report everything around the Olympics in positive way, and now they were hesitant to report the news that black widows were being sought inside the "ring of steel." Then a local blog, blogsochi.ru, posted information about these suicide bombers. When NBC reported the news, the Russian media picked up the story. The authorities felt clearly uncomfortable; they had failed to prevent the news from spreading.

Meanwhile, after the publication of our investigation in the *Guardian*, dozens of Western journalists came to us, asking anxious questions about their communications before traveling to Sochi. Some of them were on their way back from Sochi to Moscow and told us stories of odd happenings with their phones and laptops in Sochi. Wacek Radziwiniwicz from the Polish newspaper *Gazeta Wyborcza* could not connect with the server in Warsaw, and his phone received wrong SMSs. "Our technicians told us not to use public Wi-Fi," said Nataliya Vasilyeva, Moscow correspondent for the Associated Press. "But sometimes we

used it, and every time the system required to provide all details for identification. It was like enter and say, 'Hello, it's me.'"[16] Andrei opted not to bring his laptop to Sochi when he traveled to the city with an NBC crew in early January.

Boris Nemtsov, an opposition leader in Moscow and a former deputy prime minister, had written a report, published in 2013 and prepared with help from Nikolai Levshits, a civil activist, that documented some of the corruption surrounding contracts for the Olympics. He suggested that more than half of the $50 billion spent on the Games had disappeared. Just before the Games, in January 2014, Levshits applied for a spectator pass to the Olympics. He tried twice, but every time the website sent him the same message: "Your application is rejected." He also noticed that the website tried to take control of his laptop.[17]

On February 5, two days before the opening ceremonies, Dmitry Kozak, the deputy prime minister responsible for the Olympic preparations, made a tour with foreign journalists around Sochi. Kozak had a surprising response to some criticism expressed by journalists about the conditions in the hotel rooms: "We have surveillance video from the hotels that shows people turn on the shower, direct the nozzle at the wall, and then leave the room for the whole day," he said.[18] His statement was bizarre but also struck us as containing a fascinating warning: we are watching you, even in the shower.

The Games opened on February 7, and the grand opening ceremony at the Fisht Olympic Stadium lasted for three hours. Forty thousand spectators came to watch the event, and Putin personally greeted the athletes. The official theme of the ceremony was "Dreams of Russia," and the mood was festive.

That same day the website nosochi2014.com, which had been launched in 2007 to protest the Sochi Olympics and to serve as a reminder of ethnic cleansing carried out against Sochi's native people—the Circassians—by Czarist Russia, was hacked and infected by malware.[19] Citizen Lab experts looked at the site and discovered that the site included a malicious JavaScript hosted on the domain e094bcfdc2d.com, which at the time of investigation, was hosted at an address registered to the Russian State Institute of Information Technologies and Telecommunications in St. Petersburg.

On February 19, four days before the Games ended, the protest band Pussy

Riot made a trip to Sochi to perform and planned to record a new video clip. They knew it could be difficult: after the group performed a punk prayer, "Mother of God, Chase Putin Away," in Moscow's Cathedral of Christ the Savior, they were considered an enemy of the state, and three of them were imprisoned. Anastasia Kirilenko, a journalist for *Radio Liberty*, was to accompany Pussy Riot in Sochi. They were well aware of surveillance and had talked details of the coming trip via ChatSecure, an encrypted smartphone messenger. One of the group's supporters gave them new cell phones that, in Sochi, they used exclusively. But it did not help Pussy Riot avoid surveillance. Video cameras spotted their car, and the police detained them a few times under false pretexts.[20]

Nevertheless, Pussy Riot managed to perform in Sochi twice. Five girls in colorful balaclavas started to shout out "Putin will teach you to love the Motherland" in front of the Sochi-2014 banner and were immediately attacked by a group of Cossacks, who beat them with whips, ripped their masks off, and threw the group's guitar away. Journalists recorded the group's performance and the Cossacks' intrusion. A bit later the group held another performance in central Sochi next to the Olympic rings in front of the city hall. Although police watched the event, they did not intervene. The video of the clip went viral.

The Russian secret services have had a long tradition of using spying techniques not merely to spy on people but to intimidate them. The KGB had a method of "overt surveillance" in which they followed a target without concealing themselves. It was used against dissidents. After all of the evidence we found of investments in cutting-edge surveillance technologies, the FSB primarily used them for intimidation; they wanted to showcase their surveillance and did not hide it, like the "overt surveillance" of the KGB. The authorities didn't deny our investigation—in fact, it was confirmed by the *Voice of Russia*, and Medvedev's decree, openly posted, also sent a strong signal. Even Kozak's comment, though extremely bizarre, seems to make the same point—in Sochi we are watching you everywhere.

But the intimidation didn't work. Committed bloggers, foreign journalists, Pussy Riot, and activists all managed to do their thing without much restraint. If the surveillance was built to prevent protests or bottle up information, then the surveillance state built in Sochi was a paper tiger. Still, publicly Sochi became a great personal success for Putin; he got support domestically and around the world. After all, nobody wanted to question the enormous $50 billion cost of the Games.[21] It was all justified by success: Russia was back. The games went off largely without a hitch—there was no terrorism and a great deal of national pride on display.

We don't know with any degree of detail how much interception or surveillance was carried out at Sochi using such things as SORM and other technology. But we think there is another possibility, equally disturbing: the Russian secret services gathered large amounts of personal data on all visitors to the Games, including diplomats, journalists, and all kinds of officials. And these efforts were planned and conducted under guidance of the top counterintelligence official in the country, and counterintelligence officers tend to play a long game. It cannot be ruled out that someday, long after the closing ceremony of the Olympic Games, any one of these people could be approached with the information collected in February 2014 in Sochi.