2 Control and Subversion in Russian Cyberspace

Ronald Deibert and Rafal Rohozinski

Introduction

It has become a truism to link censorship in cyberspace to the practices of authoritarian regimes. Around the world, the most repressive governments—China, Burma, North Korea, Cuba, Saudi Arabia—are the ones that erect digital firewalls that restrict citizens' access to information, filter political content, and stymie freedom of speech online. When we turn to the countries of the former Soviet Union—Russia and the Commonwealth of Independent States (CIS)—we should expect no different. The Economist *index of democracy* paints a bleak picture of political freedoms in the CIS (see Table 2.1; numbers represent the country's rank in the world).[1] Only two countries, Ukraine and Moldova, rank as *flawed democracies*, with the remaining 10 countries of the region described as either *hybrid regimes* or *authoritarian*.

Throughout the CIS, this creeping authoritarianism is evident in just about every facet of social and political life. Independent media are stifled, journalists intimidated, and opposition parties and civil society groups harassed and subject to a variety of suffocating regulations. And yet, in spite of this increasingly constrained environment, the Internet remains accessible and relatively free from filtering. The ONI has tested extensively through the CIS region, far deeper and more regularly in fact than in any other region in the world. To date we have documented traditional ''Chinese-style'' Internet filtering—the deliberate and static blocking of Internet content and services by state sanction—only in Uzbekistan and Turkmenistan. For the rest of the region, while connectivity may be poor and unreliable, and suffer from the usual rent-seeking distortions found in other developing country environments, the same basic content is available there as in the most open country contexts.

In our chapter, we explore this seeming disjuncture between authoritarianism in the CIS and the relative freedom enjoyed in Russian cyberspace, commonly known as RUNET. We argue that attempts to regulate and impose controls over cyberspace in the CIS are not necessarily absent (as ONI testing results may suggest) but are *different* than in other regions of the world. We hypothesize that CIS control strategies have

Table 2.1

INDEX OF DEMOCRACY		
Less Authoritarian	**World Ranking**	
Ukraine	53	Flawed democracy
Moldova	62	
Georgia	104	Hybrid regime
Russia	107	
Armenia	113	
Kyrgyzstan	114	
Kazakhstan	127	Authoritarian
Belarus	132	
Azerbaijan	135	
Tajikistan	150	
Uzbekistan	164	
Turkmenistan	165	
More Authoritarian		

Source: The Economist Intelligence Unit, ''The Economist Intelligence Unit's Index of Democracy 2008,'' 2008, http://graphics.eiu.com/PDF/Democracy%20Index%202008.pdf.

evolved several generations ahead of those used in other regions of the world (including China and the Middle East). In RUNET, control strategies tend to be more subtle and sophisticated and designed to *shape and affect* when and how information is received by users, rather than denying access outright.

One reason for this difference may be the prior experiences of governments and opposition groups in the region. State authorities are aware of the Internet's potential for mobilizing opposition and protest that goes far beyond the nature of content that can be downloaded from Web sites, chat rooms, and blogs. These technologies have the potential to enable *regime change*, as demonstrated by the eponymous color revolutions in Ukraine, Georgia, and Kyrgyzstan. By the same token, state actors have also come to recognize that these technologies make opposition movements vulnerable, and that disruption, intimidation, and disinformation can also cause these movements to fragment and fail. The failure of opposition movements in Belarus and Azerbaijan to ignite a wider social mobilization, along with the role that targeted information controls played in fragmenting and limiting the effectiveness of these movements, also points to the possible trajectory in which controls aimed at Russian cyberspace may be moving.

Our chapter unfolds in several steps. We begin by describing some of the unique characteristics of the ''hidden'' information revolution that has taken place in Russian cyberspace since the end of the cold war. Contrary to widespread perceptions outside of

the region, Russian cyberspace is a thriving and dynamic space, vital to economics, society, and politics. Second, we outline *three generations* of cyberspace controls that emerge from the research conducted by the ONI in this region. *First-generation controls*—so-called Chinese-style filtering—are unpopular and infrequently applied. While instances of filtering have been identified in just about all CIS countries, wide-scale national filtering is only pursued as a matter of state policy in two of the CIS states. Rather, information control seems to be exercised by way of more subtle, hidden, and temporally specific forms of denial. These controls can involve legal and normative pressures and regulations designed to inculcate an environment of self-censorship. Others, like denial-of-service attacks, result in Web sites and services becoming unavailable, often during times of heightened political activity. Still others, like mass blogging by political activists on opposition Web sites, cannot be characterized as an attack per se, although the outcome of silencing these Web sites is as effective as traditional filtering (if not more so).

These *second-* and *third-generation* controls are increasingly widespread, and they are elusive to traditional ONI testing methods. They are difficult to measure and often require in-depth fieldwork to verify. Consequently, many of the examples in this chapter are based on field investigations carried out by our ONI regional partners where technical testing was used to establish the characteristics of controls, rather than measure the extent of them. We hypothesize that, although these next-generation controls emerged in the CIS, they may in fact be increasingly practiced elsewhere. In the next section of the chapter we turn our lens beyond the CIS to find examples of second- and third-generation controls.

We conclude by arguing that, contrary to initial expectations, first-generation filtering techniques may become increasingly rare outside of a few select content categories, raising serious public policy issues around accountability and transparency of information controls in cyberspace. The future of cyberspace controls, we argue, can be found in RUNET.

RUNET

On July 6, 2006, Russian President Vladimir Putin fielded questions from the Internet at an event organized by the leading Russian Web portal Yandex.[2] It was the first time a Russian leader directly engaged and interacted with an Internet audience. The event itself made few headlines in the international media, but in Russia it marked an important milestone. The Internet had graduated to the mainstream of Russian politics and was being treated by the highest levels of state authority as equal in importance to television, radio, and newspapers. The question put to President Putin by the Internet audience also revealed a sense of the informal, irreverent culture of Russian cyberspace. Over 5,640 *netizens* wrote in to ask when the President first had sex. More surprising, perhaps, was that Putin replied.[3]

The rise of the Internet to the center of Russian culture and politics remains poorly understood and insufficiently studied. With the end of the cold war and the demise of the USSR, Russia and the CIS entered into a long period of decline. Economies stagnated, political systems languished, and the pillars of superpower status—military capacities and advanced scientific and technological potential—rapidly ebbed away. Overnight, the CIS become less relevant and dynamic. The precipitously declining population rates in the Slavic heartland, a wholesale free-for-all of *mafiya*-led privatization, growing impoverishment, and failing public infrastructure, all made the distant promise of a knowledge revolution led by information technologies seem highly improbable.

Moreover, the prospects for Russia and the CIS keeping up with the Internet and telecom boom of the late 1990s and early 2000s seemed, for many, a distant reality. By the time the USSR finally collapsed in 1991, it had the lowest teledensity of any industrialized country. Its capacity for scientific development, particularly in the field of PCs (which the USSR had failed to develop) and computer networking (which was based on reverse-engineered systems pirated from European countries) was weak to nonexistent. Moreover, Russian seemed to be a declining culture and language as newly independent CIS countries adopted national languages and scripts, and preferred to send their youth to study at Western institutions. In almost every major indicator of economic progress, political reform, scientific research, and telecommunications capacity, the countries of the CIS seemed headed for the dustheap of history. Not surprisingly, scholarly and policy interest in the effects and impact of the information revolution in the CIS waned, as attention focused on the rising behemoths in Asia (particularly China and India), and the need and potential of bridging the *digital divide* in Africa and the Middle East. And yet, during the last decade the CIS has undergone a largely unnoticed information revolution. Between 2000 and 2008 the Russian portion of cyberspace, or RUNET, which encompasses the countries of the CIS, grew at an average rate of 7,208 percent, or over five times the rate of the next faster region (Middle East) and 15 times faster than Asia (see Table 2.2).

More than 55 million people are online in the CIS, and Russia is now the ninth-largest Internet country in terms of its percentage of world users, just ahead of South Korea.[4] By latest official estimates, 38 million Russians, or a third of the population of the Russian Federation, are connected, with over 60 percent of those surfing the Internet from home on broadband connections. And these figures may be low. Russian cyberspace also embraces the global Russian diaspora that, through successive waves of emigration, is estimated at above 27 million worldwide. Many Russian émigrés reside in developed countries, but tend to live *online* in the RUNET. Statistics to back this claim are methodologically problematic, but anecdotal evidence suggests that this is the case. The popular free mail service mail.ru, for example, boasts over 50 million user accounts, suggesting that the number of inhabitants in Russia cyberspace may be significantly above the 57 million users resident in the CIS. And these figures are

Table 2.2

PROFILE OF INTERNET USE, PENETRATION, AND GROWTH IN THE CIS

Country	Population (2008)	Number of Internet Users	Internet Penetration (2008)	Internet Growth (2000–2008)
Armenia	2,968,586	172,800	5.8%	476%
Azerbaijan	8,177,717	1,500,000	18.3%	12,400%
Belarus	9,685,768	2,809,800	29%	1,461%
Georgia	4,630,841	360,000	7.8%	1,700%
Kazakhstan	15,340,533	1,900,600	12.4%	2,615.1%
Kyrgyzstan	5,356,869	750,000	14%	1,353.5%
Moldova	4,324,450	700,000	16.2%	2,700%
Tajikistan	7,211,884	484,200	6.7%	24,110%
Turkmenistan	4,829,332	70,000	1.4%	3,400%
Russia	140,702,094	38,000,000	27%	1,125.8%
Ukraine	45,994,287	6,700,000	14.6%	3,250%
Uzbekistan	27,345,026	2,400,000	8.8%	31,900%
Totals	267,567,387	55,847,400	20% (average 13.5%)	7,208%

Source: Miniwatts Marketing Group, ''Internet World Statistics, 2009,'' http://www.internetworldstats.com.

set to rise—dramatically. By official predictions, Russia's Internet population is set to double to over 80 million users by 2012.[5]

Paradoxically, the very *Russianness* of the RUNET may have contributed to hiding this ''cyber revolution.'' Unlike much of the Internet, which remains dominated by English and dependent on popular applications and services that are provided by U.S.-based companies (such as Google, Yahoo, and Hotmail), RUNET is a self-contained linguistic and cultural environment with well developed and highly popular search engines, Web portals, social network sites, and free e-mail services. These sites and services are modeled on services available in the United States and the English-speaking world but are completely separate, independent, and only available in Russian.[6] In a recent ranking of Internet search engines, the Russian Web portal Yandex was one of only three non-English portals to make the top ten, and was only beaten out by a Baidu (China) and NHK (Korea), both of which have much larger absolute user base.[7] Within RUNET, Russian search engines dominate with Yandex (often called the Google of Russia), beating out Google with 70 percent of the market (Google has between 18 and 20 percent).[8]

The RUNET is also increasingly central to politics. Elections across the CIS are now fought online, as the Internet has eclipsed all the mass media in terms of its reach, readership, and especially in the degree of free speech and opportunity to mobilize that it provides. By 2008, Yandex could claim a readership larger than that of the

popular mainstream newspapers *Izvestia, Komsomolskaya Pravda*, and *Moskovsky Komsomolets* combined.[9] The Russian-language *blogosphere*—which currently makes up 3 percent of the world's 3.1 million blogs—grows by more than 7,000 new blogs per day.[10] There are currently more Russian-language blogs than there are French, German, or Portuguese, and only marginally fewer than Spanish,[11] which is spoken by a larger percentage of the world population.[12]

This shift has been fueled as much by the growing state control over the traditional mass media as it has been by the draw of what the new online environment has to offer. Well-known journalists, commentators, and political figures have all turned to the RUNET as the off-line environment suffers through more severe restrictions and sanctions. Across the CIS, especially in the increasingly authoritarian countries of Uzbekistan, Belarus, and Kazakhstan, the RUNET has become the last and only refuge of public debate. Given its rapid ascent to the popular mainstream, it is paradoxical—and certainly a puzzle—that RUNET has elided filtering controls of the kind imposed by China on its Internet in all but a few countries. In the next section, we explore why that is the case.

Next-Generation Information Controls in the CIS

Although RUNET is a wild hive of buzzing online activity, it is not completely unregulated. Since its emergence in the early 1990s, RUNET has been subject to a variety of controls. Some controls have been commercial in motivation and represent crude attempts to use formal authority to create what amounts to a monopoly over secure communications and as means to seek rents.[13] This form of control has not been unique to RUNET and has extended to every other facet of post-Soviet life, from car registration through to the supply of gasoline, as an aspect of the great scramble to *prihvatizatsia* public assets that occurred during the early to mid 1990s.[14] Other controls have emerged from a legal system inherited from the Soviet era, which criminalized activities without necessarily seeking prosecution, except selectively. These forms of control effectively form the rules of the game for all informal networks. Their emergence in the virtual online world of the RUNET is transparent and natural.

But during the late 1990s, and especially following the color revolutions that swept through the CIS region, states began to think seriously about the security implications of RUNET, and in particular its potential to enable mobilization of mass social unrest. The first attempts at formally controlling cyberspace were legal, beginning with legislation enabling surveillance (SORM-II),[15] and later in 2001 with the publication of Russia's *Doctrine of Information Security*. While the doctrine addressed mass media and did not focus on RUNET specifically, it declared the information sphere to be a vital national asset that required state protection and policing. The doctrine used strong language to describe the state's right to guide the development of this space, as well as its responsibility to ensure that information space respects ''the stability of the constitu-

tional order, sovereignty, and the territorial integrity of Russian political, economic and social stability, the unconditional ensuring of legality, law and order, and the development of equal and mutually beneficial international cooperation.''[16]

The intent of the doctrine was as much international as it was domestic, establishing demarcated borders in cyberspace, at least in principle. The international intent of the doctrine appears to have been driven by a growing concern that Russia was falling behind its major adversaries in developing a military capability in cyberspace; efforts by countries such as the United States, China, India, and others to develop covert computer network attack capabilities risked creating a strategic imbalance.[17] Domestically, the doctrine was aimed at the use of the Internet by militant groups to conduct information operations, specifically the Chechen insurgency. Within a few years, most other CIS countries had followed suit, adopting variations of the Russian doctrine.

ONI Tests for Internet Controls in RUNET

The controls outlined previously are qualitatively different from the usual types of controls for which the ONI tests. Establishing empirical evidence of the effects of policies like SORM and the Doctrine of Information Security is challenging, since their application is largely contextual, their impact at times almost metaphysical. Such controls do not yield a technological ''fingerprint'' in the way that a filtering system blocking access to Internet content does. However, they may be just as effective, if not more so, in achieving the same outcomes. In its 2007 study of the policy and practice of Internet filtering, the ONI found that substantial and pervasive attempts to technically filter content on RUNET did not begin until 2004, and even then were isolated to Turkmenistan and Uzbekistan, with lesser attempts at filtering found in most other CIS countries (see Table 2.3)[18]

These reports have remained consistent in more recent rounds of ONI tests. And yet persistent *anecdotal* reports, as well as special monitoring efforts mounted by the ONI, reveal in the majority of CIS countries that *information denial* and *access shaping* is occurring, and on a significant scale, especially around critical events such as elections. The ONI carried out a number of special investigations, including mounting monitoring efforts during the 2005 parliamentary elections in Kyrgyzstan[19] and the March 2006 Belarus presidential elections.[20] These efforts yielded the first technically verified results that the RUNET was being deliberately tampered with to achieve a political effect.

The results obtained by ONI in the CIS are unique, and they differ significantly from the results obtained in ONI's global survey. They demonstrate that information controls in the CIS have developed in different ways and using different techniques than those found in other areas of the world. They suggest a much more sophisticated approach to managing networks through denial that is highly selective and event based, and that *shapes* access to the sources of information and means of

Table 2.3

SUMMARY RESULTS FOR ONI TESTING FOR INTERNET FILTERING, 2007–2008					
	No Evidence	Suspected	Selective	Substantial	Pervasive
Armenia			•		
Azerbaijan			•		
Belarus			•		
Georgia			•		
Kazakhstan			•		
Kyrgyzstan			•		
Moldova	•				
Tajikistan			•		
Turkmenistan					•
Russia			•		
Ukraine	•				
Uzbekistan			•	•	

communication in a manner that could plausibly be explained by errant technical failures or other random network effects. In the following sections, we define the three different generations of cyberspace controls and provide examples for each from our research in the CIS region. The three generations of controls are also summarized in Table 2.4.

First-Generation Controls

First-generation controls focus on denying access to specific Internet resources by directly blocking access to servers, domains, keywords, and IP addresses. This type of filtering is typically achieved by the use of specialized software or by implementing instructions manually into routers at key Internet choke points. First-generation filtering is found throughout the world, in particular among authoritarian countries, and is the phenomenon targeted for monitoring by the ONI's methodology. In some countries, compliance with first-generation filtering is checked manually by security forces, who physically police cybercafés and ISPs.

In the CIS, first-generation controls are practiced on a wide scale only in Uzbekistan and Turkmenistan. In Uzbekistan, a special department of the SNB (KGB) monitors the Internet and develops block lists that are then conveyed to individual ISPs who in turn implement blocking against the specific resources or domain names. The filtering is universal across all ISPs, and the SNB spot-checks ISPs for compliance. In Turkmenistan, filtering is centralized on the country's sole ISP (operated by Turkmentelekom), and access is heavily filtered. Up until late 2007, Internet access in Turkmenistan was severely restricted and expensive, limiting its access and impact.

Table 2.4

SPECTRUM OF CYBERSPACE CONTENT CONTROLS IN THE CIS

	First Generation		Second Generation				Third Generation			
	Internet Filtering	Policing Cybercafés	Legal Environment for Information Control[1]	Informal Removal Requests	Technical Shutdowns	Computer Network Attack	Warrantless Surveillance	National Cyberzones	State-Sponsored Information Campaigns	Direct Action
Armenia			•	•	•	•[2]				
Azerbaijan			•	•		•[2]				•
Belarus	•		•	•	•	•	•	•	•	•
Georgia			•							
Kazakhstan	•		•	•				•	•	•
Kyrgyzstan			•	•		•[3]				
Moldova			•				•	•		
Tajikistan			•	•				•		
Turkmenistan	•	•	•				•	•		
Russia			•	•		•	•		•	•
Ukraine			•							
Uzbekistan	•	•	•				•			•

1. Legal and Normative Environment for Information Control includes the following:

a. Compelling Internet sites to register with authorities and using noncompliance as grounds for filtering ''illegal'' content.

b. Strict criteria pertaining to what is ''acceptable'' within the national media space, leading to the de-registration of sites that do not comply.

c. Expanded use of defamation, slander, and ''veracity'' laws to deter bloggers and independent media from posting material critical of the government or specific government officials.

d. Evoking national security concerns, especially at times of civic unrest, as the justification for blocking specific Internet content and services.

e. Legal regime for Internet surveillance.

2. CNA has been used by both Azeri and Armenian hackers in an ongoing series of attacks. It is unclear whether these are the actions of individual hackers, or whether these groups receive tacit or direct support from the state. Attacks are directed against the Web sites of the opposing country, so are not a content control mechanism.

3. The DDoS attacks were outsourced to commercial ''black hat'' hackers in Ukraine. The party ordering attacks is unknown, but suspicion falls on rogue elements inside the security services.

A second practice associated with first-generation blocking is policing and surveillance of Internet cafés. In Uzbekistan, SNB officers monitor Internet cafés, often enlisting café owners to notify them of individual users who try to access ''banned'' sites. Many Uzbek Internet cafés now openly post notices that viewing illegal sites is subject to fine and arrest. On several occasions, ONI researchers have manually verified the surveillance.

Second-Generation Controls

Second-generation controls aim to create a legal and normative environment and technical capabilities that enable state actors to deny access to information resources as and when needed, while reducing the possibility of blowback or discovery. Second-generation controls have an overt and a covert track. The overt track aims to legalize content controls by specifying the conditions under which access can be denied. Instruments here include the doctrine of information security as well as the application of existent laws, such as slander and defamation, to the online environment. The covert track establishes procedures and technical capabilities that allow content controls to be applied ''just in time,'' when the information being targeted has the highest value (e.g., during elections or public demonstrations), and to be applied in ways that assure plausible deniability.

The legal mechanisms used by the overt track vary from country to country, but most share the characteristic of establishing double jeopardy for RUNET users, making requirements such that compliance sets the grounds for prosecution, and noncompliance establishes a legal basis for sanction.

The following are among the more common legal mechanisms being applied:

Compelling Internet sites to register with authorities and to use noncompliance as grounds for taking down or filtering ''illegal'' content, and possibly revoking service providers' licenses. This tack is effectively used in Kazakhstan and Belarus, and it is currently being considered in Russia. The mechanism is particularly effective because it creates multiple disincentives for potential Web site owners who must go through the hassle of registering with authorities, which leaves them open to legal sanction should their site be deemed to be carrying illegal content. It also creates double jeopardy for international content providers (such as the BBC, CNN, and others) and opens the question whether they should register their services locally. In practice, the registration requirement applies to them so long as their audience is local, and a failure to comply leaves open the option to filter their content for ''noncompliance'' with local registration requirements. On the other hand, registering would make the content they carry subject to local laws, which may deem their content ''unacceptable'' or ''slanderous'' and could lead to legally sanctioned filtering.

Strict criteria pertaining to what is ''acceptable'' within the national media space, leading to the de-registration of sites that do not comply. In Kazakhstan, opposition Web sites or Web sites carrying material critical of the government are regularly de-registered from the national domain. This includes a large number of opposition sites and, notably, the *Borat* Web site, ostensibly because the owners of the site were not resident in Kazakhstan as required by the Kazakh domain authority. In Belarus, the popular portal tut.by refused to put up banners advertising opposition Web sites, possibly for fear of reprisals (although those fears were not made explicit).[21]

Expanded use of defamation, slander, and ''veracity'' laws, to deter bloggers and independent media from posting material critical of the government or specific government officials, however benignly (including humor). In Belarus, slander laws were used to prosecute an owner of a Web site posting cartoons of the president. In both Belarus and Uzbekistan, the law on mass media requires that reporting passes the ''objectivity test.'' Journalists and editors are held responsible for the ''veracity'' of publications and postings, leading to a high degree of self-censorship. In Kazakhstan, there are several cases of oppositional and independent media Web sites being suspended for providing links to publications about corruption among senior state offices and the president.

Evoking national security concerns, especially at times of civic unrest, as the justification for blocking specific Internet content and services. Most recently, this justification was evoked in Armenia when the opposition demonstrations that followed the February 2008 presidential elections turned to violence leading to the death and injury of several dozen protesters. A 20-day state of emergency was declared by President Kocharian, which also led to the de-registration of popular Armenian political and news sites, including a site carrying the Armenian-language BBC service and the filtering of YouTube (ostensibly because of allegations that footage of the rioting had been posted to the popular video sharing site).[22] Similar filtering occurred during the Russian-Georgian crisis of 2008 when Georgia ordered ISPs to block access to Russian media. The blocks had the unintended consequence of creating panic in Tbilisi, as some Georgians perceived the blocks as a signal of impending Russian invasion of the capital.

The technical capabilities typical of second-generation controls are calibrated to effect ''just-in-time'' or event-based denial of selected content or services.[23] These techniques can be difficult to verify, as they can be made to look like technical errors. One of the more common techniques involves formal and informal requests to ISPs. Providers in the CIS are under constant pressure to comply with government requests or face any number of possible sanctions if they do not, from visits from the taxation police to revocations of their licenses. Such pressures make them vulnerable to requests from authorities, especially those that are conveyed informally. In Russia, top-level ISPs are in the hands of large telecommunication companies, such as TransTeleKom and Rostelecom, with strong ties to the government. These providers appear

responsive to informal requests to make certain content inaccessible, particularly when information could prove embarrassing to the government or its officials. In one such case, the popular Russian site—Kompromat.ru—known for publishing documents and photographs of corrupt or illegal practices (roughly analogous to the Web site wikileaks.com) was de-registered or filtered by several top-level ISPs (including TransTeleKom and Rostelekom). Service was later restored, and the blocking of the site was deemed ''accidental.'' Nonetheless, the Web site was inaccessible throughout the February 2008 Russian presidential poll.[24] Similar incidents have been documented in Azerbaijan, where Web sites critical of President Ilham Aliyev were filtered by ISPs, apparently at the request of the security department of the office of the president. [25] A similar dynamic is found in Kazakhstan, where a number of Web sites are inaccessible on a regular basis, with no official reason ever being given.[26]

Other, less subtle but nonetheless effective technical means include shutting down Internet access, as well as selected telecommunications services such as cell phone services and especially short message services (SMS). Temporary outages of the Internet and SMS services were employed by Belarus authorities during the February 2006 presidential elections as a means to limit the ability of the opposition to launch street demonstrations of the type that precipitated the color revolutions in Ukraine, Georgia, and Kyrgyzstan. At first, authorities denied that any interruptions had taken place, and later they attributed the failures to technical reasons.[27] Similar instances were reported (although not verified) to have occurred during the 2007 elections in Azerbaijan.

Second-generation techniques also make extensive use of computer network attacks, especially the use of distributed denial of service (DDoS) attacks, which can overwhelm ISPs and selected sites, and which make tracking down perpetrators difficult, since the attacks themselves are sold and engineered by ''black hat hackers'' and can be ordered by anyone. Such attacks were used extensively during the 2005 Kyrgyz presidential elections that precipitated the Tulip revolution.[28] They were also used during the 2006 Belarus elections against opposition political and news sites. In 2008, presidential and parliamentary elections in many parts of the region saw the significant use of DDoS attacks against the Web sites of major opposition leaders as well as prominent human rights groups. Recently, computer network attacks have been conducted by state-sanctioned ''patriotic hackers'' who act as vigilantes in cyberspace. A Russian hacker who admitted that officers from the FSB encouraged him brought down the pro-Chechen Web site ''Kavkaz center'' repeatedly.[29] There is strong suspicion that the May 2007 DDoS attacks that brought down most of Estonia's networks were the work of state-sanctioned ''patriotic hackers'' responding to unofficial calls from the FSB to ''punish'' Estonia over the removal of a monument to Soviet soldiers in Tallinn. Such attacks were also a prominent feature of the Russian-Georgian crisis of 2008. Several prominent investigations have been undertaken to determine attribution

in this case—including an ongoing one by the ONI's sister project, the *Information Warfare Monitor*—and to date no definitive evidence has been found linking the attacks to the Russian security forces.

Third-Generation Controls

Unlike the first two generations of content controls, third-generation controls take a highly sophisticated, multidimensional approach to enhancing state control over national cyberspace and building capabilities *for competing in informational space* with potential adversaries and competitors. The key characteristic of third-generation controls is that the focus is less on *denying* access than successfully *competing* with potential threats through effective counterinformation campaigns that overwhelm, discredit, or demoralize opponents. Third-generation controls also focus on the active use of surveillance and data mining as means to confuse and entrap opponents.

Third-generation controls include enhancing jurisdiction over national cyberspace and expanding the powers of state surveillance. These include warrantless monitoring of Internet users and usage. In 2008, Russia expanded the powers previously established by SORM-II, which obliged ISPs to purchase and install equipment that would also permit local FSB offices to monitor the Internet activity of specific users. The new legislation makes it possible to monitor all Internet traffic and personal usage without specific warrants. The legislation effectively brings into the open covert powers that were previously assigned to FAPSI, with the twist of transferring to the ISPs the entire costs associated with installing the necessary equipment. The SORM-II law was widely used as a model for similar legislation in other CIS counties, and it is expected that the new law will likewise become a standard in the CIS. Although it is difficult to verify the use of surveillance in specific incidences, inferences can be drawn from specific examples. In July 2008, a Moldovan court ordered the seizure of the personal computers of 12 individuals for allegedly posting critical comments against the governing party. The people were accused of illegally inciting people ''to overthrow the constitutional order'' and ''threaten the stability and territorial integrity of the Republic of Moldova.'' It is unknown how the authorities obtained the names of the people, but some suggest that an ISP provided them with the IP addresses of the users.[30]

Several CIS countries are also pursuing the creation of national cyberzones. Countries such as Kazakhstan, Tajikistan, and Russia are investing heavily into expanding Internet access to schools. These institutions are being tied to special Internet connections, which limit access only to resources found in the national Internet domain. These ''national zones'' are popular among some Tajik and Kazakh ISPs because they allow the ISPs to provide low-cost connectivity, as traffic is essentially limited to the national segment. In 2007, Russian authorities floated the idea of creating a separate Cyrillic cyberzone, with its own domain space and addressing scheme. National cyberzones

are appealing because they strengthen the degree of national control over Internet content. They also appeal to consumers, since access to them is less costly and the resources that can be found there are almost exclusively in the local language.

Other aspects of third-generation controls, such as state-sponsored information campaigns in cyberspace, are difficult to document, as they use surveillance, interaction, and direct physical action to achieve a disruption of target groups or networks. The intent of these campaigns is to effect cognitive change rather than to deny access to online information or services. The ultimate source of these campaigns is also difficult to attribute and can only be established through careful research or insider knowledge, since they are designed to render opaque the role of state actors. These techniques include employing ''Internet Brigades'' to engage, confuse, or discredit individuals or sources. Such action can include the posting of prepackaged propaganda, *kompromat*, and disinformation through mass blogging and participation in Internet polls, or harassment of individual users, including the posting of personal information.[31] This technique, along with the use of surveillance of Internet traffic to affect direct action, saw a marked increase in the run-up to parliamentary and presidential polls in Russia. Numerous accounts allege that progovernment forces monitored opposition Web sites and disrupted planned rallies and marches. In some cases, members of the opposition were warned by cell phone not to participate in rallies or risk being beaten. In other cases, false information was disseminated by progovernment forces, leading to confusion among opposition supporters and, in one documented case, leading them into an ambush by progovernment supporters where several were severely beaten.

Assessing the Evolution of Next-Generation Controls in the CIS

The three generations of controls are not mutually exclusive, and several can exist concurrently. Taken together, they form a pattern of control that is both unique to each country and generalizable to the region as a whole. However, the degree to which a country is more or less authoritarian does seem to influence the choice of ''generational mix'' applied. Countries with stronger authoritarian tendencies tend to apply more comprehensive information controls in cyberspace, often using all three generations of controls. Conversely, countries that are ''more democratic'' tend to favor second- and third-generation strategies. None of the six countries scoring as ''hybrid regimes'' or ''flawed democracies'' applied first-generation controls (see Figure 2.1).

Several factors can explain this pattern. The most obvious explanation of the general tendency is that authoritarian states will seek to dominate the public sphere. These states tend to be the most vulnerable to mass unrest, prompting additional efforts by security forces to ensure that all channels of potential mobilization are controlled. A second factor worth noting is that these six counties are also experiencing the fastest rates of Internet growth and, with the exception of Belarus, have among the lowest

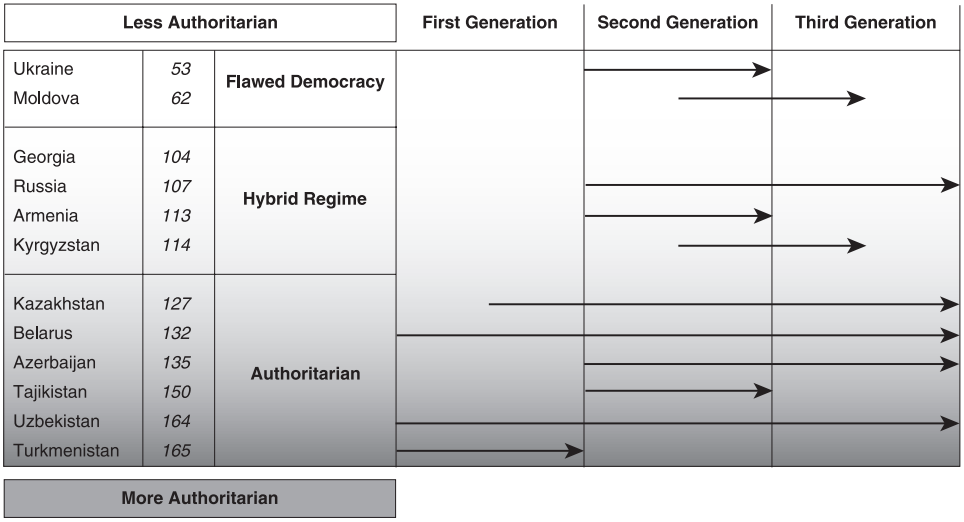

Figure 2.1
Spectrum of cyberspace content controls in the CIS (clustered by generation and EIU Index of Democracy)
Source: The Economist Intelligence Unit, "The Economist Intelligence Unit's Index of Democracy 2008," 2008, http://graphics.eiu.com/PDF/Democracy%20Index%202008.pdf.

levels of Internet penetration in the region. This latter explanation, which suggests that the RUNET in these counties has not become the locus for informal networks that it has in some of the less authoritarian countries, may make it more vulnerable and a target for filtering controls than what would be the case elsewhere in the CIS where the RUNET is more central to the political mainstream. In this respect, the maturity of the network itself seems to influence the degree to which filtering controls will be applied. This observation begs the obvious question—will the RUNET remain open even as countries in the CIS slide toward a new authoritarianism?

While the possibility of greater direct content controls being applied in the RUNET certainly exists, there is a far greater potential that information controls will continue to evolve along the evolutionary trajectory, toward strategies that seek to compete, engage, and dominate opponents in the informational battle space through persistent messaging, disinformation, intimidation, and other tactics designed to divide, confuse, and disable. In this respect, the patterns of information control in the CIS may in fact represent a model that will evolve elsewhere as governments are faced with the choice of imposing harsh controls and being labeled pariahs or doing nothing and risking that the technologies could become enablers of hyperdemocracy and undesired regime change.

Conclusion: Next-Generation Controls Beyond the CIS?

There are several obvious and not so obvious reasons to believe that second- and third-generation controls will become more common outside of the CIS and in fact may presage the future of cyberspace controls as a whole. First, the experience from other regions suggests that first-generation filtering is easy to circumvent. The ''Great Firewall of China'' is easily breached, as evidenced by the growing number of circumvention technology solutions, from Tor to Psiphon and others. As such techniques become more common, enabled and supported by large-scale and distributed efforts in the United States and Europe, the incentives to rely on less technologically static and temporally fixed methods characteristic of next-generation controls will likely grow.

It is also questionable whether first-generation controls in countries like Burma, North Korea, and China are really sustainable in the long run. In China's case, the floodgates may open sooner rather than later as the Chinese Internet itself becomes much more central to popular culture. First-generation filtering practices can produce economic and other social costs through collateral filtering and disincentives for foreign direct investment and tourism. As countries become more dependent on cyberspace for research, business, and other international communications, the friction introduced by filtering becomes increasingly unpopular, costly, and impractical.

More important than these factors, however, is the growing legitimization and frequent practice of policing the Internet through indirect and distributed means, and in particular through third parties, including the entities that actually support the cyberspace infrastructure, from connectivity to hosting to social networking platforms. Since much of cyberspace is operated by the private sector, there are practical and legal limits to the direct reach of government controls. Controls have thus evolved downward and in a distributed fashion, in a significant privatization of authority, in conformity with second- and third-generation controls outlined previously. Naturally, the scope for second- and third-generation controls differs among authoritarian and democratic countries, but examples of each can be found in both contexts.

In China, for example, while much of the attention focuses on the technologies of the Great Firewall of China filtering access to the Internet, at least as much, if not more, of the information controls exercised in that country happen in a more distributed fashion and by private actors. Web hosting and social networking services are now routinely obliged to sign self-discipline pacts and follow rigid hosting protocols that limit what can be communicated online; search engines—including those owned by American companies like Google, Microsoft, and Yahoo!—routinely filter their search results, often more aggressively than the government does itself; and in the most extreme example, volunteer citizen groups—sometimes known in China as *50 cent brigades* for the amount they are purportedly paid for each post—swarm the Internet's chat rooms, blogs, and other public forums making statements favorable to the government.[32] The latter was dramatically demonstrated, in a clear example of

third-generation controls, during the time of the Olympics, when thousands of Chinese bloggers posted aggressively to counter what they perceived as anti-Chinese propaganda.[33] Whether the volunteer posts were managed or encouraged by the state, or simply benefited the state coincidentally, or some combination, is a vexing question nearly impossible to untangle. Such attribution problems are, in fact, one of the key characteristics of second- and third-generation controls and one of their greatest challenges for research projects like the ONI.

Outside of authoritarian contexts and among democratic countries, it is now common to hear of legal and market pressures being invoked to remove content from Web hosting and social networking platforms, and there is also a very noticeable trend to offload policing activities to ISPs, particularly in the areas of content controls around pornography, hate speech, and copyright violations. In fact, most industrialized democratic countries have passed far-reaching surveillance measures that enable widespread eavesdropping on e-mail, cellular phone, and other communications activities by requiring ISPs to retain and, when required, turn over such information to legal authorities.

Perhaps the strongest impetus toward second- and third-generation controls has emerged from a growing emphasis on cyber security and the recognition of cyberspace as a domain of military action. Military actors have come to understand cyberspace as a domain equal in importance to land, air, sea, and space, requiring a full spectrum of capabilities. This has meant developing weapons and tactics designed to disrupt, destroy, and confuse potential adversaries. For the most part, these capabilities have been kept quiet and under classification, but they are similar in intent and execution to the network attacks characteristic of second-generation information controls. Russia, China, and the United States have all developed doctrines and capabilities for operations in cyberspace that include computer network attacks, as well as psychological operations designed to shape the domain through selective filtering, denial of access to information, and information engagement. The intent and effect of these emerging doctrines is the same as those we have documented in second- and third-generation controls in the CIS—to silence information that is strategically threatening and sow confusion and doubt among opponents dependent on cyberspace for information and organization.

Overall, the lexicon of cyber security is shifting norms around acceptable behavior for intervention into cyberspace and generating new incentives for technological development. Pervasive surveillance, including deep packet inspection, is now an acceptable part of compliance with good security practices, despite the impacts on privacy protections. Similarly, the political rush to secure cyberspace is generating economic opportunities not seen since the Internet boom of the 1990s. However, unlike the 1990s when the rush was led by companies seeking to open up cyberspace, the current momentum is in the other direction. The fact that defense contractors are now lining up to compete in this domain only raises the troubling concerns that some of the

valuable freedoms gained over the last 15 years in cyberspace will be sacrificed at the altar of security.

These are troubling tendencies, and ones with implications far outside of the democratic countries of the OSCE. The confluence of second- and third-generation controls, the militarization of cyberspace, and the legitimization of surveillance are contributing to a dangerous brew. The cyberspace enjoyed by the next generation of users may be a very different, more regulated, and less empowering domain than that which was taken for granted in the past.

Notes

1. The Economist Intelligence Unit, *The Economist Intelligence Unit's Index of Democracy 2008* (The Economist, 2008), http://graphics.eiu.com/PDF/Democracy%20Index%202008.pdf.

2. Radio Free Europe, ''Putin Quizzed by Internet Users,'' July 6, 2006, http://www.rferl.org/featuresarticle/2006/07/40C4C298-C619-4FCC-9D9D-D24787E10EAB.html.

3. ''When did you start to have sex?'' asked Kommersant reporter Andrei Kolesnikov on behalf of 5,640 Internet users. ''I don't remember when I started. But I can remember the last time,'' Putin replied. *St Petersburg Times*, ''Putin Weighs In on Robots, Sex Following Internet Conference,'' July 11, 2006, http://www.sptimes.ru/index.php?action_id=2&story_id=18178.

4. As of March 31, 2009, the top five countries with the highest number of Internet users, in order are China, United States, Japan, India, and Brazil. See Miniwatts Marketing Group, ''Top 20 Countries with the Highest Number of Internet Users,'' March 31, 2009, http://www.internetworldstats.com/top20.htm.

5. Between 2005 and 2007 Internet use in the Russian Federation jumped from 15% to over 28% of the population.

6. Popular sites include rutube, a Russian version of the popular U.S. site YouTube, as well as the social network sites odnoklassniki.ru and vkontakte.ru, which are modeled after Classmates.com and Facebook.com.

7. China has an estimated 298 million Internet users, while Korea possesses over 48 million users and a 76.1 percent Internet penetration. Miniwatts Marketing Group, ''Top 20 Countries with Highest Number of Internet Users,'' March 31, 2009, http://www.internetworldstats.com/top20.htm.

8. More significant yet than its impressive growth has been the emergence of RUNET at the center of Russian popular culture. Internet memes and jokes once marginalized to the community of computer specialists and aficionados are now in the mainstream of popular culture. For example, *Preved Medved*, an allusion to primitive cartoon of a bear surprising a couple having sex in a field and shouting *preved* (a deliberate misspelling of *privet*—a greeting, and *medved*—bear) has become a cultural icon, showing up on the cover of mainstream journals, in advertisements, and even, as a joke, in a question put to President Putin. Similarly, the *Olbanian* language, once an obscure Internet in-joke is now mainstream enough to have warranted a joke by President-elect Medvedev, who, when asked whether it should become a school subject, replied, ''One cannot ignore the

necessity of learning the Olbanian language.'' The slang it inspired has also led to political neologisms, such as *Putings*, which refers to political meetings in support of former President Putin, and whose usage on-air (as opposed to online) landed a Russian TV journalist a stiff fine.

9. LiveInternet, ''Report: From Search Engines, 2009,'' http://www.liveinternet.ru/stat/ru/searches.html?slice=ru.

10. Nick Wilsdon, ''Yandex Releases Autumn Report on Russian Blogosphere,'' Multilingual Search, November 12, 2007, http://www.multilingual-search.com/yandex-releases-autumn-report-on-russian-blogosphere/12/11/2007.

11. Yandex, ''*Sostoyaniye Blogosfery Rossiykogo Interneta*,'' [The State of the Russian Blogosphere], 2007, http://download.yandex.ru/company/yandex_on_blogosphere_autumn_2007.pdf.

12. Raymond Gordon, Jr., ed., *Ethnologue: Languages of the World*, 15th ed. (Dallas: SIL International, 2005).

13. For example, in mid-1995 the Federal Agency for Communication and Information (FAPSI) announced a joint venture with Relcom to create a secure business network. But FAPSI's interests in Relcom had less to do with security than with its growing business interests. FAPSI recognized that the Internet was becoming an important channel for business transactions. It wanted part of this market. Its intervention was part of a broader effort aimed at using its special position with respect to responsibility for state communications and security as means to seek rents from Russian and foreign businesses. By the time the Relcom deal had been announced, FAPSI had already secured legislation that required all use of cryptography in Russia to be licensed by FAPSI. Similarity, it had won the exclusive right to produce smart cards for the Russian market. Both moves had essentially given it a monopoly over the critical technologies required by the banking sector in Russia, as well as a future stake in all e-commerce. FAPSI was also present in the telecommunications market more broadly. The legislation creating Sviazinvest, the state-dominated holding company that owned shares in Russian telecommunications companies, required that senior officers from the service were present on the board of every major telecommunications player. Before long, the boards of most telecommunications companies were filling up with retired ex-FAPSI generals. In 1997 the FAPSI–Relcom deal collapsed, as the agency itself was disbanded over allegations of corruption by its leadership. Its assets, which included most of Russia's signal intelligence capacity, were reabsorbed into the FSB. But by that time, Relcom's dominance of the Internet market in Russia and the CIS was on the wane. The Internet was becoming a profitable business, and telecom operators where quickly entering the Internet market and putting former Relcom nodes out of business.

14. The term ''prihvatizatsia'' is slang, and a neologism of the Russian word for ''theft'' and the English term ''privatize.''

15. See the Russia country profile in this volume.

16. Security Council of the Russian Federation, *Information Security Doctrine of the Russian Federation*, 2000, http://www.scrf.gov.ru/documents/5.html.

17. Two years prior to the publication of this doctrine, Russia began actively working through the UN to establish an arms control regime in cyberspace. A. A. Streltsov, ''International Information Security: Description and Legal Aspects,'' *Disarmament Forum* 3 (2007), 5–13.

18. Ronald J. Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008).

19. OpenNet Initiative, ''Special Report: Kyrgyzstan,'' April 15, 2005, http://opennet.net/special/kg/.

20. OpenNet Initiative, ''The Internet and Elections: The 2006 Presidential Election in Belarus (and Its Implications),'' April 2006, http://opennet.net/sites/opennet.net/files/ONI_Belarus_Country_Study.pdf.

21. Mikhail Doroshevich, ''Major Belarusian Internet Portal TUT.BY Introduces Restrictions for Internet Forums,'' E-Belarus.Org, June 28, 2005, http://www.e-belarus.org/news/200506281.html.

22. OpenNet Initiative Blog, ''Armenia Imposes Internet Censorship as Unrest Breaks Out Following Disputed Presidential Elections,'' March 11, 2008, http://opennet.net/blog/2008/03/armenia-imposes-internet-censorship-unrest-breaks-out-following-disputed-presidential-e.

23. Ronald J. Deibert and Rafal Rohozinski, ''Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet,'' in *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald J. Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008), 123–149.

24. As reported by ONI field researchers.

25. See the Azerbaijan country profile in this volume.

26. Reuters, ''Kazakh Bloggers Say Can't Access Popular Website,'' October 10, 2008, http://ca.reuters.com/article/technologyNews/idCATRE4995D020081010.

27. OpenNet Initiative, ''The Internet and Elections: The 2006 Presidential Election in Belarus (and Its Implications),'' April 2006, http://opennet.net/sites/opennet.net/files/ONI_Belarus_Country_Study.pdf.

28. OpenNet Initiative, ''Special Report: Kyrgyzstan,'' April 15, 2005, http://opennet.net/special/kg/.

29. John Varoli, ''In Bleak Russia, a Young Man's Thoughts Turn to Hacking,'' New York Times, June 29, 2000, http://www.nytimes.com/2000/06/29/technology/in-bleak-russia-a-young-man-s-thoughts-turn-to-hacking.html.''

30. Sami Ben Gharbia, ''Moldavia: Sequestration of Personal Computers of 12 Young People for Posting Critical Comments Online,'' Global Voices Advocacy, June 13, 2008, http://advocacy.globalvoicesonline.org/2008/06/13/moldavia-destruction-of-personal-computers/.

31. Anna Polyanskaya, Andrei Krivov, and Ivan Lomko, ''Commissars of the Internet: The FSB at the Computer,'' Vestnik Online, April 30, 2003, http://www.vestnik.com/issues/2003/0430/win/polyanskaya_krivov_lomko.htm.

32. David Bandurski, ''China's Guerrilla War for the Web,'' *Far Eastern Economic Review*, July 2008, http://www.feer.com/essays/2008/august/chinas-guerrilla-war-for-the-web.

33. See the China country profile in this volume.