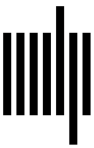
Access Controlled

The Shaping of Power, Rights, and Rule in Cyberspace

Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain

Citation:

Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace
Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain
DOI: 10.7551/mitpress/8551.001.0001
ISBN (electronic): 9780262266031
Publisher: The MIT Press
Published: 2010



The MIT Press

CIS Overview

Over the past four years the scale and reach of the Internet in the Commonwealth of Independent States (CIS) has continued to expand. As it has grown, a vibrant cyber culture has emerged, strengthened by a Soviet legacy, which has bequeathed the region with Russian as a lingua franca and common cultural and historical reference that continues to bridge the national boundaries between the former Soviet states.

Commensurate with its growth, the Internet domain in the CIS has emerged as a dynamic and complex environment in which states, cyber criminals, nongovernmental organizations, businesses, and individuals actively collude and compete. The region is currently driving the evolution of next-generation information controls encompassing legal regulation as well as innovative tactics such as the alleged use of third-party actors to generate crowd sourced denial of service attacks and other offensive means. These control tactics shape the information space through competition, rather than traditional filtering. There are also indications that these tactics and techniques are now being adopted in other regions.

Consequently, since the last OpenNet Initiative (ONI) volume, *Access Denied*, the CIS region has provided a number of new developments in information controls. The region witnessed two cyberwars. The first was a campaign by pro-Russian (and allegedly state-sponsored) hackers, which paralyzed the Estonian Internet in May 2007. The second

was a similar campaign (also allegedly organized by nationalist pro-government Russian hackers) that occurred at the same time as major combat operations in Georgia (August 2008). The latter campaign targeting Georgian online media and government Web sites led Georgian authorities to filter access to Russian Internet sites (allegedly as a means of self-defense against Russian cyber propaganda) and resulted in an information vacuum in Tbilisi during the critical days where it was unclear whether Russian troops would stop their advance into Georgia.

Next-generation Internet controls have also been utilized during elections. For example, reports indicate that in Belarus, Kyrgyzstan and (allegedly) Russia[1] pro-government forces selectively used denial-of-service (DoS) attacks during elections in order to silence opposition and independent media. During periods of heightened political tensions, countries such as Armenia and Belarus have employed legal and technical means to seize control of domain space, or shut down access to the Internet.

In the last 20 years, rapid changes have been a constant phenomenon in the CIS, but Western-sponsored democratic reforms have only been partially successful. In recent years a new authoritarianism has emerged in the region, with many governments seeking to reassert control over the national information sphere.

At the same time, many countries of the CIS have adopted national development strategies that emphasize information technology (IT) as a means for economic growth, with some even declaring their intent to become regional ''IT powerhouses.'' However, as a consequence of the color revolutions in the early to mid-2000s in Ukraine, Georgia, and Kyrgyzstan, many CIS states—particularly those with authoritarian tendencies—are aware of the consequences that this ''technological empowerment'' may prompt. Many in the region now see the Internet and other communications channels in national strategic terms, and these countries have increasingly turned to security-based arguments—such as the need to secure ''national informational space''—to justify regulation of the sector. Consequently, the region is a leader in the development of next-generation information controls.

In 2007 and 2008, ONI tested for the presence of filtering in all CIS countries: Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan.

The results of ONI testing yield significant patterns of first-generation filtering in Uzbekistan and Turkmenistan. Uzbekistan pursued pervasive filtering of the kind found in China and Iran. Turkmenistan's Internet is even more tightly restricted, with access available only through a single government provider. In other countries, strong evidence of second- and third-generation controls is emerging, with filtering occurring at strategic junctures, as well as in indirect and less detectable ways often supported by restrictive legal regimes. In almost all countries, filtering also occurred on corporate networks (such as educational and research networks), where accepted usage policies (AUPs) dictated that inappropriate content was not permitted; or in ''edge locations''

such as Internet cafés, where the reasons for filtering were more benign (conserving bandwidth) or left to the discretion of the Internet café owners themselves.

The ONI methodology makes it difficult to detect second- or third-generation techniques, which often involve DoS attacks, or other means of eliminating or silencing Web sites that do not rely on filtering. In these cases, which include Kyrgyzstan, Armenia, Belarus, Estonia, and the Russian-Georgian war, the ONI relied on a network of researchers within these countries to run ad hoc and one-time tests, as well as to investigate specific instances where DoS attacks, or other forms of technical manipulation, were used to silence Web sites or other Internet-based communication tools.

The CIS Region: Ethnocultural Diversity and a Shared Historical Space

The CIS—a loose and largely ineffectual political organization—occupies most of the territory that once constituted the Union of Soviet Socialist Republics (USSR). Straddling a swath of Eurasia from the Pacific to the doorsteps of Europe, the Arctic Circle, and the deserts of Central Asia, this vast land mass encompasses 12 time zones, some 350 million people, and more than 100 distinct ethnic groups including all the world's major religions and at least three major linguistic communities (Slavic, Turkic, Farsi). The CIS remains dominated by the Russian Federation, which maintains its influence through economic, political, and defense ties, as well as popular culture that continues to predominate within the region. Russia is currently a major energy supplier to many CIS states, giving it considerable political muscle in the region.

The region's shared political heritage, together with the fact that many present-day leaders in the CIS governments and economies were also in positions of authority during the Soviet era, means that much formal and informal coordination continues to exist among and between member states, despite political differences that are at times difficult. On some occasions, this coordination has led to the adoption of similar approaches in legal and political development. Furthermore, the loose, informal coordination among officials is helped along by the fact that most countries share the same legal tradition, as well as similar organizational characteristics of the security forces and the distribution of powers among the judicial, executive, and legislative branches of government.

Notwithstanding their shared past, over the past few years CIS governments have not hesitated to challenge Russia's hegemony by seeking other political and military alliances with Western Europe and the United States. At an accelerating pace, governments are looking beyond their traditional partners to discover new international trade and economic routes. This approach even more distinctively defines the CIS as a quickly changing region: although CIS countries share a common cultural heritage, they are increasingly taking diverging paths in their political and economic development, mainly because of foreign influence and an emerging rivalry among them.

Access to the Internet in the CIS

Internet penetration rates in the CIS region have experienced significant growth over the last couple of years, though the figures are still low in comparison to Europe and other regions. Internet access is mainly clustered in urban areas and spread among youth. In contrast to gender penetration rates in most Asian and Middle East and North African (MENA) countries, the percentage of male and female users in the CIS is almost the same, perhaps reflecting the "equality" between sexes prevailing in the Soviet era.[2] Income levels in the CIS are generally low, while the costs of computers and connectivity are relatively high. Overall, Internet penetration in Russia lags behind that of other industrialized nations (27 percent as of 2008)[3] and is relatively high only in large cities (particularly Moscow and St. Petersburg). Among the CIS countries, Belarus has the highest Internet penetration rate, 29 percent for 2008. The popularity of the Internet in this country might be a response, at least in part, to the fact that Belarus is one of the countries with the toughest governmental control in the CIS. As a result, the Internet remains one of the few media where citizens can exchange viewpoints and obtain uncensored information from international sources.

Ukraine (with a 14.6 percent penetration rate) and Moldova (16.2 percent) have almost doubled their Internet access rates over the last couple of years. The states of Central Asia have also shown considerable growth in their Internet penetration rates: Kyrgyzstan (13.8 percent) has become a leader in this subgroup partly as a result of the state's policies aiming at further market liberalization. Kazakhstan (12.3 percent) follows closely. Uzbekistan and Tajikistan have measured a swift increase in the number of Internet users, with Uzbekistan at 8.8 percent and Tajikistan at 6.6 percent in 2008. Turkmenistan measures very low Internet penetration (1.4 percent), since until recently the Internet was a privilege only for elites. As of 2008 Azerbaijan had an Internet penetration rate of 18.3 percent, while Armenia and Georgia had penetration rates of 5.8 percent and 7.8 percent, respectively.[4]

Official figures, in most cases, are far from being accurate. Depending on the country, local sources show either higher Internet penetration rates or considerably lower (in Kyrgyzstan local sources show that only 7 percent of the population had access at the end of 2008).[5] Even among international organizations the estimates are strikingly different: the United Nations (UN) *e-Government Survey*[6] states that in Kyrgyzstan, Internet penetration was no more than 5.6 percent for 2008, while the International Telecommunications Union (ITU) provides figures almost three times higher for 2008. These discrepancies are partly due to difficulties in calculating the number of users in countries where most people share Internet access through their places of work or study (for example, workplaces account for over 51 percent of all users in Kyrgyzstan[7] and Belarus), as well as via Internet cafés, whose use is very high in some countries (around 30 percent for Uzbekistan). This shared use, and in some cases the creative

use of networks such as Fidonet to route traffic to and from the Internet, may result in considerable underestimation of the actual number of users.[8] In addition, some Internet service providers (ISPs) do not reveal the real number of customers in order to conceal their proceeds.

The Role of New Technology in the CIS

The CIS region showcases examples of just how profoundly the Internet can affect social and political life. The importance of the Internet to political and social life is affected by the general openness of the media in the country. In Uzbekistan and Belarus, for example, where the government controls the media and stifles political opposition, the relevance of the Internet to political and social life is very high. In Tajikistan relevance remains low, while in Turkmenistan the Internet is still reined in by the government to such an extent that simple access remains a problem, leaving little room for the Internet to significantly influence political and social life.

The Internet constitutes an effective political tool in the hands of the people. During sensitive times, when governments attempt a tough crackdown on the media, the Internet remains the only available source of information, a fact that determines its high impact on shaping groups and affecting behavior. At times, when faced with a ''state of emergency,'' governments attempt to shut down online news sources in order to limit the spread of oppositional materials. For example, in Armenia the president imposed severe restrictions on the media and the Internet after the presidential elections in February 2008. This situation by itself triggered waves of discontented reactions by bloggers and online media journalists, who were among the few who reported on these events outside the country. Their condemnation of the imposed restrictions was quickly taken on, spread on the Internet, and hence multiplied the effect of the government's critics both inside and outside the country.

The CIS demonstrates that information and communication technology (ICT) is not always deterred by low incomes, and its significance to political life grows quickly when people want to voice their opinion. Such examples were the Ukrainian Orange Revolution (November 2004),[9] the Rose Revolution in Georgia (2003), and recently the so-called Twitter Revolution in Moldova (April 2009). Even though Moldova is one of the poorest countries in Europe, Moldovans demonstrated that they are prepared to resort to the latest technologies when needed to unite and voice their discontent. Communicating by means of Twitter through the General Packet Radio Service (GPRS) on their mobile telephones, Moldovans revealed the growing role of social media in Eastern Europe as a political tool. Surprisingly, poor countries show a growing appetite for adopting new technology and catching up with the West. Turkmenistan is another example of how quickly technology can reach people when it is offered at competitive prices. For years operating only with one state ISP and limited access,

the country has been showing the lowest Internet penetration rate in the region. When a license for a private operator was granted, MTS began offering new services (GPRS/EDGE for the country). More than 500,000 people joined for about half a year,[10] which is 9–10 percent of the population. Citizens in CIS countries have expressed a growing enthusiasm for the Internet and 3G mobile services and have manifested their ''e-readiness'' in politically sensitive times. This trend raises the concern that governments already accustomed to controlling media and communications may wish to develop means to close down free speech outlets any time they feel threatened.

Government officials recognize the power of the Internet to affect political and social life, and have actively moved to compete for influence in the space. In Moldova and Azerbaijan, for example, ministers and heads of agencies are now required to maintain Web sites and blogs, and regularly give interviews to student organizations, broadcasting them over YouTube or IPTV as an effective means to reach out to young people. This is a relatively new development that demonstrates an awareness among the political elites that the Internet is an important channel for exerting influence over domestic audiences.

Moreover, a key aspect of the Internet's political significance remains understudied: as a person-to-person back channel for communications and social networking essential to daily life in Russia, where personal contacts and an ''informal economy of favors'' remain keys to ''getting ahead.''[11] In this sense, it is interesting to note that in Uzbekistan information obtained from the Internet is accepted as being more accurate than that secured from other sources, reflecting the culture's strong social networking aspect.

Legal and Regulatory Mechanisms to Control the Internet in the CIS

In recent years, the trend in all CIS states has been toward greater regulation of the national information space, which includes the Internet. While the constitutions of (nearly) all countries enshrine the principles of freedom of information and freedom of expression, the authorities have taken various legal steps to regulate and shape participation in this space. Such measures are described in the following subsections.

Restrictions on Access to or Dissemination of Certain Types of Content

Restriction of Internet Content under State General Laws Freedom of expression is an important feature in almost all constitutions in the CIS. But increasingly, laws, decrees, and administrative orders are used to limit the extent of these freedoms, and in general the tendency is toward restrictions which contradict in spirit, if not in law, the rights enshrined in constitutional documents. For example, freedom of information can be restricted when necessary to protect moral values, public order, national security, state secrets, and other privileged data (Belarus, Russia, and Tajikistan). Uzbekistan goes even further to limit freedom of information to safeguard national, spiritual, cul-

tural, and scientific potential. No specific laws explain satisfactorily the meaning behind such notions as ''public order.'' By referring to broadly defined values, the text apparently leaves leeway for authorities to prosecute users for any type of content that it considers ''illegal.''

In some cases, government officials have demanded that the ISPs—formally or informally—temporarily suspend sites detrimental to ''public order'' (Tajikistan). Some of these sites remain suspended for an indefinite period of time (Kazakhstan).

Restrictions Envisioned in the Internet Service Agreements between the ISPs and their Customers Meant to be an open medium encouraging freedom of speech and expression, the Internet has increasingly become a target for strict regulation. Governments are frequently expanding the scope of content that is not to be allowed on the Internet. At times, ISPs are setting strict rules for the users, which, if not complied with, can lead to the termination of service agreements. Some providers set broad restrictive rules as preconditions in the contract with the user (e.g., TurkmenTelecom, Kazakhstan); others may decide to limit access if they subsequently decide that the accessed content is ''inappropriate'' (Uzbekistan). Such ''inappropriate'' content is not strictly defined and open to broad interpretations and arbitrary decisions by the ISPs, or state authorities.

In some cases, ISPs are part of the state administration and are directly instructed by the government to introduce such restrictive legal provisions in the customer agreement. One such example is TurkmenTelecom, which cautions its users that Internet is not a ''place for unconsidered behavior'' and provides an extensive list of types of content that users are forbidden to access or disseminate online, such as violent behavior, foul language, and defamatory remarks, among others.[12] On other occasions, ISPs have been directly instructed by the state to envision restrictions to accessing online content. In Kazakhstan, for example, ISPs prohibit their customers from disseminating pornographic, extremist, or terrorist materials or ''any other information not in accordance with the country's laws'' over the Internet.[13] Such vague categorization opens the door for authorities to prosecute online journalists and bloggers on a broad range of issues. Such uncertainty contributes to growing self-censorship.

In a third category of cases, ISPs may not have been instructed by authorities to apply measures against certain online behavior or types of content posted on the Internet, but based on the repressive climate encouraging self-censorship, these ISPs are attempting to anticipate what the authorities may find objectionable and act accordingly in order to avoid losing their license, as is the case in Russia.

Registration Requirements for Internet Web Sites

CIS states are increasingly requiring Web sites to register as mass media, making them subject to national legislation governing content, defamation, and copyright, criminal offense to the state and officials, and others. Officials increasingly speak in favor of

registering all information outlets, including the Internet, as a means to exert control over the quality and character of media content (e.g., Belarus, Russia, Kazakhstan). Requiring such registration for Web sites would have a chilling effect on anyone seeking to publish on the Internet. They would become vulnerable to criminal or civil liability and would be an easy target for government prosecution, especially as the laws describing ''undesired content'' weigh in favor of the state. Moreover, failure to register a Web site creates a valid legal pretext under which such content can be deemed ''illegal'' by state authorities, thus providing a legal case for filtering the content or suspending the licenses of the ISPs. Posting ''illegal'' content also carries the risk of prosecution for the site owner or the user who posted such material, contributing to a climate of self-censorship, and generally dissuading anyone from posting content on the Internet.

In Uzbekistan, the law on mass media that holds journalists and editors responsible for the ''veracity'' of published materials has already brought about self-censorship among journalists and bloggers. The ''objectivity'' test is applied also in Belarus, where independent journalists, editors, and opposition leaders are frequently subject to arbitrary prosecution and arrest. In Russia, online forums have been added to the definition of mass media, setting a precedent for prosecution of social networking sites.

Defamatory Provisions

Defamation laws have been used successfully to prosecute civil and criminal cases against Web site owners for allegedly hosting ''defamatory'' content. In Belarus, for example, the definition of defamation and slander laws has been expanded to selectively prosecute and deter bloggers, opposition leaders, and independent media from posting material critical of the government or specific government officials. On numerous occasions, Russian officials have spoken of the need to introduce specific legal measures that would allow them to prosecute online participants for defamation of members of the federal or regional state administration. In Russia, Uzbekistan, Kazakhstan, and Belarus, there are numerous cases of online journalists and bloggers being charged for defamation and subsequently jailed.

National Security Concerns

The need to develop ICT is a national priority in many CIS countries. Almost all CIS governments have adopted national ICT strategies that set ambitious targets for the development of the Internet in government, education, and industry. At the same time, most countries have also adopted national information security doctrines, which, on one hand, underline their understanding of the need to encourage development of the information sphere and, on the other, document their growing security concerns with regard to the Internet. Russia remains a significant influence in leading these tendencies within the region, and has been increasingly proactive in exporting its exper-

tise to other CIS states. Since late 2000, Russia's ''Doctrine of Information Security'' has been adapted (in various forms and guises) as the basic precept defining the national strategic value of the Internet and the ''national informational space'' in most CIS countries.[14]

Governments see the Internet as a very direct and personal media that reaches into people's homes faster and deeper than traditional media. As it is subject to less regulation and less control than the traditional media, its potential impact on national security is seen as greater than that of mass media. Consequently, several governments have actively moved to restrict foreign influences ostensibly to safeguard the citizens from being exposed to any ''damaging'' and subversive content online. This is the case in Kazakhstan and Turkmenistan, and in 2009 the issue of designating the Internet as a national strategic sector of the economy was included in Russian legislation for a second time.[15] Such a designation would limit the percentage of foreign investment in Internet companies and would expose the sector to a number of usage restrictions.

Surveillance

Russia's legal approach to Internet surveillance for law enforcement (that is, the System for Operational-Investigative Activities or SORM-II, which allows security services unfettered physical access to ISP networks) has influenced the way in which other CIS countries have approached surveillance of the Internet.

At the regulatory and technical level, SORM-II, (which came into effect in Russia in 2000[16]) requires ISPs to provide the Federal Security Service (FSB) with statistics about all Internet traffic that goes through the ISP servers (including the time of an online session, the IP address of the user, and the data that were transmitted).[17] The ISPs themselves are responsible for the cost and maintenance of the hardware and connections. Providers' objections to SORM-II, which raised concerns about individual privacy, resulted in the ISPs being stripped of their licenses.[18]

In many respects, SORM-II is not unlike a combination of the United States' Communications Assistance to Law Enforcement Act (CALEA)[19] and the recent ''warrantless'' provisions for wiretapping, including the PATRIOT Act[20] passed after the attacks of 9/11. Russian legislation formally protects individual privacy, prohibiting wiretapping of any kind without a court order.[21] As a consequence, SORM-II requires government personnel to obtain a court order to intercept telephone conversations, electronic communications, or postal correspondence. In reality, however, the FSB does not bother to seek a warrant. Recently, a senior FSB official sought to apply similar registration requirements for all mobile phones with Internet capabilities. However, despite this formidable surveillance potential, there is doubt about the actual capacity of the FSB to analyze the data collected.[22]

Most CIS countries have followed Russia's lead in implementing Internet surveillance. These include the following:

- Kazakhstan followed the Russian example, requiring ISPs to install SORM-II in order to register and maintain electronic records of customers' Internet activities.
- Azerbaijan made an unsuccessful attempt to employ technologies similar to SORM-II. As of 2009, surveillance does occur, but mainly by way of visits to ISPs and Internet cafés by officials from the State Security Service.
- In Uzbekistan, the principal intelligence agency, the National Security Service (SNB), monitors the Uzbek segment of the Internet and works with the main regulatory body to impose censorship. As all ISPs must rent channels from the state monopoly provider, available evidence strongly suggests that Internet traffic is recorded and monitored by means of a centralized system. SNB officers frequently visit ISPs and Internet cafés to monitor compliance.
- In Ukraine, the security services have developed a capacity to monitor Internet traffic, and legislation has been proposed to limit access to ''questionable'' content for reasons of national security. The security services are also empowered to initiate criminal investigations and use wiretapping devices.
- In Belarus, special services conduct active and warrantless surveillance of Internet activities under the pretext of national security using a system similar to SORM-II.

Russia, Belarus, Moldova, and Ukraine have all established specialized units under the Ministry of Internal Affairs (Department ''K'') trained in combating cyber crime. Specialized technical units have also been established in other security services and ministries of defense in these countries.

Other Means to Control the Internet

The ONI has documented the use of a wide range of measures to control the Internet—legal, administrative, and technological, as well as psychological: threats and physical violence, which usually are designed to cultivate a culture of self-censorship among Internet users. In some cases these measures are used only at times of heightened political tensions and are limited in scope and duration, making them difficult to document and report.

The following subsections list some of the second- and third-generation techniques documented by the ONI during the last four years.

Event-Based Interventions The CIS is the first region in which ONI research documented the presence of ''event-based'' filtering. This form of filtering differs in technical execution from more conventional filtering forms (such as those that rely on block lists) and is more difficult to track and definitively ascertain.

The Case of Kyrgyzstan (2005) During Kyrgyzstan's 2005 parliamentary elections, two ISPs were disrupted by distributed denial of service (DDoS) attacks. Following the

attacks, a ''hacker for hire'' posted threats to the affected ISPs' visitor logs, stating that unless these sites stayed off-line the attacks would continue.[23] The DDoS attacks effectively disrupted the ISPs' services because the hacker exploited the ISPs' narrow bandwidths and dependence on a single satellite-based connection. It remains unclear who hired the hackers responsible for the attack, although an investigation by ONI found that they were based in Ukraine (and were also responsible for an attack on a U.S. site using the same ''bot'' network). The opposition accused the government of ordering the attacks as a means of undermining them. The government responded by ordering the affected ISPs to keep their resources online, but it was impossible to do so because the DDoS attack had degraded their ability to provide any services. In the end, the attack was stopped as a result of U.S. legal action against the originating ''botnet,'' which had also been attacking a U.S. site. When the ''botnet'' was taken down, the attacks against the Kyrgyz sites also stopped.

The Case of Belarus (2006) During the March 2006 presidential elections in Belarus, several opposition Web sites became suddenly inaccessible, ostensibly because of innocuous network faults and domain name system (DNS) failures. Likewise, at the peak of protests against the election results, a major Minsk-based ISP ceased to provide dial-up services owing to ''technical problems.'' These occurrences meant that important independent media and opposition political Web sites were not accessible at periods when the information they were conveying could have had political significance or acted as a catalyst for further political action. Although nothing transpired that could be identified as extralegal filtering, de facto access was not available when and where needed, with some evidence suggesting that tampering may have occured.[24]

This form of ''event-based'' information control, which temporally shapes Internet access, can be said to represent the emerging next-generation Internet controls. Not unlike the shorter supply-line chains that boosted manufacturing efficiencies under ''just-in-time'' production, event-based filtering can also be considered to be ''just-in-time,'' as it offers greater efficiencies in denying access to information when and where it is needed. At the same time, the fact that this form of targeted and time-limited filtering is much harder to prove also removes the potential liabilities of being caught undertaking more deliberative filtering.

Crowd-Sourced Attacks: Pro-Government or Patriotic Hacktivists

During the August 2008 Russia-Georgia war over the breakaway territory of Ossetia, pro-government Russian hackers launched DDoS attacks against a wide range of Georgian ISPs and Web sites. As a consequence, the majority of Georgian government Web sites, as well as official media sites were inaccessible throughout the conflict. In response, Georgian ISPs filtered Russian Internet sites to prevent the dissemination of what they considered inaccurate and inflammatory reports by Russian media.[25] The effect of the Russian DDoS attacks and Georgian filtering was to create an information

vacuum in Georgia during crucial moments of the conflict, particularly as Russian troops crossed the Ossetian border and moved in the direction of the Georgian capital. While the Russian government denied responsibility for the cyber campaign, it did little to stop these activities, even though most of the attacks originated from crowdsourcing on Russian Web sites and chat rooms.[26] In many respects, the cyber campaign against Georgia resembled a scaled-up version of techniques previously used against opposition Web sites and independent media during elections in the CIS, and the earlier cyber attack against Estonia.

The emergence of cross-border hacktivist activities, however, is not a new phenomenon within the CIS. Similar attacks—albeit on a much smaller scale—have taken place between Armenia and Azerbaijan for more than a decade, where the moribund conflict over the region of Nagorno Karabakh continues in cyberspace.

Administrative Mechanisms to Shut Down Access to the Internet

Legal Deregistration of Domain Names and Web Sites Authorities often resort to various quasi-legal or ''administrative'' mechanisms to suppress ''inappropriate'' information or shut down oppositional domain names (e.g., Kazakhstan, Kyrgyzstan). In Armenia, the president created an unprecedented media and Internet blackout after announcing a state of emergency following public protests. Based on the president's instructions, the registrar of the top-level country domain suspended a number of independent media and opposition Web sites.

Pro-government and patriotic social activism has become a feature of politics in several CIS countries. In Russia, the pro-government *Nashi* youth movement ran an aggressive campaign in cyberspace in support of the government during the 2008 parliamentary and 2009 presidential elections.[27] The volume of blogs, online newspapers, and even posts to opposition and independent media sites overwhelmed and overmatched critical posts or articles, and has proven a more successful mechanism for silencing the opposition than resorting to Internet filtering or other more heavy handed repressive measures.

Self-Censorship The constitutions of the CIS countries prohibit censorship. Nonetheless, the net effect of the various sanctions (legal, administrative, technological) is creating a general climate of self-censorship among ISPs in many CIS states, which are fearful of jeopardizing their licenses, and among individuals for whom prosecution or imprisonment is too high a price to pay for voicing criticism. Often, self-censorship is aided by opaque state practices. Many CIS countries deny that they filter the Internet or resort to extralegal methods. In Azerbaijan, for example, the author of Web sites critical of the government was detained on a number of occasions (on no legal grounds) without any follow-up or prosecution. In other cases, such as the pervasive filtering

policies of Internet cafés throughout the region, the decision to limit content is formally controlled by the café owners, so it is difficult to argue whether their filtering results from a fear of sanction for allowing politically sensitive material to be accessed or from personal choice. Certainly, for most Internet café owners, the objective is to make a living, not to defy state policy. In Russia, self-censorship is sometimes perceived as a citizen's responsibility. In Tajikistan, however, research suggests that filtering is based on economic factors rather than fear of persecution from the security forces.

Emerging Second- and Third-Generation Controls in the CIS

Overt Internet filtering, such as that undertaken by China or Iran, is unlikely to occur in the CIS for several reasons. First, only in a very few cases (Uzbekistan, Turkmenistan) is the government disposed to effect an informational blockade of the country that could, in turn, jeopardize economic prospects and stifle the ''scientific potential'' of these technologies. Second, as noted earlier, governments generally have more subtle legal and quasi-legal methods for putting pressure on content and access providers to remove or otherwise eliminate ''undesirable'' content, so there is little need to resort to overt technical means such as filtering. Third, many CIS states are dependent on development aid and trade, and have oriented themselves toward integration with the global economy and are actively seeking to lower barriers on trade. Engaging in widespread filtering of the kind conducted by China or Iran would present the risk of being labeled as an ''international human rights pariah,'' an eventuality that most CIS countries would rather avoid. Fourth, and perhaps most important, CIS states that are concerned about the Internet's empowering potential—that is, its potential to make possible further ''color revolutions''—have found more subtle technical means for ensuring that these capacities are curtailed, if and when necessary.

Telecoms and ISP Market Players Until recently, almost all CIS governments preserved the monopoly right of the state telecommunication provider over international traffic. Under the pressure of international organizations (such as the European Bank for Reconstruction and Development, the World Bank, and the World Trade Organization), some CIS countries are abolishing the exclusivity provision over international traffic (Armenia). However, the need to demonopolize the service continues to be a significant problem in the rest (Kazakhstan, Turkmenistan, Uzbekistan). Since the traffic of all ISPs has to go through the state incumbent's channels, filtering can be achieved easily, without outside control, while using centralized resources. The ISPs may unknowingly receive filtered content because the main operator could install filters on any information that it deems inappropriate.

Russia, for example, does not require that the ISPs buy international traffic from a major state provider. Nonetheless, Russia has introduced other practices

unprecedented for other industrialized countries. There are multiple players on the Internet market, but few of these are the major ISPs that provide international traffic to the groups of small regional providers. Interestingly, most of the big telecommunication operators (if not all) are owned or controlled by the large state company Svyazinvest. Control in Russia is not easily detectable but permeates the ownership and control structure of the operators. The Russian Internet (including operators and popular blog servers) remains a playground of interests for the state and progovernment oligarchs.

Upstream Filtering

For its size, the CIS region has a relatively underdeveloped telecommunications system, much of which remains centered on Russia. At the same time, the region itself is contiguous with (or borders) Europe, Asia, and—via the circumpolar route—North America. This centrality means that most countries in the region obtain connectivity from several different sources beyond Russia. This situation has created some interesting patterns in filtering behavior, such as similar content becoming inaccessible across several different countries, but with different filtering patterns among content providers within any single country.

Some of the CIS countries are buying connectivity from European and Asian operators. An interesting phenomenon that ONI confirmed is that private operators sometimes effectively influence online behavior of foreign operators. For example, in 2008, YouTube was not accessible in Georgia for a few days because the main ISP in the country was buying international traffic from TurkTelecom. The Turkish operator, however, often executes bans against the multimedia site in the implementation of the controversial Internet law.[28] Since the local ISP provides Internet service to more than 85 percent of the users, this block rendered YouTube inaccessible to the majority of Georgians.

Judging by common indicators appearing in almost all CIS countries, ONI research suggests that providers reselling connectivity to CIS countries may be providing prefiltered access, passing on filtered content either as part of their service offering or as a consequence of the policies they use to manage traffic on their own networks. This form of blocking, which we have dubbed ''upstream'' filtering (indicating that the filtering is happening in a jurisdiction other than that of the state in question), was first observed during ONI testing in Uzbekistan in 2004. At that time, the traffic of one Uzbek ISP was clearly filtered using a pattern similar to that employed by Chinese ISPs. Further investigation revealed that the Uzbek ISP was buying connectivity from China Telecom, which in this case may have sold access to its network as it would to a regular Chinese client. Testing conducted by the ONI in 2006, 2007, and 2008 reveals similar patterns of prepackaged filtering affecting Internet services within several other CIS states where ISPs had purchased their connectivity from a Russian provider.

Conclusion

The CIS region is experiencing a general trend toward greater regulation and control of the national information space, which includes the Internet. Although most CIS countries do not practice substantive or pervasive filtering—with the exception of Uzbekistan and Turkmenistan—Internet content control through regulation or intimidation is growing throughout the region. Countries deny allegations that filtering based on ''official'' requests is taking place. Governments are becoming more creative in designing new ways to influence the content posted online and to shape the information environment. At times, filtering is justified by national interests or by other broad notions like ''public morals'' that answer the needs of the ruling elite and submit the rest to self-censorship.

Moreover, the laws are often unevenly applied, with ''flexible'' implementation often paired with other more subtle (but effective) measures designed to promote self-restraint (or self-censorship) of both ISPs and content producers. Information control —in particular the protection of national informational space—is clearly an issue of concern throughout the CIS, and it has encouraged more stringent attention to telecommunications surveillance. In addition, measures to deny access to Internet content at sensitive times, flagged as ''event-based filtering,'' to limit access to content geographically through ''upstream filtering,'' or to influence accessed information in a neighboring country because of international control of the Internet traffic routes are indicative of a new seriousness with which strategies for information control are being developed. The CIS region is leading the world in the evolution of second- and third-generation information controls. The trend toward new authoritarianism, combined with shifts in regional power relations that include a relative decline in U.S. influence and Chinese ascendancy, suggests a tendency toward greater control. These are unlikely to manifest themselves in Internet filtering as overt censorship, but rather will take the form of attempts to shape the information space creating a growing climate of self-censorship. The success (or lack thereof) of this approach is likely to shape policy choices well beyond the CIS region.

Notes

1. The OpenNet Initiative did not conduct formal testing or monitoring during the 2008 Russian parliamentary elections or the 2009 presidential elections. However, persistent allegations of denial of service attacks being used against opposition Web sites, and the mobilization of pro-government hacktivism by pro-government groups such as *Nashi*, were widely reported in the press. These tactics are consistent with those observed and documented by the ONI in Kyrgyzstan and Belarus.

2. Internet users in the CIS are predominantly young, aged between 15 and 25. Around 55 percent of all users in Azerbaijan belong to this age group, compared with 60 percent in Kyrgyzstan

and similar percentages in Uzbekistan. The number of women using the Internet in Uzbekistan and Kazakhstan is equal to or larger than the number of their male counterparts. The proportion is slightly in favor of men in Ukraine, while in Tajikistan only 22.5 percent of the Internet users are women.

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

4. Ibid.

5. Bishkek, ''Isledovanie auditorii Internet v Kyrgyzstane'' [Survey on the Internet Auditorium in Kyrgyzstan], 2009.

6. United Nations, *United Nations e-Government Survey 2008: From e-Government to Connected Governance*, http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN028607.pdf.

7. ''Obshtestvenyi Fond 'Grajdanskaya initsiativa internet politiki''' [Social Fund 'Civil Initiative for Internet Policy'].

8. Rafal Rohozinski, ''Mapping Russian Cyberspace: Perspectives on Democracy and the Net,'' United Nations Research Institute for Social Development (UNRISD) Discussion Paper 115, October 1999, http://unpan1.un.org/intradoc/groups/public/documents/UNTC/UNPAN015092.pdf.

9. Joshua Goldstein, ''The Role of Digital Networked Technologies in the Ukrainian Orange Revolution,'' Berkman Center Research Publication No. 2007-14, December 2007, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein_Ukraine_2007.pdf.

10. *Turkmenistan.ru*, ''MTS Podlklychila Turkmenov k Internetu'' [MTS Connected Turkmens to the Internet], April 18, 2008, http://www.turkmenistan.ru/?page_id=3&lang_id=ru&elem_id=12590&type=event&sort=date_desc.

11. Alena Ledeneva, *How Russia Really Works: The Informal Practices That Shaped Post-Soviet Politics and Business* (Ithaca, NY: Cornell University Press, 2006).

12. TurkmenTelecom, http://www.online.tm.

13. See the general user agreement between Nursat, a major ISP, and its customers at ''Public Contract,'' http://www.nursat.kz/?72.

14. Doctrine of the Information Security of the Russian Federation, September 9, 2000, No. Pr-1895, http://www.medialaw.ru/e_pages/laws/project/d2-4.htm.

15. An earlier attempt in 2008 to include the Internet in state legislation defining strategic sectors was removed upon second reading in the parliament.

16. Prikaz Minsviazi RF, Order of Ministry of Communications of the Russian Federation, 25 July 2000, http://www.libertarium.ru/libertarium/37988.

17. Freedom House, ''Russia'' in *Freedom on the Internet: A Global Assessment of Internet and Digital Media*, http://www.freedomhouse.org/printer_friendly.cfm?page=384&key=202&parent=19&report=79, (last accessed October 26, 2009).

18. Jeanette Borzo, ''Russian ISP Finds Court Victory Sometimes Is No Victory at All,'' *Wall Street Journal Interactive Edition*, October 5, 1999, http://www.libertarium.ru/libertarium/14424/def_article_t?PRINT_VIEW=YES.

19. The Communications Assistance for Law Enforcement Act (CALEA), passed in 1994 (P.L. 103–414, 108 Stat. 4279).

20. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (H.R. 3162), http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:.

21. Article 23 of the Constitution of the Russian Federation, http://www.constitution.ru/en/10003000-01.htm.

22. Interview with Andrei Richter, Director, Media Law and Policy Institute, Moscow State University, in Moscow, Russia, March 28, 2006; Interview with Alexey Simonov, President, Glasnost Defense Foundation, in Moscow, Russia, March 27, 2006.

23. OpenNet Initiative, ''Election Monitoring in Kyrgyzstan,'' February 15, 2005, http://opennet.net/special/kg/.

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

25. For more information on the Russia-Georgia cyberwar, refer to the Information Warfare Monitor (http://www.infowar-monitor.net), which followed and analyzed developments.

26. Ibid.

27. For more information on this new phenomenon, please refer to the Russia country profile in this volume.

28. For more information, refer to the Turkey country profile in this volume.

For information about special quantity discounts, please email special_sales@mitpress.mit.edu

This book was set in Stone Serif and Stone Sans on 3B2 by Asco Typesetters, Hong Kong.

Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Access controlled : the shaping of power, rights, and rule in cyberspace / edited by Ronald Deibert . . . [et al.] ; foreword by Miklos Haraszti.
p. cm. — (Information revolution and global politics)
Report from the OpenNet Initiative.
Includes bibliographical references and index.
ISBN 978-0-262-01434-2 (hardcover : alk. paper) — ISBN 978-0-262-51435-4 (pbk. : alk. paper)
1. Cyberspace—Government policy. 2. Internet—Government policy. 3. Computers—Access control. 4. Internet—Censorship. I. Deibert, Ronald. II. OpenNet Initiative.
HM851.A254 2010
005.8—dc22 2009049632

10 9 8 7 6 5 4 3 2 1