Internet Filtering in the **Commonwealth of Independent States**

Overview

As a former superpower—with a tradition of authoritarianism, poorly developed independent media, and lack of private rights—the Commonwealth of Independent States (CIS) would seem to be an ideal setting for substantial and pervasive Internet controls.[1] The reality, however, is variegated and complex. While the CIS region is home to some of the world's most repressive measures and advanced techniques for subtly "shaping" Internet access, it also showcases examples of just how profoundly the Internet can affect social and political life.

States within this region have a conflicted relationship with the Internet. Most 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." IT development is favored because it is seen to leverage the comparative advantage of the ex-Soviet educational system with its emphasis on mathematics and engineering, and the strong tradition of innovation in the computing and technology sector. Until its demise in 1991, the Union of Soviet Socialist Republics (USSR) was one of the few countries with a "homegrown" capacity in supercomputing, cryptography/crypto-analysis, and worldwide signals intelligence gathering. Currently many former Soviet citizens are among the leaders of the global IT industry.

At the same time, CIS governments are wary of the civil networking and resistance activities that these technologies make possible. In recent years, Ukraine, Georgia, and Kyrgyzstan have experienced "color revolutions," where networked opposition movements (albeit movements that are more reliant on cell phones than on the Internet) have effectively challenged and overturned the results of unpopular (or allegedly fraudulent) elections. Neighboring governments fear that these challenges were made possible by opposition groups leveraging IT to organize domestic protest (often with the help of foreign-

funded NGOs) and are therefore wary of leaving the sector unregulated and without control. Many 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.

In 2006 ONI tested for the presence of filtering in eight of the eleven CIS countries: Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, Ukraine, and Uzbekistan. Background and baseline testing was also carried out in a further two countries: the Russian Federation and Turkmenistan, although in these two cases limitations on the testing methodology do not allow us to claim comprehensive results.

Of the eight countries in which ONI tested, our results did not yield significant patterns of substantial or pervasive filtering. Only Uzbekistan pursued pervasive filtering of the kind found in China, Iran, and some parts of the Middle East.[2] In almost all countries some degree of filtering was present, but this filtering occurred mostly 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.

At the same time, in all eight countries authorities had taken steps of one kind or another to restrict or regulate their national informational space. These measures include:

- expanded use of defamation and slander laws to selectively prosecute and deter bloggers and independent media from posting material critical of the government or specific government officials (however benignly, including, as was the case in Belarus, through the use of humor);
- strict criteria pertaining to what is "acceptable" within the national media space, leading to the deregistration of sites that did not comply (Kazakhstan);
- moves to compel Internet sites to register as mass media, with noncompliance then being used as grounds for filtering "illegal" content;
- national security concerns (Ukraine); and,
- formal or informal "requests" of ISPs.

The net effect of these sanctions (legal and quasi-legal) is to create overall environments that encourage varying degrees of self-censorship among ISPs, who are fearful of jeopardizing their licenses, and among individuals for whom prosecution or imprisonment is too high a price to pay for voicing criticism, which at times amounts to little more than a form of digital graffiti.

The CIS region: Ethno-cultural diversity and a shared historical space

To define the CIS as a region understates the sheer diversity of the countries and peoples that fall within the former Soviet Union's historical boundaries. Straddling a swath of Eurasia from the Pacific to the doorsteps of Europe, the Arctic Circle, and the deserts of Central Asia, this vast landmass takes in twelve time zones, some 350 million people, and more than a hundred distinct ethnic groups encompassing all the world's major religions and at least three major linguistic communities (Slavic, Turkic, Farsi). At the ethno-cultural level, diversity is a defining commonality of this region.

At the same time, the CIS forms an historical community that for seventy years constituted the world's second major economic, military, and political superpower of the twentieth century, rooted in the same traditions of modernism as the West but oriented around a different set of

ideological and organizational principles. These principles emphasized a centralized and administered form of governance where the state rather than the market decided issues of economic and social production and where overarching leadership was vested in the Communist Party, whose rule was substantiated by ideological precepts that did not allow for dissention or opposition.

Despite this complex multinationalism, the former Soviet Union was dominated by Russia, which endowed the region with a common language (Russian) and popular culture, as well as defined trade, political, and even social ties (including the creation of substantial Russian minorities in some states, which persist to the present day). Even following the USSR's dissolution and the newly independent states' adoption of national languages and scripts (in Azerbaijan, Ukraine, Uzbekistan, and others), CIS countries retained strong ties with Russia. Transportation, communications, and energy routes continue to bind the region together. Russia is currently a major energy supplier to many CIS states, giving it considerable political muscle in the region (which it has not been shy to flex, when needed).

The region's shared political heritage, and 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 a great deal of formal and informal coordination exists among and between member states, despite political differences that are at times difficult. Furthermore, the loose, informal coordination among officials is helped along by the fact that most countries share the same legal codes and procedures, as well as similar organizational characteristics of the security forces and the distribution of powers among the judiciary, executive, and legislative branches of government.

The Internet in the CIS: Access and political significance

Internet penetration rates in the CIS region are relatively low and clustered among the urban youth—both male and female, perhaps reflecting the "equality" between sexes of the Soviet period.[3] Income levels in the CIS are generally low, while the costs of computers and connectivity are relatively high. This means that Internet use is lower than would be expected. Overall, Internet penetration in Russia lags behind that of other industrialized nations (15 percent as of 2005),[4] and is relatively high only in large cities (particularly Moscow and St. Petersburg). Among the CIS countries, Belarus has the highest Internet penetration rate of 30 percent; Ukraine and Moldova lag behind with less than 10 percent penetration rate, while the states of Central Asia have the lowest Internet penetration rates. Azerbaijan and Kazakhstan lead this latter subgroup with around 8 percent, followed by Kyrgyzstan. The least connected countries are Uzbekistan (3 percent for 2004) and Tajikistan, where only 1 percent of the population has access to the Internet.

However, in all cases these figures may be misleading. Most Internet users rely on shared Internet access, through their places of work or study, as well as via Internet cafés, whose use is very high in some countries, (for example, Internet cafés users account for over 50 percent of all users in Kyrgyzstan).[5] 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.[6]

The importance of the Internet to political life varies from low in Tajikistan to high in Uzbekistan. In Russia the relevance of the Internet as a source of news is reported as low; however, this estimation is changing as the Internet remains one of the few outlets for direct criticism of the government. Moreover, an important aspect of the Internet's political significance—as a person-to-person backchannel for communications and social networking essential to daily life in Russia (where personal contacts and an "informal economy of favors" remains a key to "getting ahead")—remains understudied.[7] In this sense, it

is interesting to note that in Uzbekistan information obtained from the Internet is accepted as being more accurate than from other sources, reflecting the culture's strong social networking aspect.

Legal and normative environment

In general, the tendency in all CIS countries has been toward greater government regulation of the Internet to bring it in line with existing regulations that control the mass media (in Russia, Uzbekistan, and Belarus, for example). To date, government actions to enforce more restrictive Internet environments have rarely been challenged—perhaps a reflection overall of the weakness of "opposition" parties in most countries, as well as poorly defined or tested laws governing the role of independent media. Nonetheless, some exceptions exist. For example, in Tajikistan and Azerbaijan concerted (if quiet) action by "civic" actors led to the reversal of policies aimed at removing politically sensitive content from cyberspace. In Tajikistan political Web sites that were banned during the December 2006 election were restored. In Azerbaijan a banned Web site that was critical of the government's policy of raising prices was restored and its author released from police detention. Both cases are significant because the initial order to "ban" the Web sites was opaque from a legal perspective.

The constitutions of nearly all CIS countries enshrine principles of freedom of expression and prohibit censorship. Nevertheless, often these provisions are interpreted "flexibly" when it comes to implementation. In Kazakhstan authorities often resort to various quasi-legal or "administrative" mechanisms to suppress "inappropriate" information or shut down oppositional domain names. In Uzbekistan the law on mass media holds journalists and editors responsible for the "veracity" of published materials, which has caused independent media and bloggers to practice self-censorship. The "objectivity" test is applied also in Belarus, where independent journalists, editors, and opposition leaders are frequently subject to prosecutions and arrests.

In legislation and regulation, Russia remains a leader in the region, and increasingly has been proactive in seeking influence and extending assistance 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. [8] Likewise, 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 the problem (see the next section). Some, including Kazakhstan, have adopted the Russian system, while others have mirrored its approach. In Russia, Belarus, Moldova, and Ukraine, specialized units under the Ministry of Internal Affairs (Department "K") have been established to combat "computer crime" with specialized technical units also established in other security services.

Surveillance

Obtaining a telecommunications license in Russia and other CIS states requires close cooperation with state security agencies. Since the mid-1990s a key requirement has been that providers allow law enforcement and other security agencies full monitoring access to the communications systems. In Russia the enabling acts and system used to monitor telecommunications, including the Internet, comes under the rubric of SORM-II, which came into effect in 2000.[9]

At the regulatory and technical level, SORM-II 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).[10] ISPs themselves are responsible for the cost and maintenance of the hardware and connections. ISP objections to SORM-II, which raised concerns about individual privacy, resulted in the providers being stripped of their licenses.[11]

In many respects, SORM is not unlike a combination of the Unites States' Communications Assistance to Law Enforcement Act (CALEA)[12] and the recent "warrantless" provisions for wiretapping, including the USA PATRIOT Act[13] passed after the attacks of 9/11. Russian legislation formally protects individual privacy, prohibiting wiretapping of any kind without a court order.[14] As a consequence, SORM requires government personnel to obtain a court order to intercept telephone conversations, electronic communications, or postal correspondence.[15] In reality, however, the FSB will 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.[16]

At present, several CIS countries have followed Russia's lead in implementing Internet surveillance.

- Kazakhstan followed the Russian example requiring ISPs to install special software in order to register and maintain electronic records of customers' Internet activities.
- Azerbaijan made an unsuccessful attempt to employ technologies similar to the SORM-II. At present 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 providers. Credible anecdotal evidence strongly suggests that Internet traffic is recorded and monitored via a centralized system purchased from an Israeli vendor.
- 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.

Transparency

Former British Prime Minister Winston Churchill once said when asked about the Soviet Union, "It is a riddle, wrapped in a mystery, inside an enigma; but perhaps there is a key. That key is… national interest." Transparency with regard to filtering practices varies across the region, but in all cases it is defined by the interest of the state (or the group that holds the reins of power). Protection of state interests (usually cast in terms of national security or the protection of public or cultural values) generally trump the written rules for regulation of Internet content, although often the laws themselves are ambiguous and open to interpretation. In addition, the restrictive practices of states are often fairly subtle. As an example, Uzbekistan—which was until recently the most egregious Internet censor in the region—denied that it was engaged in censorship practices. The plausibility of this claim was increased because filtering was neither uniform nor universal across all ISPs, which left open the possible, although highly improbable, chance that observed filtering practices were self-imposed by ISPs rather than proscribed by higher ups. Such subtle approach-

es allow the state "plausible deniability" of any wrongdoing and require a great deal of contextual research to uncover the sources of the practice.

Overall a general lack of transparency affects most political/legal issues in the CIS, not only the issue of Internet filtering. Often official laws are breached in subtle but effective ways. For example, in Azerbaijan the author of a Web site critical of the government was detained without formal arrest; this was never followed up by any formal legal sanctions. 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 run for office. If certain content stands in the way of business, then it is not a difficult choice to decide what measures to take. In Tajikistan, for example, research suggests that filtering is really based on economic choices rather than any overt fear of political sanction from the security forces.

Emergent forms of information control

Overt Internet filtering, such as that undertaken by China or Iran, is unlikely to occur in the CIS. First, only in a very few cases (Uzbekistan, Turkmenistan) is the government willing to create an informational blockade of the country that could, in turn, jeopardize economic prospects and stifle the "scientific potential" of these technologies. Second, as noted above, 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 Europe and the broader global economic system. 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, those CIS states that are concerned by the Internet's empowering potential—that is, their potential to make possible further "color revolutions"—have found more subtle technical means for ensuring that these capacities are curtailed, if and when necessary.

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 bloc lists) and is more difficult to track and definitively ascertain. For example, during Kyrgyzstan's 2005 parliamentary elections, two ISPs were disrupted by distributed denial of service attacks (DOS), and then a "hacker for hire" posted threats to the affected ISPs' visitor logs, stating that unless these sites stayed offline the attacks would continue.[17] The DOS attacks effectively disrupted the ISPs' services because the hacker exploited the ISPs' narrow bandwidths and dependence on a single satellite-based connection. To this day is it 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 the opposition. The government responded by ordering the affected ISPs to keep their resources online, but this was impossible because the DOS 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 "bot net," which had also been attacking a U.S. site. When the

"bot net" was taken down, the attacks against the Kyrgyz sites also stopped.

During the March 2006 presidential elections in Belarus, several opposition Web sites became suddenly inaccessible, ostensibly by innocuous network faults and DNS failures. Likewise, at the peak of protests against the election results, a major Minsk-based ISP ceased to provide dialup 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 been afoot.[18]

This form of "event-based" information control, which temporally "shapes" Internet access, can be said to represent the emerging "2.0 version of Internet controls." Not unlike the shorter supply line chains that boasted 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 this form of targeted and time-limited filtering is much harder to prove, which also removes the potential liabilities of being "caught" undertaking more deliberative filtering.

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 amongst content providers within any single country. ONI research into this phenomenon is still preliminary, and thus we are not yet in a position to provide conclusive evidence or observations on its implications.

However, preliminary indications suggest that providers reselling connectivity to CIS countries may be providing pre-filtered 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. Our 2006 testing suggested 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 the substantive or pervasive filtering—Uzbekistan and Turkmenistan excepted—Internet content control through regulation or intimidation is growing throughout the region. In most cases, the legislative and judicial framework for filtering (or other restrictions) is ambiguous and open to interpretation. 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 ISP providers as well as content producers. Information control—in particular the protection of national informational space—is clearly an issue of concern throughout the CIS, and has encouraged more stringent attention to telecommunications surveillance (as has been happening in other parts of the world, most notably the United States). In addition, measures to protect regimes in power and stifle opposition are often couched in the language of "national security" and have resulted in the development of new measures and techniques aimed at temporally "shaping" access to information at strategic moments, such as "event-based filtering." Another innovation that merits further investigation is "upstream filtering." Although these new measures are not present in all CIS countries, they are indicative of a new seriousness with which strategies for information control are being developed.

In 2007 a number of critical elections will take place in Russia and several other CIS countries. In Russia, exiled billionaire Boris Berezovsky has expressed his intent to overturn the existing regime. The Internet and other forms of communications technologies are expected to play an important role in the electoral process, and as such they will no doubt be the object of many actors' attention.

Last, the re-emergence of stronger states in the region following more than a decade of transition and general unhappiness concerning U.S. policies in the region (which have, over the past ten years, promoted media freedom and an active if foreign-funded civil society), is also sparking a degree of "blow-back" and renewed competition between East and West. For example, ONI research found that many ".mil" sites are not reachable in the CIS, suggesting that these may be subject to "supply-side" filtering by U.S. authorities.[19] Between greater assertiveness on the part of CIS states and the stimulus of renewed interstate competition, the CIS is a region to watch as a global actor shaping norms that will govern the Internet into the future.

Authors: Rafal Rohozinski, Vesselina Haralampieva

NOTES

1. The CIS consists of eleven countries: Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Ukraine, and Uzbekistan. Turkmenistan has been an associated member since 2005. With a strong political and economic influence over its neighboring countries, Russia remains the predominant political actor and strategic economic power in the group.
2. Turkmenistan's Internet is even more tightly restricted, with access available only via a single government provider. While our lack of test results do not allow us to conclusively map the extent of filtered content, preliminary analysis indicates that the Turkmen authorities employ a "white list" that allows only permitted sites to be visited.
3. Internet users in the CIS are predominantly young, aged between fifteen and twenty-five. 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 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.
4. See International Telecommunication Union, *World Telecommunication Indicators 2006.*
5. In Kazakhstan 28.4 percent of users access Internet at home, and 27.5 percent in Azerbaijan. The workplace is also a critical access point in Kazakhstan (27.2 percent), Moldova, Belarus, and Uzbekistan. In contrast, cybercafés in Kyrgyzstan are the main Internet access point in the country (for approximately 57 percent of users).
6. Rafal Rohozinski, "Mapping Russian cyberspace: Perspectives on democracy and the Net," United Nations Research Institute for Social Development (UNRISD) Discussion Paper 115, October 1999. Available at unpan1.un.org/intradoc/groups/public/documents/UNTC/UNPAN016092.pdf.
7. Alena Ledeneva, *How Russia Really Works: The Informal Practices That Shaped Post-Soviet Politics and Business,* Ithica: Cornell University Press, 2006.
8. 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.

9. See http://www.libertarium.ru/libertarium/37988.
10. See http://www.iworld.ru/magazine/index.phtml?fnct=page&p=93433812, (last accessed April 10, 2007).
11. See http://www.libertarium.ru/libertarium/14424/def_article_t?PRINT_VIEW=YES and http://www.techweb.com/wire/story/TWB19990726S0003 (last accessed April 1, 2007).
12. The Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994).
13. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, (H.R.3162), http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR.
14. Article 23 of the Constitution of the Russian Federation, http://www.constitution.ru/en/10003000-01.htm.
15. See http://www.worldpoliticswatch.com/article.aspx?id=416.
16. 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.
17. See "Election monitoring in Kyrgyzstan," ONI Special Report, February 15, 2005, http://www.opennetinitiative.net/special/kg/.
18. See "The Internet and elections: The 2006 presidential election in Belarus," ONI Internet Watch 001, http:// www.opennetinitiative.net/belarus/.
19. The inaccessibility of U.S.military Web sites was not limited to the CIS region but was also observed in numerous countries around the world. Future research will focus on this issue of filtering that is carried out by Web site hosts based on geolocation.