Citizen Lab at the Munk Center for International Studies, University of Toronto
Berkman Center for Internet & Society at Harvard Law School
Oxford Internet Institute at the University of Oxford
Advanced Network Research Group at the Cambridge Security Programme, Cambridge University

May 18, 2007
Oxford

A Summary of the OpenNet Initiative's First Global Study of Internet Filtering

The OpenNet Initiative has been testing Internet filtering around the world for over five years. The incidence of filtering in these five years has expanded from a small number of states, including China, Iran and Saudi Arabia, to become a growing global phenomenon. During 2006 and early 2007, ONI carried out empirical testing in forty-one countries. We have written summaries for each of these countries that briefly describe filtering practices and overall political and legal context. Additionally, there are eight regional overviews that compare and contrast the targets and strategies for regulating Internet content around the world. These country profiles and regional overviews are available at the ONI website: www.opennet.net. The testing conducted this past year produced the first global-level comparison of filtering practices. This testing establishes a baseline against which future filtering can be compared.

The conclusions from this first year of global testing highlight that Internet filtering is growing in scope, scale and sophistication worldwide. At least twenty-five of the forty-one countries ONI tested are engaged in some form of technical Internet filtering. The results of the testing exhibit a few principal targets of filtering activity, including political expression, social themes, and topics deemed dangerous to national security. However, very few countries limit their filtering to a narrowly defined set of targeted subjects. Instead, a majority of the countries filter a broad set of topics, suggesting that filtering regimes, once put into place, generally expand beyond their initial mandate.

The project has also made a number of technological advances in the methodology and tools for testing Internet censorship in the field. Our next steps include finding ways to include more people from more places in the research, and conducting more policy-relevant work, including testing for accessibility to the Internet during elections. We are set to embark on a major expansion of ONI's research in Asia with the addition of local partners from that region.

In future years, ONI will investigate Internet surveillance, and will develop methods to test for filtering of content available through "edge locations" (such as cybercafes) and cellular networks, including SMS.

A detailed explication of the political, social and technical aspects of filtering will be presented in our forthcoming book Access Denied: The Practice and Policy of Global Internet Filtering, to be published by MIT Press in late 2007.

Filtering Assessments

ONI testing demonstrates that at least twenty-five of the forty-one states studied are engaging in technological Internet filtering to some degree.

Filtering by State

Evidence of Filtering	Suspected Filtering	No Evidence of Filtering
Azerbaijan	Belarus	Afghanistan
Bahrain	Kazakhstan	Algeria
Burma/Myanmar		Egypt
China		Iraq
Ethiopia		Israel
India		Kyrgyzstan
Iran		Malaysia
Jordan		Moldova
Libya		Nepal
Morocco		Russia*
Oman		Ukraine
Pakistan		Venezuela
Saudi Arabia		West Bank/Gaza
Singapore		Zimbabwe
South Korea		
Sudan		
Syria		
Tajikistan		
Thailand		
Tunisia		
Turkmenistan		
United Arab Emirates		
Uzbekistan		
Vietnam		
Yemen		

*Testing in Russia was limited to a selection of ISPs in Moscow; these preliminary results may not extend beyond this sample.

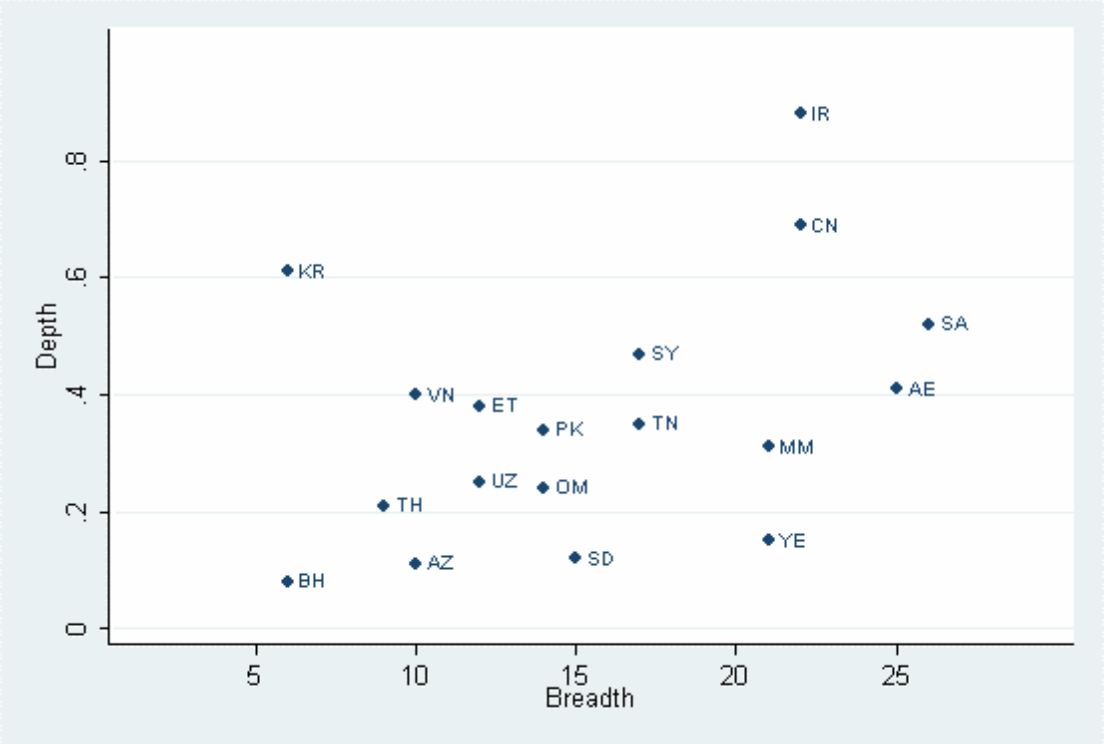
As the chart above reflects, there are a number of countries in which ONI found no evidence of filtering. Within this list are countries that might be considered "anomalies" – places where one might think there would be Internet filtering but no evidence of filtering was found. There are other non-technical strategies for controlling Internet content that may be deployed in these countries, however. These strategies include the threat of legal action or arrest; identification, licensing and registration requirements for Internet users, content providers and service providers; monitoring and surveillance of Internet traffic and users; and informal requests or threats by private or public parties. These non-technical means may serve as supplements to or substitutes for technological Internet filtering.

The range of blocking behavior varies greatly amongst the countries listed above that filter. A number of countries (eg Azerbaijan, Jordan, and Tajikistan) have exhibited only a few isolated incidents of state-sponsored filtering while others have firmly-established, wide-reaching filtering regimes.

There are a number of countries in which ONI did not carry out extensive empirical testing, including the United States, Canada, Australia, and a number of European countries that are known to employ either mandatory filtering regimes, voluntary filtering programs promoted by the state, or notice and takedown systems to regulate Internet content.

Internet filtering regimes can be characterized by the number of topics that are filtered (the *breadth* of filtering) and the degree to which a given topic is filtered (the *depth* of filtering). ONI found considerable variation in the breadth and depth of filtering across countries.

Filtering: Overall Breadth and Depth



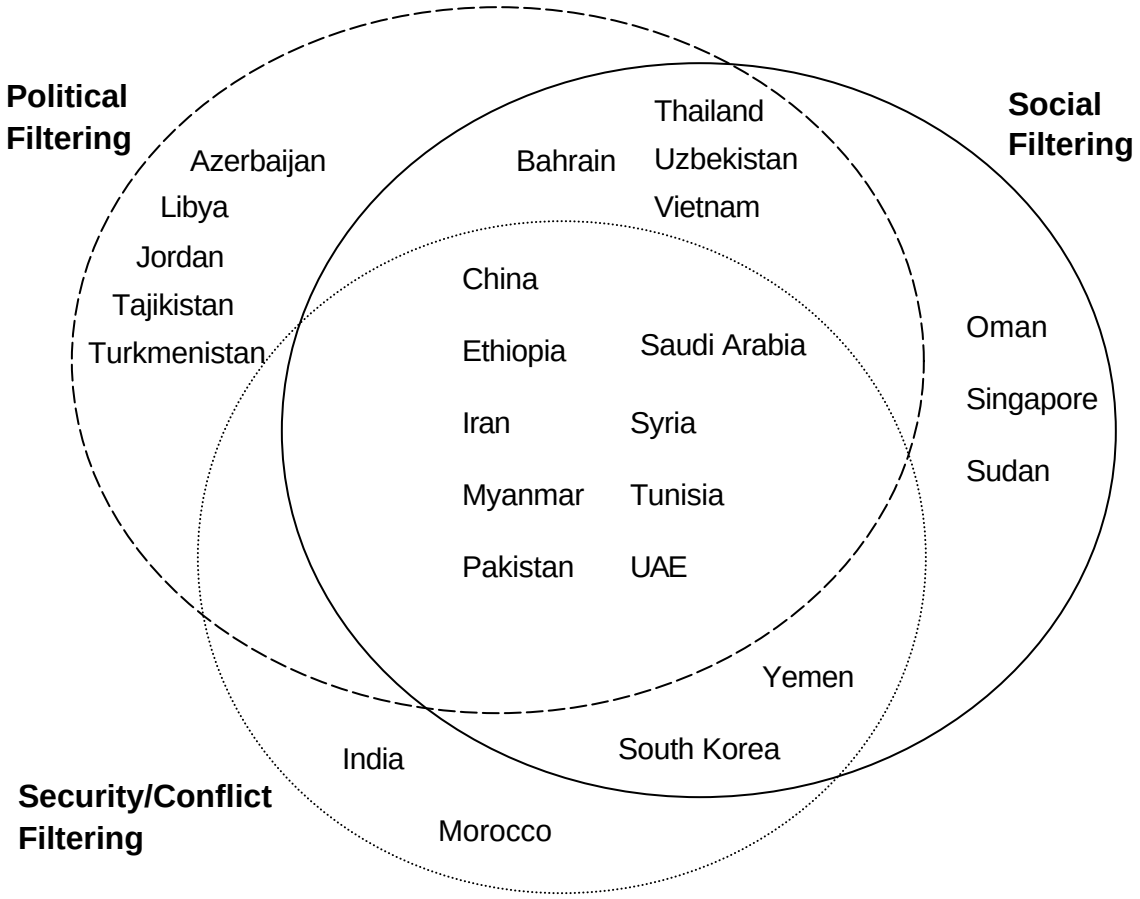
AE - United Arab Emirates; AZ – Azerbaijan; BH – Bahrain; CN – China; ET – Ethiopia; IR – Iran; JO – Jordan; KR - South Korea; LY – Libya; MM – Burma/Myanmar; OM – Oman; PK – Pakistan; SA - Saudi Arabia; SD – Sudan; SY – Syria; TH – Thailand; TH – Tunisia; UZ – Uzbekistan; VN – Vietnam; YE – Yemen. A number of countries that filter a small number of sites are omitted from this diagram, including Belarus, India, Jordan, Kazakhstan, Morocco, Singapore, and Tajikistan.

To provide another perspective on testing results from the past year, ONI researchers evaluated Internet filtering across four major thematic areas: political content, social content, content related to conflict and security, and Internet tools.

- **Political content:** Content that expresses views in opposition to those of the current government. Content more broadly related to human rights, freedom of expression, minority rights, and religious movements is also considered here.
- **Social content:** Content related to sexuality, gambling, and illegal drugs and alcohol, as well as other topics that may be socially sensitive or perceived as offensive, including hate speech.
- **Content related to conflict & security:** Content related to armed conflicts, border disputes, separatist movements, and militant groups.
- **Internet tools:** Web sites that provide e-mail, Internet hosting, search, translation, Voice over Internet Protocol (VoIP) telephone service, and circumvention methods are grouped in this category.

The focus of filtering varies by state, as illustrated below.

Filtering: Content Type



In addition, ONI has assessed the breadth and depth of filtering within each of the thematic areas.

- **Pervasive filtering.** Filtering that is characterized by both its *depth* — a blocking regime that blocks a large portion of the targeted content in a given category — and its *breadth* — a blocking regime that includes filtering in several categories in a given theme.
- **Substantial filtering.** Filtering that has either *depth* or *breadth*: either a number of categories are subject to a medium level of filtering or a low level of filtering is carried out across many categories.
- **Selective filtering.** Narrowly targeted filtering that blocks a small number of specific sites across a few categories or filtering that targets a single category or issue.
- **Suspected filtering.** Connectivity abnormalities are present that suggest the presence of filtering, although diagnostic work was unable to confirm conclusively that inaccessible Web sites are the result of deliberate actions.
- **No evidence of filtering.** ONI testing did not uncover any evidence of Web sites being blocked.

The table below illustrates the differences in filtering within and across themes.

Filtering: Theme and Degree

	Political	Social	Conflict & Security	Internet Tools
Azerbaijan	?	–	–	–
Bahrain	? ?	?	–	?
Belarus	?	?	–	–
Burma/Myanmar	? ? ?	? ?	? ?	? ?
China	? ? ?	? ?	? ? ?	? ?
Ethiopia	? ?	?	?	?
India	–	–	?	?
Iran	? ? ?	? ? ?	? ?	? ? ?
Jordan	?	–	–	–
Kazakhstan	?	–	–	–
Libya	? ?	–	–	–
Morocco	–	–	?	?
Oman	–	? ? ?	–	? ?
Pakistan	?	? ?	? ? ?	?
Saudi Arabia	? ?	? ? ?	?	? ?
Singapore	–	?	–	–
South Korea	–	?	? ? ?	–
Sudan	–	? ? ?	–	? ?
Syria	? ? ?	?	?	? ?
Tajikistan	?	–	–	–
Thailand	?	? ?	–	?
Tunisia	? ? ?	? ? ?	?	? ?
Turkmenistan	? ?	–	–	–
United Arab Emirates	?	? ? ?	?	? ?
Uzbekistan	? ?	?	–	?
Vietnam	? ? ?	?	–	? ?
Yemen	?	? ? ?	?	? ?

? ? ? Pervasive filtering; ? ? Substantial filtering; ? Selective filtering;

? Suspected filtering; – no evidence of filtering

In addition to variation based on the specific Internet sites blocked, state filtering programs also vary in the filtering mechanisms deployed. The choice of locus of filtering – whether centralized at the Internet backbone level or decentralized at the ISP level – may affect the consistency of filtering within the state. States also vary in their willingness to acknowledge filtering activities and to restore access to inappropriately blocked sites.

Filtering: Other Variations

	Locus	Consistency	Concealed Filtering	Transparency & Accountability
Azerbaijan	D	Low		Medium
Bahrain	D	High	Yes	Low
Burma	D	Low		Medium
China	C & D	Medium	Yes	Low
Ethiopia	C	High	Yes	Low
India	D	Medium		High
Iran	D	Medium		Medium
Jordan	?	High		Low
Libya	C	High		Low
Morocco	C	High	Yes	Low
Oman	C	High		High
Pakistan	C & D	Medium	Yes	High
Saudi Arabia	C	High		High
Singapore	D	High		High
South Korea	D	High		High
Sudan	C	High		High
Syria	D	High		Medium
Tajikistan	D	Low		Medium
Thailand	D	Medium		Medium
Tunisia	C	High	Yes	Low
Turkmenistan	C	High	Yes	Low
United Arab Emirates	D	Low		Medium
Uzbekistan	C & D	High	Yes	Low
Vietnam	D	Low	Yes	Low
Yemen	D	High		Medium

The **Locus** of filtering indicates where Internet traffic is blocked. **C** indicates that traffic is blocked from a central location, presumably the Internet backbone, and affects the entire state equally. **D** indicates that blocking is decentralized, typically meaning that filtering is implemented by ISPs. (Note that this study does not include filtering at the institutional level, e.g., cybercafés, universities, or businesses.) ? - indicates the lack of conclusive information.
Consistency measures the variation in filtering within a country across different ISPs where applicable.
Concealed filtering reflects either efforts to conceal the fact that filtering is occurring or the failure to clearly indicate filtering when it occurs.
Transparency & Accountability corresponds to the overall level of openness in regard to the practice of filtering. It also considers the presence of concealed filtering, the type of notice given to users regarding blocking, provisions to appeal or report instances of inappropriate blocking, and public acknowledgement of filtering policies.

Provoking a Dialogue

The prevalence and growth of technical Internet filtering raise serious legal, political and ethical concerns. It is this series of implications that we put on the table for discussion at our first major international conference on Internet filtering, held at Oxford on May 18, 2007.

We seek to encourage discussion of the international and public policy implications of these findings. The repercussions for the development of human rights around the world are substantial, as more and more civic organizations who rely upon the Internet as a primary mode of communication have access to information and freedom of speech curtailed, undermining their ability to raise awareness and advocate for change. The importance for the growing community of online activists — hacktivists — is even more pronounced, as the flow of bits across the networks on which they operate is changing; building software that protects privacy and security online while circumventing filtering is now a major challenge for these groups.

For international lawyers, the problems of jurisdiction, choice of law, state sovereignty, and the operation of the rule of law once again come into relief in the Internet era, as they did when the Internet first came of age in the 1990s. For multinational technology companies, increasingly called upon to carry out Internet filtering and surveillance far from home, these findings hold the prospect that the importance of solving their problem of corporate ethics is only growing with each passing year. The findings resonate also for those involved in the international discussion of Internet governance and who seek to determine the appropriate role for IGOs and NGOs in the regulation of the Internet's operation.

From the perspective of national policy-making, the decision whether to filter the Internet grows more, not less, acute with time. As the importance of the Internet increases for intelligence, national security, and economic development, the tensions that lead to Internet filtering — and that mitigate against it — continue to grow. Ordinary people have much at stake in this debate. In a growing number of states around the world, Internet filtering has huge implications for how connected citizens will be to the events unfolding around them, to their own cultures, and to other cultures and shared knowledge around the world. At the same time, filtering practices raise questions about how citizens relate to the states in which they live – states that are ordinarily neither transparent about how these filtering regimes work nor accountable for the problems inherent in the way they are carried out today.

We look forward to joining you in discussion on these and other issues of global significance, in person at Oxford and online.

Acknowledgements

The OpenNet Initiative's work would not be possible without the generous support of its funders. The work of ONI has been supported by the Open Society Institute, the International Development Research Center (Canada), and the Ford Foundation at various stages since its inception. The John D. and Catherine T. MacArthur Foundation provided a $3 million grant that provided the core support for this first global survey.