Internet Filtering in the **Middle East and North Africa**

Overview

ONI conducted in-country testing for Internet filtering in sixteen countries in the North Africa and Middle East region. We found that eight of these countries broadly filter online content: Iran, Oman, Saudi Arabia, Sudan, Syria, Tunisia, United Arab Emirates, and Yemen. Another four—Bahrain, Jordan, Libya, and Morocco—carry out selective filtering of a smaller number of Web sites. ONI found no evidence of consistent technical filtering used to deny access to online content in Algiers, Egypt, Iraq, or Israel.

Most of the sites targeted for blocking are selected because of cultural and religious concerns about morality. Political filtering, however, is the common denominator in the region. Bahrain, Jordan, Libya, and Syria focus their filtering efforts primarily on political content. Iran, Oman, Saudi Arabia, Sudan, Tunisia, the United Arab Emirates, and Yemen, on the other hand, not only extensively filter political content but also pervasively block content that is perceived to be religiously, culturally, or socially inappropriate.

Regional and internal political conflicts are also behind content blocking. For example, Syria and the United Arab Emirates block all Web sites within the Israeli domain. Morocco blocks Web sites arguing for the independence of Western Sahara.

Internet censorship in the Middle East and North Africa is multilayered, relying on a number of complementary strategies in addition to technical filtering; arrest, intimidation, and a variety of legal measures are used to regulate the posting and viewing of Internet content.

Introduction

Most of the states in the Middle East and North Africa introduced the Internet in their countries to promote economic development and competitiveness; however, they soon realized that the Internet made it more difficult for them to control the flow of information both within the country and across international borders.

States' power to regulate social, economic, and political activities started to erode as citizens and other nonstate actors, empowered by the

Internet, started to create and disseminate information. The Internet, along with satellite television networks, has effectively broken the monopoly of many Middle Eastern and North African governments. The availability and accessibility of information, as well as the ability to create and disseminate information anonymously, has led to a sense of freedom among many Arab Internet users.

Internet in the Middle East and North Africa

Though some countries in the region enjoy widespread and easy access to the Internet, the region is also home to some of the least-connected countries in the world. While in 2006 some 61 percent of Israelis and 35 percent of Emiratis had regular access to the Internet, Internet penetration still lags behind in most of the region. In fact, according to the International Telecommunication Union, less than 4 percent of people in the Arab world use the Internet regularly.[1] In many countries, poor infrastructure along with economic barriers remain the biggest obstacle to expanding access to the Internet. In Yemen, for example, less than 1 percent of the population uses the Internet (there are 0.87 users per 100 inhabitants), and there are only 300,000 personal computers in the country (1.5 per 100 inhabitants).[2] In Syria fewer than six out of one hundred people regularly use the Internet. In Iraq the Internet penetration rate is 0.1 percent.

Interestingly, broadband Internet access is growing faster in the Middle East and Africa than in any other region in the world. The number of broadband subscribers grew by 38 percent in 2006, while the number of those subscribers using DSL access technology grew by 82 percent, to 4.3 million.[3]

The highest rates of broadband penetration in the region are found in Qatar, the United Arab Emirates, and Lebanon. Half of all households in Qatar, almost one-third in the United Arab Emirates, and one-quarter in Lebanon have a broadband connection. Three countries—Tunisia, Qatar, and Egypt—experienced a remarkable broadband growth rate, doubling in a year. At the same time, DSL subscriptions in the United Arab Emirates increased by almost two-thirds.[4]

State response: Censorship

As the Internet has proven to be a new space for the extension of power and for different nonstate players to compete for influence, states have perceived this as a potential threat. The response has been filtration and surveillance. For the many restrictive governments of the Middle East and North Africa, embracing the Internet meant providing citizens with access to troubling content and ideas, along with new methods to circumvent traditional controls on life and discourse. In reaction, many governments in the region have chosen to restrict online freedom, giving the Middle East and North Africa one of the most repressive Web environments in the world. The Middle East and North Africa is home to five of the thirteen countries listed as enemies of the Internet by Reporters Sans Frontieres.[5]

ONI testing has confirmed that governments and Internet service providers (ISPs) have blocked content they have designated as morally offensive, in violation of public ethics and order, or critical of governments, leaders, or ruling families.

To one degree or another, the Gulf countries, as well as Iran, Sudan, Tunsia, and Yemen, block content related to pornography, homosexuality, dating, and provocative attire. Some of these countries also censor topics considered sensitive or forbidden under Islam, such as gambling, alcohol, and drugs, along with Web sites that feature nudity, even if in a non-erotic context. A few countries, such as Saudi Arabia and the United Arab Emirates, ban access to Web sites that are critical of Islam and those that promote conversion to Christianity.

Many states in the region were found to block political content, or to have blocked such content in the past. For example, Bahrain, Saudi Arabia, Syria, and Tunisia consistently block Web sites of opposition groups. Egypt has intermittently blocked the Web site of the Muslim Brotherhood, an Islamist group critical of the government, as well as the site hosting the online version of the Labor Party's newspaper, which had previously been banned in its hard copy. Yemen temporarily blocked political Web sites in the run-up to the 2006 presidential elections, while Bahrain did the same ahead of parliamentary elections. One political Web site was found to be blocked in Jordan.

Several countries, including Bahrain, Saudi Arabia, and Tunisia, also restrict access to material from human rights organizations, particularly sites that have published reports that are especially critical about those countries.

Legal and regulatory frameworks

Communications services have been liberalized in several countries in the Middle East and North Africa in the past few years, and there are attempts to liberalize more markets in other countries. Some countries have passed legislation that regulates the telecommunications sector and allows the participation of the private sector in the communication industry. The past few years have also witnessed the establishment of telecommunications regulatory authorities.

Most of the countries in the region do not have Internet-specific legislation, though some countries have started to adopt these laws.

In February 2006 the United Arab Emirates issued a federal law designed to combat cybercrime. This law criminalizes certain online activities such as "setting up a website or publishing information for groups calling for facilitating and promoting ideas in breach of the general order and public decency," and "setting up a website or publishing information for a terrorist group under fake names with intent to facilitate contacts with their leadership, or to promote their ideologies and finance their activities, or to publish information on how to make explosives or any other substances to be used in terrorist attacks."[6]

In October 2006 Saudi Arabia also issued a law that criminalizes, among other things, "[e]avesdropping on, tapping or obstructing information sent through the Internet or a computer without legal justification," "[d]efaming others or harming them through the different means of information technology," and "[e]stablishing a Web site for terrorist organizations and/or publishing it in order to aid the leaders of these organizations or any of their members, or promoting their ideas, or financing them, or publishing how to make explosives or other weapons used in terrorist acts."[7]

Journalists and citizen journalists have been detained under emergency laws, vague media laws, or penal codes. Others have faced extralegal harassment and intimidation from security agencies. Governments have further blocked access to new services, citing security concerns. In 2006 the voice-over Internet protocol (VoIP) service Skype and Google Earth were briefly banned in Jordan and Bahrain, respectively. In both cases, the government cited security concerns.

The use of Internet is also regulated by ISPs' terms of use that in some cases mandate that users not carry out activities that contradict the social, cultural, political, religious, or economic values of the state. In some cases, users are asked to sign written agreements to this effect.

Transparency

Some countries in the region openly acknowledge their practice of Internet filtering. Saudi Arabia and Sudan publish details about what they filter, how, and why. They also make available information about their Internet filtering policies, procedures, and other related materials, such as the impact of their filtering systems on connectivity. An Iranian official recently boasted that Iran has censored ten million Web sites, and

that they add 1,000 Web sites to the blacklist every month.[8] However, even where a state admits some filtering, it may not admit targeting political opposition, dissidents, or critical human rights reports.

Some ISPs acknowledge filtering by serving blockpages when users try to access banned content. A blockpage usually alerts users that they tried to access illegal Web sites; some invite users to suggest the removal of the block on the Web sites if they think they were erroneously blocked. Some ISPs also ask users to volunteer suggestions for the blacklists.

Countries such as Syria and Tunisia attempt to hide their filtering regimes by returning blockpages disguised to look like error messages. Users in Libya receive time-out messages when they try to access banned content.

Overblocking

Internet filtering will inherently lead to either overblocking or underblocking of targeted content. Many countries in the region are reasonably successful at blocking what they openly declare to be the target of their filtering system, without excessively high rates of overblocking. Others, however—such as Iran, Saudi Arabia, and the United Arab Emirates—not only extensively block targeted content but they also unnecessarily overblock unrelated content. For instance, Iran and the United Arab Emirates block www.flickr.com entirely because they have deemed some of the photographs posted on the site objectionable. Also most of ISPs in countries such as Saudi Arabia, Syria, Tunisia, the United Arab Emirates, and Yemen prevent Internet users from legitimately using privacy and anonymizing tools and online translation services because they can be used to bypass the filtering systems.

Filtering tools

The majority of the ISPs in the region rely on commercial filtering software, primarily applications produced by U.S.-based companies Secure Computing and Websense. This software allows ISPs, often acting on the behest of governments, to filter by category based on lists of pages updated by the company. The categories that ISPs choose to filter can differ widely between countries. In some cases ISPs block individual Web sites' URLs or entire top-level domains, as in the case of Syria and the United Arab Emirates, both of which block access to the Israeli top-level domain. In addition, some ISPs block search strings that contain objectionable keywords. For example, the Yemeni ISP Ynet blocks the use of the word *sex* in search strings, and the Emirati ISP Etisalat bans the use of several keywords that could return erotic images.

In addition, some ISPs block access to cached copies of certain Web sites as an extra measure to prevent access to their content. Most notably, the U.S.-based, Arab-language online newspaper www.arabtimes.com is blocked in several Arab countries, as is access to the cached copy of the page in Google.

Iran, in addition to blocking Web sites, restricts users' ability to access online content by limiting their Internet speed. In October 2006 the Ministry of Communications and Information Technology ordered ISPs to limit the connection speed they offer to 128 Kb/s in order to hinder users' ability to download foreign cultural products (such as music and films) and to organize political opposition.[9]

Physical restrictions and filtering

An additional mode of control is to regulate the places where users access the Internet. In many countries in the Middle East and North Africa, users primarily go online at Internet cafés. Some governments require these cafés to maintain lists of their patrons and keep an eye on their activities. Yemen and Oman require that computer screens be visible to café managers at all times; indeed, Oman requires that prospective café owners submit a floor plan in their application package. The authorities give specific instruc-

tions on how Internet cafés should be designed; these instructions include the height, depth, and width of partitions between computers.

Temporary and event-based blocking

Some countries block Web sites at sensitive political moments. As stated previously, in 2006 Bahrain blocked several Web sites in the run-up to the country's parliamentary elections and Yemen banned access to several media and local politics Web sites ahead of the country's presidential elections.

Another example of temporary blocking mentioned earlier is the banning of access to the VoIP service Skype in Jordan and Google Earth in Bahrain in 2006.

Control without filters

Several countries in the region do not have technical filtering in place, or they selectively filter sensitive content. This, however, does not necessarily mean that there is no media censorship in these countries. Citizens in these countries are able to enjoy unfettered access to the Internet because filtering is either very selective or nonexistent. But sweeping media laws lead to pervasive self-censorship and, in some cases, detention. The intimidating laws discourage users from engaging in political and social conversations online.

Jordan, for example, blocks very few Web sites, but media laws curb the freedom of the press and encourage some measure of self-censorship in cyberspace.[10] Citizens have reportedly been questioned and arrested for Web content they have authored.[11] Similarly, the Egyptian government no longer blocks Web sites, but it has detained people for their online activities. On February 22, 2007, a court in Alexandria sentenced a blogger to four years in prison for "incitement to hate Muslims" and "insulting the president."[12]

The Iraqi government does not block Web sites, but the war there makes it difficult for people to access the Internet and makes it dangerous to express political opinions online.

Internet censorship: The users' response

Users may exploit alternative technologies to circumvent filtering systems when censorship imposed by ISPs restricts access to content. In Saudi Arabia, for example, 93 percent of Internet users regularly try to access blocked Web sites, according to an official at King Abdul Aziz City for Science and Technology (KACST) once responsible for overseeing the country's filtering system.[13]

Many Web sites that discuss sensitive issues and feel that they are likely to be blocked use services such as Yahoo! Groups as part of their contingency plans. Once the Web sites are blocked by ISPs, users continue to exchange content via e-mail. Because it is very difficult for ISPs to filter e-mail discussions, group conversation continues to be virtually uncensored.

Other Web sites and discussion forums post tutorials for their visitors that describe how to use circumvention tools to bypass local filtering systems even before they are actually blocked. One Arabic political Web site's home page once read, "Click here to enter our Web site and click here to learn how to access us once we are blocked."

Another trick used by Internet users is the dissemination of controversial content in a large number of Web sites that are unknown to the ISPs. When the novel *Girls of Riyadh* was banned in Saudi Arabia, for example, the full text was posted in tens of Saudi Arabian forums and blogs that have low visibility. Although this is a violation of copyright, it is also an example of how banned content is being distributed and is evidence that blocking the flow of information is not as easy as was once thought.

Some technologically sophisticated user groups went as far as developing their own circumvention tools. In fact, a special Web browser once emerged on the Internet that enabled users to access blocked Jihadi-oriented Web sites.

Conclusion

Though the Internet is growing rapidly in many countries and high-speed access is spreading, most countries in the Middle East and North Africa maintain control over what citizens can see and say online. Authorities use technology and legal and physical restrictions to limit what users can access online. While filtering is primarily based on religious and cultural concerns, most countries in the region also filter some political content.

Even in countries that filter little or no online content, legal restrictions and extralegal harassment from security agencies can still be used to cow or silence online critics.

In addition, although some countries openly acknowledge practicing Internet filtering of religiously and culturally objectionable content, there is less openness when it comes to blocking of political oppositional content. Other countries deliberately try to obscure the fact that they are filtering content by producing false error messages or time-out messages.

Furthermore, as governments try to prevent people from circumventing filtering, they inflict collateral damage on the Internet, preventing users from using useful and politically neutral services such as privacy tools and online translation services.

In sum, filtering in the MENA region demonstrates an ongoing struggle between the filtering states' desire to integrate into the global economy and their efforts to restrict and prevent access to what they deem to be dissident activities or objectionable materials.

Authors: Helmi Noman, Elijah Zarwan

NOTES

1. AME Info, Arab internet woes, http://www.ameinfo.com/80162.html.
2. International Telecommunication Union, Internet Indicators: Hosts, Users and Number of PCs (2005), http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx.
3. AME Info, "DSL Forum acclaims Middle East and Africa broadband growing faster than any region in the world," April 12, 2007, http://www.ameinfo.com/116548.html.
4. Ibid.
5. Reporters Without Borders, "List of the 13 Internet enemies in 2006," November 7, 2006, http://www.rsf.org/article.php3?id_article=19603.
6. Gulf News, "UAE cyber crimes law," February 13, 2006, http://archive.gulfnews.com/uae/uaessentials/more_stories/10018507.html.
7. Saudi Gazettee, Cyber Crime Regulations, April 7, 2007, translated, http://www.saudigazette.com.sa/index.php?option=com_content&task=view&id=28819&Itemid=146.
8. Reporters Without Borders, "Authorities boast of success in Internet filtering," September 15, 2006, http://www.rsf.org/article.php3?id_article=18864.
9. *The Guardian,* "Iran bans fast Internet to cut west's influence," October 18, 2006, http://technology.guardian.co.uk/news/story/0,,1924637,00.html.
10. Reporters Without Borders, Internet Under Surveillance 2004: Jordan, http://www.rsf.org/article.php3?id_article=10737.
11. The Initiative for an Open Arab Internet, "Implacable Adversaries: Arab Government and the Internet (2006): Jordan," http://www.openarab.net/en/reports/net2006/jordan.shtml; Human Rights Watch, "Jordan: Rise in arrests restricting free speech," June 17, 2006, http://www.hrw.org/english/docs/2006/06/17/jordan13574.htm.
12. BBC News, "Egypt blogger jailed for 'insult'," February 22, 2007, http://news.bbc.co.uk/2/hi/middle_east/6385849.stm.
13. Arab News, "Most of kingdom's Internet users aim for the forbidden," October 2, 2005, http://www.arabnews.com/?page=1&section=0&article=71012&d=2&m=10&y=2005.