



The Citizen Lab

Middle East and North Africa CyberWatch: September 22-October 5, 2012

A biweekly report on trends in online censorship, information operations,
and Internet use in the Middle East and North Africa

Table of Contents

- Censorship and Filtering (pages 1-3)

MIDDLE EAST AND NORTH AFRICA, IRAN, JORDAN, OMAN

- Cyber Attacks (page 3)

IRAN

- Technology Updates (page 3-4)

IRAN, SAUDI ARABIA

CENSORSHIP AND FILTERING

MIDDLE EAST AND NORTH AFRICA: Freedom House issues new report on Internet freedom
Freedom House has released its annual [Freedom on the Net](#) report for 2012. The report, detailing Freedom House's assessment of global Internet freedom, has raised concerns over digital rights in several countries in the Middle East and North Africa. In its [press release](#), Freedom House highlighted Iran for its "nuanced tactics" against Internet freedom, including the implementation of advanced filtering technology, compromising of digital certificates, and Iran's move towards a domestic "National Internet." The same press release also raised concerns about Egypt's "precarious and uncertain" future, as military authorities in 2012 kept extensive surveillance on ICTs and frequently arrested bloggers and other online activists for perceived anti-military activities.

Many countries in the region fared poorly in the rankings. "Scores" for Internet freedom declined since the previous year in [Bahrain](#), [Egypt](#), [Jordan](#), [Iran](#), and [Saudi Arabia](#). Only [Tunisia](#) recorded significant improvements in Internet freedom since the year prior. [Libya](#), however, which was not ranked in 2011,

scored even higher than Tunisia. The report noted Libya's "frenzy of self expression online" since the end of the Libyan Civil War, and gave the country a "partly free" rating. [Syria](#), also unassessed in 2011, was the second "least free" country in the Middle East and North Africa (Iran being the most repressive) due to the regime's vigorous persecution of bloggers and online activists, extensive filtering, and surveillance of citizens through a variety of fairly sophisticated means in the context of Syria's continuing civil conflict.

MIDDLE EAST AND NORTH AFRICA: Calls for YouTube censorship continue

Calls for censorship of the [YouTube video](#) that precipitated violent protest across the Middle East and North Africa [continued](#) into late September. Activists launched campaigns on Facebook and other social media platforms criticizing Google for continuing to make the video available in some countries and calling for a broader boycott of the company's various services. The activists [anticipated](#) that Google would lose "about \$210 million in revenues if Internet users in the Arab world boycott its search engine and that its stock price will drop."

IRAN: Government blocks Google's search engine and e-mail services

On September 22, Iran blocked access to Google and Gmail in reaction to the anti-Islam video "Innocence of Muslims." Iranian authorities later removed the block in response to numerous complaints from the public, government agencies, and members of parliament. Official and unofficial sources have given a number of conflicting reasons for the filtering of Gmail and Google. Reza Taqipour, Minister of Information, [stated](#) [Farsi] that Gmail had been filtered according to a court order, and would be unblocked pending judicial decision. The Commission to Determine Instances of Criminal Content [announced](#) [Farsi] that the Gmail filter was caused by technical problems in their effort to [block](#) [Farsi] YouTube according to public request. With the government's plans to launch the first phase of the national information network, this decision is also [taken](#) as a sign of plans to pull out of the global internet.

JORDAN: Demonstrations against new censorship laws erupt in Jordan

In a demonstration against amendments to Jordan's Press and Publications Law in Amman, participants have announced the creation of a "[Civil Coalition against the New Press and Publications Law](#)." The group has pledged to [fight](#) against the amendments through "legal and civil means." As [previously reported](#), activists have interpreted the amendments as restrictive and have warned of its detrimental effect on freedom of expression in the country.

JORDAN: Government releases parental control software

The Jordanian government will make parental control software [available](#) for citizens through Jordanian Internet service providers by the end of October. An Australian company, TCG, has [provided](#) the Ministry of Information and Communications Technology with software that will enable families to filter "undesirable content." As [previously reported](#), a grassroots movement to ban access to pornography in Jordan has been gaining support over the past few months.

OMAN: Web ethics code drafted by citizens

A group of Omani citizens have [drawn up](#) an "Omani Ethics Code for Electronic Publishing," which it hopes will help "maintain freedom of speech while maintaining the [sic] ethics." The group intends for

the document to clarify what content should and should not be published by bloggers and social media users. By educating others on the limits of admissible content, it hopes that incidences of detention of Internet users as well as [government violence](#) directed against them will decrease in the future.

CYBER ATTACKS

IRAN: Iranian hacker group attacks 370 Israeli websites

A group of hackers, called Iranian DataCoders, [announced](#) [Farsi] on September 22 that they had hacked nearly 370 websites registered to Israeli commercial, security, and economic entities. They cited recent “blasphemies against the Prophet Muhammad”, likely referring to the “Innocence of Muslims” YouTube video, as the main reason for the cyber attacks.

IRAN: Accusations of cyber attacks against US banks denied

Iran has been accused of sponsoring and undertaking a number of cyber attacks on major US banks, including JPMorgan Chase, Wells Fargo and Bank of America. In response, Gholam Reza Jalali, director of Iran’s Passive Defense Organization, officially [denied](#) [Farsi] all accusations on behalf of Iran’s government.

TECHNOLOGY UPDATES

IRAN: Experts question National Information Network Project

The Iranian government has cited the need to protect users from cyber attacks as the pretext for creating a national private Internet, also known as the National Information Network project. The project was launched despite [doubts from experts](#) [Farsi] that a separate information network will protect them from viruses like StuxNet and Flame, which were spread using removable storage devices, such as USB flash drives. Furthermore, the [Information Technology Security News Agency maintains that](#) separating the national network from the global Internet may prove to be a costly process that will impose limitations on users and pose serious challenges to government agencies.

IRAN: Domestic Search Engines

In accordance with the government’s agenda to fight sanctions by promoting domestic products, several national search engines have been [developed](#) [Farsi] over the past couple of years. Ali Hakim Javadi, Deputy Minister of Information, stated that although the government will not directly involve itself in developing national search engines, it will support public and private organizations that do so. The Ministry of Information is also planning to introduce [Fajr](#) [Farsi], a recently developed domestic search engine.

IRAN: Government organizations hesitate to use national email services

Deutsche Welle [reported](#) [Farsi] that the state has requested the employees of several government organizations to use national email services, such as Chaapaar, for their internal correspondences. Many employees are concerned about the reliability and security of domestic email services and therefore disapprove of the request.

SAUDI ARABIA: E-Government summit takes places in Riyadh

The third annual [Kingdom eGovernment Summit](#), which “aims to build awareness and accelerate the integration of e-Government in the day-to-day activities of the public sector and the services it offers to businesses and citizens,” recently took place in Riyadh. During the meeting, the government [announced](#) the launch of its Second National e-Government Action Plan. Through the plan’s 22 objectives and 46 initiatives, the Saudi government seeks to improve its relations with the public, streamline its own activities, and “increase collaboration with private companies” as a means of economic growth and job creation.

[Read previous editions](#) of the MENA Cyber Watch.