



The Citizen Lab

Middle East and North Africa CyberWatch: August 11 - August 24, 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 1-2)
IRAN, JORDAN, SAUDI ARABIA
- Blogger and Netizen Arrests (page 3)
BAHRAIN
- Cyber Attacks (page 3-4)
IRAN, SAUDI ARABIA, SYRIA
- Internet and Social Media Use (page 4)
IRAN, KUWAIT
- Technology (pages 5)
SYRIA

CENSORSHIP AND FILTERING

IRAN: Increasing number of blogs filtered daily

Alireza Shirazi, Director of BlogFa, one of the most well-known Persian blogging services, [tweeted](#) [Farsi] that approximately 100 weblogs get filtered every day. Teribon, a news agency, published a

story on Shirazi's tweet, but it was [removed](#) [Farsi] from the website following an order from the Commission to Determine Instances of Criminal Content.

IRAN: The moon of Shawwal and the filtering of Grand Ayatollahs' websites

The official websites of two Shi'a Grand Ayatollahs were temporarily [blocked](#) [Farsi] and one other hacked after they announced that the holiday of *Eid al-Fitr* was to fall on a different day than that announced by Ayatollah Khamenei. The appearance of the moon of *Shawwal* (*Estehlal*), which marks the end of Ramadan, has always been an important point of controversy between Grand Ayatollahs. Several years ago, the Iranian newspaper Kayhan [asked](#) [Farsi] Iran's Grand Ayatollahs to approve Khamenei's official announcement and avoid publicly announcing dates contradictory to the Supreme Leader.

IRAN: More restrictions on Iranian websites and weblogs

The Ministry of Culture and Islamic Guidance has [formed](#) [Farsi] a new working group, called Rasad (*Observation*), to monitor 38,000 registered websites more closely and identify any instances of immoral or politically disruptive content. As previously [reported](#), the working group is one of many organizations that assist the Commission to Determine Instances of Criminal Content, the main decision making body that works under attorney general's guidance, in controlling cyberspace. After detecting such instances, the Commission [makes the final decision](#) [Farsi] and issues judicial orders as appropriate.

IRAN: Filtering of Apple's App Store and iTunes

The Iranian government has blocked access to Apple's iTunes and App Store after months of allowing free access to Iranians users to the two services. IT Iran [published](#) [Farsi] an article on the decision, calling the ban "an unfair action and additional obstacle for Iranian people who are already facing various challenges in accessing the information and software products, including applications with Islamic themes, or in Persian language, that they need."

JORDAN: Supporting Internet freedom through social media

The [Jordan Open Source Association](#) recently announced that it will launch a social media campaign in defence of Internet freedom as a response to the [previously reported](#) anti-pornography movement underway in the country. The association has been critical of the Ministry of Information and Communication Technology's [request](#) that Internet service providers block pornographic sites. It has also [condemned](#) amendments to the [1998 Press and Publications Law](#) [PDF] that give the government the right to block non-Jordanian sites considered in violation of law.

SAUDI ARABIA: Objections over new web extensions

Saudi Arabia's Communication and Information Technology Commission has [objected](#) to 163 new top-level domain extensions on "moral' and health grounds." These complaints have been lodged with the Internet Corporation for Assigned Numbers and Names (ICANN), and have included objections to such extensions as [.casino](#), [.bar](#), [.sex](#) and [.gay](#), amongst others.

BLOGGER AND NETIZEN ARRESTS

BAHRAIN: Activist Nabeel Rajab sentenced

Bahraini activist Nabeel Rajab, who [had been arrested](#) early this year for his criticism of the Bahraini government on Twitter, was [sentenced](#) to three years in prison for participating in illegal assemblies. A written [statement](#) by several members of the United State's Congress sent to Bahrain's King Hamad al-Khalifa has expressed concern over the arrest of Rajab and other Bahrainis on crimes relating to freedom of expression. Rajab's conviction for his comments on Twitter has been recently [overturned](#), though the conviction on his alleged participation in illegal assemblies has remained unchanged. Bahrain has arrested many [bloggers and online activists](#) over the past few months, and has recently cracked down on online activity considered [blasphemous](#) and detrimental to sectarian relations in the country.

CYBER ATTACKS

IRAN: Preparations for upcoming cyber attacks during the 16th summit of the Non-Aligned Movement in Tehran

Mahmoud Khosravi, CEO of Iran's government-controlled Telecommunications Infrastructure Company, [announced](#) [Farsi] that Iran is fully prepared for any possible cyber attacks during the 16th [Summit](#) of the Non-Aligned Movement in Tehran. It is very likely that the summit, Iran's largest international summit in years and featuring dozens of leaders from the developing world, would have significant [implications](#) for regional peace and stability.

IRAN: Armed forces involvement in battling cyber war

Fars News Agency [reported](#) [Farsi] that Iran is planning to involve its armed forces in combating possible cyber attacks. Brigadier General Masoud Jazayeri, the deputy chief of Iran's joint armed forces, announced that, in collaboration with other organizations, the armed forces will set up a separate headquarters to take part in areas of cyber war, cyber defence, and cultural invasions.

SAUDI ARABIA: Hackers post fake story about Saudi Arabia to Reuters

On August 15, Reuters news agency [reported](#) that hackers had gained access to its website and posted a false news story about the death of Saudi Foreign Minister Prince Saud al-Faisal. The report [claimed](#) that the minister had passed away due to medical complications shortly after stomach surgery. As Citizen Lab [previously reported](#), Reuters has recently been subject to similar attacks aimed at spreading disinformation about the ongoing Syrian conflict.

SAUDI ARABIA: Saudi Aramco hit by computer virus

Saudi Aramco, the national oil company of Saudi Arabia, was [hit by a computer virus](#) on August 15. Saudi Aramco posted a [response](#) to the attack on its Facebook page, stating that the “interruption has had no impact whatsoever on any of the company’s production operations” and that the virus had likely originated on the personal workstations of its employees. The “Arab Youth Group” [claimed responsibility](#) for the attack on Pastebin and warned Saudi rulers that they “will face more severe action” if they “continue to betray the nation.”

SYRIA: Pro-government hackers use fake anti-hacking tool to target activists

Eva Galperin of the Electronic Frontier Foundation and Morgan Marquis-Boire, a Technical Advisor at the Citizen Lab, have [issued a report](#) on the discovery of new malware targeted at Syrian opposition groups. A fake security program called “AntiHacker” claims to provide “Auto-Protect & Auto-Detect & Security & Quick scan and analysing.” In reality, the programs installs a remote administration tool called Dark Comet RAT. Citizen Lab has previously reported numerous instances of targeted malware attacks against anti-government opposition groups, most notably [BlackShades RAT](#).

INTERNET AND SOCIAL MEDIA USE

IRAN: Government requires registration of social networking websites

Social networking websites, like other public forums and weblogs, must [register](#) [Farsi] in the Iranian government’s database and apply for a permit from the country’s Information Technology and Digital Media Development Center. According to Hassan Alizadeh, director of the Center, social networking websites will face legal obstacles if they do not take both steps.

IRAN: Users refuse to set up national e-mail address to protect their identities

As previously [reported](#), the Iranian government has encouraged Iranians to use “.ir” e-mail addresses. However, Iranian users have expressed concerns against signing up for a national e-mail address because the registration process requires that users provide a significant amount of personal information. Ali Hakim Javadi, head of Iran’s Information Technology Organization, [stated](#) [Farsi] that although the ultimate goal is to be able to identify individual users, e-mail providers have been asked to minimize the amount of personal data that they collect.

KUWAIT: Twitter attacked as a vehicle for discord

The Arab Network for Human Rights Information (ANHRI) has [condemned](#) a statement made by Suleiman Hamoud, Undersecretary of the Kuwaiti Ministry of Information, in which he publicly attacked Twitter as a vehicle for “spreading discord.” In its statement, ANHRI called on Kuwaiti authorities to “stop the campaign launched against ‘Twitter’ and leave space for its users to express their views.” Kuwait has proposed [criminalizing the “misuse” of social media](#) and, [as previously reported](#), has even arrested a member of the Kuwaiti royal family for political remarks made on Twitter.

TECHNOLOGY UPDATES

SYRIA: Syrian government seeks out Chinese companies for Internet bandwidth

In light of growing international pressure and US-imposed sanctions, the Syrian Telecommunications Establishment has [established](#) business links with Chinese companies for Internet bandwidth. Renesys, a global Internet intelligence firm, [reported](#) on its blog that PCCW, a Hong Kong-based telecom company, is now providing the majority of Syria's Internet traffic. Unlike the US and many European countries, China has not imposed economic or political sanctions on Bashar al-Assad's government.

[Read previous editions](#) of the Middle East and North Africa CyberWatch.