The Citizen Lab

Middle East and North Africa CyberWatch:

May 2013

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

EGYPT: Government promises "open" Internet to EU
In a meeting with a representative of the European Commission's Digital Agenda, Egyptian Telecommunications Minister Atef Helmy pledged that the country would maintain an "'open' Internet that

would not be subject to government shut downs." The Egyptian government notoriously switched off all Internet connectivity during the Arab Spring protests of January 2011. Egypt also affirmed that it will support the European Commission's Global Internet Policy Observatory, which will "act as a clearinghouse for monitoring Internet policy, regulatory and technological developments across the world."

IRAN: Intensified Internet controls leading up to the presidential elections
In the weeks leading up to the 2013 presidential elections, the Iranian government has filtered or shut down multiple domestic websites. Four websites affiliated with Ahmadinejad's government and supportive of Esfandiar Rahim Mashaei, the president's Chief of Staff and now-disqualified candidate, were filtered. The four included Meyar-News, Roshanaee, Baharna, and Bahar-Online. Further, Bahar Newspaper's website has been blocked twice over the past week. So far, the government has provided no official reason for the filtering of this news outlet, which is affiliated with the reformist movement in Iran. Before the Guardian Council's official announcement on the list of nominees for the upcoming presidential election, the Committee to Determine Instances of Criminal Content stated that the publication of unofficial statements regarding the disqualification of any of the nominees would constitute a "dissemination of lies," which is a cause for filtering. The spokesperson from the committee clarified that the political affiliation of the websites is not a determining factor in filtering.

The Iranian online community has also faced extended disruptions in Internet service, including a decrease in connection speed. Problems with bandwidth speed have been most evident while accessing web pages with an "https" protocol. Deputy Minister of Communication and Information Technology Ali Hakim-Javidi stated the upcoming elections is not among the many factors that affect Internet speed in the country. Other officials have cited the disconnection of international cables in the Suez Canal as the cause of the recent spate of Internet disruptions. Intensified Internet controls have rendered the use of circumvention tools even more difficult than before, thereby prompting much speculation with regards to the initiation of the National Information Network in the country.

SYRIA: Internet outage amidst fighting
On May 7, Syria's Internet went offline for 19 hours, a situation that Syrian state news described as the result of an "optic cable malfunction." Some Internet experts, however, contended it was a deliberate act by the Syrian government. Another outage was reported on May 15 for several hours. Activists have argued that these blackouts have always been conducted by the Syrian government as part of an effort to curtail information on government military operations, as happened in the city of Aleppo in August 2012.

UAE: Arab Media Forum debates merits of electronic regulation
The Arab Media Forum, an annual gathering of "journalists and media professionals," held a session in mid-May on the topic of Internet freedom versus the need for online restrictions. Academic and professional experts agreed that, despite the benefits of the Internet, regulation models are still needed. As previously reported, there is some concern over revisions to the UAE's "Cybercrime Law," which critics argue will further curtail online freedoms.

SURVEILLANCE

BAHRAIN: Judicial review sought over sale of surveillance technology

Recently, a Bahraini opposition activist sought a judicial review in the UK to examine the British government's failure to provide information on the [sale of commercial surveillance](#) technology to foreign regimes. FinSpy, which is distributed by British company Gamma International, was among the technologies cited in the case. [Citizen Lab research has shown that FinSpy is actively used in Bahrain](#) and many other countries.

SYRIA: More Blue Coat servers found in Syria

Telecomix, an online activist group, has [released findings](#) that 34 Blue Coat servers "dedicated to intercepting communications and data circulating on the Internet" were operational in Syria as of May 22. The groups claims that its findings indicate that the Syrian government continues to acquire and use surveillance equipment from Western companies and that the Internet shutdown on May 7 was "probably used to install the new surveillance infrastructure." Last year, [Telecomix found 15 Blue Coat servers](#) in Syria. Moreover, Citizen Lab has documented the existence of Blue Coat devices in [Syria and Burma](#), as well as [around the globe](#). Blue Coat is a California-based company that produces technology capable of filtering and surveillance. Reporters Without Borders has named Blue Coat one of five corporate "[Enemies of the Internet](#)" and most recently [called on the company](#) to "explain the presence of 34 of its servers in Syria and their use by the regime to track down its opponents."

BLOGGER AND NETIZEN ARRESTS

BAHRAIN: Missing blogger resurfaces in London

Ali Abdulemam, a Bahraini blogger who disappeared from public life almost two years ago, has [resurfaced](#) in London. Andulemam, founder of opposition website [BahrainOnline.org](#), had been hiding from Bahraini authorities since 2011, around the same time that he was sentenced *in absentia* to 15 years imprisonment for plotting a coup. Bloggers and other activists continue to face prosecution by Bahraini authorities. Recently, [six Twitter users](#) were sentenced to one year in prison for *lèse majesté* offenses against King Hamid bin Isa al-Khalifa.

IRAN: Arrest of Baztab website editor and journalist

Foad Sadeghi, journalist and editor in chief of [Baztab website](#), has been [detained](#) by authorities following the shutdown of the website and the arrest of its manager. Mr. Sadeghi has been detained by authorities before and the website has been shut down multiple times in the past. In the weeks leading up to the official nominations of the 2013 presidential candidates, the website had been vocal about the need for free and fair elections and the participation of all political parties. Baztab is one of the forerunners in the field of online media activism in Iran.

OMAN: Omani authorities detain blogger

Omani security forces [arrested](#) a blogger in the town of Sinaw on May 20. Blogger Diab al-Amiri was [released](#) days later and may be charged with violating the country's cyber crime laws for comments on social media websites related to protests over a land controversy in the Mudhaibi region. As [previously](#)

reported, scores of Omanis have been arrested and charged by authorities over violations of the country's Cybercrime Law.

CYBER ATTACKS

ALGERIA: Algerian hacker Hamza Bendelladj extradited to the US
Thailand has extradited Algerian national Hamza Bendelladj to the United States on charges of developing and marketing malware designed to steal private information. The malware, a derivative of the "Zeus" botnet toolkit called "SpyEye," has been described as "among the most widely-used financial fraud malware packages in the world." Bendelladj was arrested early this year by Thai authorities.

IRAN: Stuxnet helped Iran's nuclear programme
According to a report from the journal of the Royal United Services Institute (RUSI), Iran's nuclear program has progressed significantly since the Stuxnet attack on its Natanz facilities. The report, written by Ivanka Barzashka, suggests that the Stuxnet attack exposed some of the shortcomings of the program which would have otherwise gone unnoticed.

SYRIA: Syrian Electronic Army hacks the Financial Times
The Syrian Electronic Army [SEA] has claimed responsibility for the hacking and defacement of the website of the Financial Times, a British newspaper. Headlines on the website's front page were altered to read "Hacked By Syrian Electronic Army," while the Financial Times' Twitter account linked to a YouTube video that allegedly depicts Syrian rebels executing members of the Syrian armed forces. Reuters questioned whether Twitter was a sufficiently secure platform, noting that the SEA has managed to commandeer several high-profile accounts over the past year. Twitter introduced two-factor authentication just days later.

TECHNOLOGY

IRAN: Iranian users denied access to Google I/O 2013
Internet users in Iran were denied access to the Google I/O page and told that the "service is not available for your country." Google had invited all of its users to tune into the two day conference, which brings together developers from all around the world. This feature, however, was not available for Iranian users on account of the digital sanctions placed on Iran by companies such as Google.

IRAN: Recent Internet statistics
The National Internet Development Management Center (MATMA) has placed the total number of Internet users in Iran at 45,005,644. This figure reflects a 59.5 per cent Internet penetration rate. Internet usage through mobile devices (GPRS) rank the highest, accounting for 36.46 per cent of all connections, followed by dial-up and ADSL connections in second and third place respectively.

PALESTINE: Google recognizes Palestine
As of May 1, Google now officially uses the term "Palestine" on its localized search engine. Historically,

Google has referred to the disputed area as the "Palestinian Territories." The company announced that it was "following the lead of the UN... and other international organisations." Israel expressed disapproval at the gesture, arguing that the new policy "pushes peace further away, pushes away negotiations, and creates among the Palestinian leadership the illusion that in this manner they can achieve the result." The United Nations elevated Palestine's status from "non-member observer entity" to "Non-Member Observer State" last November.

Read previous editions of the Middle East and North Africa CyberWatch.