UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Middle East and North Africa CyberWatch: March 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

TUNISIA: Interior Minister calls for new Internet monitoring body

Tunisian Minister of the Interior Lotfi Ben Jeddou has proposed that Tunisia establish an Internet monitoring body to investigate cybercrime and other Internet violations in coordination with the Tunisian Ministry of Communication Technologies. In this proposal, the Tunisian Internet Agency (ATI), which had previously monitored Internet content, would be relegated to focusing on the development of Tunisia's Internet services. The proposal has been met with criticism from groups such

as Anonymous Tunisia and the Tunisian Pirate Party who fear it could lead to a revitalization of online censorship in the country.

UAE: Emirati telecom provider unblocks Skype

UAE based telecommunications operator Etisalat announced in early April that they had unblocked Skype, allowing users the ability to access the website. The government's Telecommunications Regulatory Authority (TRA) did make a statement, however, that Skype was still prohibited in the country. Defending its decision, Etisalat claimed that the TRA had stated in 2010 that telecommunications operators could offer Skype without submitting requests to the regulatory authority.

EGYPT: US embassy pulls down Twitter feed

The United States' Egyptian Embassy recently pulled down its Twitter feed temporarily after the office of President Mohammed Morsi raised objections to a controversial tweet. The former tweeted a link to a video of US comedian Jon Stewart, who criticized the Egyptian government's arrest of satirist Bassem Yousef. Morsi's Twitter account responded by chastising the embassy for engaging in "political propaganda." Since 2011, many Egyptian online political critics and activists have faced government prosecution.

IRAN: Filtering of 1,500 anti-Islamic websites per month

(Note: Cross posted at iranmediaresearch.org)
Mohammad Reza Aghamiri, a member of the Committee to Determine Instances of Criminal Content, stated [Farsi] that an average of 1,500 websites with anti-Islamic content are filtered on a monthly basis. Aghamiri added that "the monitoring of websites is done manually, so in comparison to automatic monitoring of the content, it is less probable that we make mistakes." Aghamiri also referred to discussions regarding filters within the National Information Network (NIN). He clarified that the NIN will not be monitored and content blockage will be unnecessary because the network operates as a "pure" system.

IRAN: Filtering of 'Rise of Morning Hope' websites

(Note: Cross posted at iranmediaresearch.org)
Two websites were launched by The Rise of Morning Hope (Aftab-e Sobh-e Omid) campaign in support of Mohammad Khatami, an Iranian scholar and former president. SalamKhatami.com [Farsi] was developed to gather signatures from Khatami's supporters and encourage him to run again for the presidency. The second website, SalamKhatami.org [Farsi], serves to cover the latest news related to his possible candidacy. Both websites were filtered [Farsi] shortly after being launched by the order of Iran's filtering committee.

IRAN: Baztab-e Emrooz news website filtered

News website Baztab-e Emrooz was filtered [Farsi] after reporting [Farsi] that President Mahmoud Ahmadinejad had threatened to release confidential conversations between himself and election

officials in 2009 if the Guardian Council failed to approve the candidacy of Esfandiar Rahim Mashaei, the current Chief of Staff. The conversations allegedly reveal that election officials falsely reported that Ahmadinejad won by 24 million votes, when in fact he won by 16 million, in order to prevent a recount. The report, which was deleted 50 minutes after it was posted on April 27th, claimed Ahmadinejad contacted officials and argued that voting results should not be rigged. After the story was removed from the Baztab-e Emrooz website, others such as Digarban [Farsi] and Balatarin [Farsi] circulated the story, leading Baztab to once again publish the report on April 28. Baztab-e Emrooz has faced filtering [Farsi] several times during the past year and was not accessible for users inside Iran. After publishing news about Ahmadinejad's claims that the regime defrauded the voters in the 2009 presidential election, Baztab-e Emrooz was completely shut down.

SURVEILLANCE

SAUDI ARABIA: Criticizing new monitoring scheme

Global Voices Advocacy reported on the Saudi Arabian government's intention to surveil online communications over platforms like Skype. While the news was originally reported in the form of a leaked memo [Arabic] on Twitter, the state's Communications and Information Technology Commission confirmed its veracity on March 31. The Commission asserted that communications surveillance would be aimed at "preserving values and principles, protecting the rights of everyone and protecting society from any negative aspects that could undermine the public well-being." Companies that do not comply with government directives risk being blocked entirely. Last month, Saudi Arabia threatened to ban messaging applications like Skype, Viber, and WhatsApp in light of its inability to adequately monitor their use.

IRAN: Election headquarters organized by police forces to monitor cyberspace

(Note: cross posted at iranmediaresearch.org)
Newspapers Jam-e Jam and Kayhan reported [Farsi] that the Islamic Republic of Iran Police (NAJA) has formed an election headquarters named Fajr. Social Deputy of Police Forces Saeed Montazer al-Mahdi announced that, in order to ensure the "security and safety of the election process," Fajr will monitor satellite channels, anti-regime websites, and social networking sites. Since Iranians previously used Facebook to organize rallies after the disputed 2009 elections, Fajr will monitor [Farsi] social networking websites closely to find and restrict similar instances.

IRAN: 20 new regulations for Internet cafés

Iran's Cyber Police (FATA) issued [Farsi] a new set of 20 rules that Internet cafés are to abide by. According to this new set of guidelines, owners of cybercafés should be "committed, married individuals who have no criminal records" and must set up 24-hour surveillance cameras in their cafés. Staff at Internet cafes must start collecting the details of their customers' identities, address, national ID number, and telephone number. Businesses have also been asked to keep detailed records of when and how their customers use the internet, including a list of the websites they visited. In addition, the government has emphasized that the use of VPNs and any other types of circumvention tools is forbidden. The full list of regulations can be found here.

BLOGGER AND NETIZEN ARRESTS

IRAN: Pro-Khamenei blogger arrested for criticizing Supreme Leader

(Note: Cross posted at iranmediaresearch.org)
A pro-Khamenei cyber activist Mojtaba Daneshtalab was sentenced to six months in prison and 35 dollars in fines over charges of "propaganda against the regime" and "insulting Ali Khamenei." A day before his imprisonment, Daneshtalab wrote [Farsi] in his blog that he has not become an "anti-revolutionary" person and that he did not have any "bad intentions." Many of Daneshtalab's fellow bloggers and other pro-Khamenei cyber activists have used social media to show their disapproval of Daneshtalab's conviction.

IRAN: Arrest of a circumvention tool distributor

FATA's chief police officer in the province of Ghazvin announced [Farsi] that, in accordance with FATA's mission to identify cyber criminals and monitor cyberspace, the organization had arrested a person accused of marketing and selling circumvention tools online. It is reported that the arrested individual was not aware that the sale of circumvention tools is illegal. The Computer Crimes Law dictates that the sale and marketing of circumvention tools and the teaching of methods to bypass censorship is illegal.

UAE: Arrest of an activist for tweeting from a courtroom

Abdullah al-Hadidi, an activist based in the UAE, was recently sentenced to 10 months in jail for live-tweeting his father's trial from an Abu Dhabi courtroom. He was arrested on March 22 and charged with "disseminating false information." His father had been detained for "plotting the overthrow of the government" in collaboration with a cell of 94 other people.

BAHRAIN: Bahraini prosecution appeals decision to acquit activist

The Arabic Network for Human Rights Information (ANHRI) has voiced concerns over attempts by the Bahraini prosecution to appeal a decision by the Supreme Criminal Court. The decision would acquit Said Yousif Al-Muhafdah, Vice-President of the Bahrain Center for Human Rights. Al-Muhafdah was charged with tweeting "false information" that security forces had used birdshot against protesters in December 2012.

MOROCCO: Atheist blogger in hiding

Imad Iddine Habib, a Moroccan blogger and self-identified atheist, has gone into hiding due to concerns over his personal safety. Habib had voiced concerns that Moroccan police wanted to arrest him and that his life was "at high risk." In March, Habib created the Council of Ex-Muslims of Morocco (CeMM), described as "the first public atheist and non-religious organisation in a country with Islam as its state religion."

CYBER ATTACKS

ISRAEL: Israeli Hackers vs. Anonymous

Israeli hackers and Anonymous have been embroiled in an ongoing cyber battle. On April 7, pro-Palestinian hackers targeted Israeli websites using DDoS attacks and defacements, but failed to make a significant impact. Targets included the Ministry of Foreign Affairs and the website of Israel's Holocaust memorial. Prior to the attacks, Anonymous had announced its intention to "disrupt and erase Israel from cyberspace" in response to Israeli policies toward Palestinians. Days later, OpIsrael.com—a website allegedly belonging to Anonymous—was defaced by Israeli hackers, who posted pro-Israel propaganda and taunted the hacktivist collective.

SYRIA: Syrian Electronic Army targets CBS and NPR Twitter accounts

The Syrian Electronic Army (SEA) attacked a number of high-profile Twitter accounts over the past month. On April 15, the organization attacked NPR.org and its Twitter account in response to the broadcaster's coverage of the Syrian conflict. Days later, it gained access to CBS' 60 Minutes Twitter account. The hackers posted messages accusing the United States of cooperating with terrorists and later took responsibility for the attack via a YouTube video. The SEA also claimed responsibility for compromising the Twitter account of the Associated Press and posting a fake news story about a bombing at the White House on April 23. The group has regularly hacked Twitter accounts in the past, including those of Al Jazeera.

OMAN: Moroccan hackers attack sites in Oman via DNS poisoning

On April 21, hackers from Morocco gained access to the Oman Telecommunication Company's servers and defaced the website of Google Oman (google.com.om). Two people under the handles "Z0mbi3_Ma" and "SQL_Master" diverted traffic from Google Oman's URL to an outside website via DNS poisoning, whereby hackers alter information on a DNS server's database. A similar attack occurred on Google Bosnia.

TECHNOLOGY

IRAN: Iran plans 'Islamic Google Earth'

(Note: cross posted at iranmediaresearch.org)

Iran's Minister for Information and Communications Technology, Mohammad Hassan Nami, announced that "Iran is developing a 3D world map project similar to Google Earth, which will be launched in the next four months as a national portal, providing service on a global scale." Nami stated that this new service will be created with "Islamic views." Several Iranian officials have commented that Google Earth is in fact a spying tool and it is often blocked in Iran. Experts have expressed doubt that the Iranian government will be able to accomplish a project on such a large scale over the next four months in the current economy.

Read previous editions of the Middle East and North Africa Cyber Watch.