UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Middle East and North Africa CyberWatch: October 20-November 4, 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

QATAR: Human Rights Watch calls on Qatari emir not to support media law

Human Rights Watch (HRW) has called on Qatar's ruling emir, Sheikh Hamad bin Khalifa al-Thani, not to approve a draft media law that it says creates a "double standard on free expression" in a country previously known for its relatively free media compared to the rest of the region. HRW criticized the ambiguously worded provisions in the law which penalizes criticism of Qatar or neighboring governments in the Persian Gulf. Qatar's commitment to free expression was also questioned due to the case of Muhammad Ibn al-Dheeb al-Ajami, a poet who was arrested for circulating a poem online that allegedly criticized the emir.

BLOGGER AND NETIZEN ARRESTS

BAHRAIN: PEN International alert on poor health of incarcerated blogger
PEN International has issued a statement of concern over the health of detained blogger and activist Dr. Abduljalil Al-Singace, who has been on hunger strike in protest against the poor prison conditions. Al-Singace was sentenced to 15 years imprisonment in October 2011 for "plotting to topple" the regime. His blog [Arabic] has been blocked in Bahrain since 2009 for his anti-government writings.

IRAN: Arrest of Facebook users for "illegal online activities"
According to Mehdi Bakhshi, Attorney General of Sirjan, a city in the Kerman Province, four Facebook users have been arrested [Farsi] for activities deemed to be anti-government and insulting to officials. Referring to previous cases of arrests that have been made as a result of online activities, Bakhshi warned Internet users against carrying out "any illegal online activities, such as publishing photos of women not wearing hijab," or else face "legal consequences."

CYBER ATTACKS

IRAN: Cyber-attacks taking a toll on Iran Shipping Lines
Mohammad Hossein Dajmar, the Managing Director of the Islamic Republic of Iran Shipping Lines (IRISL), reported [Farsi] that a number of cyber attacks were committed against IRISL in August. Dajmar explained that the attacks were similar to previous ones against Iran's Ministry of Oil. He added that, as a result of these attacks, shipping addresses have been mixed up and a considerable amount of cargo has been lost.

IRAN: Updates on MiniFlame
Mehr News Agency reported [Farsi] from Kaspersky Lab that although MiniFlame was initially introduced as a component of Flame, it is now an "independent module" that can operate either without the main modules of Flame in the system or as a plug-in for both Flame and Gauss malware. According to Kaspersky Lab's data, the number of machines affected by MiniFlame total around 10 to 20 machines, a relatively low number compared to infections caused by Flame and Gauss. These cases are mainly found in Lebanon, with fewer seen in Iran, Sudan, and Syria.

IRAN: Hackers use Iranian IP addresses for cyber attacks
Ali Hakim Javadi, Iran's Deputy Minister of Information and Communications Technology, stated [Farsi] that "Iran's government has not launched any cyber attacks because it believes that cyberspace should not be misused." He also added that "some countries are using Iranian IP addresses in cyber attacks against other countries."

IRAN: Revolutionary Guards denies involvement in cyber attacks against US banks
The Iranian Revolutionary Guard Corps (IRGC) Commander, Mohsen Kazemini, denied [Farsi] the IRGC's involvement in cyber attacks against US banks. Kazemini stated that, despite accusations to the contrary, IRGC's cyber army is only involved in "web surveillance" and "cultural activities such as blogging".

IRAN: New plans for the Passive Defense Organization

Gholam Reza Jalali, the director of Iran's Passive Defense Organization, announced [Farsi] that the organization is planning to set up a reference lab in the country's Ministry of Defence. The lab will identify malware, develop anti-malware software, and protect the country against cyber weapons. According to Jalali, the lab will be operational by March 2013. Jalali also explained the organization's plans to set up a national Supervisory Control and Data Acquisition (SCADA) management system.

SAUDI ARABIA and QATAR: Oil companies targeted in cyber attacks

The United States and Israel have recently expressed concern over a series of cyber attacks against oil and gas companies in the Arabian Peninsula. In August, there were reported attacks against RasGas, a Qatari producer of liquefied natural gas, and Saudi Aramco, the national oil company of Saudi Arabia. US Secretary of Defense Leon Panetta called the virus that affected both firms "the most destructive attack that the private sector has seen to date." US intelligence officials have blamed Iran for the attacks, citing them as retaliation for Flame, Stuxnet, and other cyber attacks believed to have been launched by the US and Israel.

GOVERNMENT SURVEILLANCE

IRAN: Cyber space under full surveillance

Kamal Hadianfar, chief of the Cyber and Information Exchange Police (FETA), has stated [Farsi] that FETA is taking various approaches to educate the public on cyber crimes, identifying and preventing crimes, and fighting cyber criminals. Recently, Chief of Gilan Province's branch of FETA announced [Farsi] that 491 websites were involved in criminal online activities that will soon face legal consequences. The most recent updates show [Farsi] that about 30 percent of complaints filed in Tehran are related to morality concerns with Facebook.

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