UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Middle East and North Africa CyberWatch: September 8-September 21, 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)

  MIDDLE EAST AND NORTH AFRICA, JORDAN, TUNISIA

- Blogger and Netizen Arrests (pages 2)

  OMAN

- Cyber Attacks (page 2-3)

  IRAN, SYRIA

- Internet and Social Media Use (pages 3-4)

  BAHRAIN, IRAN

- Technology Updates (page 4)

  IRAN

CENSORSHIP AND FILTERING

MIDDLE EAST AND NORTH AFRICA: Google blocks YouTube video in response to popular protest

On September 11, protesters stormed the US Embassy in Cairo, Egypt in response to a 14-minute YouTube video that was deemed insulting to Islam. Hours later, armed men attacked the US Consulate in Benghazi, Libya and killed four staff members. Protests subsequently spread to Yemen,

Lebanon, Tunisia, and other Muslim-majority countries. Google, which owns YouTube, blocked access to the video in Egypt, Libya, and Saudi Arabia. The move was highly controversial and provoked debate as to whether "exceptional circumstances" justify censorship and the violation of free speech.

JORDAN: Continuing controversy over press law amendments
Jordan's King Abdullah II has issued a decree in support of controversial changes to the country's existing Press and Publications Law. These amendments include obliging web editors to join the Jordan Press Association and mandating that news websites apply for licenses from the government. As previously reported, journalists and other activists have voiced their objection to these amendments, claiming that changes will curtail free expression online and inhibit Jordan's growing Internet economy.

TUNISIA: Official end to Internet censorship declared
Tunisia's Internet censorship policies have officially come to an end according to the country's Information and Communications Minister, Mongi Marzoug. Former President Zine El Abidine Ben Ali promoted the censorship policy, popularly referred to as "Ammar 404" after the "404" error message received by Tunisian users when accessing blocked sites. The relaxation of Internet controls was one of the last promises made by Ben Ali to the people shortly before he went into exile.

BLOGGER AND NETIZEN ARRESTS

OMAN: Blogger convicted of "slander"
Journalist and blogger Mukhtar bin Muhammad bin Saif al-Hinai was convicted of slander and unspecified "violations of media codes" for alleged anti-government writings. As previously reported, online activists have been extensively prosecuted for comments seen as defaming the ruling Sultan of Oman, Qaboos bin Said al Said.

CYBER ATTACKS

IRAN: White-hat hackers are invited to work with the Cyber and Information Exchange Police
Iran's Cyber and Information Exchange Police (FETA) has invited [Farsi] tech-savvy citizens to form a group of "white hat hackers." According to FETA's chief, Kamal Hadianfar, they will assist the police in "identifying vulnerabilities in the system". FETA will also continue to track and arrest "black hat hackers" or "crackers." In hacker parlance, "white hats" are those who break security for ostensibly altruistic reasons, while "black hats" are commonly seen as malicious computer criminals.

IRAN: Facebook fan page of a well-known caricaturist hacked
A week after the formation of the "white-hat hackers" group, the Facebook fan page of Mana Neyestani, an Iranian caricaturist, was compromised by a group called "Islam's Soldiers". The group defaced the page with caricatures featuring pro-Assad, anti-Israel, and anti-Saudi Arabia themes within

hours of having control over the site. Neyestani is known for his criticisms of the Iranian government and was previously detained for his controversial work.

IRAN: Partnership with North Korea to fight against cyber attacks developed by western countries

Iran and North Korea signed [Farsi] a technical cooperation contract to join forces in the fight against malware attacks such as Duqu, Flame and Stuxnet. According to Mikko Hypponen, chief research officer of the Finnish computer security company, F-Secure, the main purposes behind the agreement were to mutually develop protection against cyber attacks, expand cyber security capabilities, and possibly collaborate on their own cyber attacks.

IRAN: Minister of Information urges governmental agencies to prepare against cyber attacks

Reza Taqipour, Minister of Information and Communications Technology, announced [Farsi] that all governmental agencies are required to form "cyber rescue teams" and make preparations to defend against potential cyber attacks. The Ministry of Information and Communication Technology would also create a national center to collaborate with these teams and assist them in withstanding any attacks.

SYRIA: Pro-government Syrian hackers send fake Al-Jazeera texts

In the latest series of cyber attacks launched by supporters of the Syrian government, the Syrian Electronic Army compromised Al Jazeera's SMS service. The news network reported [Arabic] the incident on its Twitter feed and warned that those responsible had sent fake news stories, including one that claimed that the Qatari prime minister had been assassinated.

INTERNET AND SOCIAL MEDIA USE

BAHRAIN: Ministry of Interior to tackle crimes related to social media use

Bahrain's Ministry of Interior has recently announced that it will soon prosecute those guilty of "defamation and abuse" on social media platforms. The Acting General Director of Anti-Corruption and Electronic and Economic Security further clarified that such offenses would include insulting public figures, a number of whom have complained to the Ministry about victimization and abuse online. In June, the Ministry of State for Information Affairs stated that the "unrest in Bahrain last year was fueled by the irresponsible use of such media" and consequently announced that authorities were planning to regulate social media networks.

IRAN: Discussions on the meaning of Iran's "National Information Network"

With Iran having recently made much progress on its "National Information Network", Reza Taqipour, stated [Farsi] that full implementation of a national Intranet does not mean that Iranians will be cut from the Internet. However, Donya-e-Eqtesad, an Iranian newspaper, suggested [Farsi] in an editorial that a national network would not protect Iranian users from cyber attacks, and cautioned that there is no guarantee that governmental organizations would not be the target of malware attacks.

IRAN: Minister of Information describes causes for slow Internet speed

Reza Taqipour also addressed complaints about the slow speed of Internet in Iran, announcing [Farsi]

that an increasing number of cyber attacks have necessitated stricter security and that these security measures may decrease Internet speeds. He also noted that problems with Iran's undersea Internet cable, which have recently been resolved through the construction of a parallel cable, likely contributed to reduced Internet speeds in the country.

TECHNOLOGY UPDATES

IRAN: New graduate programs in fields of cyber security

Brigadier General Hossein Valivand, Commander of the Islamic Republic's University of Military Science, announced [Farsi] that the university will soon admit masters students in the fields of cyber science, soft warfare, and information warfare. Valivand argued that Western countries use "constantly changing and increasingly complex strategies to weaken Iran", and that Iran must consequently revise its educational system to meet these challenges.

IRAN: Importation of non-Iranian cyber security products is not banned

Ali Hakim Javadi, Iran's Deputy Minister of Information and Communications Technology, denied recent reports that the government has banned importation of non-Iranian anti-virus products. Minister Javadi explained [Farsi] that importing foreign software and hardware products is not entirely banned, but that potential importers must obtain a permit from Iran's Information Technology Organization beforehand.

Read previous editions of the MENA Cyber Watch.