The Citizen Lab

Middle East and North Africa CyberWatch: October 6-October 19, 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

ISRAEL: Courts reject petition to censor anti-Islamic video

On October 15, the Jerusalem District Court ruled that Google and YouTube are not required to block access to the *Innocence of Muslims* video in Israel. Knesset member Taleb a-Sanaa submitted a petition to block the video, but Judge Miriam Mizrahi struck it down on the basis that it failed to name both Google and YouTube as responsible legal entities. The court would have likely rejected the request regardless of the technicality, as it endorsed Google's position that viewers had to actively seek out the video and could only be exposed to it by their own volition.

IRAN: Websites filtered over currency crisis
With the escalation of the currency crisis in Iran, currency and gold price, websites such as Mazaneh were blocked [Farsi] on October 3. The official website for Iran's union for gold, jewelry, and coins was also made unavailable.

IRAN: Blocking of Media File Downloads
Iranian users are no longer able to download MP3, MP4, AVI, and SWF files hosted on foreign servers. Iran's government has started blocking [Farsi] specific file extensions, thereby preventing users from accessing a significant portion of audio-visual content hosted on servers outside of Iran. As a result, many websites designed using Flash technology will no longer be available to Iranian users, though they are not technically filtered. The aim of this decision may be to restrict access to Internet radio stations and online podcasts.

PALESTINE: Concerns over possible blocking of news sites
Reports indicate that Palestinian Internet users in the Hamas-controlled Gaza Strip could have difficulty accessing certain news sites, such as Israeli newspaper Haaretz, prompting fears that political sites may be censored in the near future. As previously reported, Hamas has already instructed service providers to block pornographic websites starting in September.

SAUDI ARABIA: Kingdom of Saudi Arabia calls for international censorship body
In response to last month's *Innocence of Muslims* controversy, Saudi Arabia has called for the establishment of an international organization to oversee the censorship of offensive Internet content. Saudi officials equated the film and similar material with "malicious and criminal activities such as child pornography, identity theft, spam, denial of service attacks, and malware" and argued that states must collaborate to address such issues.

BLOGGER AND NETIZEN ARRESTS

ALGERIA: Algerian blogger and human rights activist arrested
Police officers beat and arrested human rights activist Yacine Zaid on the grounds of showing a "lack of respect" toward the police. Zaid, who is a blogger [French] and member of the Algerian League for the Defense of Human Rights was released [French] on October 8 after receiving a fine and a suspended sentence.

BAHRAIN: Arrests over "misuse of social media"
Authorities in Bahrain arrested four people for "defaming public figures on social media" as part of the government's efforts to monitor the "misuse" of social media. If found guilty, a penalty of five years imprisonment could be imposed on the accused. As previously reported, Bahrain's Ministry of Interior has pledged to vigorously prosecute citizens for posting what they see as defamatory and abusive comments on social media.

TUNISIA: Trial of Tunisian blogger adjourned
The trial of Sofiane Shurabi, a Tunisian blogger who has been critical of both the ruling Ennahda party and the former regime, was adjourned until October 16. Shurabi was arrested in August for drinking

alcohol in public during the month of Ramadan. There have been several instances of blogger arrests and prosecutions in Tunisia since the fall of President Zine el-Abidine Ben Ali in 2011.

CYBER ATTACKS

ISRAEL: Israeli Defense Forces increasing cyber-warfare recruiting

Israeli newspaper Haaretz reported that the Israel Defense Forces (IDF) has adopted a new policy aimed at recruiting more soldiers capable of conducting cyber warfare and increasing its budget for cyber-related activities. The announcement followed a statement by Prime Minister Benjamin Netanyahu on October 14 that "there have been increasing efforts to carry out cyberattacks on Israel's computer infrastructure." The IDF already allocates some NIS 1 billion (over US$262 million) to cyber defense.

IRAN: New spyware found

A new form of spyware called "MiniFlame", which appears to have originated from the same malware factory that created Stuxnet and Flame, has been discovered [Farsi] in Iran. According to the chief security expert at Kaspersky, a Moscow-based cyber security company, MiniFlame conducts in-depth surveillance and cyber espionage against high-value targets. The main targets include Iranian and Lebanese banks that are are suspected of laundering money for Iran and Hizbullah.

IRAN: Recent cyber attacks against Iranian Offshore Oil Company

According to Mohammad Reza Golshani, IT manager of the Iranian Offshore Oil Company, the company was the target [Farsi] of several cyber attacks during the past two weeks. These cyber attacks have affected the communications systems of the entire company, including its oil platforms. No further damage to the computer system has been found as the company has an internal computer network and is not connected to the global Internet.

IRAN: Average of 500 daily cyber attacks against Iran

According to Reza Taqipour, Minister of Information and Communication Technology, over 500 attacks [Farsi] are directed against Iran on a daily basis, though only major attacks receive media coverage. The Chief of Iran's Cyber and Information Exchange Police (FETA) also stated [Farsi] that, in spite of continuous attacks against Iran, no government website has been severely damaged.

SYRIA: Syria accused of disrupting BBC services

BBC services to Europe and the Middle East have been jammed in Syria and Eutelsat, a French-based satellite company, has blamed the Assad government for the disruption. Many sources have also accused Iran of supporting Syria in disrupting these services. Prior to this attack, Eutelsat recently blocked 19 Iranian radio and television broadcasters in compliance with European Union sanctions against the Iranian government.

INTERNET AND SOCIAL MEDIA USE

SAUDI ARABIA: First defamation case via Twitter

A Saudi woman has accused [Arabic] a young man of publicly cursing and defaming her via Twitter.

The woman took screenshots and delivered them to local police authorities in Medina, who in turn referred the case to the Authority for Investigation and Prosecution. The incident is the first of its kind in Saudi Arabia and comes after Riyadh's recent approval of penalties for those engaged in libel and defamation on social networking websites.

TECHNOLOGY UPDATES

IRAN: Uncertain future for national anti-virus product

Six months after the introduction [Farsi] of Iran's national antivirus project, the developers—Shiraz University's Computer Emergency Response Team of Academic Protection and Awareness (APA)— have yet to provide an update [Farsi] on the project's progress. According to Gholam Reza Jalali, the director of Iran's Passive Defense Organization, the project is 60 percent complete. However, the APA has refused to comment on either the technical aspects or progress of the project. Asr-e Ertebat, a weekly Iranian magazine, recently argued that, although it is essential to develop and support national anti-malware and antivirus products, the future of the project is uncertain.

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