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

MIDDLE EAST AND NORTH AFRICA: Reporters Without Borders releases its Enemies of the Internet list

Reporters Without Borders (RSF) has released its 2013 Enemies of the Internet list, focusing primarily on surveillance and surveillance technology. Among the five states listed as "Enemies of the Internet," three are from the Middle East and North Africa region: Iran, Bahrain, and Syria. The report focuses

the use of Western commercial technology (including those sold by companies such as Blue Coat Systems in Syria, Gamma International in Bahrain, and Trovicor in Iran) to spy on the online activities of dissidents and citizens. RSF urges greater legislative oversight to control the export of commercial technology that could undermine human rights in authoritarian regimes. Research by the Citizen Lab on Gamma International's FinFisher toolset used by Bahraini authorities was cited in this report.

EGYPT: Egypt overturns YouTube ban

Upon appeal by Egypt's National Telecommunications Regulatory Authority (NTRA), the country's Administrative Court has halted a February order to ban YouTube for one month as a response to the video-sharing site hosting the anti-Islamic film "Innocence of Muslims." The NTRA argued that, as an American company, YouTube could only be shut down in the United States. YouTube had previously blocked access to the video in Egypt, a move considered controversial by many Internet freedom advocates. The NTRA has also made an announcement that they are positioned to ban pornographic sites in Egypt according to a November directive by the former Prosecutor General, Abdel Maguid Mahmoud.

IRAN: The government shuts down VPN ports across the country

Unauthorized VPN ports in Iran were shut down [Farsi] on March 9. Government officials had previously announced [Farsi] that all illegal VPNs would be closed down by the end of Nowruz, the Persian new year. Financial institutions and other organizations that might need to use VPNs for security reasons could register to receive "legal VPNs." Experts believe that legal VPNs would enable authorities to monitor Internet traffic more easily. While this decision could be motivated [Farsi] by the fast approaching election season, some consider [Farsi] this decision a step forward toward the complete implementation of the National Information Network project.

SAUDI ARABIA: Messaging application threatened with prohibition

Saudi Arabia has threatened to ban messaging applications such as Skype, WhatsApp, and Viber due to the state's inability to adequately regulate and monitor them. The government has asked telecommunications providers in the Kingdom to develop ways of controlling these applications. Human rights activists have criticized the move, arguing that it violates an article in a convention signed by Saudi Arabia that protects the secrecy of transmitted data over phone calls. The Saudi government hardened its stance in a statement on March 31, warning that it would take "suitable measures" if instant messaging companies do not comply with its requests.

SURVEILLANCE

IRAN: Text messages under government's surveillance

Hamid Shahriari, Deputy Judiciary and head of the judiciary's Information Technology Center stated [Farsi] that during the 2009 election unrest, the authorities opted to to block all text messages as a precaution. He said that now the government is better prepared for the upcoming election in June and, with new surveillance technology, will block text messages that "threaten national security" only.

BLOGGER AND NETIZEN ARRESTS

BAHRAIN: Bahraini court acquits leading activist

Said Yousif al-Muhafdah, Vice-President of the Bahrain Center for Human Rights (BCHR), has been acquitted of charges that he had tweeted "false information" -- that birdshot was used by police against protesters -- in December 2012. Amnesty International has stated that the real reason for the arrest was likely due to al-Muhafdah's continuing human rights work with the BCHR.

EGYPT: Blogger hands himself in to authorities

On March 26, Alaa Abdel-Fattah, a famous Egyptian blogger, handed himself in to Egyptian authorities after facing accusations of "instigating violence" against the Muslim Brotherhood via social media. He was released from custody later that day after demanding an investigative judge be put in charge of his case instead of government prosecutors. While inside the prosecutor's office, both Abdel-Fattah and prosecutors updated followers on Twitter and Facebook with conflicting stories about the detained blogger's questioning. The allegations against Abdel-Fattah raise questions as to whether President Morsi is inappropriately using the judiciary to silence his critics.

IRAN: Iranian student arrested for unknown reason

Iman Amiri, an Iranian network security student in Sweden, was arrested on January 21 upon arrival in Tehran. It is reported that Amiri is being held at Evin prison and has had only a brief meeting with his brother since being arrested.

OMAN: Internet activists released

Following an order from Sultan Qaboos bin Saeed, the Omani government has pardoned and released activists imprisoned for insulting the monarchy or "violating the country's cyber laws." Last January, an Omani court upheld the jail terms of several detained bloggers accused of defaming the monarchy. Approximately 49 Omanis have been tried to date for online activity, often under the recent Cybercrime Law.

SAUDI ARABIA: Human Rights Watch asks for release of Saudi activists

Human Rights Watch (HRW) has advocated for the release of Mohammed al-Gahtani and Abdullah al-Hamed, two Saudi activists convicted of violating a law on "cybercriminality" by using Twitter to criticize life in Saudi Arabia. Al-Gahtani and al-Hamed have been sentenced to jail terms of 10 and five years respectively. HRW has denounced the sentencing as motivated solely to punish the activists' right to free expression. The government is moving toward greater restrictions on the use of social media, including finding means to end the anonymity of Twitter users through the registration of personal identification.

SYRIA: Family of Syrian open-source engineer appeals for release

The family of Bassel Khartabil (also known as Bassel Safadi), a Syrian open-source software engineer of Palestinian origin, has appealed to the European Union for assistance in securing his release. He was

arrested the previous year in Damascus by Syrian authorities, although no formal charges have been laid against him. Foreign Policy magazine listed Khartabil as one of their Top 100 Global Thinkers for "fostering an open-source community in a country long on the margins of the Internet's youth culture."

CYBER ATTACKS

MIDDLE EAST AND NORTH AFRICA: Muslim hacker group warns of future attacks

A group of hackers calling themselves the "Cyber Fighters of Izz ad-Din al-Qassam" reportedly launched a DDoS attack in late February and warned that more is to come. The Cyber Fighters announced the launch of the "third phase of Operation Ababil," which has almost exclusive targeted US banks, and demanding that YouTube remove all copies of the "Innocence of Muslims" video. The same group previously took credit for attacks on many US financial institutions last September. The group's tactics revolve around using compromised US servers to redirect traffic and overload a targeted website with hits. The US government has blamed the attacks on Iran, though Iran's Revolutionary Guard Corps [Farsi] and Ministry of Information and Communication Technology [Farsi] have both denied the accusations.

IRAN: NATO researchers; Stuxnet attack against Iran was illegal

A group of NATO legal and technology experts believe that the deployment of the Stuxnet worm against Iran in 2009-2010 constituted a "cyber attack" and is considered an illegal "act of force" based on the UN charter.

SYRIA: Syrian Electronic Army hacks the BBC and Qatar Foundation social media accounts

The Syrian Electronic Army (SEA) recently compromised a number of the BBC's official Twitter accounts. The hacker group first posted a series of strange messages on BBC Weather's account, such as "Saudi weather station down due to head-on collision with camel." It later became clear that they had gained access to other accounts, including BBC Arabic and Radio Ulster. The BBC regained control of its accounts and subsequently posted an apology in English and Arabic. The SEA also compromised the Twitter and Facebook accounts of the Qatar Foundation, a partly government-funded non-profit organization, and accused them of funding terrorists. Citizen Lab has previously reported on the SEA's hacking of al-Jazeera, Amnesty International, and Reuters.

TECHNOLOGY

MIDDLE EAST AND NORTH AFRICA: New Arabic search engine — Ya Arabi

A group of developers will launch [Arabic] the first beta version of Ya Arabi—an Arabic search engine—this May. Chief Executive Officer 'Abd al-Rahman Tahboub stated that the service would block websites deemed "offensive to moral and humanitarian values" and those that promote "violence, crime, and hatred."

IRAN: Updates on the national network of cyber defence

Amirkabir University's information security team is working on a "national network of cyber defence," which will be partly finished in the next Persian year. Iran has made past attempts at advancing technology in the fields of cyber security and defence. Shiraz University, for example, has been working on a national anti-virus project. Although it has failed to attract Iranian users, Gholam Reza Jalali, the Director of the Passive Defence Organization, still believes [Farsi] that the government should continue to support such initiatives and enforce the ban on foreign anti-virus and other digital security products.

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