

Syrian Opposition Targets the Regime Online

May 18, 2012



Brief Analysis

Syrian activists have stepped up their social media efforts and cyber attacks against the Assad regime, and Washington should take more steps to support them.

In addition to its brutal physical repression of the Syrian people, Bashar al-Assad's regime has an abysmal free press record. According to Reporters Without Borders, Syria ranks 176th out of 179 countries in press freedoms. Despite this suppression, opposition activists have successfully leveraged social media and internet communication over the past year, broadcasting, explaining, and promoting the uprising to the world. They have also fought back with cyber attacks, turning the tools used by pro-Assad hackers against the regime. Although these measures have not prevented the slaughter of thousands, regime atrocities would be even worse without the spotlight cast by YouTube and other technologies. Washington therefore has an interest in providing the opposition with the equipment and technical support needed to continue the cyber campaign against Assad.

BACKGROUND

Unlike the Egyptian opposition, which set up satellite phones and dial-up connections to internet service providers in Europe and Israel as backup measures once the revolution was already underway, the Syrian opposition has employed satellite phones/modems as their primary means of communication from the start. According to activist Shakeeb al-Jabri, approximately 60 percent of opposition communication takes place via Skype or Thuraya satellite phones. In addition, Syrians located close to the border with Lebanon and Turkey often use those countries' servers to access internet and mobile networks while evading Syrian web surveillance.

The opposition is heavily dependent on social media -- the video documentation of regime violence uploaded to YouTube, Facebook, and other sites has become the primary source of details on developments in the country. For example, one Facebook page ("[Syrian Uprising 2011 Information Centre](http://www.facebook.com/syrianuprising) (<http://www.facebook.com/syrianuprising>)") offers daily tallies of opposition and civilian deaths and plots the location of every protest on a Google map. Activists also reportedly created the iPhone app "Souria Wa Bas" ("Syria, That's It") to broadcast information about incidents and instantaneously refute government explanations of these events. Within weeks of the app's release, the regime banned the iPhone completely and threatened to prosecute anyone found using one.

ONLINE ATTACKS

Reporters Without Borders has estimated that just over 17 percent of Syrians -- roughly 4 million out of 22 million -- are internet users. Although these individuals have been prolific and innovative in their use of technology, the low level of internet penetration in Syrian society makes it relatively easy for the regime to track their cyber activity.

According to the *New York Times*, this vulnerability has led many activists to establish multiple accounts on social media sites. If an activist is arrested or kidnapped, certain accounts can then be erased without removing the individual's entire online presence. Protestors in Syria and elsewhere in the region have also widely circulated tips on organizing and holding protests, ensuring online anonymity, and circumventing attempts to shut down the internet by using satellite phones and landline internet connections.

In addition, Information Warfare Monitor reports that the opposition has attacked Facebook pages belonging to members of the Syrian Electronic Army (SEA), a pro-Assad cyber force. It has also acquired hacking software created by the SEA and altered it to launch distributed denial of service (DDoS) attacks on pro-regime sites. During such an attack, a website is bombarded with huge amounts of data, preventing legitimate traffic and eventually crashing the site. In February, anti-regime activists also infiltrated the text-message service of the state television station network Addounia.

In another now-famous attack, the opposition group Supreme Council of the Revolution intercepted thousands of emails from the president and first lady's accounts over a period of months. Made public in February, the emails -- which revealed Asma al-Assad's shopping sprees, regime efforts to cultivate sympathetic American journalists, Bashar's disdain for the Syrian people and political reform, as well as his romantic exchanges with an unknown woman -- were a public relations blow to Damascus.

INVOLVEMENT OF HACKER GROUPS AND INTERNET FIRMS

Hacker networks have been instrumental in helping the opposition spread its message. For example, Telecomix -- a loosely organized group of cyber activists -- has used Twitter and Facebook to broadcast dial-up connection information and Skype numbers. This information allows Syrians to leave messages for the group that Telecomix then tweets worldwide. And in August 2011, the group emailed 6,000 Syrian activists with tips for avoiding the government's cyber crackdown. It later created a website dedicated to online security tools for the same purpose. And in October, Telecomix reported that it had released data proving that the regime was using Western technology to track Syrian internet activities.

Another group, the Cairo-based Activists News Association, has helped spread news emanating from Syria by posting video to social media sites and sending it to professional media outlets such as Aljazeera. YouTube's managers have also played a direct role in assisting the opposition. When the gruesome video of thirteen-year-old Hamza al-Khatib -- who was tortured and killed by the regime in May 2011 -- was removed from the site, YouTube responded to popular demands and reposted it. As a YouTube spokesperson later explained, although the site has a policy barring "shocking and disgusting content," it makes exceptions for videos that have "clear educational, documentary, scientific, or artistic value."

Other companies have policies that are more problematic for the opposition. Facebook and Google Plus, for example, require users to provide their legal names as opposed to pseudonyms, making activists more vulnerable to government arrest. Fortunately, the policy is difficult to enforce and is usually only applied when other users -- in this case regime or pro-regime activists -- complain.

POLICY RECOMMENDATIONS

At the April 1 "Friends of Syria" meeting in Istanbul, Secretary of State Hillary Clinton said, "The United States is going beyond humanitarian aid and providing additional assistance, including communications equipment that will help activists organize, evade attacks by the regime, and connect to the outside world." Indeed, State Department internet freedom grants are supporting a number of communications initiatives for use inside repressive countries, including Syria. One particularly innovative technology is the "panic button" for cell phones, which allows activists to quickly erase contact lists if they are arrested. Another initiative aims at overcoming cyber attacks on websites,

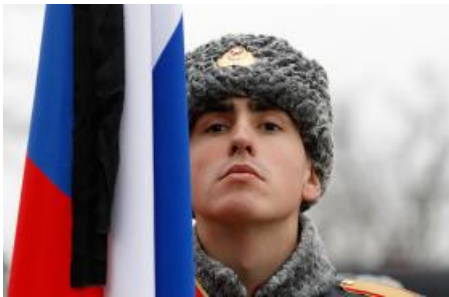
enabling activists to use the sites uninterrupted. The department has also funded Psiphon encryption software to help activists evade internet crackdowns; the system is in use in Syria. Additionally, Washington has provided a \$2 million grant for the development of "internet in a suitcase," a compact system that creates a wireless connection using a laptop or cellphone without a centralized hub, bypassing a country's official network.

Although these steps are useful, more can and should be done. Given the opposition's reliance on satellite phones and the regime's apparent use of satellite signals to target activists, providing evasion tools should be a top U.S. priority. To this end, Washington should encourage satellite phone companies to ensure the privacy of user locations by enhancing encryption and disabling phone tracking features. It should also provide activists with GPS jamming devices to prevent the regime from pinpointing satellite signals. In addition, the United States should encourage social media sites with problematic identification policies to modify their requirements in a way that ensures the anonymity of opposition figures. Finally, Washington should work with Jordan and Turkey to boost cell tower signals along their borders, enabling activists in Syria to take better advantage of those networks.

Of course, these steps will not end the Assad regime in of themselves. In lieu of a more robust U.S. policy, however, supporting the opposition's cyber campaign will at least ensure the continued flow of information about regime atrocities.

Margaret Weiss is a research associate at The Washington Institute. ❖

RECOMMENDED



ARTICLES & TESTIMONY

[The Ukraine Crisis Isn't Over: Russia Has Lied About Troop Withdrawals Before](#)

Feb 16, 2022

◆
Anna Borshchevskaya

[\(/policy-analysis/ukraine-crisis-isnt-over-russia-has-lied-about-troop-withdrawals\)](#)



ARTICLES & TESTIMONY

[As China Thrives in the Post-9/11 Middle East, the US Must Counter](#)

Feb 16, 2022

◆
Jay Solomon

(/policy-analysis/china-thrives-post-911-middle-east-us-must-counter)



BRIEF ANALYSIS

Unpacking the UAE F-35 Negotiations

Feb 15, 2022

◆
Grant Rumley

(/policy-analysis/unpacking-uae-f-35-negotiations)

TOPICS

Arab & Islamic Politics (/policy-analysis/arab-islamic-politics)

Democracy & Reform (/policy-analysis/democracy-reform)

REGIONS & COUNTRIES

Syria (/policy-analysis/syria)