Assad's Secretive Cyber Force

Apr 12, 2012

Brief Analysis

Cyber bullets are bullets nonetheless.

For the past year, the Assad regime's brutal repression of the opposition has received extensive coverage in the mainstream media. Less well reported, however, has been the regime's equally comprehensive crackdown on its internet opponents. Syria has a long and distinguished record of cyber repression, earning a Reporters Without Borders "Enemy of the Internet" sobriquet three years running. And since the revolution started, with the technological assistance of Iran and the Lebanese Shiite militia Hizballah, the operational tempo of the pro-regime Syrian Electronic Army (SEA) has increased dramatically. With no end in sight to the fighting on the ground, the cyber battles promise to escalate.

REGIME TACTICS

One of the regime's techniques is to slow internet transmission speeds and periodically shut down the internet completely before a major demonstration in order to hamper the ability of anti-regime protestors to organize. Opposition activists become unable to upload photos or videos or to provide live coverage of events on the ground. It has been reported that the internet and mobile phones were shut down during the regime's recent assault in Baba Amr. Meanwhile, internet intelligence company Renesys reports that on June 3, 2011, two-thirds of Syrian networks were shut down, presumably in an attempt to prevent opposition activists from organizing following the regime's brutal murder of thirteen-year-old Hamza al-Khatib. Syria's internet depends on one major internet service provider, or ISP, the state-owned Syrian Telecom Establishment, making a shutdown relatively easy. (In contrast, internet traffic in Egypt passes through multiple ISPs, which is why the attempted shutdown during the early days of the Tahrir Square demonstrations was unsuccessful.)

The Syrian regime has also used other cyber techniques to undermine the opposition. During the early days of the uprising, opposition activists on Twitter used the hashtag "#Syria" to spread information about the demonstrations and the violent government crackdown that ensued. Within a couple of months, however, #Syria became bombarded by pro-regime messages, threats, and verbal attacks. Syrian intelligence agents were thought to be behind the spamming. In addition, spam bots -- accounts set up to send spam -- were created to barrage #Syria at fixed intervals with topics ranging from photography to pro-regime news and threats against opposition tweeters.

Pro-regime elements also used a cyber technique referred to as "man-in-the-middle," whereby an attacker controls a victim's communications by intercepting incoming and outgoing messages, unbeknownst to the victim. In May 2011, Information Warfare Monitor (IWM) reported that Syrians who logged onto the secure HTTPS version of Facebook fell victim to man-in-the-middle attacks by a perpetrator -- thought to be the Syrian Telecom Ministry -- who substituted Facebook's security certificate with a fake one. The attacker was thus able to access their Facebook accounts and direct all communications.

THE MYSTERIOUS SEA

Although the SEA is the regime's prime weapon in the cyber crackdown, the extent of the group's ties to the regime is uncertain. IWM has done in-depth work on the SEA, providing much information about its activities. As described by IWM, the domain name for the SEA's website was registered by the Syrian Computer Society, which Bashar al-Assad headed in the 1990s before becoming president. Assad affirmed his continued support of the SEA in a June 2011 speech: "Young people...have proven themselves to be an active power. There is the electronic army which has been a real army in virtual reality."

According to IWM, the SEA's focus is two-pronged: promoting a pro-Assad narrative about events inside Syria and opposing anti-regime activists. The SEA defaces what it perceives as hostile news and opposition sites, and has barraged Facebook pages belonging to no less than the European Union, President Obama, the State Department, Oprah Winfrey, Human Rights Watch, and Aljazeera with pro-Assad comments. (The SEA explained that Winfrey's page was targeted to influence U.S. public opinion.) The SEA has also targeted Israeli websites, many of which contain no political content.

IWM also describes how one of the SEA's first Facebook pages (the group has created numerous pages, only to have them removed by Facebook) offered supporters software to launch distributed denial of service (DDoS) attacks against "enemy" websites. In such an attack, the offending website is bombarded with huge amounts of data, preventing legitimate traffic from accessing the site and eventually causing it to crash. Websites attacked in this way include a Syrian news forum, a UK town council, a number of Italian online stores, an Italian tourism guide, and a Syrian singer living in Egypt who expressed support for the revolution. A Facebook page called the Syrian Hackers School, which appears to have been removed, provided pro-regime activists with basic software that could easily be tailored to their own purposes.

In addition, IWM points out that the more than 100 websites defaced by the SEA in June 2011 resolve to just 15 IP addresses: by exploiting one vulnerability on a shared server, the hackers were able to breach the websites en masse. Moreover, because many of the sites targeted by the SEA contained no political or Syria-related content whatsoever, they were likely attacked simply because they were easy targets. Furthermore, IWM notes that the SEA released information about hacked Israeli sites gradually, likely in an effort to create excitement among its fans and avoid having to work to find new vulnerable sites. Lastly, the DoS software posted to Facebook by the SEA was very basic and allowed opposition activists to easily convert it for their own purposes.

EFFECTIVENESS OF CYBER CRACKDOWN

The number of arrests, tortures, or deaths of opposition activists that have occurred as a result of the regime's cyber activities is difficult to determine. But the crackdown is more sophisticated than similar efforts in other countries, such as Egypt. The SEA and other pro-Assad activists are familiar with the social media sites and tools regularly employed by the opposition and have effectively targeted opposition members. According to the Committee to Protect Journalists, eight journalists in Syria have been killed so far in 2011 and 2012. Others have been arrested and threatened or tortured and then released; still others have gone missing. It is widely believed that American journalist Marie Colvin was killed in Homs thanks to Iranian software that pinpointed her satellite phone transmissions.

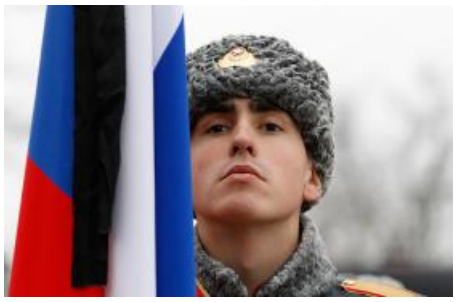
CONCLUSION

The cyber crackdown remains an underreported aspect of the violence in Syria, but it is an issue worthy of more attention. Not only do these regime activities hurt the opposition, they limit visibility into what is really happening on the ground and undermine efforts to build a stronger international consensus on Syria.

Going forward, the United States should do more to prevent American products from reaching the Syrian regime. For example, it is known that the regime used California-based Blue Coat Technology's internet filtering technology to prevent access to opposition websites. At a minimum, the administration should take a cue from the European Parliament, which recently passed a resolution placing controls on the export of dual-use products, including those that can be used to violate human rights. Representative Chris Smith (R-NJ) has already sponsored a bill that would regulate the export of this technology. Additionally Washington should follow the lead of the EU and the UK, and impose sanctions on Syrians and Iranians who are intimately involved in the cyber war. Absent direct U.S. action on the ground or on the web, these steps will put cyber warriors and the companies that arm them on notice that aiding Assad's crackdown on the internet will be treated with the same gravity as selling arms to the regime.

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)