Disinformation flies in Syria's growing cyber war

Peter Apps, Political Risk Correspondent, Reuters

(Reuters) - On Sunday, it was a hijacked Reuters twitter feed trying to create the impression of a rebel collapse in Aleppo. On Monday, it was another account purporting to be a Russian diplomat announcing the death in Damascus of Syrian President Bashar al-Assad.

As the situation on the ground becomes ever more bloody, both sides in Syria [1] are also waging what seems to be an intensifying conflict in cyberspace, often attempting to use misinformation and rumor to tilt the war in reality.

On Friday, Reuters was forced to temporarily shut down its system for posting blogs on www.Reuters.com after the appearance of a series of unauthorized, and inaccurate, reports citing opposition military reverses in Syria.

On Sunday, the company took similar action to suspend the @ReutersTech twitter account after it appeared to have been seized, renamed and used to send a series of false tweets apparently designed to undermine the rebel Free Syrian Army. Both incidents remain under investigation.

The attacks were not the first time a major media or other organization had been targeted apparently by supporters of Assad. Some - including the defacement of a Harvard University website last year to post a picture of Assad in military uniform -- have been claimed by the "Syrian Electronic Army".

But Assad's government too have had their own embarrassments in cyberspace. Hacker group Anonymous claimed credit for stealing thousands of internal Syrian government e-mails including personal communications between Assad and his wife. The entire tranche was later published online by Wikileaks.

"It's not surprising that Syria has attempted to develop a cyber warfare capability. It's in line with their chemical and biological warfare program and their aspirations as a regional power," said John Bassett, former senior official at British signals intelligence agency GCHQ and now a senior fellow at London's Royal United Services Institute.

"But the regime's technical capabilities look pretty basic, and the opposition hacking of the personal emails of Assad and his wife earlier this year show the regime's cyber defenses have serious weaknesses."

The opposition too, many suspect, have been doing what they can do to spread rumors about their opponents. On Monday afternoon, a twitter account purporting to be that of a senior Russian official said Assad had been killed in Damascus, prompting a flurry of speculation and telephone calls by agencies such as Reuters before the Russian Foreign Ministry confirmed the news was fake.

"Cyber attacks are the new reality of modern warfare," said Hayat Alvi, lecturer in Middle Eastern studies at the US Naval War College. "We can expect more... from all directions. In war, the greatest casualty is the truth. Each side will try to manipulate information to make their own side look like it is gaining while the other is losing."

With Assad's opponents desperate to attract defectors - such as Prime Minister Riyad Hijab who fled on Monday - and the government keen to avoid further foreign support for rebels already backed by Turkey, Saudi Arabia [2] and Qatar, the stakes are undoubtedly high. The Alawite-dominated government needs to demonstrate it can survive, while the rebels must present themselves as a coherent government in waiting and keep down talk of potential Al Qaeda infiltration.

In recent months, the "Syrian Electronic Army" (SEA) in particular looks to have adopted a strategy to target media outlets to spread disinformation helpful to the Damascus government or harmful to its foes.

In April, Saudi-based broadcaster Al Arabiya briefly lost control of one of its twitter accounts, which was then used to spread a string of stories suggesting a political crisis in Qatar. Tweets included claims that the Qatari prime minister had been sacked, his daughter arrested in London and that a coup orchestrated by the army chief was underway.

In July, Al Jazeera suffered a similar attack, with one of its twitter feeds used to send a series of pro-Assad messages including accusing the Qatar-based channel of fabricating evidence of civilian casualties in Syria.

Such exchanges, experts say, are increasingly becoming part of any conflict. During the 2008 Georgia war, Russian and Georgian hackers - either state-backed or operating independently - each mounted a range of attacks on each other's official websites.

STRICTLY LIMITED EFFECT

In reality, however, there seems little sign such incidents made a significant difference either on the ground in Syria or to the wider geopolitical picture.

The assorted Reuters blog postings on Friday published through a now closed vulnerability in the WordPress software used to manage the site, bore a superficially convincing resemblance to other genuine entries.

But the written style - as well as some of the grammar and style - were notably different to real Reuters reports, which continued to be posted without difficulty and disseminated to Reuters media, financial and other clients.

While some of the false blog posts were at least briefly shared via social media by readers who believed they were honest reports from Aleppo, it is far from clear whether anyone in the embattled city itself ever saw them.

A Reuters reporter on the ground quickly confirmed the reported rebel collapse in several key named suburbs appeared to be false, and postings themselves were quickly removed - although occasional screenshots remain on the Internet.

Nor does it appear that anyone was particularly convinced by the Sunday flurry of tweets from the captured @ReutersTech twitter account, hastily renamed @ReutersME in an apparent attempt to present itself as a Middle East-based feed.

Again, there was a series of messages detailing a supposed rebel defeat in Aleppo, where heavy fighting continued on Monday with opposition forces still in control of much of the city. The account said rebel forces were out of ammunition and in "a sad situation" while the Syrian army boasted the fight was like "shooting fish in a barrel".

It then went on to claim that the White House had confirmed it was arming Al Qaeda militants within Syria as part of its support for the fight against Assad. In the final handful of tweets before access was cut, the user said Washington had always funded Al Qaeda even in the decade since the September 11, 2001 attacks and then accused Reuters itself of being in the "iron grip" of the Rothschild banking dynasty.

"The problem with these attacks is that they are always quickly noticed and even if they are successful in grabbing headlines and fooling people for a short period of time, they have very limited effect," said Tal Be'ery, web security research team leader at IT security firm Imperva.

"They are not that technically sophisticated, and my assessment is that they would most likely be from amateurs rather than the regime itself. That tells us that Assad still has some support amongst people able to do this both inside and outside the country, but that is about it."

TRACKING OPPOSITION REAL PRIORITY

Monday's twitter-fuelled rumors of Assad's demise, knocked down within minutes, could conceivably have shaken some of his supporters but are unlikely to have lasted long.

The true priority for the real computer experts of both the government and opposition, most believe, will be the cat and mouse game between government surveillance systems and the opposition networks they are trying to track.

For Assad's opponents, evading government detection has long been a matter of life and death. Autocratic governments around the world, specialists say, have put considerable effort into tightening their Internet surveillance on potential dissidents since last year's "Arab spring" ousted rulers in Tunisia [3], Egypt, Libya and Yemen.

"The primary target of SEA is certainly their own citizens," said Alexander Klimburg, cyber security expert and fellow at the Austrian Institute for International Affairs.

"It is hard to estimate how successful they are trading the protesters, but it seems they are much better at it than the former Tunisian or Egyptian secret police, and seemed just as good as the Iranian security forces in this regard."

Some believe Assad may be getting technical support from his long-term allies in Tehran, who successfully crushed their own post-election protests that were in part organized over the Internet. China [4] and Russia too are has amongst the world leaders in managing online political activism and dissent, with the latter at least also seen likely helping out in Syria.

"We know that they have been having a lot of success with fake online Facebook profiles, ssl certificates and other methods to break into the opposition," said Imperva's Be'ery. "We know that Russia [5] was very involved in setting up the Syrian signals intelligence system and it is possible they still have access to Russian expertise and even experts."

The opposition too may also have foreign support. Some suspect the hand of a western signals intelligence agency in the Assad e-mail leak, while the U.S. State Department says it has given them technical advice and equipment to help stay one step ahead of government monitoring.

But Syria's Assad, experts say, has long taken an interest in the Internet and its potential uses. Before taking the presidency, he was president of the "Syrian Computer Society", a group now widely believed to have been something of a precursor to the "Syrian Electronic Army". "It is probably not officially integrated into the security services," Klimburg said. "As such, it performs similar tasks to the "Shabbiha" militias - intimidation of local anti-government forces and direct operations that the Assad regime thinks are best not associated with it."

(Reporting By Jon Hemming)

Links:
[1] http://www.reuters.com/places/syria
[2] http://www.reuters.com/places/saudi-arabia
[3] http://www.reuters.com/places/tunisia
[4] http://www.reuters.com/places/china
[5] http://www.reuters.com/places/russia