Syria's online troops wage counter-revolutionary cyber war

June 9 2013, by Thomas Watkins And Serene Assir

Sometimes, attacks in Syria's bloody civil war start not with a bullet or a bomb blast, but with an innocuous-looking email. Hackers from the Syrian Electronic Army are snatching sensitive information in the name of spreading counter-revolutionary propaganda and hitting back at news outlets that they say slant reporting on the conflict.

Sometimes, attacks in Syria's bloody civil war start not with a bullet or a bomb blast, but with an innocuous-looking email. A message pings into an inbox, apparently from a friend or colleague. The recipient clicks a

link, and suddenly hackers are one step closer to snatching sensitive information - including passwords to a company's social media sites.

It's an old trick, but one effectively deployed time and again by the Syrian Electronic Army in recent months. The supporters of Syrian President Bashar al-Assad's regime have duped numerous Western media outlets into handing over the electronic keys to their Facebook, Twitter and other accounts, leaving many organisations red-faced and scrambling to regain control of their social media streams.

The group's aim: to spread counter-revolutionary propaganda and hit back at news outlets it says slant their reporting of the conflict that began in March 2011 and has so far claimed an estimated 94,000 lives and displaced millions more.

"We have literally hacked the planet when it comes to news organisations," a spokesman for the group told AFP in an email exchange. "There only remains a few untouched social media targets that we fully intend to pay a visit to soon."

All sides in Syria's war have used social media to try to drum up support and document atrocities being inflicted on an almost daily basis. Opposition groups were quick to build Facebook pages and post videos depicting gruesome acts by regime forces, but the Syrian Electronic Army - or SEA, as it calls itself - has pushed back in the high-stakes battle to shape public opinion in the West.

The most notorious hack was of The Associated Press's Twitter stream, resulting in a false tweet saying President Barack Obama had been injured after two blasts at the White House. The message saw the Dow Jones Industrial Average suffer a "flash crash" before traders realised the tweet was false.

Other victims of SEA hacks include the AFP photo department's Twitter account, the BBC, Al Jazeera, the Financial Times and the Guardian. Even US satirical news site the Onion was hijacked, and on Wednesday the SEA said it had hacked into a Turkish government site.

Compromised accounts often link to images or reports of abuses apparently carried out by opposition forces. The SEA was quick to try to capitalise on gruesome videos filmed this year apparently showing opposition fighters executing regime troops. Another video purportedly shows a rebel cutting out a dead soldier's heart and biting into it.

The SEA spokesman, who identified himself only by his online name, Th3Pr0, said the group had thousands of members, mostly young people, who live in Syria and operate as volunteers.

"We are completely unfunded and many of us are facing hardship due to western sanctions on the country that target its people," he said.

Opposition activists dismiss such claims, saying the SEA is a de-facto wing of the Assad government, funded by an influential cousin of the president, the wealthy businessman Rami Makhlouf.

Tareq Al-Jazairi, an activist who lives in Istanbul and is now affiliated with the opposition Syrian National Council, said he knows several people who work for the SEA and are paid between $500 and $1,000 a month. The hackers are based in Syria and Dubai, he said, and receive technical assistance from experts in Russia, Syria's main international supporter.

But despite the SEA's technical savvy and ability to repeatedly crack social media accounts, many of its members "are just trolls whose work is limited to going onto international news websites and leaving comments on articles that corroborate the regime's narrative that there is

no revolt in Syria, and that the army is fighting a war on foreign terrorists," said Abu Ghazi, an opposition activist from Hama in central Syria.

Abu Ghazi said the opposition movement had drawn some negative attention in recent weeks after the rebel abuse videos were posted online. He condemned these, but said they were an inevitable outcome for a country whose population has suffered daily since the start of the popular uprising against Assad, which quickly became an armed revolt when the regime cracked down.

"Rebels are not angels. When your neighbour hits you once or twice, you may not respond. But the third time, you'll hit back for sure," he said. "Children are being killed, peaceful activists are being killed. There is a lot of rage. I don't agree with it but what do you expect?"

While news organisations have remained tight-lipped about how their accounts were hacked, they are thought to have fallen for "spear phishing" attacks, where an email coaxes a recipient into clicking on a malicious link and entering vital security information. The Onion described falling victim to such tactics when it was hacked last month.

Twitter has responded by saying it is beefing up security measures and implementing an optional new login verification system requiring users to go through an extra hoop to access accounts.

What the SEA's activities show is that "cyberspace is an important part of every contemporary conflict and the severe effects cyber-attacks can have globally," said Jarno Limnell, director of cyber security for Finnish network security firm Stonesoft.

"The conclusion to be drawn from the effects of Syria's cyber conflict is that the use of cyberspace needs to be seen as an integral part of any

contemporary and future conflict. ... Its effects are and will be felt in the physical world too," he added.

© 2013 AFP