The Vicious Cyber-War Against Venezuela

By Manuel E. Yepe
Global Research, July 04, 2017
CounterPunch 30 June 2017

Region: Latin America & Caribbean, USA
Theme: Intelligence, Media Disinformation,
US NATO War Agenda
In-depth Report: FAKE INTELLIGENCE

Havana. The psychological warfare being waged by the oligarchic opposition in Venezuela –following the strategic and tactical objectives of US imperialism– has strong support in a well-organized Twitter operation that promotes protests from the Miami-based DolarToday platform. This is described in a research article published by the well-known specialist **Erin Gallagher***.*

DolarToday is a US website based in Miami that, according to Wikipedia, "is more known for being an exchange rate reference to the Venezuelan bolivar" and "monitoring the Venezuelan economy."

Currently, with no other reliable source other than the black market exchange rates, these rates are used by *Reuters*, *CNBC*, and several media news agencies and networks.

Source: Venezuela Analysis

The Economist states in its defense that the rates calculated by *DolarToday* are "erratic", but that they are "more realistic than the three official rates" released by the Venezuelan government. It maintains that it is not true that the rates published by *DolarToday* are manipulated in order to undercut the Venezuelan government.

The *DolarToday* website has been denounced by the Venezuelan State for setting a parallel dollar artificial price marker (black market). It has also been the target of a lawsuit by the Central Bank of Venezuela for falsifying the country's exchange rates.

In 2013, **President Maduro** accused the website of "fueling an economic war against his government, and manipulating the exchange rate."

> "DolarToday is also promoting opposition protests in Venezuela. Its tweets are being boosted by automated accounts that exhibit repetitive, bot-like

characteristics and are using a social media management tool called IFTTT (If This Then That) to automate their tweets", says Erin Gallagher.

"What immediately caught my attention in the #TeamHDP hashtag data were the shared networks between the influencers (real persons of high credibility)," explained the specialist.

Trolls and bots carry out coordinated attacks to create false trends, congest or disrupt networks, and disseminate misinformation. Sometimes they succeed having a respected media –by neglect or mistake– disseminate their fake information and misleading headlines.

"Bots" are automated systems or programs –that can be run on home computers or on sophisticated servers—which use non-existent Twitter accounts to repeat a certain phrase hundreds or thousands of times. Thus they can turn those phrases into "trends"; that is to make them appear among the 10 or 20 topics that Twitter considers the subjects most discussed in recent hours.

Bot experts disguise themselves as "digital marketing companies", create dozens or hundreds of fake Twitter accounts, and then use "bots" so that these accounts simultaneously tweet certain content, including headlines from news sites.

Because many journalists in the print media, radio and television use Twitter trends to determine what topics to deal with in their media, whoever dominates Twitter trends can get to determine the topics most talked about in the country's media.

Gallagher says it is relatively easy to discover the use of these systems: when you enter a tag on Twitter and then click "Most Recent", you will notice that there are hundreds or thousands of accounts tweeting exactly the same phrase.

This is not the first time robotic cyber actions have been observed in Venezuelan networks. Mexican researchers from the platform "LoQueSigue" used, in 2014, bots with the hashtag #PrayForVenezuela, which denounced "the violence, the repression and the supposed "censorship" of the protests in Venezuela," which became a worldwide trend.

In addition, NoBotsPolitico of Spain documented fake accounts that supported the protests in Venezuela until June 2014, then remained silent for eight months, but went back to tweeting propaganda against Podemos in hashtags related to the 2015 elections in Spain.

Bloomberg published a feature on an investigation of March 2016 titled "How to Hack an Election" about the Colombian hacker **Andrés Sepulveda**, who worked with a team of hackers to manipulate information about the elections in Latin America. Sepulveda is currently serving 10 years in prison for crimes such as abusive access to computer networks, violation of personal data, espionage, and the use of malicious software during the 2014 election in Colombia.

It is not difficult to guess who controls the automated accounts that support #TeamHDP. The counterrevolution will someday have to answer for so much crime against the Venezuelan people.

Manuel E. Yepe is a lawyer, economist and journalist. He is a professor at the Higher Institute of International Relations in Havana.

Featured image from Twitter

The original source of this article is [CounterPunch](#)
Copyright © [Manuel E. Yepe](#), [CounterPunch](#), 2017

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: **[Manuel E. Yepe](#)**