# Hired guns of disinformation proliferate online, report finds

August 26 2020, by Gopal Ratnam, Cq-Roll Call

Credit: CC0 Public Domain

A variety of online tools and companies offering disinformation campaigns as a service are flourishing online, making it easier for state-sponsored and other hackers to mount such campaigns with little effort,

the technology firm Cisco said in a report released Wednesday.

Calling themselves digital marketing companies, the purveyors of disinformation have played a role in trying to influence elections from Canada's British Columbia province to suppressing dissent in the United Arab Emirates, according to the report—"The Building Blocks of Disinformation," produced by Cisco's security research arm called Talos.

The report recounted several previously reported incidents involving private companies offering disinformation services, including UReputation, a Tunisian company that attempted to influence the country's 2019 presidential election. Facebook later took down the company's presence on its platform.

The Cisco report also noted the role of AggregateIQ's role in swaying the 2016 Brexit vote in the U.K., the Israeli company Archimedes that targeted the 2019 Nigerian elections, and Newave, a company that helped the UAE spread anti-Muslim Brotherhood messages.

"In rare cases, there are known direct links between digital marketing companies and politicians or state actors," Cisco said in its report. "Most often though, while companies' messaging aligns with the political goals of a government or party, direct links between these marketing firms and state governments or individuals are often difficult to find."

The involvement of private disinformation companies obscures the role of state-sponsored hackers and politicians who may be lurking behind the commercial entities, Nick Biasini, one of the authors of the Cisco report, said in an interview with CQ Roll Call.

"That's one of the reasons why we're really starting to see this grow," Biasini said, referring to the role of private companies. It allows nation-states and their intelligence apparatus to hide, "so they can maintain a

little bit of isolation from the actual activity, making it difficult to identify groups behind it."

Private security companies and U.S. government officials have said that after mounting a successful disinformation and influence campaign during the 2016 presidential election—as recounted by Special Counsel Robert S. Mueller III and the Senate Intelligence Committee—Russia and other countries are adapting and learning the lessons from those efforts.

In a recent warning, William Evanina, director of the National Counterintelligence and Security Center. said Russia was still actively interfering in the 2020 election, and "some Kremlin-linked actors are also seeking to boost President (Donald) Trump's candidacy on social media and Russian television." Evanina said China was rooting for Democratic presidential nominee, former Vice President Joe Biden.

Companies offering disinformation tools have become so sophisticated they're able to track the spread of their content, assess their impact and refine their strategies, Cisco found.

"Mature agencies will often gather insights to tune their dissemination efforts," the report said. "For instance, by collecting likes, friends, regions and even response times to posted content, agencies can better assess their targets and deliver custom content."

A software called NationBuilder is one such tool that "targets and manages communications with expectant voters," Cisco said.

To make content look more believable, some companies are creating fake personas of journalists, with false LinkedIn profiles and web histories. They'll use the profile of a fake journalist to then push content that might be picked up by genuine news sites, Cisco said.

Social media companies including Twitter and Facebook have mounted large-scale efforts to crack down on foreign sources of disinformation, including imposing tough requirements such as having a legitimate phone number and a mobile SIM card to create accounts.

But some for-hire disinformation companies seem to be offering legitimate SIM cards as a service, Cisco said. "In a recent takedown of a suspected Russian bot farm in Ukraine, photos show a plethora of SIM-related hardware," Cisco said.

Drawing on open-source information, Cisco estimated the photos show about $10,000 in hardware costs alone just from the devices identified in the photos, the report said.

Despite the efforts of social media sites to counter disinformation, their platforms continue to present ripe opportunities for anyone looking to launch an effort, Cisco said, citing the example of a group called March to Replace Biden that it found on Facebook.

"The group was also organizing a public demonstration and encouraging users to share disparaging memes and news articles, many of which were being tagged by Facebook as potential misinformation," Cisco said. "We identified this group within minutes of starting our search, highlighting the ease at which a disinformation actor could do the same."