GlobalResearch
Center for Research on Globalization

Interfering in Elections? Israel Uses High-technology to Influence Results

By Philip Giraldi
Global Research, March 14, 2023

Region: Middle East & North Africa, USA
Theme: Intelligence

***

*A week ago an interesting story surfaced briefly in the news about how the developing Republican presidential candidate bids by **Nikki Haley** and others had been attacked over the past eleven months by possibly as many as hundreds of thousands of false automated personas, referred to in the trade as "bots," on Twitter and other internet based social media. Interestingly, the activity was discovered and shared with Associated Press by an Israeli internet security company called Cyabra, which also claimed that the "bots" generation seem to have originated in three separate networks of false Twitter accounts. The accounts appear to have been created in the United States and it is believed that Artificial Intelligence (AI) applications are increasingly being used to create completely lifelike fake personas, extremely difficult for security filters and censors to detect.*

The article claimed that those thousands of electronically generated non-personas had been programmed to disparage Haley and Ron DeSantis and others, often using "fake news" or alleged leaks of embarrassing personal information, while also praising the virtues of Donald Trump. The apparent intention was to build popular support for Trump by exploiting the social media sites' algorithms to reach a large audience at the expense of the other possible GOP candidates. There are also concerns among some Republicans that the effort to give life to the Trump campaign by materially impacting on online political discussion might possibly be orchestrated and paid for by major outside interests that could actually be either foreign or criminal. Of course, as the operation has been exposed by an Israeli company, the possibility exists that the story is itself at least in part a false flag to plausibly deny any involvement by the Jewish state if that were to be demonstrable.

The story is nevertheless of interest, to be sure, based on its own merits, but it surfaced at the same time as a much bigger tale of international subversion, also linked to Israel, that was in addition linked to elections and regime change. While the United States must certainly be considered the world leader in compelling all nations to conform to the political and moral values that it insists be adhered to, Israel has stealthily become the nation that covertly uses its prowess in cyberwar and technology, particularly via the internet, to

penetrate and disrupt the activities of friend and foe alike. One recalls the unleashing of the computer virus *Stuxnet* against Iran prior to 2010 and the more recent placement of cellphone surveillance listening devices near the White House and other federal buildings in Washington.

Israel's prowess apparently includes the ability to influence more foreign elections than anyone else. Curiously enough, a leading Israeli group, referred to by its founder Tal Hanan as *Team Jorge*, has particular expertise in hacking and spreading disinformation using thousands of false identities and profiles, very much like the story of the Republican Party hijinks. The organization has been exposed in long articles appearing in a number of European publications which had been party to an undercover investigation of its activities, but oddly enough no US media picked it up and ran with it even though there were clear similarities to what had been taking place with the Republicans.

The investigation determined that *Team Jorge* has worked for a number of apparently mostly private clients, including political organizations, who pay generously for the special services it provides. Its activities, now exposed, add to a growing body of evidence that there exist shadowy private firms across the world that are exploiting invasive hacking tools and the power of online social media platforms to manipulate public opinion and even to sway voters in elections.

Hanan, a former Israeli special forces operative, claims his company, which he regards as a legitimate corporate contractor, has been operating under the radar for two decades out of an office near Tel Aviv. *Team Jorge* also has six overseas affiliates which have been providing services both to political groups and businesses. Hanan is not shy about his successes. He boasted that "We are now involved in one election in Africa… We have a team in Greece and a team in [the] Emirates… [We have completed] 33 presidential-level campaigns, 27 of which were successful… Most of the campaigns – two-thirds – were in Africa" but Hanan also claimed "work" in Latin America, the US and Europe. He said at one point that he was involved in two "major projects" in the US but denied interfering directly in US politics. No matter where it operates, *Team Jorge*'s business is profitable. Tal Hanan told one potential client that he would accept payments in a variety of currencies. Interference in an election would cost between 6 and 15 million Euros.

Hanan was exposed by a team of three undercover reporters who posed as prospective clients in the latter half of 2022. The story appeared in the British *Guardian* on February 15th, and was also picked up by the *Daily Mail*. It also appeared in the French and German media. The lengthy articles revealed the content of secretly recorded meetings in which Tal Hanan described in detail how his services, which some might describe as "black ops", were available to intelligence agencies, political campaigns and private companies that wanted to secretly manipulate public opinion. To demonstrate the power of his hacking tools, Hanan hacked into the Gmail inbox and Telegram account of several political operatives in Kenya a few days before a presidential election there. Telegram is marketed as a top-level security communications system.

Team Jorge's most sought-after service is a sophisticated software package, Advanced Impact Media Solutions, or AIMS. Per Hanan, it can create and control thousands of fake social media profiles on Twitter, LinkedIn, Facebook, Telegram, Gmail, Instagram and YouTube. Some of the AIMS avatars even have backup credit accounts to establish their bona fides, using bank cards, bitcoin wallets and Airbnb account numbers.

Team Jorge also has had what might be described as a business relationship with the now notorious British consulting firm Cambridge Analytica. Cambridge Analyticais now out of business but it participated in a Nigerian election with *Team Jorge*. It is best known for having stolen the personal data belonging to 87 million Facebook users. It then allegedly used the data to provide analytical assistance to the 2016 presidential campaigns of both Ted Cruz and Donald Trump and some believe the service provided may have influenced the result of the subsequent US presidential election.

Israel has long been the home of start-up cyberwarfare companies due to its government's intense focus on developing the tools and skills to attack targets like Iran's alleged nuclear program. It now might also face increased international pressure to rein in the former employees who were schooled in its military technology sector. Most of Hanan's employees are, in fact, formerly with the government. The *Team Jorge* revelations come on top of accounts of how the powerful Israeli-made Pegasus spyware had been developed and sold by the cyber intelligence company NSO Group Technologies to various governments and other users. NSO reportedly spent lavishly in a bid to convince the US government to buy its advanced spyware. It even paid a consulting fee of $100,000 to Michael Flynn before he became President Donald Trump's National Security Adviser. The company's software was reportedly used internationally by governments to spy on political dissidents and, in particular, on journalists. Some others targeted by Pegasus included human rights activists and religious leaders, as well as politicians including French President Emmanuel Macron.

There has been a sharp reaction within the social media and internet communications communities since the revelations about *Team Jorge*. Meta, the owner of *Facebook*, immediately took steps to identify and take down possible AIMS-linked identities on its platform. It is presumed that other companies are doing the same. *Team Jorge*claims to have had great success in its disinformation efforts relating to elections, but until someone does an essentially forensic analysis of what was done and how, no one will ever know the truth. Presumably the company has already destroyed any and all particularly embarrassing documents. What is known, however, is that the toxic mix of Israel's advanced cyberwar programs combined with the private enterprise of those cyberwarriors who leave government and apply their skills is something that has to be addressed. It has to be regulated or controlled in some fashion or the credibility of the social media and communications systems that current bind much of the world together will be suspect, which is precisely what some observers of what has just been revealed regarding the Republican Party nomination process should be thinking.

*

Note to readers: Please click the share buttons above. Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

This article was originally published on The Unz Review.

***Philip M. Giraldi, Ph.D.**, is Executive Director of the Council for the National Interest, a 501(c)3 tax deductible educational foundation (Federal ID Number #52-1739023) that seeks a more interests-based U.S. foreign policy in the Middle East. Website is councilforthenationalinterest.org, address is P.O. Box 2157, Purcellville VA 20134 and its email is inform@cnionline.org.*

He is a regular contributor to Global Research.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Philip Giraldi**