BESA PERSPECTIVES
THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES

Russian Hacking in the US and the Gulf

by Dr. James M. Dorsey

BESA Center Perspectives Paper No. 901, July 23, 2018

EXECUTIVE SUMMARY: The covert cyberwar that helped spark the 13-month-old Gulf crisis, which pits a Saudi-United Arab Emirates-led alliance against Qatar, may have just gotten murkier with the indictment of 12 Russian intelligence agents by US Special Counsel Robert Mueller.

US Special Counsel Robert Mueller's indictment of 12 Russian intelligence agents provided detail on website DCLeaks, which was allegedly registered by Russian intelligence officers. The website initially distributed illicitly obtained documents associated with people connected to the Republican Party and later hacked emails from individuals affiliated with the election campaign of Democratic presidential candidate Hillary Clinton.

"Starting in or around June 2016 and continuing through the 2016 U.S. presidential election, the Conspirators used DCLeaks to release emails stolen from individuals affiliated with the Clinton Campaign," the indictment reads.

The indictment focuses exclusively on hacking related to the US election that in 2017 brought Donald J. Trump to office. It makes no mention of hacking related to the 13-month-old Gulf crisis that pits a UAE-Saudi-led alliance against Qatar.

Yet the indictment's repeated references to DCLeaks raises the question whether there might also be a Russian link to the hacking last year of the email of Yousef al-Otaiba, the UAE's ambassador to the US.

Otaiba's revealing and potentially damaging emails, which seemed to help Qatar in its public diplomacy campaign, were distributed to major media and analysts, including this writer, by an entity that identified itself as Global Leaks.

Questions about a potential link between Global Leaks, DCLeaks, and Russia stem not only from Global Leak's use of a Russian provider that offers free email service but also by the group's own reference to DCLeaks. The group's initial email had "DCLeaks" in its subject line.

It remains unclear whether the use of a Russian provider was coincidental and whether the reference to DCLeaks was meant to mislead or create a false impression.

Global Leaks initially identified itself in an email as "a new group which is bringing to limelight human right violations, terror funding, illegal lobbying in US/UK to limelight of people to help make USA and UK great again and bring justice to rich sponsors of crime and terror."

When pressed about its identity, the group said that "we believe that (the) Gulf in general has been crippling the American policy by involving us in their regional objectives. Lately it's been (the) UAE who has bought America and traditionally it was their bigger neighbor (Saudi Arabia). If we had to hurt UAE, we have so much of documents given by source that it will not only hurt their image and economy but also legally and will for sure result in UN sanctions at the least. But that is not our goal.

"Our goal is plain and simple, back off in playing with American interests and law, don't manipulate our system, don't use money as a tool to hurt our foreign policy…. It may be a coincidence that most things [we are leaking] do relate to UAE but in times to come if they continue and not stop these acts, we will release all the documents which may hurt all the countries including Bahrain and Qatar," the group said.

Global Leaks' allegation that the UAE was seeking to suck the US into Gulf affairs predated reports that Mueller, the special counsel, was – in addition to investigating the Russia angle – was also looking into whether George Nader, a highly paid Lebanese-American advisor to UAE Crown Prince Muhammad bin Zayed, had funneled funds to the Trump campaign.

Mueller is further investigating a meeting in the Seychelles between Blackwater founder Erik Prince and Kirill Dmitriev, CEO of the Russian Direct Investment Fund, the country's sovereign wealth fund, which was brokered by the UAE. Prince and Dmitriev have denied that the meeting had anything to do with Donald Trump.

Trump has not publicly addressed reports that his election campaign may have received Gulf funding. But at a news conference with Russian President Vladimir Putin on Monday, Trump declined to endorse his government's

assessment that Russia interfered in the 2016 presidential election, saying he doesn't "see any reason why Russia would be responsible."

British public relations watchdog Spinwatch Public Interest Investigations said, in a report published last week detailing UAE lobby efforts, that ever since the 2011 popular Arab revolts, the Emirates had tasked public relations companies in the US and Britain with linking members of Qatar's ruling family to terrorism.

The lobbying effort also aimed to get the Qatar-backed Muslim Brotherhood banned, involved UAE threats to withhold lucrative trade deals from Britain if allegedly pro-Brotherhood reporting by the BBC was not curtailed, and targeted journalists and academics critical of the Gulf country, according to the report.

US intelligence officials said that last year, the UAE orchestrated the hacking of Qatari government news and social media sites in order to post incendiary false quotes attributed to Qatar's emir, Sheikh Tamim Bin Hamad al-Thani. The hacking provided the pretext for the UAE-Saudi-led economic and diplomatic boycott of the Gulf state. The UAE has denied this assertion.

US and Qatari officials said earlier that Russian hackers for hire had executed the attack on the Qatari websites. Cybersecurity experts said at the time that the hackers worked for various Gulf states. They said the methods used in the hacking of the Qatari website and the hacking of Otaiba's email were similar.

"They seem to be hackers-for-hire, freelancing for all sorts of different clients, and adapting their skills as needed," said security expert Collin Anderson.

Two cybersecurity firms, ThreatConnect and Fidelis Cybersecurity, said in 2016 that they had indications that the hackers who hit the Democratic National Committee were preparing a fake version of the UAE Ministry of Foreign Affairs website that could be used in phishing attacks.

The UAE-Qatari cyberwar was indeed likely enabled by Russian hackers working for their own account rather than in coordination with the Russian government. It is however equally possible that the same hackers put their services at the disposal of Russia.

None of what is known about the murky world of Russian hackers is conclusive, let alone produces a smoking gun. The various strands of Mueller's investigation, however, suggest grounds to query not only Russian cyber efforts to influence the US election but also the involvement of Russian nationals in the cyber war in the Gulf and potential links between the two operations.

Dr. James M. Dorsey, a non-resident Senior Associate at the BESA Center, is a senior fellow at the S. Rajaratnam School of International Studies at Singapore's Nanyang Technological University and co-director of the University of Würzburg's Institute for Fan Culture.

BESA Center Perspectives Papers are published through the generosity of the Greg Rosshandler Family