Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

Analytical Brief
Précis **analytique**

SECRET

CAB 2022-23/76
March 23, 2023

Team Jorge Offers Covert Cyber-Enabled Influence Activities for Hire

An increasing number of actors are now capable of conducting a broad range of disruptive threat activity in cyberspace as the proliferation of cyber capabilities 'levels the playing field'. The use of cyber cognitive aggression[1] and cyber-enabled influence activities by non-traditional threat actors' poses a serious threat to Western democratic values. This Analytical Brief assesses recent journalistic revelations[2] that have exposed an Israel-based business, known as Team Jorge—and the threats posed by its cyber cognitive aggression activities. It also highlights the wider implications presented by an increasing number of cyberspace actors who are capable of conducting a broad range of threat activity including election meddling, hacking, sabotage and automated cognitive aggression across social media platforms to manipulate public opinion. (S/

Team Jorge's business model and capabilities

Team Jorge is an Israeli-based business headed by Tal Hanan, a former Israeli special forces operative, that offers its clients cognitive aggression services on a global scale using its fake social media profiles—in excess of 30,000. Team Jorge is comprised of Israeli contractors who specialize in malicious cyber activities including hacking, sabotage and botnet[3] activity, to covertly interfere in elections and/or manipulate public opinion on behalf of their clients. (U)

A key part of Team Jorge's services is the use of Advanced Impact Media Solutions (AIMS), a software package designed to spread propaganda or cognitive aggression online. The AIMS software can create avatars and automated content in any language with a "positive," "negative" or "neutral" tone, which can then be disseminated in the form of posts, articles, comments or tweets. AIMS controls thousands of fake social media profiles and/or avatars on Twitter, LinkedIn, Facebook, Telegram, Gmail, Instagram and YouTube. As revealed through journalistic investigation, these fake profiles can be created in a mere instant, using different features such as nationality, gender, language and pictures (stolen from genuine profiles) to go along with the names. In an effort to provide increased plausibility, some fake profiles have Amazon and Airbnb accounts with credit cards and Bitcoin wallets. (U)

Clientele and impacts

Team Jorge claims to have covertly influenced 33 presidential-level elections around the world – of which it claims 27 were successful. Team Jorge's customers allegedly include intelligence agencies, political campaigns and private entities.

---

1 Cognitive aggression, also referred to as cognitive warfare, is a strategy for attacking the cognitive processes, mental biases or reflexive thinking of a target in order to provoke thought distortions, influence decision-making and hinder actions—with negative effects—both at the individual and collective levels. (U)

2 In February 2023, journalists from 30 reputable news outlets published the results of their joint investigation into the work of Team Jorge. (U)

3 A botnet is a group of compromised Internet-connected devices that are infected with malware without the owner's awareness and are remotely controlled by a threat actor to perform malicious tasks. Botnets are used for a multitude of purposes, such as conducting distributed denial of service (DDoS) attacks, spreading ransomware and malware, conducting ad fraud campaigns, sending spam, diverting traffic, stealing data, and manipulating, amplifying, and/or suppressing social media and Web platform content to impact public discourse. (U)

Analytical Brief
Précis analytique

CAB 2022-23/76
March 23, 2023

SECRET

- Team Jorge's work reportedly dates back to the 2012 Venezuelan presidential election. Hanan claims to have disseminated false information to an ABC News network against former President Hugo Chavez, who nonetheless managed to win the election.(U)
- Journalistic investigation revealed that Hanan collaborated with Cambridge Analytica[4] in 2015, when they allegedly meddled in the Nigerian Presidential elections. At that time, Hanan and Cambridge Analytica attempted—unsuccessfully—to engineer the re-election of Nigeria's president, Goodluck Jonathan, by discrediting the campaign of opposition leader Muhammadu Buhari. (U)
- In 2022, Hanan's team reportedly meddled in Kenyan presidential elections by hacking the Gmail and Telegram accounts of political advisors who were close to Kenya's President, William Ruto. Two of the campaign staffers whose accounts were compromised continue to be accused of hacking the election committee and "stealing" the votes. (U)
- AIMS-linked avatars have reportedly been used to create and amplify commercial disputes in numerous countries including Canada, Belarus, Ecuador, Germany, Greece, India, Mexico, Morocco, Panama, Senegal, Switzerland, the United Kingdom (UK), the United Arab Emirates (UAE), the United States (US) and Zimbabwe. For instance, a notable example of Team Jorge's reported activities in relation to Canada is the #MeToo controversy concerning Canadian fashion tycoon Peter Nygard. Hanan claims that a client paid him to help facilitate Nygard's arrest for alleged sex crimes. Hanan's reported aim was to make public allegations that Nygard was a serial rapist and to push for his indictment, trial and conviction by calling him "the Canadian Jeffrey Epstein" online. Other examples included (i) nuclear power dispute in California; (ii) a campaign involving a Qatari UN official in France; and, (iii) a controversy involving a clinic in the United Kingdom that was under investigation for providing false COVID-19 testing results. (U)

Conclusion

[4] Cambridge Analytica is a political data firm involved in multiple scandals, including those revealed in both 2015 and 2018. The firm obtained the data of 50 million Facebook users, constructed 30 million personality profiles, and sold the data to American politicians running for office in order to influence voters, without the users' consent. Cambridge Analytica is also reported to have influenced the outcome of the 2016 UK referendum on the country's departure from the European Union. (U)
[5] For additional details on NSO Group's Pegasus spyware, refer to CSIS CAB 2021-22/102. (S/)

Analytical Brief
Précis analytique

CAB 2022-23/76
March 23, 2023

SECRET/[redacted]

[redacted]
CSIS_PUBLICATIONS / SCRS_ PUBLICATIONS