Chapter 12
Multidimensional Mappings of Political Accounts for Malicious Political Socialbot Identification:
Exploring Social Networks, Geographies, and Strategic Messaging

Shalin Hai-Jew
Kansas State University, USA

ABSTRACT

Malicious political socialbots used to sway public opinion regarding the U.S. government and its functions have been identified as part of a larger information warfare effort by the Russian government. This work asks what is knowable from a web-based sleuthing approach regarding the following four factors: 1) the ability to identify malicious political socialbot accounts based on their ego neighborhoods at 1, 1.5, and 2 degrees; 2) the ability to identify malicious political socialbot accounts based on the claimed and linked geographical locations of their accounts, their ego neighborhoods, and their #hashtag networks; 3) the ability to identify malicious political socialbot accounts based on their strategic messaging (content, sentiment, and language structures) on respective social media platforms; and 4) the ability to identify and describe "maliciousness" in malicious political socialbot accounts based on observable behaviors on that account on three social media platform types: (a) microblogging, (b) social networking, and (c) crowd-sourced encyclopedia content sharing.

INTRODUCTION

A U.S. presidential election, which occurs every four years, is a high-stakes, high-impact endeavor with a large number of stakeholders, not least of which are the 326 million U.S. citizens ("U.S. Population (live)," 2018). This is not to say there have not been high levels of apathy regarding voting in presidential elections and low levels of civic engagement. Even though presidential powers in a democracy are limited by law, by practice (checks and balances), by mass media, and by the public will, it is still a

DOI: 10.4018/978-1-5225-5927-6.ch012

position with inordinate influence. In most such elections, the choice is practically between two surviving candidates, each one backed by either the Republican or Democratic Party, and each representing different platforms. In the American democracy, the reduction to a two-way race means this offers a political chokepoint and, therefore, a system-based "weaknesses" which may be prone to manipulation.

In the current political moment, the U.S. is engaged in coming to terms with what "Russian meddling" during the 2016 U.S. presidential election and setting up a defense against further anticipated meddling in the 2018 midterm elections and into the future. The core question being addressed is whether the U.S. emplaced a "Manchurian candidate" in 2016 who might have been focused on trading power and influence for monetary and other gains from the Russian and other foreign governments. The story arc has evolved as investigators from various intelligence agencies have explored this Kremlin influence operation, with its agents creating social media platform accounts and using robots ('bots or automated agents) to promote particular storylines, to discredit democracy and to promote one presidential candidate (Donald J. Trump) over the other (Hillary Clinton). An initial perusal of the first facts may have led an individual to downplay the importance of the effort. As more details emerge, the seriousness becomes somewhat clearer.

The actual investments into the effort were not minimal, with early efforts starting in 2014. There was a test run with #fakenews by disseminating false information claiming a family became ill from consuming a Walmart turkey (Earle, 2018). The Russian government apparently spent up to US$1.25 million a month and paid hundreds for this endeavor (Tamkin, 2018). According to a U.S. government indictment, Russian agents were sent to collect intelligence and research in multiple states prior to the presidential election to better target the messaging. In the U.S. District Court for the District of Columbia, based on an indictment filed on Feb. 16, 2018, the U.S. Special Counsel's Office identified 13 Russian individuals involved in this endeavor. The identification of these 13 individuals, across borders, cultures, technologies, and languages, demonstrated the reach of American intelligence and law enforcement. The indictment deftly cited witting and unwitting individuals manipulated by this information operation. In the following section, the indictment describes some of the Russian agents' travel to the U.S.:

Only KRYLOVA and BOGACHEVA received visas, and from approximately June 4, 2014 through June 26, 2014, KRYLOVA and BOGACHEVA traveled in and around the United States, including stops in Nevada, California, New Mexico, Colorado, Illinois, Michigan, Louisiana, Texas, and New York to gather intelligence. After the trip, KRYLOVA and BURCHIK exchanged an intelligence report regarding the trip.

Another co-conspirator who worked for the ORGANIZATION traveled to Atlanta, Georgia from approximately November 26, 2014 through November 30, 2014. Following the trip, the co-conspirator provided POLOZOV a summary of his trip's itinerary and expenses. ("United States of America v. Internet Research Agency LLC…," Feb. 16, 2018, p. 13)

The indictment documents the setup of virtual private networks (VPNs) inside the U.S. ("United States of America v. Internet Research Agency LLC…," 2018, pp. 15 – 16). Such technologies create a false sense that the computers used to access social media platforms seem to be U.S.-based. The effort itself was made possible by a Russian government military doctrine known as the Gerasimov Doctrine, according to cybersecurity expert Jim Lewis, Senior VP at the Center for Strategic and International Studies (Garrett, 2018).