PIPS

Bad Bots

The Weaponization of Social Media

PIPS White Paper 9.2: *Executive Summary*

Matthew Bondy, Research Fellow
Christopher D. Elsner, Research Intern

In the next several years, hostile states or non-state actors will accelerate their use of social media bots to undermine democracy, recruit terrorists, disrupt markets, and stymie open-source intelligence collection. This report conducts an alternative futures analysis in order to help policymakers identify options to mitigate the threats of social media bots. In the worst-case and most-likely scenario, a technological stalemate between bots and bot-detection leads to a false sense of confidence in social media information, which allows for breakthroughs in bot technology to create disruptions until bot-detection technology advances.

The Emerging Threat of Social Media Bots

A social media bot (SMB) is a computer program that controls an account on a social media platform, such as Twitter or Facebook. Technological advances will allow more effective and numerous SMBs to manipulate social media, which threatens the United States in several domains:

- *Democracy*. Social media bots could be used to influence election outcomes, undermine public confidence in elections, or drown out dissidents' voices.

- *Economy*. Social media bots could manipulate stock prices by spoofing high-frequency trading systems or persuading human investors into making particular trades.

- *Terrorism*. Terrorist groups could employ SMBs to enhance their social media operations, such as recruitment. Additionally, SMBs can inspire lone-wolf acts of terrorism.

- *Intelligence*. Social media bots are likely to have a distorting effect on the field of sentiment analysis—a forecasting method that is increasingly used in open-source intelligence—if analysts do not have a reliable method of separating bots from real users.

Alternative Futures Analysis

Rapid advances in artificial intelligence and the wide array of actors involved in information warfare make it difficult to predict the future of SMBs five to ten years from now, but two "known unknowns," are likely to play a key role: (1) the bot versus counter-bot technology "arms race" and (2) the vulnerability of the public, private industry, and governments to social media manipulation. In the best-case scenario, bots are easily detected and eliminated. At the opposite extreme of the technology arms race, where bot-detection fails, society might adapt to reduce its reliance on social media. In the most likely and worst-case scenario, however, a technological stalemate results and society remains vulnerable in a "Survival of the Fittest" world, where:

- *The public is vulnerable to manipulation.* Social media users have no way to distinguish sophisticated bots from real users, so regimes use SMBs to shape discussion both within their own countries and abroad, and terrorist networks use bots to amplify their messages.

- *Industry and government suffer from overconfidence.* Governments and private industry invest in technologies that can filter out bot traffic, leading to overconfidence in social media data. However, hostile actors develop new SMBs that can circumvent detection systems, which leads to high-level financial crime and intelligence failures.

Some potential "X-factors," such as a new social media revolution or the intentional de-legitimizing of social media, could alter this analysis. Regardless, policymakers will need to be prepared to deal with the threat of SMBs.

Countering Social Media Bots

Current policy places the role of countering foreign propaganda under the State Department, which lacks the resources to adequately combat the threat. A new coordinated effort between the State Department, Department of Defense, and the intelligence community is needed. Social media companies also will play an important role, but independently, the U.S. government has several policy instruments available to mitigate the threat of SMBs:

- *Invest in bot-detection technology.* Government agencies may develop bot-detection capabilities themselves or through partners in academia. This technology would be necessary in order for the government to take subsequent steps, for instance, incentivizing social media companies to flag or remove bad bots.

- *Harden our society.* Policymakers could make the public less susceptible to bot misinformation by formalizing media literacy education requirements or encouraging civic society efforts such as public education campaigns.

- *Maintain multi-domain deterrence.* If Washington is serious about deterring SMB attacks, it will need to show that responses in other domains—including covert, cyber, diplomatic, or military action—remain on the table.

If left unchecked, SMBs are likely to complicate U.S. national security policy. Even modest problems in several domains or in several regions could add up to constitute a major challenge for Washington. Policymakers would be wise to confront these issues sooner rather than later.