OFFICE of INTELLIGENCE and ANALYSIS

INTELLIGENCE IN BRIEF

3 MARCH 2021 IA-48020-21

FOREIGN INFLUENCE

(U) Russian Malign Influence Use of Permissive Social Media Platforms

(U//FOUO) ***We assess that Russian malign influencers probably will increasingly use US social media platforms that offer more permissive operating environments.*** We base this assessment on the reduced effectiveness of Russian influence operations on established US social media platforms and current Russian proxy activity on these growing US platforms. Our assessment also is based on the assumption that Russian malign influences see operational advantages in sites with less active effort to ban false information, offensive language, and inauthentic behavior.

- *(U)* Some established US social media platforms as of October 2020 had blocked or suspended activity of Russian proxy websites, one known for publishing divisive narratives on US race, immigration, and election-related topics, according to a cybersecurity firm. However, these proxy sites maintained active accounts on other new, increasingly popular social media platforms with more permissive approaches to content moderation, according to a press report and a Department of State report.

- *(U)* A US social media platform that offers a more permissive operating environment saw its membership grow from 4.5 million users to about 8 million users in a single week in early November 2020, according to a US press report. A separate US social media platform offering a similar permissive operating environment also saw record growth, with 7.15 million visits to its site the same week, compared to 7.7 million visits in the preceding month, according to a statement on its website.

- *(U)* Russian malign influencers in 2016 used social media to conduct influence operations intended to exacerbate societal divisions in the United States, according to a US Senate investigation. Social media companies such as Facebook$^{\text{USPER}}$ and Twitter$^{\text{USPER}}$, following the 2016 election, took steps to shut down this type of activity, decreasing the effectiveness of foreign influence operations on their platforms, according to reports from a reputable press outlet.

(U) Prepared by the Cyber Mission Center. For questions, contact DHS-SPS-RFI@hq.dhs.gov

(U) Content Moderation Policies

(U) Some of the increasingly popular US social media platforms with less restrictive moderation policies market themselves as strong proponents of First Amendment rights and portray other established US platforms as having strict censorship policies, according to a reputable US media outlet and our review of these platforms' policies. A newer US social media platform—with a growing user base that markets itself as a network for free speech—contained 2.4 times the concentration of content that was restricted by an established US platform, according to a US academic study conducted in 2018. Some sites with less restrictive moderation also do not publicly label the accounts of key government officials and state-sponsored media pages and do not have the procedures and capabilities in place to identify and label manipulated media. These sites also have not removed known Russian proxies from their sites, as is common practice among a small number of more established US social media platforms, according to a press report and our review of publicly available social media platforms' policies.

Source, Reference, and Dissemination Information

Source Summary Statement

(U//FOUO) **We assess that Russian malign influencers probably will increasingly use US social media platforms that offer more permissive operating environments.** We have **medium confidence** in this assessment based on a body of credible open source reporting, a report from a reputable social media analysis company, and a think tank assessment. Russian influencers were identified using two social media sites known for having less restrictive editorial policies, the first time they had been known to use these platforms.

Definitions

(U) **Content Moderation -** Content moderation is when a media publisher determines if content can be posted on their platform based on their platform rules and guidelines.

(U//FOUO) **Disinformation** - A foreign government's deliberate use of false or misleading information intentionally directed at another government's decisionmakers and decision-making processes to mislead the target, force it to waste resources, or influence a decision in favor of a foreign government's interests.

Dissemination

(U) Senior DHS leadership and cleared federal officials, governors, lieutenant governors, secretaries of state, homeland security advisors, fusion center directors and their staff, as well as private sector partners.

Reporting Suspicious Activity

(U) To report a computer security incident, please contact CISA at 888-282-0870; or go to https://forms.us-cert.gov/report. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form. The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

(U) To report this incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov. DHS I&A Field Operations officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.

Warning Notices & Handling Caveats

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

(U) This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label USPER and should be handled in accordance with the recipient's intelligence oversight and/or information handling

procedures. Other US person information has been minimized. Should you require the minimized US person information on weekends or after normal weekday hours during exigent and time sensitive circumstances, contact the Current and Emerging Threat Watch Office at 202-447-3688, CETC.OSCO@hq.dhs.gov. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U) Russian Malign Influence Use of Permissive Social Media Platforms

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: Select One **and function:** Select One

2. What is the highest level of intelligence information that you receive? Select One

3. Please complete the following sentence: "I focus most of my time on:" Select One

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

- □ Drive planning and preparedness efforts, training, and/or emergency response operations
- □ Observe, identify, and/or disrupt threats
- □ Share with partners
- □ Allocate resources (e.g. equipment and personnel)
- □ Reprioritize organizational focus
- □ Author or adjust policies and guidelines
- □ Initiate a law enforcement investigation
- □ Intiate your own regional-specific analysis
- □ Intiate your own topic-specific analysis
- □ Develop long-term homeland security strategies
- □ Do not plan to use
- □ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disgree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name:

Organization:

Contact Number:

Position:

State:

Email:

Submit Feedback

Privacy Act Statement

Product Serial Number: IA-48020-21

REV: 01 August 2017