OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS
29 MARCH 2021 IA-48434-21

TERRORISM

(U//FOUO) Militia Violent Extremists Developing Online Networks Despite Content Removal Efforts

(U//FOUO) ***We assess that some militia violent extremists (MVEs) are actively disguising their online social media outreach to promote violent anti-government narratives, connect with others espousing violent extremist views, and share tactical information by using layered communications, despite social media companies' efforts to suppress violent extremist content online in 2020 and early 2021***.[a] This communications strategy entails the use of publicly accessible groups on social media platforms to appeal to a broader pool of potential recruits—including platforms perceived as being more permissive—before transitioning to more secure methods, such as private social media groups and encrypted applications.[b] Some MVEs have obfuscated potential detection of their online activity by mirroring their communications with patterns observed in lawful social media groups. Movement to these more secure channels helps MVEs filter or disguise online communications to protect operational security, avoid violating social media platforms' terms of service, and reserve detailed operational discussions for more secure platforms.

- *(U//FOUO)* In August and October 2020, an identified individual requested others in an open online social media group to recruit new members to their "exclusive club" in an effort to add more members to a private social media group, according to FBI reporting.[c] In July 2020, a separate MVE connected with another MVE via public social media posts after seeing they were connected through a mutual friend, according to separate FBI report.

---

[a] *(U//FOUO)* The use of these social media platforms and encrypted messaging applications alone is not indicative of an individual's involvement in domestic terrorism and are often used for constitutionally protected communication.

[b] *(U//FOUO)* Please see attached graphic for a detailed representation of this layered communications strategy.

[c] *(U//FOUO)* Some MVEs call themselves Three Percenters (III%ers), based on the belief that only three percent of the American colonists took up arms against the British Government during the Revolutionary War. Some III%ers regard the present-day US Government as analogous to the British monarchy during the 18th century in terms of its alleged infringements on civil liberties. The term generally represents the perception that a small force with a perceived just cause can overthrow a tyrannical government if armed and prepared. Involvement in the III%ers alone is not indicative of violent activity and not all III%ers are considered to be MVEs.

(U) Prepared by the Counterterrorism Mission Center. Coordinated within the DHS Intelligence Enterprise (CBP, ICE, TSA, and USCG) and with FBI and NCTC.
For questions, contact DHS-SPS-RFI@hq.dhs.gov

- *(U//FOUO)* Like many other social media users, some MVEs are transitioning to other social media platforms perceived as either having more permissive terms of service policies or viewed as providing enhanced data privacy, such as MeWe and Parler, according to open source reporting. As of October 2020, an identified MVE stated that in addition to using an identified public social media group to communicate, he used MeWe and Signal, and that most of the communication for the "boogaloo" was conducted over MeWe, according to FBI reporting. Additionally, as of June 2020, a separate identified MVE allegedly used the MyMilitia forum to advocate violence, according to a federal criminal complaint.
- *(U//LES)* In 2020, MVEs used or expressed interest in using a variety of more secure and often encrypted messaging applications—including Zello, Telegram, Signal, and Threema—to discuss operational activity, according to FBI and open source reporting. In May, an identified Maryland-based MVE used Signal and the search engine DuckDuckGo to discuss targeting law enforcement and share bomb making instructions, according to FBI reporting.

(U//FOUO) **Foreign Terrorist Organization Supporters Use a Similar Layered Communications Strategy**

(U//FOUO) Foreign terrorist organizations (FTOs) and their supporters have historically used a similar approach for spreading FTO media, recruiting like-minded individuals, and operational planning purposes. However, unlike domestic terrorism movements, the designation of overseas groups as FTO by the US Government almost certainly presents a lower threshold for social media companies to remove this content due to the illegality of providing material support to a designated FTO, which includes "expert advice and assistance."

(U//FOUO) ***MVEs' attempts to obfuscate their recruitment of others into these tighter-knit online communities using innocuous postings in public groups probably hinders social media companies' efforts to identify and remove MVE content.*** Although some social media companies have already begun content removal efforts, these efforts have largely been limited to overt threats of violence. We judge that increased US Government engagement with private sector partners to develop indicators of operational planning and recruitment for MVE activity probably would increase social media companies' insight into how MVEs are attempting to circumvent their platforms' terms of service agreements and would probably enhance our ability to detect and disrupt operational planning and recruitment online.

- *(U//FOUO)* In mid-August, an associate of a public social media group—who expressed support for violent action in furtherance of the MVE ideology—was advised by a prominent network member that unspecified operational plans were underway but could not be discussed on that social media platform, which suggests members of the network may have been filtering online communications for operational security purposes and to avoid violating the social media platforms' terms of service.

- *(U)* In October, a West Virginia-based suspected MVE was arrested on charges related to his online business that sold drop-in auto sears, which could be used to convert semi-automatic rifles to fully automatic. The components were openly advertised as benign home furnishings called "portable wall hangers" and marketed directly to other MVEs via public-facing social media and websites, according to court documents.
- *(U)* Current social media removal efforts of MVE content appears to be limited to only the most popular platforms. Recently, one popular social media platform began redirecting some searches related to QAnon—a conspiracy theory which has influenced some MVEs—to credible research from the Global Internet Forum Countering Terrorism's (GIFCT) Global Network on Extremism and Technology, a practice which we judge could be leveraged in a similar form for other domestic terrorism movements.[d]

(U//FOUO) Improved US Government collection against MVEs' online activities and deeper collaboration among private sector, law enforcement, and Intelligence Community partners probably would enhance our ability to develop indicators of MVE content online. Existing partnerships with international and private sector partners through the GIFCT, Tech Against Terrorism—an organization which empowers smaller, emerging social media companies to increase their capacity to enforce their terms of services as they address terrorism, violent extremism, and mobilization to violence on their platforms—and a variety of other counter violent extremist messaging working groups primarily have focused on preventing foreign terrorist and white supremacist extremists' use of the internet and provide opportunities to coordinate efforts against MVEs.

[d] *(U//FOUO)* Generating, accessing, discussing, or otherwise interacting with QAnon-related content without engaging in violence or other criminal activity may be legal and protected by the First Amendment.

Homeland Security

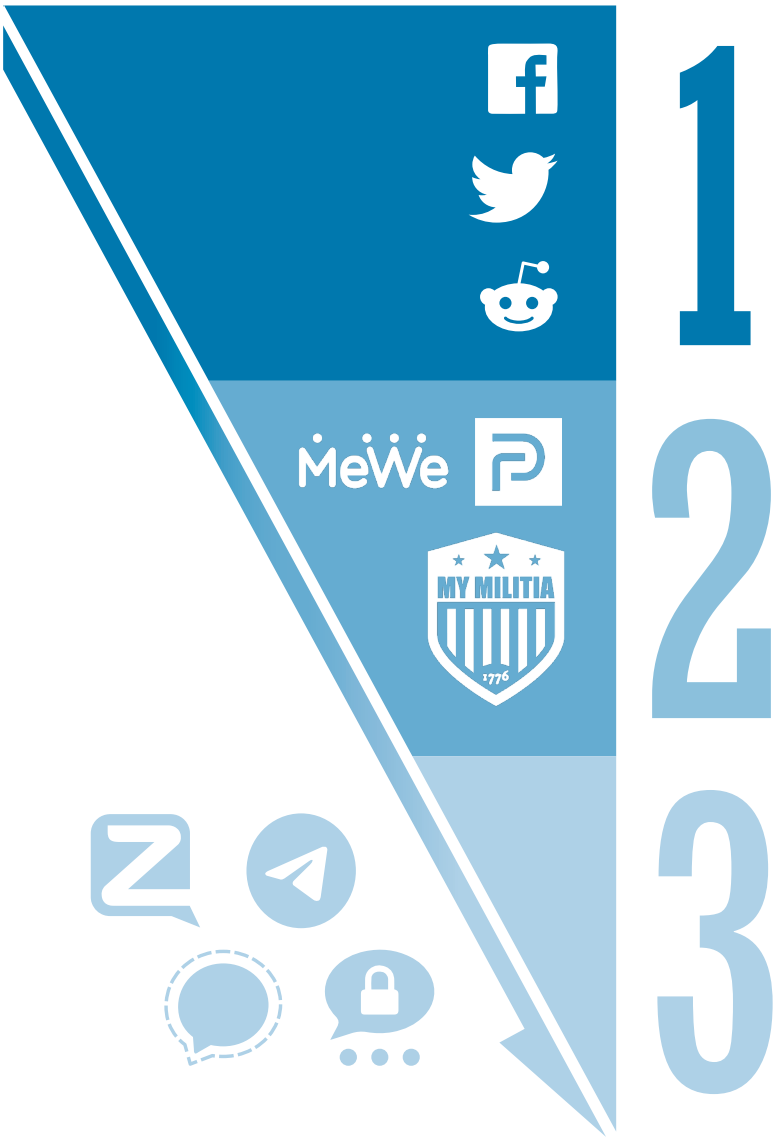
OFFICE OF INTELLIGENCE & ANALYSIS

MARCH 2021

(U//FOUO) Militia Violent Extremists' Three Stages of Layered Communications

(U//FOUO) This graphic depicts a model visualizing three stages of layered communications typically employed by militia violent extremists (MVEs) when operating within online environments. For the purposes of this graphic, layered communications refers to the process in which MVEs attempt to recruit prospective members from ideologically consistent public-facing social media and transition them to either invitation-only or secure applications they perceive to be more permissible to share their violent extremist messaging and operational planning. The process of transitioning between these public-facing platforms to more secure applications may also occur between stage one and two, albeit to a lesser degree.[e]

OVERALL GRAPHIC CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY



1

Stage One: Public-Facing Recruitment

- Public social media and social networking groups.
- Limited use of violent extremist language as they are likely cognizant of law enforcement and government monitoring.
- Likely active within ideologically consistent social media groups that are constitutionally protected.

2

Stage 2: Invitation to Private Groups or More Permissive Platforms[f]

- May shift to emerging social media with perceived less restrictive content moderation.
- Typically used as a way of vetting potential recruits.
- Privitized groups provide additional layer of operational security.
- May share some violent extremist messaging to gather reactions by potential recruits.

3

Stage 3: Transition to Secure Platforms

- Invitations to official private membership group(s).
- Likely have simultaneously shifted to encrypted messaging applications at this point for additional operational security.
- May also include receiving list of membership contact information.
- Frequent communication of violent extremist messaging, sharing of weapons and tactical guides, and other tactics, techniques, and procedures.

[a] (U//FOUO) The mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics does not constitute criminality or violent extremism, and is constitutionally protected.

[b] (U//FOUO) Once an individual transitions to using private social media groups or encrypted messaging applications, our ability to monitor for potential violent extremist activity becomes limited.

Source, Reference, and Dissemination Information	
Source Summary Statement	*(U//FOUO)* We have **medium confidence** in our assessment that some MVEs are broadening their outreach on social media to promote violent anti-government narratives, connect with others espousing violent extremist views, and share tactical information by using layered communications. This assessment was informed by a large body of recent FBI reporting on domestic terrorism subjects, open source reporting, court documents, and press reporting. *(U//FOUO)* We have **medium confidence** in our judgment that MVEs' attempts to obfuscate their recruitment of others into these tighter-knit online communities using innocuous postings in public groups hinders social media companies' efforts to remove MVE content. This judgment is based on open source reporting, FBI reporting on domestic terrorism subjects, court documents, and an information exchange with the DHS Office of Targeted Violence and Terrorism Prevention.
Definitions	*(U//FOUO)* **Boogaloo:** The boogaloo is a term used by some domestic terrorist actors to refer to the start of the second Civil War driven by perceptions of government overreach, including firearms legislation; or a race war driven by white supremacist extremism. Domestic terrorist actors who may adhere to this idea include some MVEs, white supremacist extremists, and other anti-government extremists. *(U//FOUO)* **Militia Violent Extremists:** Groups or individuals who facilitate or engage in acts of unlawful violence directed at federal, state, or local government officials or infrastructure in response to their belief that the government deliberately is stripping Americans of their freedoms and is attempting to establish a totalitarian regime. These individuals consequently oppose many federal and state authorities' laws and regulations, particularly those related to firearms ownership, and often belong to armed paramilitary groups. They often conduct paramilitary training designed to violently resist perceived government oppression or to violently overthrow the US Government. *(U//FOUO)* **White Supremacist Extremists**: Groups or individuals who facilitate or engage in acts of unlawful violence directed at the federal government, ethnic minorities, or Jewish persons in support of their belief that Caucasians are intellectually and morally superior to other races and their perception that the government is controlled by Jewish persons.
Reporting Suspicious Activity	*(U)* **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit http://nsi.ncirc.gov/resources.aspx.
Dissemination	*(U)* Federal, state, local, territorial, and tribal authorities and law enforcement partners.
Civil Rights and Civil Liberties	*(U//FOUO)* US persons linking, citing, quoting, or voicing the same arguments raised by these influence activities likely are engaging in First Amendment-protected activity, unless they are acting at the direction or under the control of a threat actor. Furthermore, variants of the topics covered in this product, even those that include divisive terms, should not be assumed to reflect foreign influence or malign activity absent information specifically attributing the content to malign foreign actors. This information should be considered in the context of all applicable legal and policy authorities to use open source information while protecting privacy, civil rights, and civil liberties.

Warning Notices & Handling Caveats	*(U)* **LAW ENFORCEMENT SENSITIVE**: The information marked (U//LES) in this document is the property of FBI and may be distributed within the Federal Government (and its contractors), US intelligence, law enforcement, public safety or protection officials, and individuals with a need to know. Distribution beyond these entities without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website on an unclassified network. *(U)* **Warning:** This document contains UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO) 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 not share this document with critical infrastructure and key resource personnel or private sector security officials without further approval from DHS. *(U)* All US person information has been minimized. Should you require 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-SPSRFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.

CLASSIFICATION: **UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Militia Violent Extremists Developing Online Networks Despite Content Removal Efforts

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:		*Position:*	
Organization:		*State:*	
Contact Number:		*Email:*	

Submit Feedback

Privacy Act Statement

CLASSIFICATION: **UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE**

Product Serial Number: IA-48434-21 REV: 01 August 2017