OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS
15 APRIL 2024 DHS-IA-IF-2024-10270

TERRORISM

(U//FOUO) Domestic Violent Extremists Express Interest in Targeting Fiber Optic Cables, Raising Potential for Widespread Disruption

(U//FOUO) ***Scope Note:*** *This is DHS I&A's first assessment of Domestic Violent Extremist threats to US fiber optic cable lines. This assessment seeks to provide law enforcement and public safety partners with an overview of how DVEs could adopt tactics used by criminal actors to damage US critical infrastructure to further their ideological goals.*

(U//FOUO) **Domestic Violent Extremists (DVEs) have increasingly discussed targeting terrestrial fiber optic cables across the United States, raising the threat to fiber-dependent infrastructure sectors.** DVEs frequently discuss that fiber optic cables are a preferred target to disrupt critical infrastructure pursuant to their ideological goals of dismantling current societal structures. The spread of the COVID-19 virus prompted increased telework that has persisted, creating dependencies on fiber optic cable networks that were highlighted within information sharing platforms utilized by some DVEs.

- *(U//FOUO)* Since 2020, DHS and open-source reporting have shown an uptick in DVEs across ideologies sharing simple tactics specifically related to fiber optic cables. In 2024, a blog utilized by some anarchist violent extremists used a military target assessment method to encourage attacking fiber optics as an "easy" target while referencing past attacks. In 2023, a channel frequently used by environmental violent extremists shared five issues of a magazine that critiqued the tactics used in successful previous attacks. In 2022, the Terrorgram Collective publication discussed tactics for targeting fiber cables, including the use of firearms, arson, and power tools.
- *(U//FOUO)* Several discussions in recent years among users of an online forum frequented by DVEs describe fiber optic cables as low-cost/high-reward targets to disrupt critical infrastructure. These users indicate a preference for fiber optic cable cuts due to the perceived simplicity and ability to avoid law enforcement interdiction.
- *(U//FOUO)* Fiber optic cable cuts often cause cascading effects on critical infrastructure sectors, such as communications, and delay emergency services

from responding to incidents. Across the United States, fiber optic cable cuts have disrupted 911 services and forced police stations to redirect personnel to field emergency calls through non-emergency lines. Individuals from North Carolina, who intentionally cut fiber optic cables in Connecticut, disabled communications and internet-based financial services to thousands of homes and businesses for hours.

(U//FOUO) **While DVEs have focused on opportunistic or simple attacks thus far, online narratives about fiber optic vulnerability and increased information sharing could inspire DVEs to engage in larger-scale, pre-planned fiber attacks in the Homeland.** Recent attacks in France and Germany that used multiple and coordinated cuts to fiber optics surrounding a target area resulted in blackouts and communications stoppages that strained emergency services' responses.

- *(U//FOUO)* Information shared online about fiber optic systems and media coverage of attacks could inform DVE attack planning and operations. In February 2024, an online user claiming to be a former cable worker provided a detailed description of how a coordinated group of individuals could disrupt communications for an entire city. In 2023, online discussions, in response to news media coverage of recent attacks, dissected attacks in Sacramento, California, from 2014 and examined the nature of the successful attacks to develop methods for making future attacks more severe, indicating potential pre-planning by actors.
- *(U//FOUO)* DVEs could also draw inspiration from European attacks that disrupted citywide telecommunications and transportation. Violent extremists in France caused massive disruptions to telecommunications by targeting primary fiber optic cables in several regions. In Germany, travelers were left stranded after actors cut fiber optic lines and caused hours-long train stoppages.
- *(U//FOUO)* Possible indicators of pre-operational planning for a large-scale fiber optic attack include unauthorized surveillance around fiber optic sites, particularly connection locations; signs of trespassing or digging around known fiber connection locations; and successful small-scale fiber optic cuts.

Source, Reference, and Dissemination Information	
Definitions	*(U//FOUO)* **Domestic Violent Extremist (DVE)**: An individual based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seeks to further political or social goals, wholly or in part, through unlawful acts of force or violence. The mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics alone does not constitute violent extremism and may be constitutionally protected. DVEs can fit within one or multiple categories of ideological motivation and can span a broad range of groups or movements. I&A utilizes this term synonymously with "domestic terrorist." *(U//FOUO)* **Terrorgram Collective:** An online collective of Telegram channels maintained by some racially or ethnically motivated violent extremists. *(U//FOUO)* **Anarchist Violent Extremists (AVEs):** Individuals who seek, wholly or in part, through unlawful acts of force or violence, to further their opposition to all forms of capitalism, corporate globalization, and governing institutions, which they perceive as harmful to society. *(U//FOUO)* **Animal Rights/Environmental Violent Extremists (AREVEs):** Groups or individuals who facilitate or engage in the unlawful use or threat of force or violence or intent to intimidate or coerce, in furtherance of political and/or social agendas by those seeking to end or mitigate perceived cruelty, harm, or exploitation of animals or perceived exploitation or destruction of natural resources and the environment.
Reporting Suspicious Activity	*(U//FOUO)* **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 www.dhs.gov/nsi. *(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.
Privacy, Civil Rights, Civil Liberties Notice	*(U//FOUO)* US persons linking, citing, quoting, or voicing the same arguments or symbols are likely engaging in First Amendment-protected activity, unless they are acting at the direction or control of a domestic violent extremist group or actor.

	Furthermore, variants of the topics covered in this product, even those that include divisive terms, should not be assumed to reflect violent extremism absent information specifically attributing the content to domestic violent extremists. 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)* **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)* All US person information has been minimized. 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.

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Domestic Violent Extremists Express Interest in Targeting Fiber Optic Cables, Raising Potential

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 Disagree	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//FOR OFFICIAL USE ONLY**