OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN BRIEF
24 MAY 2021 IA-51494-21

PUBLIC SAFETY & SECURITY

(U//FOUO) Threats to Emergency Communications in Northeast Region

(U//FOUO) ***We assess that recent incidents targeting communications infrastructure in New York and Pennsylvania highlight the enduring threat to this sector and potential for disrupting emergency communications, including from anti-government and other domestic violent extremists (DVEs).*** Incidents have disrupted a range of communications for hours to days at a time, including local and regional governments and first responder networks that rely on wireless connectivity, according to DHS field intelligence and US media reports.

- (U//FOUO) Some DVEs, adhering to their version of "accelerationism," have threatened communications infrastructure to advance their ideological goals of disrupting government operations to eventually overthrow the US Government. In December 2020, a public instant messaging administrator for a self-described racially or ethnically motivated violent extremist-white supremacist group portrayed a government communications platform for public safety agencies and first responders as a key target and posted facility locations in the Northeast and other parts of the United States, according to DHS reporting derived from social media information.
- (U//FOUO) Separately, misinformation online linking wireless infrastructure—especially 5G technology—to health problems, including the spread of COVID-19, probably has contributed to threats to emergency communications infrastructure, judging from a peer-reviewed academic article and a national media report.[a] In December 2020, an identified USPER confessed to having cut cables or turned off power at multiple cell phone towers in central New York, according to a DHS report based on information from New York state and local police forces and a central New York press report. The incidents disrupted law enforcement and first responder communications in the area. On social media, the subject frequently discusses theories regarding cellular communications and 5G, their use to spread COVID-19, and their negative effect on health in general.

[a] (U//FOUO) For more information on misinformation linking 5G and COVID-19, see DHS Intelligence Enterprise *Homeland Intelligence Article* titled, "(U//FOUO) 5G, COVID-19 Conspiracy Theories Inciting Attacks Against Communications Infrastructure," IA-44214-20, dated 13 May 2020.

(U) Prepared by the Field Operations Division – Northeast Region. Coordinated within the DHS Intelligence Enterprise (CTMC, CYMC, and CISA).
For questions, contact DHS-SPS-RFI@hq.dhs.gov

- *(U//FOUO)* Since April 2020, more than 100 communications infrastructure-related incidents have been reported globally, according to a body of DHS field intelligence reports and US national and state media reporting. Attackers have committed arson, cut cables, shot equipment, and—in Nashville in late 2020—detonated improvised explosive devices, according to the same sources.

(U//FOUO) **Media Coverage Highlights Communications Sector Vulnerabilities**

(U) Media coverage of the 25 December bombing at the AT&T switching center in Nashville, Tennessee, included details about the vulnerabilities of communications infrastructure and the impact on 911 operations, air traffic control operations, and commercial bandwidth connectivity—highlighting how integrated network disruptions negatively impact a wide range of civil institutions and commercial actors. Media reporting about infrastructure incidents in the Northeast region has provided similar information. For example, in January 2021, a single fiber cut near Philadelphia disrupted Pennsylvania State Police lines and 911 centers in 13 Pennsylvania counties for up to 24 hours, according to Carlisle, Pennsylvania, local media reporting.

(U//FOUO) Federal, state, and local authorities and private sector entities can draw on several measures to mitigate against disruptions to emergency communications, as noted in CISA and FBI publications.

- *(U)* Evaluate existing security measures to protect communications infrastructure, including installing appropriate fencing and barriers, cyber-intrusion detection systems, closed-circuit television, and monitoring drone activity near towers.
- *(U)* Develop continuity of operations plans to provide redundancy and backup capabilities in the event of emergency communications disruptions.
- *(U)* Establish clear communications channels to ensure damage or attacks affecting communications infrastructure are reported promptly, including to relevant law enforcement agencies.
- *(U)* Additional resources are available at https://www.cisa.gov/infrastructure-security.

Source, Reference, and Dissemination Information

Source Summary Statement	*(U//FOUO)* We have **medium confidence** in our assessment that recent incidents targeting communications infrastructure in New York and Pennsylvania highlight the enduring threat to this sector and potential for disrupting emergency communications, including from anti-government and other DVEs. Our confidence is derived from DHS intelligence reporting and a body of reliable and corroborating national and local media articles and social media postings about new threat actors targeting communications infrastructure. Additional, credible reporting linking the cited threats to identified violent extremist actors or groups, increases in threatening posts gaining traction across multiple online forums, or indications of advanced logistical preparations specifically targeting emergency communications systems would increase our confidence in this assessment.
Definitions	*(U//FOUO)* **Accelerationism:** Accelerationism is a concept suggesting the existing social order should be pushed to such a degree that Western countries become failed states, giving rise to changes that would reshape the world in radical ways. Domestic terrorists following an anti-government extremist version of accelerationism advocate for acts of social disruption, up to and including violence, and taking violent action to prompt responses that would gain support from those advocating for overthrow of the US Government. *(U//FOUO)* **Anti-Government or Anti-Authority Violent Extremists (AGAAVEs):** Groups or individuals who facilitate or engage in the potentially unlawful use or threat of force or violence with intent to intimidate or coerce, in furtherance of political and/or social agendas, which are deemed to derive from anti-government or anti-authority sentiment, including opposition to perceived economic, social, or racial hierarchies; or perceived government overreach, negligence, or illegitimacy. The mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics may not constitute extremism and may be constitutionally protected. *(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 does not constitute 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)* **Misinformation:** Use of false or misleading information. Misinformation overlaps with some elements of propaganda; it is broader than disinformation because it targets a wide audience, rather than a specific group. *(U//FOUO)* **Racially or Ethnically Motivated Violent Extremists-White Supremacist (RMVE-WS):** Groups or individuals who facilitate or engage in acts of unlawful violence or intent to intimidate or coerce the federal government, ethnic and racial minorities, or non-Christian faiths, and often specifically Jewish persons, in support of their belief in the inferiority of nonwhites and non-Christians.
Civil Rights and Civil Liberties	*(U//FOUO)* US persons linking, citing, quoting, or voicing arguments raised by violent extremists 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 violent extremism absent information specifically attributing the content to malign 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.
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. *(U)* **To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us- cert.gov/report/ and complete the US-CERT Incident Reporting System form.** The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. 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.
Dissemination	*(U)* Federal, state, local, tribal, and territorial authorities and law enforcement and private sector security partners.
Warning Notices & Handling Caveats	*(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 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//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Threats to Emergency Communications in Northeast Region

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//FOR OFFICIAL USE ONLY**