Response Considerations for Increased Threat Reporting to US Telecommunications Infrastructure

SCOPE: This product provides situational awareness to first responders and the private sector regarding continued interest in targeting US-based telecommunications infrastructure.

In dozens of incidents, telecommunication cellular towers were vandalized by arson and employees physically assaulted in Europe in the spring of 2020.[1] The media attention garnered by these incidents and the widespread messaging, to include conspiracy theories, circulated via social media platforms may cause a near-term increase in US-based threat reporting and generate additional interest in targeting US-based telecommunications infrastructure, and possibly its employees. Awareness of this potential threat by first responders and the private sector is paramount for reporting and vetting suspicious activity and threats to ensure scene preservation, chain of custody for potential evidence, and notification of the FBI in the event of a possible terrorism nexus.

- From 1 March to 1 May 2020, there were ten eGuardian[2] incidents reported as either expressed or implied threats or attempted breaches to cellular towers across eight FBI field office areas of responsibility. This was an increase from the three eGuardian incidents reported from 1 December 2019 to 29 February 2020.
- In August 2019, an identified US-based violent extremist discussed in an online chat group a plan to conduct an attack within the United States, to include destroying cell towers. In September 2019, authorities arrested the subject and, in February 2020, the subject pled guilty to the distribution of information related to explosives, destructive devices, and weapons of mass destruction.

CONSIDERATIONS: It is important that first responders remain apprised of the latest tactics, techniques, and procedures, and train for scenarios beyond the routine. For example, violent extremists can use arson in combination with other weapons and tactics to increase the severity of an attack, and it is almost certain the tactic will continue to evolve. Information sharing and outreach by public safety and private sector entities acts as a force multiplier in recognizing and reporting suspicious activity that may disrupt a plot or enhance mitigation of an attack. Engagement supports information exchanges that can increase the safety of first responders and telecommunications personnel by ensuring the reporting, vetting, and investigating of local threats or suspicious activities, and ensure that all partners are aware of the current local threat picture. This interaction will also help to ensure all facets of emergency planning (such as for a disruption in telecommunications) are current, disseminated, practiced, and

[1] These attacks are linked primarily to the unsubstantiated theories claiming 5G technology has negative health implications in conjunction with COVID-19. Individuals unaffiliated with violent extremist ideologies may socialize these unsubstantiated theories, potentially spurring non-affiliated actors to attack infrastructure.

[2] The eGuardian system is a sensitive but unclassified information-sharing platform hosted by the FBI's Criminal Justice Information Services (CJIS) Division as a service on the Law Enforcement Enterprise Portal (LEEP).

10 JUNE 2020
AUTHORED BY NCTC, DHS, FBI

implemented. Established partnerships between the private sector and neighboring state and local fire investigators can be invaluable during investigations.

- **PRIVATE SECTOR:**
  - Reporting indicators of suspicious activity through established reporting mechanisms is a vital step and helps the investigating law enforcement agencies to carefully assess the information.
  - When inspecting telecommunication infrastructure, such as cellular towers, be alert for signs of trespassing, tampering, or vandalism. Nefarious actors are targeting cellular towers, in the United States and abroad, regardless of the technology contained on the tower. Indications of targeting may include:
    - Unusual, repeated, or prolonged interest in or surveillance of a facility;
    - Loitering, parking, or standing in the same location for an unusual period of time or on multiple occasions with no reasonable explanation;
    - Interest in security measures and assets, attention to or avoidance of surveillance cameras, and interest in access controls, doors, gates, or locks; and
    - Out-of-place or unusual items near structures, such as bottles of liquid, and empty or used packaging or materials that could be used to disguise incendiary devices or explosives, or hidden sharp objects (razor blades, needles) which are intentionally placed to injure employees.
  - Telecommunications employees, particularly those working in the field, should maintain awareness of their surroundings for unusual behavior (verbal threats, luring, and surveillance) by individuals and avoid unnecessary advertisement of their occupation while off duty.

EXPLOSIVE ORDNANCE DISPOSAL: The handling of an incendiary device, homemade explosive, or IED may cause detonation, and/or contaminate forensic evidence. EOD and Public Safety Bomb Squad (PSBS) personnel are the best source of information on the ever-evolving tactics and trends in HMEs and IEDs, detection methods, and safety and security measures, underscoring the importance of training and collaboration. To identify EOD personnel in a specific jurisdiction contact Naval Sea Systems Command NSWCIHEODTD at 1-877-EOD INFO (363-4636). To identify PSBS in a specific jurisdiction, contact your local FBI field office at www.fbi.gov/contact-us/field-offices.

- **FIRST RESPONDERS:**
  - Scene preservation is critical to the collection and exploitation of evidence. Photograph and collect physical evidence such items as hate literature, cans of spray paint, graffiti, threatening letters, and symbolic objects of groups.
  - Coordinate with responding fire and emergency medical services personnel until they render the scene safe to enter.
  - Use witness statements, established tip lines, neighborhood canvassing, CCTV video from surrounding areas, 911 calls, security, safety and fire alarm logs, and property records to assist investigations.
  - Properly collect, document, and maintain through a chain of custody threats and violent extremist rhetoric expressed on social media, other suspicious behaviors, and all real-time video of an attack. This evidence can assist law enforcement in identifying individuals of interest, facilitate information sharing between public safety and private sector entities, and then be used in court.

- Efforts to manufacture incendiary devices, homemade explosives, or construct improvised explosive devices may result in telltale injuries requiring medical treatment. Recognize suspicious burns, scarring, or injuries, which when reported, may lead to further inquiry and investigation.
- Exercise extreme caution if you must approach burning explosives. The failed detonation of a homemade explosive or IED may result in a fire rather than an explosion. Burning explosives may transition into a deflagration or detonation.
- Be alert for unusual odors, such as from cleaning solvents, fuel, chemical products, including containers, as well as unusual stains, burn marks, patterns, or discoloration.
- The presence of large or unusual quantities of flammable or multipurpose products, cleaning solvents, repurposed containers or containers that may have had the labels removed, propane canisters, gasoline, or precursor chemicals or production materials in or around the burn area may warrant further inquiries and investigation.

RESOURCES:

- **eGuardian** allows law enforcement agencies to combine new suspicious activity reports (SARs) of incidents like these with existing (legacy) SAR reporting systems to form a single information repository accessible to thousands of law enforcement personnel and analysts directly supporting law enforcement. https://www.fbi.gov/resources/law-enforcement/eguardian
- **If You See Something, Say Something®:** Across the country and in our communities, we share everyday moments with our neighbors, family, coworkers, and friends. We go to work or school, the grocery store, or the gas station. It is easy to overlook these routine moments, but as you are going about your day, if you see something that doesn't seem quite right, say something. By being alert and reporting suspicious activity to your local law enforcement, you can protect your family, neighbors, and community. https://www.dhs.gov/see-something-say-something
- **Nationwide Suspicious Activity Reporting Initiative (NSI):** A partnership among federal, state, local, tribal, and territorial law enforcement that establishes a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information—also referred to as the SAR process—in a manner that rigorously protects the privacy, civil rights, and civil liberties of Americans. https://www.dhs.gov/nationwide-sar-initiative-nsi/online-sar-training
- **DHS OFFICE FOR BOMBING PREVENTION (OPB)** offers training to build counter-IED capabilities and enhance awareness of IED threats is available in traditional classroom settings, online independent study, and virtual instructor-led training platforms. (https://www.dhs.gov/bombing_prevention_training).
- **BOMB MAKING MATERIALS AWARENESS PROGRAM (BMAP)** is a national outreach initiative to promote private sector point-of-sale awareness and suspicious activity reporting to prevent misuse of common household items as explosives precursor chemicals and IED components. (https://www.dhs.gov//bmap)

JOINT COUNTERTERRORISM ASSESSMENT TEAM | JCAT

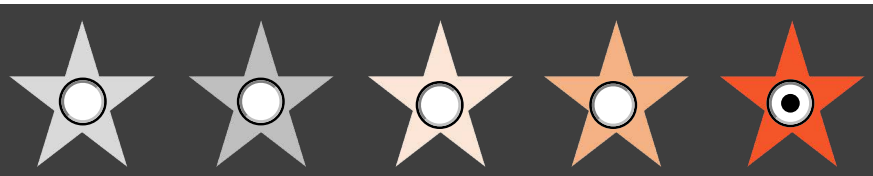
PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and ORG:

DISCIPLINE: ☐ LE ☐ FIRE ☐ EMS ☐ HEALTH ☐ ANALYSIS ☐ PRIVATE SECTOR DATE:

PRODUCT TITLE: NCTC-FBI-DHS (U) First Responders Toolbox - Telecommunications Infrastructure

POOR  GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS.

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT

028706 ID 5-16