Complex Operating Environment: Oil and Gas Pipelines

SCOPE: This product highlights the importance of established partnerships and information sharing among federal, state, local, tribal, and territorial partners and private-sector companies as a critical and essential component to the security and safety of pipelines against terrorist attack.

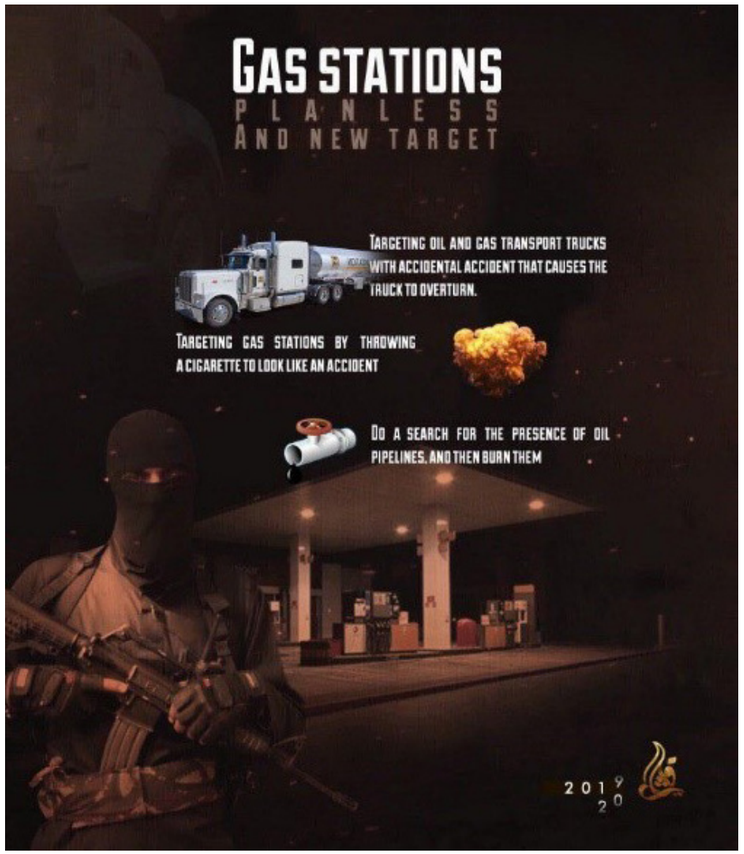
There are over 2.5 million miles of privately owned pipelines spread throughout the United States that transport oil and gas products. While attacks against oil and gas pipelines in the US have been rare (most pipelines are located underground), terrorists have demonstrated interest in targeting easily accessible energy-sector objectives. First responders, public-safety personnel, and emergency managers should be familiar with related stakeholders, infrastructure, and best practices when responding to pipeline-related incidents in their areas of responsibility (AOR).

- In November 2019, a pro-ISIS media outlet released a poster on social media calling on followers to target gas stations, gas tanker trucks, and oil pipelines. The poster encouraged "targeting oil and gas transport trucks with accidental accident [sic] that causes the truck to overturn;" "targeting gas stations by throwing a cigarette to look like an accident;" and "do a search for the presence of oil pipelines, and then burn them."
- In December 2018, authorities sentenced two individuals for planning terrorist attacks against multiple targets, including an interstate pipeline. The individuals referenced the Charleston church and Columbine High School shootings, possessed Nazi literature and mentioned anarchist, and environmentalist motivations for carrying out attacks.

PHYSICAL ATTACKS: Pipelines cover large swaths of often-remote territory, and attacks against them may create a complex operating environment for first responders and other stakeholders. Non-state actors abroad have disrupted pipeline operations using coordinated attacks or by leveraging state-sponsored capabilities; while attempted attacks against pipelines in the US have been more rudimentary.

- In May 2019, Iranian-backed Houthi militants claimed responsibility for attacking two oil-pumping stations for the East-West Pipeline with explosive-laden unmanned aerial systems (UAS) in Saudi Arabia. Pipeline operations were halted temporarily to assess the damage and resumed operations the next day.
- In September 2019, a federal grand jury charged two individuals each with one count of conspiracy to damage an energy facility, four counts of use of fire in the commission of a felony, and four counts of malicious use of fire. The charges were related to multiple incidents in 2017 when the individuals allegedly used oxyacetylene cutting torches to damage exposed, empty pipeline valves up and down the Dakota Access Pipeline across Iowa and South Dakota. The attack did not halt operations.

CYBERATTACKS: Worldwide cyberattacks conducted by both state and non-state actors have become more prevalent, including against the energy sector. Terrorist cyber capabilities are largely limited to nuisance-level disruptions, and terrorists are not known to have targeted pipeline infrastructure with cyberattacks; however, other malicious state and criminal actors have subjected the energy sector to a range of attacks that vary in sophistication and impact.



GAS STATIONS: Image from pro-ISIS media outlet

01 EXTRACTION

Oil and gas must first be extracted from the earth, which can be done on land or at sea. This raw material is then moved to refineries.

02 REFINEMENT

Oil and gas must be refined prior to being used as an end product, and occurs at numerous refineries around the country.

03 TRANSPORTATION

Following refinement of the oil and gas, the product must be transported in order to be consumed by end users. Transportation can occur via pipeline, rail, road, or waterway.

04 CONSUMPTION

Once oil and gas are refined and transported, they are consumed as is or used in the manufacture of other products.

NCTC 036105 ID 2-20

19 FEBRUARY 2020
AUTHORED BY NCTC, DHS, FBI

SECURING PIPELINE INFRASTRUCTURE: Despite the security efforts of many US oil and gas production facilities, including tank farms and refineries, the physical security of pipelines is a challenge for all responsible stakeholders. Public-safety personnel should be familiar with the locations, operators, and contents of aboveground pipeline sections and access points in their AORs. Developing relationships with the owners and operators of these systems will assist with identifying the appropriate response in case of an attack or natural disaster.

INDICATORS OF ATTACK: Terrorists may use a variety of weapons, tools and tactics to carry out an attack on an oil or natural gas pipeline with little to no warning. Furthermore, given the vast area of land covered by pipelines and valves, there may often be no observable indicators preceding an attack; however, basic indicators of a physical attack may include:

- Recent damage to fencing around valve access points, or damage to perimeter lighting, cameras, or sensors
- Loitering or extraneous activity around pipelines in urban areas without a reasonable explanation
- Unauthorized access to secured areas containing pipelines by unknown individuals or unfamiliar service or contract personnel with passable credentials
- Evidence of attempted arson at pipeline sites
- Suspicious photography or unauthorized UAS activity near a pipeline
- Unattended packages or other suspicious items near a pipeline
- Persons with unusual interest in pipeline security measures and access controls

INSIDER THREAT: Terrorists have used insiders to facilitate and conduct attacks, and may view insiders as valuable assets for obtaining vital information, gaining access to targets, exploiting potential vulnerabilities, challenging security countermeasures, and conducting attacks. Insider threats may also come from unwitting or complacent personnel. Best practices to mitigate insider threat include:

- Establish policies, procedures, and training used to detect or deter insider threats
- Establish procedures for reporting suspicious activity within the organization
- Conduct periodic background checks and monitoring of employee access and behaviors indicative of an insider threat

GENERAL CONSIDERATIONS: Response to pipeline incidents may pose challenges due to involvement by multiple public-safety jurisdictions and the private sector, and the remote location of pipeline-access points. First responders should frequently coordinate and collaborate with public-safety and government partners and pipeline and facility operators in their AORs to improve communication, strengthen security, and establish effective response plans.

- Encourage the use of suspicious-activity reporting mechanisms by all stakeholders
- Educate stakeholders of suspicious activity to minimize false reporting or non-reporting of possible concerning incidents
- Ensure all stakeholders are familiar with Incident Command System (ICS) principles and procedures
- Conduct regular meetings or working groups with key pipeline-security stakeholders to discuss issues, threats, and unusual events in the industry
- Actively engage with other agencies, including the local FBI field office, and state and major urban area fusion center to improve awareness of the threat environment and to improve response to an incident
- In the event of an attack, establish a command post that, per established guidelines, is uphill and upwind from any attack and is far enough from the area to avoid impact if the affected zone grows in size
- Use pre-established 'white-hat zones' to facilitate coordination between the first responders and pipeline operators for responses at aboveground locations
- Designate a 'process liaison' positioned at a command post to relay pertinent information, including continual feedback to response actions
- Ensure communications interoperability between first responders and pipeline operators
- Establish mutual-aid agreements and relationships with local hazardous materials teams
- Develop standard operating procedures for disseminating information to the workers, media, and residents
- Work with owners, operators, and users of pipelines to help them understand and coordinate response roles
- Establish familiarization with related facilities through walk-throughs to gain an understanding of normal operations, and hazardous or high value components

USEFUL TERMINOLOGY: When planning for a pipeline-related event, first responders should be familiar with common terminology used in the industry to help prevent miscommunication and breakdown in requests for assistance.

- **PIPELINE:** All parts of a physical facility where commodities specific to pipeline operations, such as natural gas, crude oil, or water are transported.
- **VALVE:** A mechanical device installed in a pipeline that is used to control the flow of a gas or liquid. The types of valves installed and found in pipelines include:
  - **RELIEF VALVE:** A valve that acts as a safety device designed to protect a pressurized vessel or system during an overpressure event.
  - **BLOCK VALVE:** A valve that can be closed to block the flow of oil or gas to isolate a segment of pipeline for maintenance and emergencies.
  - **CHECK VALVE:** A valve that allows liquids or gases in the pipeline to flow only in one direction. Frequently installed in underground pipelines, check valves work by mechanical principle and are therefore harder to identify without previous familiarity.
  - **MAINLINE VALVE:** A type of block valve used to isolate portions of pipeline and to control product flow.
- **OFFSHORE PIPELINE:** Pipelines located off the coast of the US, where large quantities of natural gas and crude oil are produced from beneath the ocean floor. Offshore pipelines transport these products from the offshore production areas to onshore processing plants and pipelines or from onshore processing and storage to offshore export terminals.
- **UPSTREAM:** Activities related to the exploration and production of oil or natural gas products. This includes drilling and other efforts to remove the products from the ground.
- **MIDSTREAM:** The methods of transporting and storing crude oil and natural gas prior to it being refined into fuels or materials used for other everyday products. These include pipelines, pumping stations, gas plants, tanker trucks, and transcontinental tankers.
- **DOWNSTREAM:** The final production process of oil and gas into final products, including fuels and other everyday products. Downstream facilities include refineries, gas processing plants, and distribution terminals.

RESOURCES

- **BUREAU OF TRANSPORTATION STATISTICS – US OIL AND GAS PIPELINE MILEAGE** https://www.bts.gov/content/us-oil-and-gas-pipeline-mileage
- **DEPARTMENT OF HOMELAND SECURITY OFFICE FOR BOMBING PREVENTION (OPB)** https://www.dhs.gov/bombing_prevention_training
- **DOWNSTREAM NATURAL GAS INFORMATION SHARING AND ANALYSIS CENTER (DNG-ISAC)** https://dngisac.com
- **THE EMERGENCY RESPONSE GUIDEBOOK** https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/docs/ERG2016.pdf
- **FIRE DEPARTMENT PIPELINE RESPONSE, EMERGENCY PLANNING, AND PREPAREDNESS TOOLKIT** https://www.nvfc.org/wp-content/uploads/2018/07/FD-PREPP-Toolkit.pdf
- **HOMELAND SECURITY INFORMATION NETWORK (HSIN)** https://hsin.dhs.gov
- **INCIDENT COMMAND SYSTEM (ICS)** https://www.fema.gov/incident-command-system-resources
- **JOINT TERRORISM TASK FORCE (JTTF)** http://www.fbi.gov/contact-us/field
- **THE NATIONAL PIPELINE MAPPING SYSTEM (NPMS)** https://www.npms.phmsa.dot.gov
- **NATIONAL RESPONSE CENTER (NRC)** http://nrc.uscg.mil/Default.aspx
- **PIPELINE ASSOCIATION FOR PUBLIC AWARENESS** https://pipelineawareness.org/
- **PIPELINE EMERGENCY RESPONSE GUIDELINES (2019 EDITION)** https://pipelineawareness.org/media/1537/2019-pipeline-emergency-response-guidelines.pdf
- **STATE AND MAJOR URBAN FUSION CENTERS** https://www.dhs.gov/fusion-center-locations-and-contact-information
- **TRIPWIRE OR TECHNICAL RESOURCE FOR INCIDENT PREVENTION** https://tripwire.dhs.gov

NCTC 036105 ID 2-20

19 FEBRUARY 2020
AUTHORED BY NCTC, DHS, FBI

JOINT COUNTERTERRORISM ASSESSMENT TEAM | JCAT

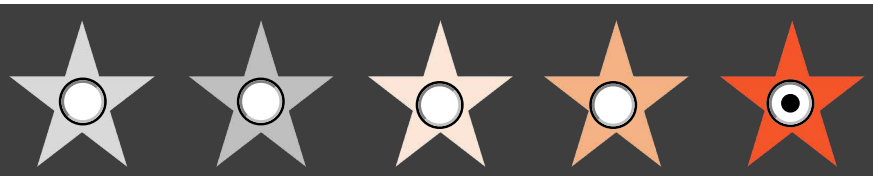
PRODUCT FEEDBACK FORM

(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 Responder's Toolbox - Complex Operating Environment - Oil and

POOR  GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS.

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT