THREATS TO THE OIL AND NATURAL GAS INDUSTRY

FBI Perspective

El Paso Division, FBI

OVERVIEW

- Criminal Activity
  - Permian Basin Oilfield Theft Task Force
- National Security Threats
  - Counterterrorism
  - Counterintelligence

Permian Basin OTTF

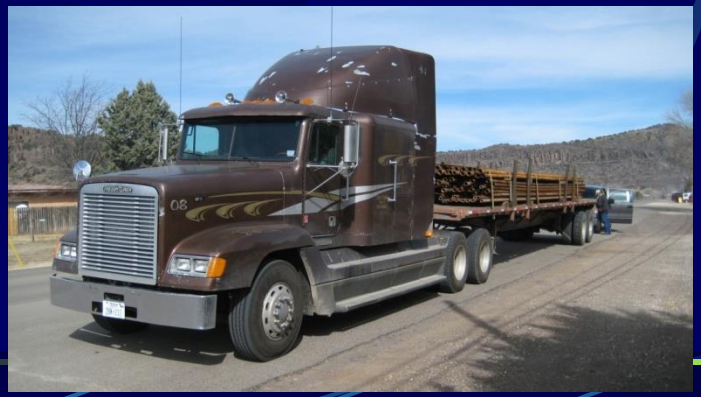
- Created in 2008
  - With Energy Security Council & FBI Assistance
- LEO and Industry Partnership
  - Intel/Trend Exchanges
- LEO Partners
  - Federal, State, Local LEOs
  - TFOs: Ector, Midland, Andrews Counties
  - Enforcing all levels of laws, but TFOs Deputized Federal Officers with jurisdiction extending across the entire Permian Basin

Permian Basin OTTF

- Task Force Mission
  - Continuously gathering and sharing Intel from LEO and Corporate Security
  - Identify patterns and organizations
  - Aggressive prosecutions and asset forfeiture with cooperation of USAO
  - Utilizing advanced techniques
    - Title III (Wiretaps)
    - Undercover Operations

Successes

- Major Equipment Theft
  - Federal Interstate Trans. Stolen Property
  - Federal Penalties/ 10 Years/Fines
  - High Levels of Theft
  - Many prosecutions in Permian Basin



Successes

- Copper Wiring Theft
  - Generator lead wires stolen from a drilling rig.
  - Title 18 U.S. Code 1366 – Destruction of an Energy Facility -
  - 20 Years/ $100,000 Fine
  - In 2010, seven people were successfully prosecuted for the first time in an oilfield case

Successes (cont.)

- Oil Theft Guilty Plea Jan. 2015
  - Federal Law ITSP
  - Creative application of law (Interstate)
  - Federal Penalty up to 10 Years/Fines
  - Theft of 5 tanker loads, $58,000
  - First such prosecution in Permian Basin

Successes (cont.)

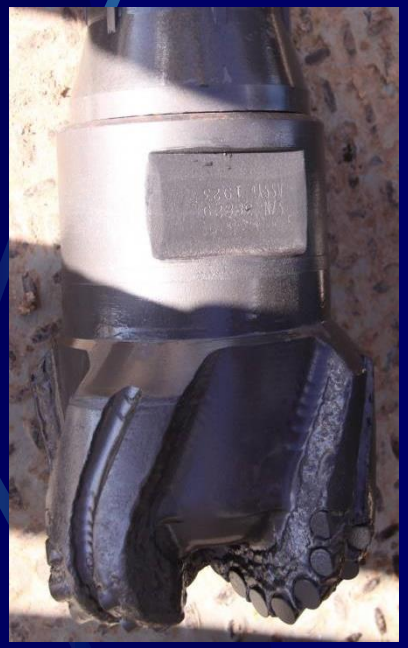
- Permian Basin OTTF Prosecutions 2014 - 2015
  - State Prosecutions 12
    - Theft of Equipment
  - Federal Prosecutions 6
    - Oil & Diesel Fuel Theft, Wire/Mail Fraud
  - Pending Federal Prosecutions 6
    - Mainly Fraudulent Billing, Wire/Mail Fraud

Trending

- Fraudulent Billing for Services
  - Trucking Companies are submitting fraudulent work tickets to the oil companies.
  - Truck Drivers are submitting false run times.
- Trucking companies are emailing and faxing fraudulent work tickets. (Wire Fraud)
- Oil Companies mailing payments based on fraudulent invoices from the trucking companies. (Mail Fraud)

Next Up

- Theft/Resale Drill Bits
  - Federal Law ITSP
  - Concealing Origin; New Serial #s
  - Up to 10 Years/Fines
- Replicate Permian Basin OTTFs in areas
  - Share information across states/regions

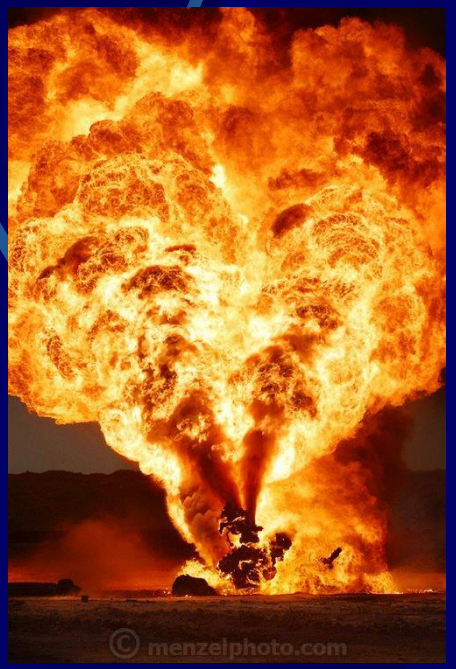


Counterterrorism

- ONG sites can be a target
- Domestic Terrorist Groups
  - Opposed to ONG drilling
  - Try to damage/discredit ONG for Cause
- International Terrorist Groups
  - Disrupt US Economy
  - Create a Major Disaster
  - Press Coverage for Cause

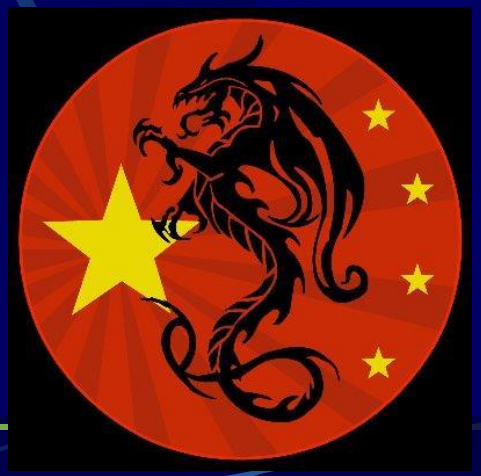
Counterterrorism

- ONG Sites Vulnerable
  - Remote Locations
  - Light/Little Physical Security
  - SCADA System Attacks
- New Trend: UAVs
  - Over-flights of facilities
  - Tank Farms
  - Drilling Sites
  - Possible CT Scouting or Operations



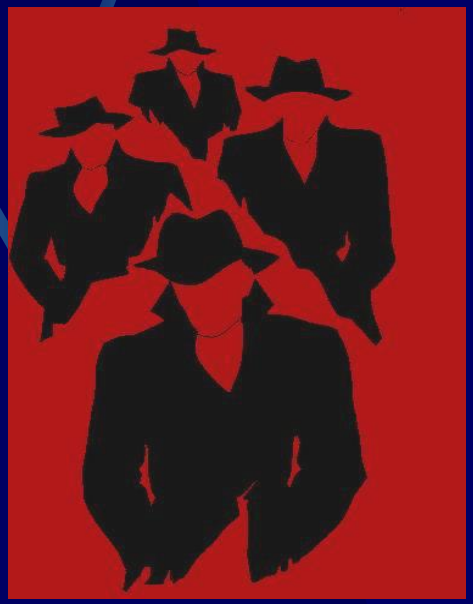
Counterintelligence

- ONG Global Commodity
- It is a National Security Issue for the US and many other countries
- Some countries use their professional intelligence services to assist their companies get the upper hand
- Advantage: Foreign Intel Service



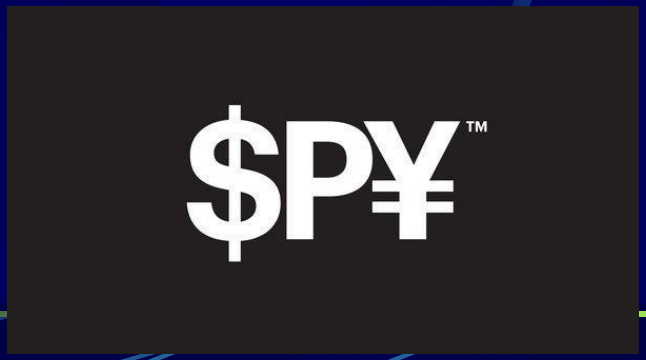
Counterintelligence

- Foreign Intel Service has:
  - The latest equipment
  - Global reach
  - Nearly unlimited resources/funds
  - Multi-pronged attack capabilities
- FIS wants:
  - Proprietary Technology
  - Business Information/Strategies
  - Knowledgeable Employees
  - An Advantage!



Counterintelligence

- FIS Areas of focus:
  - ONG HQ complexes/employees
  - ONG Drilling Sites
  - ONG Distribution Sites
  - ONG Future Expansion Plans/Sites



Joint Business Ventures

- Joint Ventures
- Mergers
- Acquisitions
- CFIUS Transactions
  - Many Energy Deals
- CNOOC/Nexen Deal
  - CNOOC now has access to Gulf Oil Rigs

CNOOC

nexen

A CNOOC LIMITED COMPANY

Economic Espionage

- *"Our foreign adversaries and competitors are determined to acquire, steal, or transfer a broad range of trade secrets in which the United States maintains a definitive innovation advantage. This technological lead gives our nation a competitive advantage in today's globalized, knowledge-based economy. Protecting this competitive advantage is vital to our economic security and our national security."*

Randall C. Coleman

Assistant Director, Counterintelligence Division

Economic Espionage Act of 1996

- Economic Espionage-18 U.S.C. §1831
- "Economic espionage is:
- (1) whoever knowingly performs targeting or acquisition of trade secrets to
- (2) knowingly benefit any foreign government, foreign instrumentalityor foreign agent."
  - Theft of Trade Secrets-18 U.S.C. §1832
  - -Commonly called Industrial Espionage
- "Theft of trade secrets is:
- (1) whoever knowingly performs targeting or acquisition of trade secrets or intends to convert a trade secret to
- (2) knowingly benefit anyoneother than the owner."

Oil and Natural Gas Intellectual Property and the Threat

- Oil and natural gas intellectual property (IP) includes a company's trade secrets, proprietary information, and research.
- This ranges from drilling equipment to pipeline insulation, which if stolen could result in lost revenue, lost employment, damaged reputation, lost investment for research and development (R&D), and interruption in production.

Organizational Factors

- The availability and ease of acquiring proprietary, classified, or other protected materials. Providing access privileges to those who do not need it.
- Proprietary or classified information is not labeled as such, or is incorrectly labeled.
- The ease that someone may exit the facility (or network system) with proprietary, classified or other protected materials.
- Undefined policies regarding working from home on projects of a sensitive or proprietary nature.

Organizational Factors

- The perception that security is lax and the consequences for theft are minimal or non-existent.
- Time pressure: Employees who are rushed may inadequately secure proprietary or protected materials, or not fully consider the consequences of their actions.
- Employees are not trained on how to properly protect proprietary information.

Behavioral Indicators

- Without need or authorization, takes proprietary or other material home via documents, thumb drives, computer disks, or e-mail.
- Inappropriately seeks or obtains proprietary or classified information on subjects not related to their work duties.
- Interest in matters outside the scope of their duties, particularly those of interest to foreign entities or business competitors.
- Unnecessarily copies material, especially if it is proprietary or classified.

Behavioral Indicators

Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or unreported overseas travel.

- Short trips to foreign countries for unexplained or strange reasons.
- Unexplained affluence; buys things that they cannot afford on their household income.
- Engages in suspicious personal contacts, such as with competitors, business partners or other unauthorized individuals.

Best Practices to Make A Difference

- Educate and regularly train employees on security or other protocols.
- Ensure that proprietary information is adequately, if not robustly, protected.
- Use appropriate screening processes to select new employees.
- Provide non-threatening, convenient ways for employees to report suspicions.
- Routinely monitor computer networks for suspicious activity.

FBI Role

- The FBI can identify what global economic and environmental trends may motivate individuals to steal your intellectual property, improving your outward considerations on what items make you a target of, and more vulnerable to, economic espionage.
- The FBI can provide notice of potential security concerns when partnering with suspicious domestic and foreign companies. This ensures business deals meant to increase energy efficiency, diversify supply, and invest in energy production honestly contribute to the future of your business.
- The FBI can provide threat awareness information for consideration during multiple phases of domestic and foreign company partner engagement to assist in ensuring the fidelity of the business relationship.

Questions?