Security staff outside an oil plant checks a pipeline.

Physical Threats to Pipeline Critical Infrastructure

By **Vincent Maloney,** Founder, **Patriot Pipeline Safety, Corp.**

As the globe emerges from its first pandemic in about 100 years, tensions among individuals and governments are high. The existing energy infrastructure is targeted for change. As a colleague once noted, "We did not leave the stone age because there were no more rocks." Yet, the civility of any transition is a choice.

As the oil and gas industry in the United States again adjusts to social, political and financial pressures with strategic and systemic changes, it is essential that the fundamentals of protecting existing and developing assets remain a priority.

The importance of physical threat awareness toward critical pipeline infrastructure has never been greater. Safeguarding against physical threats are just as important, if not more important, as cyber-threats to protecting our nation's pipeline systems, terminals and facilities.

The intent, technology and geopolitics of people who intend harm vary in name and motivation, but they are similar in a goal of disruption. While a project is under development or in construction, disruption players may include environmental extremists, climate activists, threat actors or protestors. Because of the magnitude and expense of damage, some categorize these groups as terrorists or eco-terrorists.

For projects in service, threats can include disgruntled employees and intoxicated thrill seekers. And moving forward from the pandemic, sanctions and shifting alliances across the globe create a new web of potential retaliation targeting U.S. infrastructure.

No matter what the source of the threat, it is critical that public safety and energy supply remain safeguarded by vigilance against attacks to our nation's pipeline infrastructure, including protection against physical threats.

Reframing the analysis of security as a pyramid, rather than bowtie approach, more accurately depicts the concern; physical pipeline security is the foundation. As we look at the landscape for security of our nation's infrastructure, we see a growing focus on cybersecurity in the discussions. Prioritizing cyber-threat over physical threat is risky for a number of reasons:

- Cybersecurity is not a comprehensive deterrent, and in some instances a physical attack may be the preferred approach over cyberattack by groups or individuals focused on disrupting energy transportation.
- Information technology (IT) is specialized, in part due to the ever-increasing complexity of the field; consequently, many professionals involved in cybersecurity solutions have nominal experience working on or around the very infrastructure they are attempting to secure.
- The multidisciplinary approach required to accurately dissect a SCADA system for a potential breach is challenging to assemble and execute.
- For disrupters seeking media attention, physical attacks are more visible. Even if a pipeline system did experience a cyber-attack or intrusion on its operations, there are mechanical and pneumatic systems independent of the SCADA systems that protect the pipeline from catastrophic failure.

- Assuming that the risk of "getting caught" in the execution of cyberattacks and physical attacks is similar, then physical attempts may be the preferred approach by disrupters who do not use the internet as their primary weapon. Cyberattacks leave evidence of code that is available for analysis by forensics; physical attack frequently incinerates the evidence, making it more potentially difficult to discern between intentional and accidental events.

While IT and ensuing potential cyberattacks are indeed evolving at an unprecedented rate, preparation against physical attacks remains the bedrock on which a security program should be laid and maintained.

Evolution of Opposition

Major construction of our current pipeline systems began during and post-WWII in an entirely different regulatory framework, and much of the U.S. population were galvanized to focus on growth.

It was the age of America's love affair with the automobile and new roads, the advancements of plastics, suburbs and strip malls. It was post-War America celebrating a thriving economy with new technologies, homes and travel. This took energy to make possible, and oil and gas infrastructure was a welcomed solution to accommodate America's growth.

Miles of pipelines constructed between 1945 and 1975 still span across America's heartland and cities today. Post-War America was a time for production, and energy companies rose to the challenge to meet America's growing energy demand as quickly as possible. Pipeline engineering and design was influenced by this time frame when, in general, America strongly supported the expanding energy infrastructure.

Change is inevitable, societies evolve and today we live in a different world than when large spans of pipeline infrastructure were constructed. Even though new pipelines are built with stronger coating and steel, increased safety in engineering, improved inspection design, cutting edge emissions technology and better construction practices than initial infrastructure build out, they are deemed a hazard to the environment by disrupters.

Some disrupters consider maintenance and growth of pipeline infrastructure to be an impediment to the advancement of alternative energies, concluding these projects must be shut down by any means possible. And while the environmental regulations have been effective in prohibiting the widespread pollution that led to rivers catching fire, there is a gap of appreciation for the transportation of feedstock to refineries that ultimately provide the plastic for modern necessities, e.g., cell phones for communication and tires for vehicles.

Similarly, there is a gap of appreciation for the cheap, reliable energy that allows power plants to consistently charge these same phones and contribute to internet connectivity. Today in the quest for change, a line is being drawn in the U.S. where supporters for renewable fuels and proponents of existing fossil fuels tend to stand on separate sides.

Opponents to pipelines, exacerbated by generational age gaps, do not fully consider the roles that transporting fossil fuels play in millions of people's daily lives. In general, emotionally driven opposition lacks technical understanding and recognition of the significant harm attacking pipelines could do to cities or rural communities.

The merits of alternative energies versus current reliance on fossil fuels are important to the security discussion because the schism has intensified dramatically in the last five years. While protests against pipeline projects have been around for decades, it is the last five years that has really brought this conversation to the front headlines.

Initially, protesters began disturbing pipeline projects under construction. These disturbances have intensified as certain environmental groups have matured in size and funding. They've also become more organized through shared goals and use of social media tools. With every pipeline construction season, these organizations have expanded their understanding of construction practices and pipeline operations to meet their goals of disturbance, and even shutdowns, to both pipelines in operation and major mainline projects under construction.

Unfortunately, the disrupters seem to have advanced in knowledge faster than many energy companies have developed the preparations and actions necessary to understand and counter these threats.

The volumes written about "conflict resolution" apply to pipelines; conversations by opposing parties break down, or violence erupts due to poor structure and organization. Violence and acts of physical disturbance have impacted innocent protestors, companies and workers.

Acts of extreme equipment vandalism, harmful physical altercations and acts of vandalism or terrorism on pipelines new and in operation occur. To make matters worse, the news media is influenced to report what will fuel ratings. For high-profile pipeline development projects, the realities of interactions between companies, workers and resistance groups on projects rarely are reportedly accurately on the nightly news.

There have been peaceful demonstrations reported for the violence, and violence has been reported where peace prevailed. Consistently, however, the external public never really receives the most accurate, more mundane, depiction of the situation.

Cyber vs. Physical

Cybersecurity is newsworthy and often depicted as the primary focus for protecting critical forms of infrastructure, including pipelines. Similar to some environmental issues, the IT industry in the United States has focused on self-regulations to address the lagging regulatory framework to identify and prevent cybersecurity threats. Consequently, much cybersecurity expertise lies in the IT private sector.

What is the risk to pipelines from cyberattacks? In the past, it has been phishing emails, surveillance breaches and worker identity risks. While there have been "proof of concept" attacks on other utilities, actual threats to SCADA systems to date fortunately have been minimal. However, security has the same critical flaw as safety metrics – are the numbers low because the incidents did not occur or because the measures in place were successful and deterring the occurrence?

Like the most successful safety program, successful security programs have no incidents to report. Similar to the continuous monitoring of pipeline systems for leaks, there are human equivalents conducting analytics for cyber-breaches. Surveillance is effective, and, consequently, if an attack to a pipeline's communications did occur, the likelihood of the cyber-attack being discovered in its infancy is comparatively high relative to a physical attack lacking similar vigilance.

The threat of physical attacks is amplified both by the lack of technical sophistication required to execute them and, ironically, enhanced by location technology that has evolved to mainstream. Location technology providing recent photographs of pipelines and electrical transmission systems exposed in remote areas are now public information.

Details that were once filed as "Critical

Energy/Electric Infrastructure" (CEII) according to the Federal Power Act are readily and publicly available via simple software downloaded on personal cell phones. In the midst of focusing on revamping the nation's infrastructure, perhaps it is also important to evaluate the effects of federally protected infrastructure deemed CEII evolving to become publicly available and potentially expendable.

Physical Attacks

Physical threats and physical attacks are growing in occurrence due to their benefits and simplicity over cyber-attacks. Many exposed facilities lack adequate protection and are not monitored for physical security because the purpose of production, or age, or work environments have changed.

When many of the systems were constructed, more employees were needed to operate them by physically adjusting pipeline parameters to changing weather conditions. Today's pipelines transport more energy with less resources in the field due to automation in operations, budgets and changing business models.

Existing field staff are time-constrained by increased administrative duties, multidisciplined responsibilities and training that keeps the employee out of the field where they historically provided physical surveillance for the pipelines. Employees not in the field equates to less monitoring and increased risk.

Unfortunately, the reasons to physically harm a pipeline fit many objectives for both domestic and foreign parties. Local environmental groups, tasked with saving the environment, are becoming more sophisticated with their techniques to impede pipeline maintenance and operations, even though harming pipelines can be catastrophic to the environment.

Physical disruption to critical pipeline infrastructure aligns with strategic goals by disrupting the reliance on fossil fuels. The consequences of disruption on energy transportation during peak usage, which correlates with extreme weather and densely populated regions, is severe. Physical disruption can also impact exporting capabilities, which harms the domestic upstream market.

Physical pipeline attack is an effective means to impact commerce, navigable waterway transportation, public transportation, rail roads and electrical grids. If approached with the intent to disrupt or harm multiple forms of critical infrastructure at the same time, a physical pipeline attack would create devastating harm to the U.S. economy.

Many companies have been working behind the scenes to build on working relationships with private and government organizations to address this growing concern. Task force teams and committees are meeting to discuss the latest threats, social media buzz, technology benefits, risks and networking.

Difficult lessons have been learned about project security and operation security for pipelines. These lessons have been shared across the industry as many companies share the same common goals for prevention. Furthermore, tailored security approaches are being implemented to increase surveillance on assets deemed critical to their operations.

Mitigating Attacks

Pipeline operators are also advancing on their relationships with the Pipeline and Hazardous Materials Safety Administration (PHMSA) and the Transportation Security Administration (TSA) in this arena. There are growing field relationships that are sharing knowledge, information and resources to identify and prevent physical attacks.

Proactively developed websites for the general public discuss the facts of new projects to offset the perpetuation of misinformation. Energy companies are making more efforts to provide resources for the public to study so they can make an educated opinion and decision about a project in their area.

Benefits of tying field experience to public relations for public meetings include a resource to immediately address technically difficult questions that are asked by the public. The responses detail visual and acoustic changes created by the project, and why those design decisions were made.

In the same way it takes a hacker to deter a hacker for IT, experienced field pipeline staff are required to dissect the possibilities of a physical attack. It takes years of working field experience to be able to carry out a quality physical risk security vulnerability assessment, one that helps companies improve actual weak areas along their pipeline system. For a host of reasons, each segment of pipe is a little different.

Pipeline companies nowadays are increasing drone operations to increase surveillance for environmental compliance. As drone ranges increase, they can also be used when staff are not available. Drones are also increasing pipeline right-of-way patrols to better monitor their assets and to meet the increasing threat toward our nation's pipeline infrastructure. This helps protect current infrastructure until energy transitions.

Tomorrow

The evolution of pipeline opposition in the United States includes both a shifting attitude and demographics. Simultaneously there is a movement away from the benefits of fossil fuels during a period of social unrest and focus on change.

While some states in the United States have set lofty goals to end the use of fossil fuels in as little as five years, this timeline does not detail a systematic or uniform process by which this transition can occur. This nation's fossil fuel infrastructure evolved over many years alongside the development of safety and environmental regulatory framework.

Supplanting fossil fuels with alternative and sustainable energy without impacting low-cost electricity and fuel or compromising reliability will be a challenge. And while financial incentives and manpower are addressing these issues in tandem, the potential increase of disenfranchised individuals and governments create physical and cybersecurity risk for the existing energy infrastructure.

In conclusion, a responsible transition to renewable energy will take time, and it is important that this transition is proactive and not reactive. The energy industry must continue to prioritize the safety of the public in the approaches to this new landscape, and the focus on service must accompany renewable energy's approach to support a reasonable transition, with practical goals, to progress to a cleaner future.

To be blunt, before closing that valve on fossil fuels, all parties should be very sure renewable energy can support the way we live. ***P&GJ***

Author: Vincent Maloney *started in pipeline operations with Midwestern Gas Transmission before pursuing a career in the pipeline construction industry with Minnesota Limited in 2012. He founded Patriot Pipeline Safety Corp., a resource for pipeline safety and industry-related damage prevention innovations.*

Attacks on US Pipelines

These instances of physical attacks on pipelines and other forms of vital energy infrastructure to date, both in construction and operation, provide an indication of the heavy financial impacts that would be levied by a strategic attack in the United States.

This list is not comprehensive. Omissions include the multiple attacks that have damaged pipeline integrity in the United States in the last five years, and the well-documented bombing attacks in the 1990s and 2000s to pipelines in British Columbia and Alberta, Canada.

It also excludes the regular attacks on pipelines that take place in war zones in the Middle East, and attacks on pipelines by disenfranchised populations in Mexico and Nigeria.

Feb. 19, 2021 – Suspicious packages were thrown onto the Enbridge Line 3 construction site during construction in Minnesota. Improvised explosive devices (IEDs) were fake, but disturbance to work and valuable resources resulted.

Dec. 26, 2020 – A Federal Bureau of Investigation (FBI)-classified intentional attack occurred near Aspen, Colo., on three unsecured Black Hill Energy facilities, shutting off gas to 3,500 homes.

March 13, 2017 – A hole was torched through Energy Transfer aboveground mainline valve in Iowa before it was purged. This was one of multiple attacks that week on the same system.

Feb. 27, 2017 – Sabal Trail Pipeline Project in Florida. Armed shooter James Marker shot at and damaged a portion of pipeline to be installed with workers on the right-of-way. The suspect was later shot and killed by law enforcement.

Oct. 11, 2016 – Five activists trespassed onto property owned by five different pipeline operators, cut locks and chains on valves, and turned valves to the closed position with a 10-15-minute prior warning to pipeline operators. All were arrested.

April 16, 2013 – A sniper attacked the PG&E Metcalf, Calif., substation, causing 17 electric transformers to be destroyed, damaged electronics and leaking oil.

Aug. 7. 2011 – An Oklahoma man placed a homemade IED on a natural gas pipeline at Enerfin Resources substation and then turned himself into law enforcement.

October 2001 – A man fired a piercing bullet into the Trans Alaskan Pipeline, spilling about 300,000 gallons of crude oil.

Feb. 15, 1978 – An IED was successfully detonated on the Trans Alaskan Pipeline. An estimated 12,000 to 14,000 barrels of crude oil were released.

PIConfluence
AN ENERACT COMPANY
Optimize Stakeholder Communication
Use Program Suite To Gain Valuable Stakeholder Feedback
POEMS CERTIFIED
Learn More About Our Tools →
PIConfluence.com/schedule-demo/
Summary Statistics
Storage Risk Matrix
Top Wells with Highest Risk
POF Distribution
Risk Distribution
COF Distribution
MacBook Pro