DRK Insight - A Strategic Target: Oil and Gas Pipelines

Key Takeaways

Oil and gas pipelines and their major components- specifically pumping and compression stations- are new Achilles heel of energy sector and are vulnerable to attacks in a wide spectrum.

An incident or an act of terrorism - physical or cyberattack- on energy infrastructure would not be unexpected under the current security environment, if happened, would result in a potentially devastating circumstance not only for the region it passes through but also globally.

A short review of the situation

Today, despite the significant rise of renewables and other alternative energy sources, statistics show that fossil fuels will remain their dominant position in global energy mix. In such a context, where we are still living in a fossil fuel world, having the control over energy resources (mainly over oil and gas) is still considered to be an essential dimension of "power".

Lately, transportation via pipelines became primary since the technologic advances lower the costs. Also, flow rate and security gave the privilege to pipelines over other transmission methods. Besides the abundance or scarcity, their concentration and location of energy resources; the discussion on oil and gas pipelines and their resilience problematic bring Oil & Gas transportation sector under sharp focus.

Oil and gas pipelines and their major components- specifically pumping and compression stations- through which about 40% of world's oil flows are new Achilles heel of energy sector and are vulnerable to attacks that could disrupt services and negatively impact economy mainly because the lines are too long, they pass over more than one country, and are managed by the private sector. Also, attackers find the lines attractive due to their effect on the international economy and politics. The companies that control the lines consider as immense power, and by attacking them, they can expose easily. Moreover, the damage will be huge.

According to the University of Maryland's Global Terrorism Database, terrorist threats targeting oil and gas sectors have risen sharply. More precisely, during the mid-1990's, attacks on oil and installations reflected less than 2.5 of all attacks whereas in 2013, 600 out of 2600 total terror attacks targeted oil and gas sectors.

For example, between 2003 and 2007, 449 pipeline attacks were reported in Iraq. Additionally, 67 major pipeline attacks were reported in Columbia between January and

June 2012. Similarly, attacks on Yemen's pipelines cost $US 15m per day in 2012.

As seen in the examples above, even an incident is an act of terrorism or sabotage, a small attack on pipelines could have devastating and expensive consequences.

For instance, in October 2001, a single gun-shot caused a leak of 285,000 gallons of oil spill from Trans-Alaska Pipeline. The clean-up took several months, and cost estimated $13 million. Another figure is explaining the cost of repairs to USA Onshore Pipelines according to 2004's prices as below:

Cost of Repairs to USA Onshore Pipelines

Repair	**Cost (Prices 2004), $million**
Repair (non-leaking) to the gas pipeline (depends on whether the supply is interrupted)	$20,000 to $40,000
Repair (leaking) to the gas pipeline	~$200,000 to $400,000
Major Failure to Gas Line	~$5,000,000

Source: Penspen Integrity Virtual Library, 2008

As such while there haven't been major incidents involving a cyberattack on the pipeline infrastructure, the risks are increasing exponentially. A major cyberattack on energy infrastructure would not be unexpected under the current security environment, if happened, would result in a potentially devastating circumstance not only for the region it passes through but also globally.

As a quotation from a November 2015 survey issued by security vendor Tripwire, ''The 82% of oil and gas industry respondents in USA reported their organizations experienced an increase in cyberattacks over the previous 12 months. Additionally, 53% of respondents stated that the rate of cyberattacks had increased between 50% and 100% during that same period. The survey noted further that almost seven out of ten respondents indicated a lack of confidence in their organizations to detect and stop attacks. Potentially, these intrusions could result in millions.''

How to Manage the Risks and Protect Oil and Gas Infrastructures

Even though, empirical data and researchers show that there is an apparent link between energy resources, infrastructures and existing conflicts, making a typology and taxonomy to understand the main reason is challenging and it requires a case-specific approach for analyzing each incident.

As various researchers pointed out, energy resources or infrastructures could be the primary objective in a conflict or could be used as a tool to increase the tension or gaining political or economic leverage in a conflict. Furthermore, terrorist organizations have always been interested in targeting oil and gas facilities. Striking pipelines, tankers, refineries and oil fields accomplishes two desired goals: undermining the internal stability of the regimes they are fighting, and economically weakening foreign powers with vested interests in their region.

Consequently, the protection dimension of the energy infrastructure needs a coherent and holistic security strategy. Mechanical approaches like using CCTV, balloons, drones, fences, barriers may have a critical role in security nevertheless they could sometimes remain limited and could be easily

disabled. On the other hand, responding the non-traditional and hybrid threats by employing the traditional security measures is very difficult, and a new security mindset for the energy industry is required. In this regard, in responding these unconventional threats, the solution should not be solely technical, social tactics should be included in a multilayered protection approach. For example, partnering with all stakeholders and recognizing the requirements and characteristics of local communities as well as implementing some social projects could give a tactical advantage for defenders.

Finally, conducting a threat assessment and risk and business impact analysis seems to be a pre-condition in securing the critical assets where multiple scenario-based and **Business Continuity** Management approaches could have a crucial role in the development of the strategic security plans.

''With the courtesy of Ms. Ayhan Gucuyener-freelance analyst on energy security''