



# Terror on the Home Front

How real is the threat to America's oil and gas infrastructure, and what's being done to protect it?

## From the French tanker set ablaze off the coast

of Yemen in October 2002, to repeated explosions and fires along the critical pipeline that exports oil from Iraq's northern Kirkuk fields, Americans have gotten used to seeing terrorist attacks on vital energy infrastructure components overseas. But what about here? How vulnerable are U.S. pipelines and refineries in this new age of terrorism? Perhaps more important, what's being done about it?

The Sept. 11, 2001 attacks on the World Trade Center and the Pentagon served as a stark wake-up call that the United States is not the safe haven from terrorism that many Americans believed it to be. The United States has enemies that have declared their intention to inflict damage on this country and its way of life, and they have demonstrated their capabilities to do just that. With little doubt that they will attempt to strike again in the future, the question becomes, what will their targets be?

David A. Moore, president and CEO

of AcuTech Consulting Group, a division of Chemetica, Inc., based in San Francisco, notes that the bulk of the attacks taking place in Iraq are targeted to specific pipelines and facilities, suggesting that terrorists pick their targets for strategic reasons. "The targets are revenue-generating facilities, and taking them offline disrupts not only the flow of oil, but the flow of money as well," he says.

The consistency and persistence of the attacks seem to bear out Moore's theory. Prior to the start of the war, Iraq's northern pipeline pumped one million barrels

# “It would take a massive attack on systems to seriously disrupt the flow

of oil a day to the Turkish port of Ceyhan, less than half of the country's prewar oil exports of 2.4 million barrels a day. Disabling the pipeline would wipe out \$7 million a day in revenues. In just the first month after the pipeline resumed pumping oil, saboteurs hit it on four separate occasions with attacks intense enough to shut it down.

Paul Bremer, the top U.S. administrator in Iraq, initially had hoped the country's oil exports could return to prewar levels by October 2004, and U.S. officials had been counting on Iraqi oil revenues to finance reconstruction efforts. However, the difficulties of exporting oil are driving up costs, and increased security risks have slowed plans by U.S. oil companies to open offices in Iraq — all of which suggests that the terrorists' approach of strategic targeting has been effective.

To be sure, the situation in this country is vastly different. One million barrels represents less than 5 percent of the United States' daily consumption of oil, and the infrastructure that supplies it is vast, diverse and in some cases redundant. Still, security experts consider pipelines, refineries, depots and other oil and gas facilities to be attractive targets to terrorists, and industry participants are working with government agencies to strengthen security measures.

## Taking the Threat Seriously

While it is unclear whether the attacks in northern Iraq are the work of Saddam Hussein loyalists or foreign terrorists, there is no question about the intentions of at least one terrorist group to attack energy sector infrastructure around the world. In a June 2003 article, *Jane's Intelligence Review* cited recent attacks against the petroleum supply chain, such as the

bombing of the French-flagged supertanker *Limburg* off the coast of Yemen, as proof that Al-Qaeda's call to target the oil industry is “more than mere rhetoric.”

Both the U.S. government and private sector companies in the oil and gas industry are taking the threat seriously. In the document detailing its national strategy for homeland security, the White House acknowledges that protecting America's critical infrastructure is “a formidable challenge,” one made more difficult by our open and technologically complex society. The only realistic way to meet that challenge, it concludes, is through a cooperative effort between the public and private sectors.

Reports from the U.S. State Department and the Federal Bureau of Investigation confirm that the oil and gas industry is targeted by various terrorist groups. According to the American Petroleum Institute (API), the industry is subject to these threats primarily because of two factors:

- ▶ The physical and chemical properties of the materials processed, stored and handled at the industry's facilities may create attractive targets for terrorists to cause malicious release with the intent to harm a neighboring population
- ▶ The critical importance of the products supplied by oil and gas companies to the domestic and international infrastructure and to other businesses and individuals may make disruption of operations of the petroleum industry an attractive option.

The U.S. petroleum industry is made up of five broad segments: exploration and production, refining, transportation (liquids), marine transportation, and distribution and marketing. The level of threat terrorism poses to individual segments varies, as does each segment's

degree of vulnerability. Like most businesses today, the petroleum industry relies heavily on its information technology infrastructure, and that is treated as a separate security issue.

“The lion's share of our critical infrastructures and key assets are owned and operated by the private sector,” the White House notes in *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. “Moreover, in the present threat environment, the private sector generally remains the first line of defense for its own facilities.”

## Mining Global Experience

The petroleum industry is probably better prepared to meet the President's call to serve as a first line of defense against terrorism than many of its private sector counterparts. Historically, oil and gas companies have maintained facilities and work forces all over the world, and they have garnered valuable experience working in politically unstable countries where security is a constant concern.

In the wake of the 9/11 attacks, industry participants have doubled and tripled their commitment to protecting installations, workers and surrounding communities from the threat of terrorism, notes the API. The industry now has weekly consultations with the U.S. Department of Homeland Security, the FBI and other government agencies that provide intelligence and information about specific and general threats of attack.

A key element of its stepped-up efforts to protect energy installations from terrorist attack is a document called “Security Guidelines for the Petroleum Industry,” which it developed in close cooperation with the U.S. Department of Energy and other government agen-

# a number of pipeline of energy. ”

cies. The document serves as a roadmap for managers to use in assessing vulnerabilities of pipelines, terminals, refineries and drilling platforms.

Terrorist threats against the oil and gas industry fall into seven distinct categories, according to Tamara Makarenko, a researcher at the Centre for the Study of Terrorism and Political Violence at the University of St. Andrews and author of *The Crime-Terror Nexus* (C. Hurst & Co. Publishers Ltd., December 2003). Makarenko also serves as a special advisor to *Jane's Intelligence Review* on systematic transnational crime.

The seven threat categories are pipeline bombings; other pipeline sabotage; attacks on corporate offices of oil and gas companies; attacks on depots, refineries and retail outlets; hijacking of energy installations, accompanied by the taking of hostages; direct, armed attacks on oil and gas facility personnel; and kidnappings of oil and gas company personnel. Among all categories of terrorist threat to the oil and gas industry, pipeline bombings are the most common, Makarenko says.

While there have been few recorded acts of sabotage against U.S. petroleum pipelines, there is little reason to believe they would be any less attractive a target to terrorists in this country than they are in other parts of the world. Indeed, the Federal Energy Regulatory Commission has taken steps to limit access to information about the location of pipelines and other energy infrastructure facilities — information that had been freely available on its Web site to anyone prior to October 2001.

“The oil pipeline network is a valuable national asset and the irreplaceable core of the U.S. petroleum transportation system,” acknowledges Marty Matheson,

general manager for pipeline issues at API. “Oil pipeline shipments account for 17 percent of all domestic freight in the U.S.”

He points out, however, that from a security standpoint the pipeline network is diverse, flexible and widespread. “An attack on one pipeline would not disrupt the system,” Matheson says. “It would take a massive attack on a number of pipeline systems to seriously disrupt the flow of energy. Even then, most damage to pipelines can be quickly repaired. So the chances are that the U.S. economy would not be harmed by a single terrorist attack on a pipeline.”

With about 55,000 miles of crude oil trunk lines, 30,000 to 40,000 miles of smaller gathering lines and 20,000 miles of natural gas lines, the U.S. pipeline network is the largest in the world, according to the Association of Oil Pipe Lines. It is about 10 times the size of the pipeline network that serves all of Europe, and it accounts for 68 percent of total domestic shipments of petroleum.

That size and diversity are a limiting factor on the scope of the damage likely to result from a terrorist attack on a pipeline. Even so, Matheson is quick to note, “That is not to say that the industry is not doing everything it can to protect itself.”

In July 2002, API published “Guidelines for Developing and Implementing Security Plans for Petroleum Pipelines.” Safeguards have been installed to beef up physical security and also to protect against attacks on the sophisticated com-



puter systems that keep fuel surging through the pipelines.

“Background checks on new employees and visitors to pipeline control centers have been improved,” Matheson says. “The industry also was instrumental in establishing an Energy Information Sharing and Analysis Center, which is a computerized system for instantly passing intelligence reports about possible attacks to companies that need the information.”

## ‘Valuable and Vulnerable’

The pipeline industry has a long history of partnering with the federal, state and local agencies that regulate it on security matters, and that partnership has intensified since Sept. 11. The Department of Transportation (DOT) has established a system of seeking assurances from pipeline operators that they have assessed their vulnerabilities and are improving all aspects of their security to the greatest extent possible.

“As of last April, DOT’s Office of Pipeline Safety had received security cer-

# “A greater challenge lies in the and the possibility of an ‘electronic



tifications from operators covering 95 percent of the U.S. pipeline system,” Matheson says. “More recently, the Office of Pipeline Safety has been inspecting facilities to verify steps taken to protect them against possible attacks.”

AcuTech’s Moore believes the cooperative approach between government and industry and the self-driven methodology being used to enhance security efforts is the right way to go. “The operators know their own facilities best — what is most valuable and what is most vulnerable. Companies are doing all sorts of things to improve security, from physical security and closed-circuit TV monitoring to intrusion protection and guard force enhancement to cyber-protection,” he says.

The starting point for all types of oil and gas facilities in this area should be a

formal security vulnerability assessment (SVA), and that is the approach API has adopted in its guidelines. (See “Anatomy of an SVA,” p. 15.) “An SVA is systematic and thorough, not just a walk-around,” Moore explains. “It steers you to a facility’s areas of greatest vulnerability and forces you to recognize them. If a target is both valuable and vulnerable, an SVA is even more important.”

One segment of the U.S. energy infrastructure that falls into that “valuable and vulnerable” category is oil refineries. Bobby Gillham, manager of global security for ConocoPhillips and sector coordinator for energy in the government-industry partnership to protect critical infrastruc-

ture, does not view pipelines as particularly vulnerable, but refineries are another story.

“In the past 20 years, the number of refineries has been halved,” he says. “Add to that the boutique fuels requirements and federal rules that require specialized gasoline formulas to be used in certain areas, and you have a situation where if one or two refineries are knocked out, plants in other areas may not be able to pick up the slack.”

Refinery operators can reinforce existing security measures to protect the perimeters of their facilities — by building additional barriers, increasing electronic surveillance and controlling access more tightly through tougher screening and background checks of both contractors and employees, ConocoPhillips

Chairman A.W. Dunham told a meeting of the Energy Security Council last April.

Industry participants, by and large, are already taking those steps. ConocoPhillips, for example, is spending \$5 million at just one of its facilities to implement stronger perimeter control, add security personnel, upgrade onsite security technology and otherwise improve its defenses against terrorist attacks.

## The Cyber Threat

A greater challenge, however, may lie in the threat of cyber-terrorism and the possibility of an “electronic Pearl Harbor,” as some have called it. The energy sector depends on cyberspace for supervisory control and data acquisition (SCADA) operating systems that can be accessed through the Internet. As Dunham posed it to the Energy Security Council, “Why blow up a facility when you can sabotage it by computer hacking?”

The industry’s most visible response to the threat of cyber-terrorism has been the Energy Information Sharing and Analysis Center (ISAC), a coalition of oil and gas companies that provides a near-real-time threat and warning capability to members on a 24/7 basis, similar to ISAC entities that already exist in other critical industries.

The Energy ISAC consists of a secure database, analytic tools and information gathering and distribution facilities that allow authorized individuals to submit either anonymous or attributed reports about both cyber and physical threats. Although the Energy ISAC is funded by a federal grant and accepts information submitted by relevant agencies such as the National Infrastructure Protection Center, no government agencies may directly access its data.

## ANATOMY OF AN SVA

**A security vulnerability assessment is a systematic, analytical process to evaluate the likelihood of a potential threat materializing and to weigh the probable severity of the impact if it does. Based on those results, facility managers can formulate a plan to reduce the level of risk by taking appropriate actions.**

**The team-based approach of an SVA taps the expertise of those who know the facility and its operations best — usually its employees — and the specialized skills and knowledge of professionals in fields such as security and process safety. There are several SVA methodologies available from various sources, including trade and professional associations and the Sandia National Laboratories, but all have components in common:**

- ▶ Facility assessment to determine which assets need to be secured; their importance, interdependencies and infrastructure; and the consequences if they are compromised
- ▶ Identification of the source and nature of threats against those assets and evaluation of potential targets' attractiveness to each adversary
- ▶ Identification of security-related events/conditions that could threaten the system's service or integrity
- ▶ Classification of each event/condition by level of risk based on likelihood and consequences of its success
- ▶ Ranking by risk of occurrence; in the case of events deemed high risk, recommendations to reduce the threat level
- ▶ Identification and evaluation of risk-mitigation options (both net-risk reduction and benefit/cost analyses) and reassessment of risk

— M.J.McD.

# threat of cyber-terrorism Pearl Harbor.' ”

The location of the Energy ISAC is not disclosed, and the facility is operated remotely. It is physically secured, and its various components are protected through state-of-the-art security techniques, including constant monitoring for unauthorized attempts to access or alter the system.

While the Energy ISAC showcases the benefits of the cooperative approach being taken by government-industry partnerships in combating the threat of terrorism against critical infrastructure, it also shines a light on what may be its Achilles heel: its voluntary nature.

The Energy ISAC board includes representatives from some of the oil and gas industry's biggest players, such as ConocoPhillips, ChevronTexaco, Marathon Ashland Petroleum and BP. Notably absent from the organization's roster, however, are some other U.S. oil company names, including ExxonMobil.

The biggest stumbling block to broader participation in the Energy ISAC (as well as the ISACs formed in 11 other industries) is concern about liability risks companies might incur as a result. Earlier concerns about the security of data submitted to ISACs were largely addressed by a blanket Freedom of Information Act (FOIA) waiver written into the Homeland Security Act of 2002, and it appears likely a legislative solution will be required for the liability issue, as well.

In fact, while industry participants generally prefer cooperation over government "command and control," a shift toward legislated standards looks to be an emerging trend.

In October, U.S. Department of Homeland Security Secretary Tom Ridge unveiled a set of rules governing security practices in all segments of the mar-

itime industry, including oil tankers and offshore oil platforms. While the development process included input from industry participants, the new rules differ from the guidelines they replace primarily in that they now have the force of law behind them. Conducting an SVA and developing a security plan are no longer suggestions, they are requirements. The new legislation also dictates certain attributes of maritime security plans and gives the Coast Guard approval authority over them.

The Chemical Facilities Security Act of 2003, which was nearing Senate approval at press time, would impose similar requirements on facilities handling certain amounts of designated chemicals. Virtually all of the nation's 140-plus refineries and many other facilities in the oil and gas industry would fall under its umbrella.

Moore calls the SVA requirement in the Chemical Facilities Security Act of 2003 "sensible," and he lauds the proactive stance the oil and gas industry has taken in the API Security Guidelines. At the same time, he is realistic about the limitations that exist on any industry's efforts to deal with the threat of terrorism.

"An SVA is the best tool available for uncovering vulnerabilities, weighing potential countermeasures and judging their likely effectiveness," Moore says. "However, vulnerability is ubiquitous. There is no way to achieve zero risk, and, quite frankly, the threat does not justify it. On the other hand, there are targets that have to be looked at in a new light. The lesson of 9/11 is far greater than anyone thought. Existing facilities were not designed with these types of threats in mind, and dealing with that is the real challenge." ■