One of the primary responsibilities of senior managers of private energy companies is ensuring continuity of production. In many countries, one of the most significant risks is that of a terrorist attack, which could severely decrease or even interrupt production for prolonged periods of time. Recent experience in countries such as Saudi Arabia, Yemen, and the Gulf of Guinea has demonstrated that energy facilities remain attractive targets for terrorists. Unfortunately, these facilities are often highly vulnerable to terrorist attack due to a disconnect between the industrial security function provided by the private sector and the external security function provided by the governments of the host countries. Because a significant and prolonged interruption of production and export income due to a terrorist attack is clearly not in the best interest of neither the energy company nor the host nation, the situation described above is far from optimal.

What is the real risk of supply interruption due to a terrorist attack?

There is no generally agreed upon answer to this question. Rather, the answer depends upon the perspective of the respondent, as well as the geographic region in which a particular facility is located. At one end of the spectrum is the view represented in Ernst & Young's 2009 report on strategic business risks for the oil and gas industry, in which "Supply Shock" ranks number nine on their list of the top ten risks. The events postulated as potential triggers for a supply shock, however, were primarily geopolitical, including regional insecurity and instability and/or deliberate disruptions by energy exporters for political purposes. But in contrast to the 2008 report, the possibility of attacks on pipelines, offshore installations, and tankers were specifically mentioned, and it was noted that "oil installations [are] an attractive target for the disaffected." In the 2008 report, only one from the panel of experts assembled by Ernst & Young suggested that it might be wise to consider the risk of terrorist attacks on oil facilities in the Middle East as part of "a move from symbolic targets to economic targets." Although there is a slightly increased recognition of the risks of terrorist attacks, the clear message is that corporate management need not spend a great deal of time and resources to address this risk.

In contrast to this rather sanguine view, most knowledgeable observers believe that the risk of a successful terrorist attack is high, especially for energy facilities located in certain geographic regions. This view is supported by the trend in postings on jihadi websites and by recent events.

Over the past dozen years, on-line postings and statements have shown a remarkable turnaround in the jihadi view of energy facilities as suitable targets. Thus, in August 1996 Osama bin Laden released a statement that clearly indicated that energy facilities in the Islamic

world were not a target: “I would like here to alert my brothers, the Mujahideen, the sons of the nation, to protect this (oil) wealth and not to include it in the battle as it is a great Islamic wealth and a large economical power essential for the soon to be established Islamic state.” Targeting foreign personnel (“crusaders” and “infidels”) was permissible, but not the energy infrastructure itself. In contrast, in December 2006 Osama bin Laden called on his followers to focus on stopping oil production by any means possible: “One of the main causes for our enemies' gaining hegemony over our country is their stealing our oil; therefore, you should make every effort in your power to stop the greatest theft in history of the natural resources of both present and future generations… Focus your operations on it [oil production], especially in Iraq and the Gulf area, since this [lack of oil] will cause them to die off.”

This escalation of rhetoric regarding the need to attack energy facilities is reflected in fatwas and other writings from a variety of sources. For example, in June 2004 Shaykh Abdullah bin Nasser al-Rashid issued a fatwa entitled "The Laws of Targeting Petroleum-Related Interests and a Review of the Laws Pertaining to the Economic Jihad". Unfortunately, this went unnoticed in the West until al-Qaeda drew attention to it as justification for the abortive attack on Abqaiq in February 2006. Also published in 2006 was a “Decree on Targeting Oil Installations”, which gave comprehensive religious and political arguments in favor of attacks on energy facilities. In 2007, an article entitled “Bin Laden and the Oil Weapon” was published, calling for attacks worldwide on oil facilities supplying the U.S. Finally, just last year the “Decree on Targeting Oil Installations” was reposted on several jihadi websites, and a new article, “Al-Qaeda and the Battle for Oil”, was posted, claiming that al-Qaeda must use energy attacks to cause an increase in oil prices that would damage the U.S. economy.

Over the same period of time, a string of terrorist attacks indicates that the escalating rhetoric has not been falling on deaf ears. Attacks on energy facilities that actually reached the execution phase (albeit with varying degrees of success) include: the use of an explosive-laden dinghy to attack the French tanker, M/V Limburg, off the coast of Yemen in October 2002, which did significant damage to vessel; the attack on the Oasis Compound in Al-Khobar, Saudi Arabia, in May 2004, in which 19 foreign employees of oil companies were killed; the narrowly averted double vehicle bomb attack on the world’s largest petroleum facility, Abqaiq, in Saudi Arabia, in February 2006; and the unsuccessful attack on a Yemeni oil refinery in September 2006. In addition, a number of other potential attacks were uncovered and disrupted in the planning stage, including: a plot to attack the Australian electrical grid in April 2004; surveillance of oil storage facilities in Australia and the U.S. in 2005 and 2006, respectively; and a threat to Ras Tanura in Saudi Arabia and Bahraini refineries in October 2006. It seems likely that a number of other such threats have been disrupted but not publicized, for obvious reasons.

Of course, energy infrastructure constitutes a potentially attractive target for a variety of terrorist groups in addition to those motivated by jihadist rhetoric. As has been pointed out by others, the relatively low cost of such an attack in both materiel and personnel presents an opportunity for a small group to exert an impact out of all proportion to the size of their organization. For

example, "One small attack on an oil pipeline in southeast Iraq, conducted for an estimated $2,000, cost the Iraqi government more than $500 million in lost oil revenues. That is a return on investment of 25,000,000%." In addition, the extended nature of energy infrastructure such as pipelines makes them virtually impossible to defend effectively, a point neatly summarized by the term “the ten-thousand mile target”. Illustrative examples are numerous; they include: the ongoing attacks by the Movement for the Emancipation of the Niger Delta (MEND) on oil infrastructure and personnel in the Gulf of Guinea; hundreds of attacks by the National Liberation Army (ELN) on the Caño Limón-Coveñas pipeline in Colombia over the last two decades; and the coordinated attacks on Mexican pipelines, supposedly by the Popular Liberation Army (EPR) in 2007. In addition, the Kurdistan Workers Party (PKK) claimed responsibility for the explosion and resulting fire on the Turkish portion of the BTC pipeline in November 2008, although Turkish officials maintained that the incident was due to a mechanical malfunction.

Because the nature of terrorist organizations, as well as their motivations, resources, and capabilities, varies widely from one geographic region to another, it is not possible to make general statements about the risks of a terrorist attack on a generic energy facility. Instead, it is necessary to focus on the specific risks to energy infrastructure in a given region, such as Canada, Eurasia, Indonesia, Latin America, and North Africa. Of these, only the Canadian analysis reflected the sentiment of the Ernst & Young reports, concluding that the risks of a successful terrorist attack on Canadian energy infrastructure were rather low.

The U.S. government apparently agrees with the conclusion that major energy facilities in certain regions face a substantial risk of damage due to terrorist attack. In 2006, it approved a Global Critical Energy Infrastructure Protection (GCEIP) Strategy. The stated objective of the GCEIP Strategy was to work with the governments of selected countries to improve security at energy facilities that were both critical to the global energy market and likely targets for terrorist attack. Although details of the program and the identities of the partner nations remain classified, it is clear that protecting major energy facilities overseas was a high priority for the Bush administration.

The gap between the private industrial security function and the public external security function

While major energy facilities generally have very effective industrial security programs, in most cases private sector security forces are unlikely to be able to repel a determined attack by well-armed terrorists. Indeed, in most countries private security forces are generally not allowed to carry weapons (other than sidearms, and then only in a few cases), and some companies have firm “no weapons” policies at all their locations. In reality, the private security forces focus on industrial safety, accident prevention and mitigation, ensuring that only authorized personnel have access to critical facilities, and preventing pilferage or theft of products. Consequently, it is not surprising that in most of the major energy companies the heads of security report to the

board through the Health, Safety, and Environment (HSE) line, with several levels of management between them and the board. Under these circumstances, security is only one of a number of competing priorities for a senior manager.

As a result, in almost all countries real security against terrorist threats is provided by armed personnel belonging to a host government ministry or agency, such as the Ministry of the Interior. These forces are responsible for security outside the facility perimeter and usually control both vehicle and personnel access at the gates. Typically, they also work closely with the nation's intelligence professionals to identify and defeat threats before they can approach the perimeter. In principle, the government forces at the perimeter should have the personnel, weaponry, and training to repel an attack by a determined and well-armed group of terrorists using car or truck bombs, automatic weapons, and high explosives. In practice, however, experience to date indicates that the government forces are seldom up to the task, even in countries that have taken the risk of terrorist attacks very seriously.

Armed government forces may not provide adequate security for several reasons. First, most governments of hydrocarbon-rich countries have not yet designated a single ministry or office that has both the responsibility for security at energy facilities and the authority needed to implement effective security measures. Second, "stove-piping" and competition between ministries inhibits cooperation and information sharing between all of the parties involved in security issues. Third, the authority to make decisions regarding a response to an attack is usually restricted to relatively high-ranking officers rather than delegated to the junior or non-commissioned officers who would bear the brunt of an attack. As a result, no one can or will make a decision in real time to counter an attack, effectively paralyzing the defense. Fourth and finally, prevailing attitudes that "it can't happen here", or that "if it does, it is God's will and nothing can be done" (in some Muslim countries), need to be overcome.

Consequently, the senior managers of energy companies that own or operate overseas facilities with a significant risk of a terrorist attack are faced with a dilemma: they are unable to take effective action inside the facility perimeter, yet they are aware that the forces outside the perimeter are unlikely to be effective. Until these circumstances can be changed, management must rely upon good fortune. Should a successful terrorist attack occur, however, the managers could be hard-pressed to demonstrate to their board and shareholders that they exhibited due diligence and adequately discharged their fiduciary responsibility.

If it is generally recognized that the security status at many energy facilities is unsatisfactory, why does the current unsatisfactory state of affairs persist? What is preventing or delaying significant improvements in security? In most cases, a number of factors can be identified. First, in many countries the private sector operator is a partner with the national oil company, and the relationship between the two is often delicate and complex. Suggesting that the host government is not able to provide the level of security that it claims could be perceived as undiplomatic and possibly causing more problems than it solves. Second, the private sector

security chiefs usually feel that they are "doing everything they can," and that they are severely limited by budgetary constraints. As indicated above, in many companies security competes with safety and environmental issues for a single pool of resources, and an HSE director may well give a higher priority to other concerns. Third, security professionals tend to rely upon familiar approaches and tried and true solutions, and they are often intrinsically distrustful of the new and the unfamiliar. This can lead to the unfortunate situation of "doing the same thing, over and over again, but expecting different results" (Albert Einstein's pithy definition of insanity).

Using public-private partnerships to bridge the gap

The U.S. GCEIP Strategy offers a potential model for developing public-private partnerships to close the gap between the private and public security forces and improve energy facility security in many countries. This strategy was based on government-to-government outreach efforts that encouraged nations that host critical energy facilities to improve both government- and operator-provided security, with USG technical advice and assistance to ensure that expenditures actually result in improved security. The basic argument was that it was neither in the best interests of the host country nor for the US that a major energy facility be taken off-line for a prolonged period of time, and that investing a small portion of the host government's fossil fuel revenues in improved security constituted an effective insurance policy to minimize the risk of losing that revenue. This approach proved to be exceptionally effective, and virtually all countries that were approached agreed to make major expenditures to improve security at energy facilities, either in cooperation with the USG or a private sector security firm. Typically, the host government mandated that the facility operator be responsible for physical improvements to perimeter security and to security within the perimeter, while the host government was responsible for security outside the perimeter, including the armed forces that provide perimeter protection.

The model discussed above for the division of responsibility between facility operators and host government seems appropriate for many other countries, with minor modifications, depending on the magnitude of the revenues from hydrocarbon exports. In the case of major exporters like Qatar, Angola, and Kazakhstan, current or projected revenues from LNG and petroleum exports are such that there is no question that these countries can afford to improve perimeter security at major energy sites which in many cases are currently and essentially unprotected.

In contrast, a country such as Oman, with net oil exports of about 700,000 b/d, is not generally regarded as a major exporter. Although Oman's income from hydrocarbon exports is substantially lower than those of the countries mentioned above, they nonetheless account for 75% of the Sultanate's revenues. This situation constitutes a two-edged sword: on the one

hand, the government of Oman has less disposable income to invest in security improvements, but on the other hand it is especially vulnerable to the loss of that income, which would be considerable. For example, at current prices ,disruption of the approximately 550,000 b/d that Shell produces in Oman would cost Oman and Shell about $24 million and $14 million per day, respectively, in addition to the costs of reconstruction, environmental remediation, and (for Shell) potential stock losses. Although Shell would continue to make money due to its operations elsewhere, Oman would not, and a prolonged disruption of exports could prove catastrophic for the Sultanate. In a case like Oman, one cannot assume that the host nation would automatically bear all the costs of improved security at and outside the facility perimeter. However, given Oman's relatively open borders and society, and its proximity to potential sources of terrorists such as Yemen, Saudi Arabia, and Iran, a very strong argument could be made for developing a public-private partnership to improve energy facility security in cooperation with operators such as Shell. The details of cost sharing would have to be negotiated.

The key requirement for this approach is the presence of a functional central government that is able to enter into such an arrangement and keep any commitments it makes with regard to energy infrastructure security improvements. Unfortunately, not all energy producers meet this criterion. One such example that comes to mind is the situation in Nigeria, where the oil-producing regions are largely ungoverned and where the rule of law is questionable. If the current efforts of the Nigerian government to bring many of the MEND rebels into the fold via an amnesty program are successful, and if it is also able to get the culture of corruption under control and bring effective government to the region, then one might well be able to extend the public-private partnership concept to attack even this previously intractable problem.

Dr. Bruce Averill is Founder and Senior Partner of Strategic Energy Security Solutions LLC; he was formerly Senior Coordinator for Critical Energy Infrastructure Protection Policy at the U.S. Department of State.