Canadian Centre of Intelligence and Security Studies (CCISS)

The Norman Paterson School of International Affairs

CCISS

Critical Energy Infrastructure Protection Policy Research Series

The Ten-Thousand Mile Target: Energy Infrastructure and Terrorism Today

Jan K. Fedorowicz

No. 2 - 2007

This study is undertaken as part of the CCISS Critical Energy Infrastructure Protection Policy Research Project, supported by a Contribution Agreement with Natural Resources Canada, Energy Infrastructure Protection Division

MARCH 2007

CCISS
Critical Energy Infrastructure Protection
Policy Research Studies
No. 2 – 2007

The Ten-Thousand Mile Target: Energy Infrastructure and Terrorism Today

Jan K. Fedorowicz*

Canadian Centre of Intelligence and Security Studies
The Norman Paterson School of International Affairs
Carleton University, Ottawa

March 2007

The ten-thousand mile target: energy infrastructure and terrorism today

Jan K. Fedorowicz*

The threat

The recent call by al-Qaeda to attack energy infrastructure in Alberta[1] has alerted Canada to the possibility of terrorist attacks on its own soil. It has served as a reminder that Canada may also be directly affected by the waves of terror sweeping the globe.

It remains to be seen, however, if this threat is real or just psychological intimidation. And if it is real, what can a country such as Canada do, either to avert such an attack or to minimize its potential impact?

One way to inform Canadian thinking about this threat is to draw on the experiences of other countries, at least as a starting point for discussion. That is the intent of this paper, which looks at terrorist attacks on critical infrastructure in several countries and considers some of the responses to those attacks. The intention is to see what Canada can learn about what works and what does not in this rapidly evolving area of national security.

In keeping with al-Qaeda's threat, the article will confine itself largely to energy-related infrastructure, which includes the facilities of the oil, gas, nuclear, and hydroelectric industries. It should be added that these particular industries constitute a subset of the expanding discipline of critical infrastructure protection (CIP) that is devoted to ways of protecting vital economic elements from terrorist attacks and other threats.

Historical background

The use of terrorism as a deliberate political strategy emerged into prominence in Europe around the middle of the nineteenth century, though examples of terrorism can be traced to ancient times. The long list of assassinations and bombings that occurred at the end of the 19th century should be reminder that the current "war against terror" is nothing new: the use of terrorism to provoke political change has a long pedigree.

Those early attacks, however, were exclusively against people. Infrastructure was not attacked, in part because it did not yet offer targets that could fatally weaken the social order if they were destroyed. From the perspective of promoting a particular political cause, far more publicity was to be derived from the murder of a head of state than from blowing up a building.

---

* Jan K. Fedorowicz is Sessional Lecturer, Department of History, Carleton University, and Senior Partner, Lanark Network Associates.

[1] *Ottawa Citizen*, 14 February 2007, CanWest News Service.

Yet strategically significant infrastructure was emerging. To take the classic example, in the 19th century, the British established a chain of coaling stations around the globe to keep the Royal Navy supplied with fuel. When the Navy converted to oil at the beginning of the twentieth century, it suddenly confronted a different set of challenges related to the protection of this newly critical energy infrastructure.[2]

The emergence of large-scale energy infrastructure supporting industrial economies inevitably led to the idea of attacking that infrastructure in war. Interestingly, attacks on energy infrastructure during the Korean and Vietnamese wars were largely ineffective because of the less developed and decentralized nature of that infrastructure in those countries. By contrast, military planners recognized the vulnerability of the US to any nuclear attack that involved its energy facilities. Attacks on energy facilities were a factor in the Iran-Iraq War, as they were during the Iraqi invasion of Kuwait and NATO's bombing of Serbia in 1999.

Anticipating the conclusions of military planners, terrorist groups were already targeting energy infrastructure in the 1970s. *Energy, Vulnerability, and War* discusses Libyan- and Soviet-sponsored terrorism and notes that from 1970 to 1980 over 250 terrorist attacks against energy infrastructures were carried out.[3] Such attacks continued in subsequent decades.

The following examples of recent concerted attacks on energy infrastructure demonstrate just how common and widespread this tactic has become:

- In El Salvador during the 1980s, the Farabundo-Marti National Liberation Front was able to interrupt electricity services in up to 90% of the country.[4] The Front eventually entered the political mainstream and is now part of the government.

- In Colombia, since the Caño Limón-Coveñas oil pipeline opened in 1986, guerrillas of the National Liberation Army known as the ELN have repeatedly blown it up, spilling the equivalent of ten Exxon Valdez disasters into the Orinoco basin rainforests.[5] In 1999, out of 251 major oil spills in the world, 51 were caused by terrorist attacks in Colombia, and only 36 were spills from tankers, barges and oil wells.[6]

---

[2] Discussed in Yergin, Daniel. *Ensuring Energy Security*, 1 March 2006 Foreign Affairs.

[3] W. Clark, J. Page. *Energy, Vulnerability, and War*. New York. 1981, WW Norton. 251 pp.

[4] Alexander E. Farrell, Hisham Zerriffi, and Hadi Dowlatabadi, *Energy Infrastructure and Security,* Annual Review of Environmental Resources. 2004. vol. 29:pp 421–69.

[5] United States Government Accountability Office, Security Assistance: Efforts to Secure Colombia's Cano Limón-Covenas Oil Pipeline Have Reduced Attacks, but Challenges Remain. September 2005 (GAO 05-971).

[6] ICF Consulting Perspectives, International Oil Facilities Are a Top Infrastructure Target of Terrorists, Summer 2004.

- Since 1980, along with numerous other terrorist incidents, the United Liberation Front of Asom has staged attacks on oil infrastructure and pipelines in Assam, India.

- During the Angolan Civil War, in January 1993, UNITA launched an all-out offensive against the city of Soyo, located in the oil-producing northern part of Angola. The government's counter-offensive against Soyo brought threats from UNITA leader Jonas Savimbi that he would target and destroy foreign oil producing facilities in the region. Interestingly, a UNITA spokesman later retracted the threat after receiving pressure from western governments, particularly the U.S. and France, which Savimbi did not want to antagonize.

- Myanmar's Yadana pipeline project raised the opposition of the local Mon and Karen ethnic groups. In March of 1995, the Karen ambushed a military convoy protecting a pipeline survey team. This was followed in December 1995 and February 1996 by rocket attacks on the headquarters of Total, the oil company involved in the project.

- Peru's Sendero Luminoso staged attacks on ElectroPeru's facilities during its decade-long campaign in the 1980s. In 1983, it sabotaged several electrical transmission towers in Lima, causing a citywide blackout. A similar attack was staged in June 1985. The original movement withered away after the capture of its leader, Abimael Guzman, in September of 1993. However, a decade later, in Jne 2003, a remnant of Sendero Luminos kidnapped 71 Peruvian and foreign employees working on the Camisea gas line in Ayacucho Department.

- Indigenous communities and their militias have waged a campaign against oil installations in the Niger Delta for some time. As a result, Shell Oil has been forced to evacuate at least four of its facilities.[7] In January 2006, several boatloads of heavily armed Ijaw militants overran one such facility in the Delta and seized Western oil workers. This marked the intensificaiton of heralded a campaign of disruption by the Movement for the Emancipation of the Niger Delta, protesting against various local abuses. Over the next two months more than 50 oil workers were kidnapped, though many were later released. [8] Ongoing attacks against Nigeria's energy infrastructure are estimated to have reduced the country's total petroleum exports by at least 20%.

- A separatist group objecting to the allocation of resources from oil exploration declared independence for Indonesia's Aceh province in 1976. Peace has recently been established and a former leader of the Free Aceh Movement was elected as provincial governor in December of 2006.

---

[7] Mark Lindsay, *The Security Threat to Oil Companies in and out of Conflict Zones,* Business Briefing: Exploration and Production: The Oil & Gas Review 2005, Issue 2.
[8] Platts Commodity News, *Nigerian militant group threatens to blow up Shell's Bonga FPSO* 13 February 2007; Associated Press Newswires, *Gunmen in Nigeria Release 24 Hostages,* 13 February 2007.

- Continued attacks on Iraq's energy infrastructure have made it impossible for that industry to regain its 1978 peak production rate of 3.5 million barrels per day. Indeed as attacks have continued, it has been impossible to invest in the renewal and upgrading of its aging equipment. As a result, Iraqi oil exports are 30 to 40 percent below prewar levels. [9]

- In May 2002, a cell-phone detonated explosive device was attached to a tanker-truck's underside in Israel's central fuel and gas depot north of Tel Aviv. Though the truck caught fire while loading, the fuel did not ignite nor did the flames spread to the fuel drums. Had the attack succeed, Israel's main fuel depot would have been destroyed.

This list of attacks could be expanded with numerous additional examples.[10] Clearly attacks on energy infrastructure are now part of the terrorist repertoire. Thus, al-Qaeda's calls to attack Canada's energy industry deserve to be taken seriously.

Yet what is also interesting about the attacks to date is that many were thwarted and most were not as devastating as they could have been. The most memorable terrorist attacks of the past decade have still been against civilians (9/11, the Madrid train bombings, the London Underground bombings, recent train bombings in India) with a clear preference for focusing on the kinds of mass targets made available by public transportation.

Perhaps the single most spectacular example of the destruction of energy infrastructure was not an act of non-state terrorism but Sadaam Hussein's order to set fire to Kuwait's oil fields at the end of the first Gulf War. Yet even this apparent cataclysm had only a limited impact on world oil prices and the fires were eventually extinguished.

Indeed, commentators such as Pavel Baev have wondered why there have not been more and devastating attacks on energy infrastructure so far.[11] He states that the biggest recent interruptions in energy supplies were caused by Hurricane Katrina (to platforms and refineries in the Gulf o f Mexico), a short circuit (the Moscow blackout of May 2005), and a labour strike that stopped pipeline construction in Azerbaijan.

In seeking to explain this, Baev notes the availability of softer tourist targets (which can also have a devastating effect on a country's economy) and the recent "hardening" of numerous energy targets, making it more difficult for terrorists to hit them successfully. However, he also notes that there may be other strategic considerations at play.

The war in Iraq has attracted the attention of the terrorist hard core, distracting them from other targets. The Chechens could have attacked Russian refineries but did not want to

[9] Yergin, Daniel. *Ensuring Energy Security*.
[10] Numerous examples and case studies of attacks on infrastructure are provided in a massive study: *Fundamentals of Energy Infrastructure Security: Risk Mitigation in the International Environment* published by the Petroleum Economist.
[11] Pavel K. Baev, *Reevaluating the Risks of Terrorist Attacks Against Energy Infrastructure in Asia*, China and Eurasia Forum Quarterly, Volume 4, No. 2 (2006) p. 33-38.

alienate the western powers, which would have viewed such an attack as a threat to their supplies. Iran may have used its influence with radical terrorist groups to keep them from attacks in the Persian Gulf so as not to play this trump card too soon in its confrontation with the US. Islamist groups in Central Asia have avoided the region's energy infrastructure so as not to provoke external intervention, the same motivation that keeps Indonesian terrorists from attacking China's energy lifeline through the straits of Malacca.

The argument seems to be that energy infrastructure has not been attacked to the extent that it could because of larger strategic considerations. Baev goes on to suggest that this temporary alignment of factors is now coming to an end. Iraq has been a training ground for terrorists who can now export the techniques they used in attack that country's pipelines. More importantly, Saudi Arabia is now producing more or less at capacity, suggesting that there is no longer any "play" left in the energy supply system. Any disruption to that system will now be more damaging than it would have been in the past two decades.

The ultimate point of Baev's analysis is that today's tighter energy supplies have made energy infrastructure into a more attractive terrorist target. Because energy markets are tight and spare capacity is limited, a few simple attacks could disrupt the supply chain and inflict significant economic damage.

This bears out the fundamental strategic consideration that drives the calculation of terrorists. Attacks on some piece of energy infrastructure are not as appealing as high-profile civilian devastation unless they cross a threshold where rather than being lost in obscurity, they can damage particular regimes, drive up energy prices, or slow down entire economies. And unlike the many attacks listed previously that had largely local impacts, today's terrorist groups, especially al-Qaeda, are increasingly interested in impacts that are potentially global.

A final consideration may also be that heightened global awareness of terrorism after 9/11 has led governments and other organizations to tighten security around transportation networks, military bases and government installations. If all targets have been hardened, terrorists may just as well focus on energy infrastructure, especially petroleum, because, to quote al Qaeda, it has come to be recognized as the "umbilical cord and lifeline of the crusader community"[12]

Defining the danger

Clearly al-Qaeda has an interest in the damage it can do to the world's energy infrastructure as a way of damaging Western economies. How then can governments mount an effective response? Contingency planning starts with an understanding of what is vulnerable and how it can be attacked.

[12] Cited in Gal Luft and Anne Korin, *Terror's next target,* The Journal of International Security Affairs, December 2003.

Generally, critical energy infrastructure consists of four sectors: nuclear, hydroelectric, petroleum and natural gas. In a sense, the nuclear and hydroelectric sectors are interrelated because they both use the same grid to deliver electrical power. Petroleum and natural gas are related inasmuch as they use similar networks of pipelines, refineries and ships to get their products to market.

Nuclear: Nuclear facilities have not, as yet attracted much attention from terrorists. In part this is simply because most nuclear plants are located in relatively stable and developed nations that do no have a significant indigenous terrorist problem. In addition, because of inherent public concerns about safety, these facilities are highly hardened to begin with and any attack on them, though not impossible, would pose daunting operational challenges.

It would seem that the biggest threats that terrorist pose to power-generating nuclear plants come from a deliberate collision such as flying a plane into them, though most reactors are designed to withstand even that level of impact. Alternatively, an armed assault could seize control of the building and arrange a meltdown. A more immediate threat involves smaller research reactors that are located near university campuses and are not subject to the same strict security safeguards.[13]

Ultimately much depends on terrorist motivations. If the intention is simply to murder the maximum number of people, a research reactor might be an appealing target. On the other hand, if the intention is to cripple the economy, nuclear reactors as a whole are less attractive. Because there is no one nuclear generating station that accounts for a large percentage of total power output in the global economy, a successful attack on a nuclear facility might inflict incalculable damage to the area surrounding it, but it could never have the effect of bringing down a national economy, let alone the global economy.

Hydroelectric: The situation is somewhat different with hydroelectric facilities. First of all, there have been terrorist attacks on electrical transmission towers such as those carried out by Peru's Sendero Luminoso. Secondly there are examples of the massive economic disruption power outages can cause, as witnessed by the large-scale blackout in the north-eastern part of North America on August 14 2003.

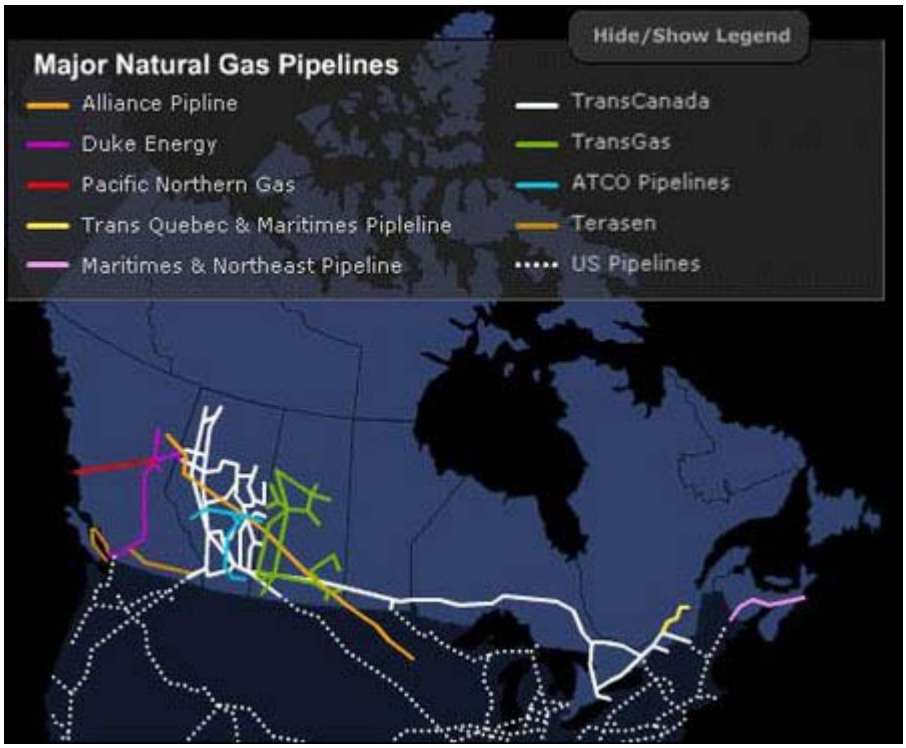
Terrorist studying such events might conclude that such blackouts in themselves have not created panic so if their motives are to sow psychological terror, the electrical grid may not be the best target. If their intent is to damage the economy, it is clear that he hydroelectric system is relatively resilient. The redundancies built into the system mean that even if a large facility were severely damaged, there are workarounds available that will soon restore power. To take one recent example, in 2000, an equipment failure caused a fire at Dominion Virginia Power's OX Substation and put it out of service.

[13] Alexander E. Farrell, Hisham Zerriffi, and Hadi Dowlatabadi, *Energy Infrastructure and Security,* Annual Review of Environmental Resources. 2004. vol. 29:p 454.

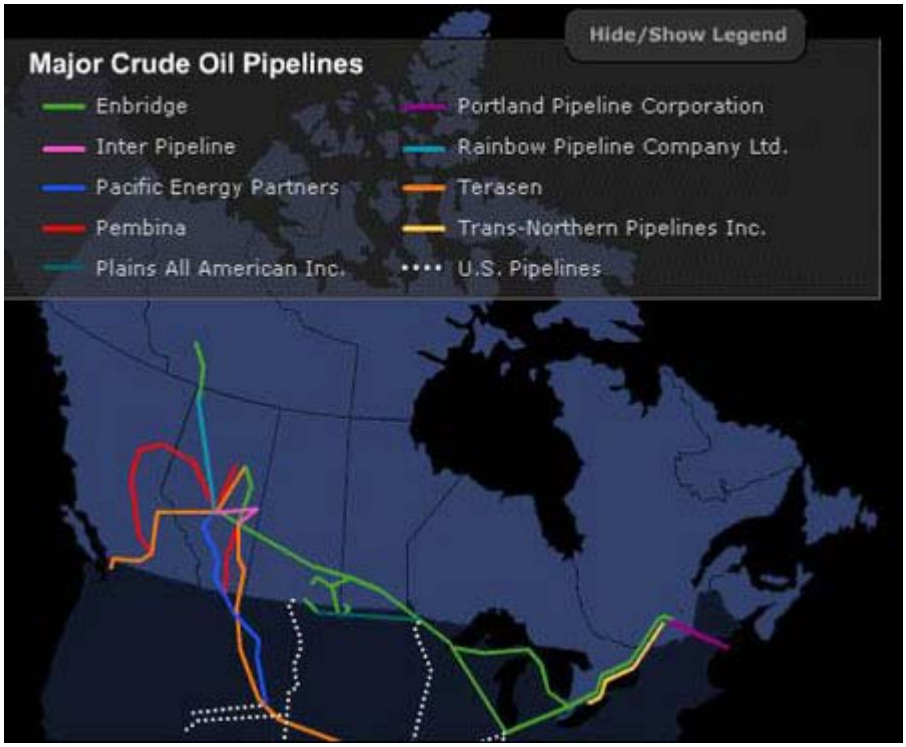
Despite the fact that the facility was a critical element in the network, workarounds meant that service was restored within one hour.[14]

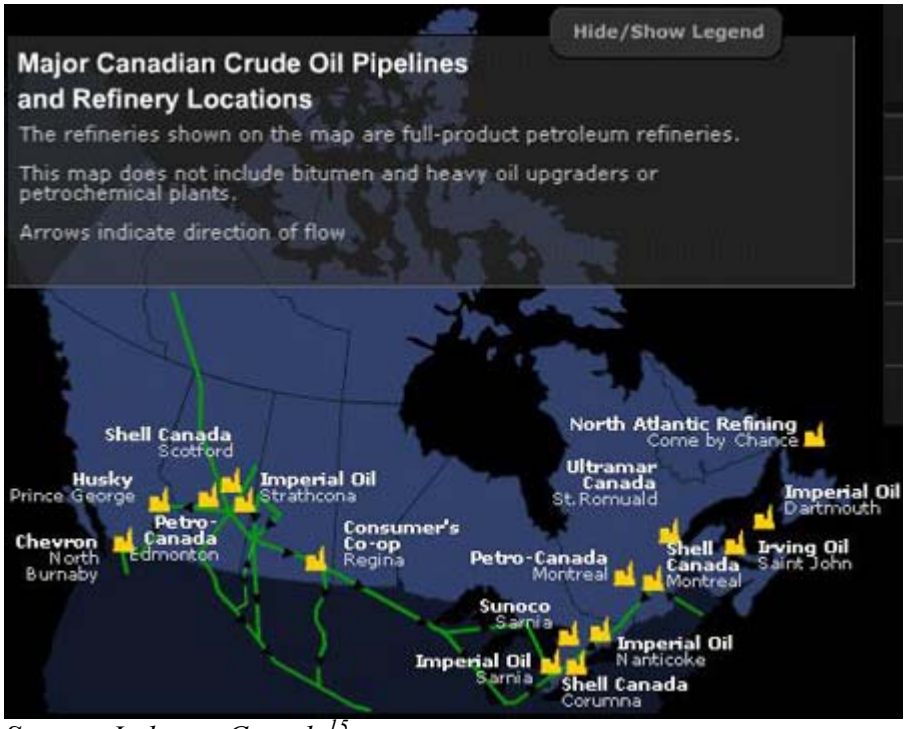
What may be more significant to terrorist planning, it is also clear that the great North American blackouts of 1965 and 2003 were less the result of any physical damage to equipment and more the result of a failure in the control systems that balanced power loads across the network. As a result, if they were tempted by the electrical grid at all, terrorists would probably be interested in the control systems underlying the network rather than any single piece of hydroelectric equipment. It is at least conceivable, though not very likely, that such systems might be compromised by remote cyber-attacks. However, as long as such control systems are properly hardened, secured and firewalled, this line of assault may not hold out much promise of success.

Petroleum and natural gas: By contrast, the petroleum and natural gas industries present a far more available though diverse target. Above all, these industries consist of vast networks of interrelated facilities, many of which are quite exposed. Figures 1-3 illustrate the extent of this infrastructure in Canada.



[14] Alexander E. Farrell, Lester B. Lave, and Granger Morgan, *Bolstering the Security of the Electrical Power System*, Issues in Science and Technology, Spring 2002.





Source: Industry Canada[15]

[15] See: http://images.google.ca/imgres?imgurl=http://ttcoilandgas.ic.gc.ca/epic/internet/inoges-msepg.nsf/vwimages/9_3_EN.jpg/%24file/9_3_EN.jpg&imgrefurl=http://ttcoilandgas.ic.gc.ca/epic/internet/inoges-msepg.nsf/en/dk00133e.html&h=357&w=449&sz=110&hl=en&start=32&tbnid=gBuiJuI3UlGRWM:&tbnh=101&tbnw=127&prev=/images%3Fq%3Doil%2Band%2Bgas%2Bpipelines%2B%26start%3D20%26gbv%3D2%26ndsp%3D20%26svnum%3D10%26hl%3Den%26sa%3DN.

Of course the energy infrastructure in the United States is far more extensive and complex. Daniel Yergin lists:

> *"more than 150 refineries, 4,000 offshore platforms, 160,000 miles of oil pipelines, facilities to handle 15 million barrels of oil a day of imports and exports… 410 underground gas storage fields, and 1.4 million miles of natural gas pipelines.*[16]

This picture is repeated all over the world. What is more, both petroleum and natural gas (in the form of liquefied natural gas or LNG) depend on long-distance supply routes that are occasionally confined to extremely vulnerable choke-points such as the Strait of Hormuz commanding the Persian Gulf, the Suez Canal, the Bab-el Mandab which controls access into the Red Sea, the Bosporus, and the Strait of Malacca. Tankers passing through these points are especially vulnerable to waterborne attacks, and these seem to be occurring with increasing frequency.

According to the US State Department, between 1996 and 2004 there were at least 80 terrorist attacks against oil companies worldwide. As a result, 722 employees were abducted, 132 were injured and 81 were killed. Of all attacks against the oil industry, half consisted of kidnappings of employees and only a quarter of the attacks involved explosives. Significantly, however, the trend seems to be toward an increasing use of explosives.[17]

In an attempt to probe US defences and test the idea of waterborne attack, on January 3, 2000, al-Qaeda loaded a small boat with explosives and attempted to ram the guided missile destroyer *The Sullivans* off the coast of Yemen. This initial attack failed since the boat was overloaded and sank under the weight of the explosives. The same technique was tried again, more successfully, on October 12 2000 when the *USS Cole* was severely damaged and 17 lives were lost. Having demonstrated that this method of attack could be effective, on October 6 2002, al-Qaeda turned its attention to commercial shipping by ramming an explosives-laden dinghy into the French tanker *Limburg.* The vessel caught fire and 90,000 barrels of oil leaked into the Gulf of Aden. Such attacks would probably have continued but in June 2002, the Moroccan government arrested al Qaeda operatives suspected of plotting attacks on British and American tankers passing through the Strait of Gibraltar.

While attacks on energy shipping may have temporarily abated, the vulnerability of this target will only grow. At present it is estimated that 40 million barrels of oil a day are shipped across the world's oceans. That number is expected to reach 67 million barrels by 2020. Over the same period, the amount of LNG crossing the oceans will triple to 460 million tons.[18] Clearly al-Qaeda will have many more vessels to strike at in the coming years.

---

[16] Yergin, Daniel. *Ensuring Energy Security*.
[17] Cited by Mark Lindsay, *The Security Threat to Oil Companies in and out of Conflict Zones*.
[18] Yergin, Daniel. *Ensuring Energy Security*.

Sea borne shipping, however, is only one of the oil and gas targets available. There are the production fields, pipelines and refineries that are the truly high value targets in this sector. Perhaps most vulnerable of all is Saudi Arabia, the world's single largest petroleum producer. That is primarily because the kingdom's petroleum industry is highly concentrated. Its oil reserves are confined to just eight fields, one of which, Ghawar, accounts for half of its production capacity. About two-thirds of Saudi Arabia's crude oil is processed at a single facility, Abqaiq. All of its oil exports pass through either Yanbu on the Red sea, or two terminals on the Persian Gulf, Ras al-Ju'aymah and Ras Tanura. The latter alone accounts for one tenth of the world's oil shipments.[19]

Given the combination of high concentration and high value represented by these facilities, it is hardly surprising that al-Qaeda has already tried several attacks. In the summer of 2002, a group of Saudis was arrested for involvement in a plot to sabotage Ras Tanura and pipelines connected to it. On May 12 2003, an attack on a housing compound killed 34 people and wounded 200 in Riyadh. A year later, on May 1 2004 seven people (six of them foreigners) were killed in a suicide attack at the oil facilities at Yanbu. In the same month, terrorists attacked the office of a Saudi oil company in Khobar, killing 19 foreigners. These were all attacks on people that were designed to send a message to foreigners to get out as much as they were intended to weaken the capacity of Saudi Arabia's petroleum industry.

A direct assault on infrastructure, however, took place on February 24 2006 when Saudi security forces thwarted an attempted suicide attack on the Abqaiq oil processing facility. Two pick-up trucks carrying two bombers tried to enter through a side gate but were challenged. The attackers detonated their explosives after security guards fired on them, but damage to the facility was minimal and no employees were hurt. Both attackers and two security guards were killed in the incident.

Even so, al-Qaeda remains determined to do serious damage to the petroleum indstry. On the fifth anniversary of the Sep. 11, 2001 attacks on the US, al-Qaeda's second-in-command, Ayman al-Zawahiri, used a taped message to call for increased attacks in the Mideast region. A few days later, a refinery and crude storage plant in Yemen were targeted in a failed suicide bombing.[20]

Though the preceding analysis has focused on the Middle East because of its obvious dominance of the petroleum market, there are other parts of the world that are also vulnerable. About 10 percent of the world's oil reserves are located in the successor states of the Soviet Union. The war in Chechnya has absorbed most of the world's attention, with its obvious implications for the Baku-Tbilisi-Ceyhan pipeline running from the Caspian Sea to the Mediterranean. There are, however, other conflicts brewing in Central Asia where the 5,000 to 10,000 members of *Hizb ut-Tahrir al-Islami* -- the Islamic Party of Liberation — challenge the governments of Uzbekistan, Kyrgyzstan,

[19] Gal Luft and Anne Korin, *Terror's next target,* The Journal of International Security Affairs, December 2003.
[20] *Oil Daily*, September 18, 2006, p.8.

Tajikistan and Kazakhstan. From the perspective of securing energy infrastructure, it is Kazakhstan which is most exposed. The country has about 4 billion tons of proven recoverable oil reserves and 2,000 cubic kilometers (480 cu mi) of gas. Estimates suggest that within a decade, it may be producing as much as 3 million barrels of petroleum a day, making it one of the top 10 oil-producers in the world.

There are other targets. In Indonesia, the leader of *Jema'ah Islamiyah* and architect of the Bali bombing, Riduan Isamuddin, also known as Hambali, is known to have also plotted attacks on oil facilities in Southeast Asia. In June 2004, pirates boarded a tanker carrying liquefied petroleum gas in Indonesia, demonstrating once again the vulnerability of energy shipping to sea borne attack. Such attacks are all the more appealing to terrorists because of the chokepoints through which this traffic moves. Approximately 13 million barrels of oil move through the Strait of Hormuz every day. Thirty percent of the world's trade, including half the sea borne oil for East Asia and 80 percent of Japan's crude oil, passes through the Strait of Malacca.[21] Not only are such areas target-rich, they are also vulnerable to blockage if vessels are sunk in these constricted passageways.

Indeed, attacks on oil facilities have become commonplace all around the world. Over the past few years, additional areas under threat have included oil reserves in north-western Algeria, which are vulnerable to attack by Islamic fundamentalists, the south-eastern Amazon region of Ecuador, where militants of the local Kichwa and Achuar communities have clashed with local security forces; and the Ituri region of the Democratic Republic of Congo, where ethnic militias have impeded oil and gas exploration activities.[22]

Finally, of course, there are the pipelines through which about 40 percent of the world's oil and gas reach refineries and ports. Saudi Arabia alone has some 10,000 miles of such pipelines. Iraq, with 4,000, shows just how vulnerable this infrastructure can be when exposed to constant sabotage using even simple explosives. Similar repeated attacks have been observed in Nigeria and Colombia. If an enemy is determined enough, it can incapacitate such infrastructure faster than oil producers or governments can repair it.

So far, however, the net effect of all of these attacks has remained manageable. Despite some temporary disruptions and dislocations, the world's petroleum and gas continues to flow. That offers, however, small comfort and no cause for complacency. It is not clear how many potential attacks on this vast network have been thwarted and thus what the real dimensions of the challenge are. It is also certain that terrorist groups have started to take a greater interest in attacking it.

> *Osama bin Laden was initially reluctant to use energy as a weapon. In August 1996 (he) released a fatwa urging the Mujahidins to protect oil and not include it in their battles. He reversed that position only a few years ago when he saw such attacks as an integral part of the strategy to weaken the US and western economies. However, he ruled out attacks on*

[21] Gal Luft and Anne Korin, *Terror's next target,* The Journal of International Security Affairs, December 2003.
[22] Mark Lindsay, *The Security Threat to Oil Companies in and out of Conflict Zones*.

> *oil wells and called for attacks on the infrastructure needed for refining and transporting oil, such as pipelines and refineries; employees of non-Muslim oil companies, ocean-going tankers and sea ports.*[23]

Forms and effects of attack

The experience of the past two decades suggests that attempts to destroy energy infrastructure have taken the form of kidnappings or murders of personnel, bombings of pipelines, attacks on shipping, and attempts to destroy larger targets such as refineries through tactics such as suicide bombings.

As it turned out, the most successful of these tactics were personnel kidnappings in Nigeria and pipeline interruptions in Colombia and Iraq. Nigeria's petroleum exports have fallen by 20 to 25 percent. Colombia has lost exports worth $500 million a year, and Iraq's production is about 30 to 40 percent below pre-war levels. What makes these cases unique and worth special study is that terrorist success comes about as a result of persistence: tactics such as kidnappings or attacks on pipelines are less spectacular than the bombing of a higher-value target such as a major refinery but they are harder to guard against and over time, they wear down production and exert a more profound impact. The industries in those three countries are suffering grievously because the attacks have been frequent rather than because the tactics were exotic or because the terrorists went after high-value targets.

Even so, the fact is that the energy markets of the world are vast and diverse. Disruptions in one part of the system have, so far, been evened out by drawing from others parts. Diversification of supply has proven to be an effective counter-measure. To have an impact, therefore, al-Qaeda would have to succeed spectacularly at one of the industry's high-value choke points, or it would have to mount a series of sustained attacks as in Iraq, Nigeria or Colombia.

That was precisely the point of the assault on Abqaiq. Had it succeeded, the impact on world energy supplies would have been catastrophic because it simply cannot be replaced. That refinery alone produces far more oil than the world's excess production capacity. In other words, had it been removed from the equation, there simply was not enough additional capacity elsewhere in the system to substitute for it and oil prices would have risen dramatically. The attack did not succeed, however, because the refinery was already sufficiently hardened that it could resist a suicide bombing successfully. Earlier attacks had tipped al-Qaeda's hand and led the Saudis and US to turn the refinery into something of a fortress. It is likely, however, that given the size and appeal of Abqaiq, al-Qaeda will try again, possibly using different tactics. It is also certain that the alerted Saudis and Americans will do everything in their power to render the facility even more impenetrable.

---

[23] Inggrid Panontongan, *Energy Industry and Terrorism in Indonesia,* IDSS Commentaries (73/2006), July 28, 2006.

Given this brief review of recent assaults on oil and gas targets, it is possible to put the recent threat to North America's energy infrastructure into some context. Al-Qaeda has explicitly stated that it is interested in attacking to in order to disrupt the US economy. Experience suggests, however, that it does not have the ability to mount sustained repeated attacks on this continent in the same manner as has been perpetrated (largely by others) in Iraq, Colombia or Nigeria.

This view is echoed by *Business Monitor International*, which stated:

> *… "al-Qaeda suffers, like all organisations, from limited resources. Indeed, while radical Islamic terrorist cells are, by definition, secret, it is not currently believed that al-Qaeda has large numbers of active cells in North America, or that domestic sympathisers are competent or well equipped enough to launch a campaign on a major scale. Thus, an Iraq-style sustained campaign on oil export pipelines and facilities - which would be required to inflict substantial damage to US energy infrastructure - would appear to be beyond its current capabilities.*[24]

BMI's conclusion is that for all its bluster about threatening the Canadian supplier to the US, it is more likely that al-Qaeda will continue its attacks in the Middle East, where it has a presence and better access, and where there are higher-value targets available. Alberta's oil sands projects simply do not present the same type of concentrated high-value target that can choke world markets at a single blow.

If it hopes to inflict large-scale and permanent economic damage in North America, al-Qaeda's only alternative may be to attempt some spectacular large-scale attack similar to the 9/11 operation. It may have to bide its time until it has the means to do it successfully. Smaller scale attacks will only alert North America to improve their counter-measures. In anticipation, North American planners should review the continent's infrastructure to identify and harden those sites that offer opportunities for such spectacular and devastating assaults.

Countermeasures

Terrorist attacks on energy infrastructure have not gone unanswered. Around the world, there are numerous initiatives under way to respond to the threat and keep energy supplies stable. Obviously a considerable amount of secrecy prevails and it is often not possible to get past security classifications. Nevertheless, on the basis of what is known, it is possible to say that there is a wide range of countermeasures that is being actively pursued.

One of the most fundamental is to restrict information about potential targets by removing information about facilities locations and layouts from the Internet and other media in the public domain. The location of hydroelectric control centres, for example, is now classified information.

[24] Business Monitor International, *Al-Qaeda Targets Canadian Infrastructure*., 01 March 2007.

The security of energy company personnel is being enhanced. For example, to protect its personnel in Myanmar, *Total* strengthened security teams, introduced very strict access and movement rules, erected protective enclosures around facilities, scheduled field work to avoid geographic scattering of personnel, and set up permanent radio links between field teams and the security control centre.

In many instances**,** perimeter security is being enhanced by maintaining constant patrols and using a variety of advanced sensors and motion detectors to warn of unauthorized penetration. Ports such as Dubai are installing floating barriers that can envelope a ship, an oil platform, or an entire port to counter attacks by small floating mines. For example, the US firm, Wave Dispersion, developed the Small Craft Intrusion Barrier (SCIB) in response to the attack on the Cole. Resembling a floating fish net, the system can incorporate motion or video sensors as part of a port defence system. Automated video analytic technology is being provided by Germany's Siemens to anticipate a broad range of threats. The buyers of these systems include not only governments but also private oil and gas companies seeking to protect their own facilities.[25]

Diversification of supply is one way of reducing vulnerability if any part of the infrastructure is attacked. Russia's reputation as a stable energy supplier has taken something of a beating because of recent disputes with Ukraine and Belarus. As it was, the disputes were quickly resolved and interruptions were temporary. But if Chechen terrorist has caused those interruptions, recovery would have been far more problematic. Thus it is no surprise that Western Europeans are currently developing alternative sources of natural gas in the northern reaches Norway, complete with a facility to liquefy the gas and carry it to market by ship.[26]

New pipelines are being built using construction techniques that impede attacks. For example, large parts of the Baku-Tbilisi-Ceyhan oil pipeline in the Caucasus are buried, making it that much harder to get at.

In some cases the focus is on rapid response delivered to threatened areas in the event of an alert. The Colombian army has been provided with 10 US helicopters that have improved its ability to react to threats to the Caño Limón-Coveñas pipeline. The US has also provided the Colombian army with $99 million in equipment (including night vision goggles) as well as training. This has allowed the army to repond more quickly and effectively to terrorist threats. As a result, attacks on the 110 miles of pipeline that is being patrolled have fallen off and terrorist attention has shifted to other areas where the Colombian army has not, as yet, received the same kind of assistance.[27]

---

[25] *The Middle East*. 1 February 2007, The Gale Group.
[26] Alexander Jung , *Snow White's Liquid Gold: Gas from Norway Could Reduce Dependency on Russia,* Spiegel Online, January 3, 2007.
[27] United States Government Accountability Office, *Security Assistance: Efforts to Secure Colombia's Cano Limón-Covenas Oil Pipeline Have Reduced Attacks, but Challenges Remain*. September 2005 (GAO 05-971).

There are a number of ways of hardening equipment to make it more resistant to direct assault. For example, new types of pipelines have been developed that are better able to withstand explosions. In addition, new sensor technologies are available that can quickly pinpoint ruptures.

Security organizations recognize that no matter how hardened a target is, it may not always be possible to prevent a determined attacker from getting through and doing damage. As the familiar calculation of asymmetry goes, security agencies need to repel 100 attacks out of 100 to get a passing grade: for the terrorist, one success out of 100 attempts is quite sufficient for success. That is why today's security doctrine also emphasizes survivability and recovery. There is a new emphasis on redundancy and workarounds to minimize the impact of any attack. Daniel Yergin speaks of

> *"…resilience, a "security margin" in the energy supply system that provides a buffer against shocks and facilitates recovery after disruptions. Resilience can come from many factors, including sufficient spare production capacity, strategic reserves, backup supplies of equipment, adequate storage capacity along the supply chain, and the stockpiling of critical parts for electric power production and distribution, as well as carefully conceived plans for responding to disruptions that may affect large regions."*[28]

All of these measures, and others like them are now part of what has come to be termed Critical Infrastructure Protection (CIP), a new area of government activity that aims to identify best practices, share information, and ultimately coordinate effective responses to the threat to energy (as well as other) infrastructure posed by terrorism. Still in its early stages, CIP has now appeared on the agendas of the major industrialized nations. For example, the governments of the United States, Canada, the European Union, Australia and New Zealand have all created CIP program initiatives.[29]

In terms of coordinating responses, the United States, in particular, has been especially energetic in mobilizing allied governments under what the State Department calls the Global Critical Energy Infrastructure Protection Strategy. Launched after the attack on Abqaiq, it encourages oil-producing countries in the Persian Gulf to share information and technology, enhance security and cooperate more closely to protect key strategic oil facilities.[30] Under this initiative, security cooperation can include sharing data on blast tests or breaching of security perimeters as well as the deployment of security personnel for consultations.

As in Colombia, the US is helping to arm its partners to enhance they ability to protect energy infrastructure. Saudi Arabia is getting a proposed $2.9 billion tank upgrade

---

[28] Yergin, Daniel. *Ensuring Energy Security*.
[29] Information about CIP initiatives can be found on the following national websites: Canada: http://www.psepc.gc.ca/prg/em/cip-en.asp; Australia: http://www.dpmc.gov.au/publications/protecting_australia/preparedness/5_infrastructure.htm; European Union: http://ec.europa.eu/justice_home/funding/epcip/funding_epcip_en.htm; New Zealand: http://www.ccip.govt.nz/; United States: http://www.dhs.gov/xres/programs/editorial_0548.shtm.
[30] *The Oil Daily*, 15 November 2006.

program, a $400 million Apache helicopter upgrade, and a $5.8 billion package of light armoured vehicles, radios and other weapons.[31]

The US is also working to enhance port security in the Middle East, including requirements that ships carrying US-bound cargoes maintain more stringent inspection, documentation and security procedures. These efforts include the Container Security Initiative (CSI), the Secure Freight programme (SF), and the Customs Trade Partnership Against Terrorism (C-TPAT)--all proposed within the past 12 months.[32]

Ports in the Persian Gulf are hardening their security by deploying gun emplacements, advanced closed circuit video and satellite monitoring systems. Dubai has declared its intention of becoming the world's safest city by 2010 when it will complete installation of a "smart system" of electronic monitoring on every building to trigger fire extinguishers and report accidents via satellites linked to a central civil defence operations room. So far, 540 buildings, 1,500 houses and 390 flats in two Dubai Marina condominium complexes are connected to the system and plans call for some 4,600 installations of this kind in more than 8,000 buildings.

The deployment of these technologies is being complemented by training, joint exercises and a variety of US support programs.[33] These initiatives extend to measures taken to defend against missiles launched by terrorists. As with other initiatives, the entire program would be tied together by enhanced information sharing as well as cooperation around counterterrorism and internal security. In addition, the U.S Navy has strengthened its own presence in the region and other countries have also increased patrols to make attacks on shipping far less likely.

Examples such as these represent a worldwide effort to enhance the security of energy infrastructure. As terrorist forces become more ambitious, security forces are seeking to match then with new technologies, procedures and weapons. All of these initiatives, however, are expensive and they give rise to the question of who pays. Security is a public good and like all public goods, the private sector has been notoriously reluctant to absorb its costs. Wherever energy infrastructure is owned by the private sector, there is a disconnect between the government's intention to secure supply (a social good) and the private sector's intention to minimize the costs of what is an increasingly expensive commodity. It has been observed that "government tends to work to improve the security of whatever infrastructure the private sector builds but often does not require the private sector to include security concerns in its investment decisions."[34]

An individual private energy company is not likely to add to its costs unless it is required to do so through regulation that applies equally to all competitors in the sector.

---

[31] *Dow Jones Newswires*, 16 August 2006.
[32] *The Middle East*, 1 February 2007, The Gale Group.
[33] *Inside the Navy*, 27 November 2006, Vol. 19, No. 47.
[34] Alexander E. Farrell, Hisham Zerriffi, and Hadi Dowlatabadi, *Energy Infrastructure and Security.*

> *Competitive markets will force the adoption of the lowest-cost solutions to providing electricity under the stipulated rules. If security is not an attractive investment above a minimal level, companies will not be able to make investments. Because security is a class public good … it will not be an attractive investment. Thus, it is up to government to answer questions concerning how much the nation is willing to pay for additional security, what organizations will be charged with ensuring it, and who should pay.*[35]

Because of the potential that public and private interests will diverge, governments in developed countries are looking for ways of strengthening public-private sector cooperation against terrorism. During the recent G8 Summit in St. Petersburg in October 2006, 200 participants gathered in Moscow for a one-day "Seminar on Specific Proposals for Strengthening Partnerships Between Governments and Businesses to Counter Terrorism." organized by the Russian Foreign Ministry in cooperation with the East-West Institute.[36] The solutions considered at this event attempted to strengthen partnerships and show that the private sector also had a compelling interest in security.

Some conclusions

The world's energy infrastructure is vast, complex, and vulnerable, but it is also diverse, and it is its diversity that is probably its single most significant asset vis-à-vis terrorist attack. Certainly it offers numerous soft targets, and there is no way of patrolling every single part of the system or of predicting where attacks will come. On the other hand, the global energy system also includes redundancies, spare capacity, stockpiles, and workarounds that make it reasonably resilient and capable of accommodating all but the most drastic assaults.

The history of terrorist attacks on energy infrastructure suggests that they can inflict local disruptions, some of considerable severity, but in many cases that was quite sufficient for the groups staging them. To date, however, no attacks have succeeded in having a longer-term impact on the world's energy markets as a whole.

What is true at the global level is also true for Canada. While there are extensive facilities across Canada, many of which could be termed "soft" targets, Canada does not seem to have key chokepoints to the same extent as exist in other parts of the world. A review of figures 1-3 suggests that there are no specific nodes in the infrastructure that could, if attacked, bring down the entire energy system.

That means that terrorist attacks in Canada, while possible and potentially disruptive, are not likely to have the profound, long-term economic impact that al Qaeda is looking for. On the other hand, mounting any attacks in North America, far from al Qaeda's base of

---

[35] Alexander E. Farrell, Lester B. Lave, and Granger Morgan, *Bolstering the Security of the Electrical Power System*.

[36] East-West Institute, *Report on Seminar on Specific Proposals for Strengthening Partnerships between Governments and Businesses to Counter Terrorism,* October 11, 2006, Moscow.

operations poses significant logistical challenges. Such attacks would almost certainly require homegrown collaborators to have any chance of success whatsoever, and even then the damage done is not likely to be irreparable. Even a spectacular attack that succeeds in destroying an entire refinery or nuclear plant – by no means an easy thing to organize or carry out – would only represent a temporary disruption unlikely to permanently cripple the entire North American economy.

A lot depends on al Qaeda's objectives. If it really intends to disrupt global energy markets and bring the US economy to its knees, it will probably focus on Middle Eastern chokepoints such as Abqaiq, which, if destroyed, are more likely to achieve those objectives. The only other way in which al Qaeda could weaken the North American economy would be to mount sustained and continuous attacks on its energy infrastructure, as was done in Colombia and Nigeria. There is no evidence that al Qaeda has the capacity to wage such a continuous campaign on this continent. Moreover, it should also be recognized that terrorism succeed in Colombian and Nigeria precisely because of the obvious chokepoints that were vulnerable to attack – a single pipeline in Colombia, the river delta in Nigeria. By contrast, the North American energy system is simply too scattered to succumb in the same way.

Of course, al Qaeda may have different objectives entirely. It has a history of issuing blood-curdling threats that are primarily designed for psychological effect and intended to inspire its supporters. It may be that this was the primary purpose behind its recently announced threats to Canada's energy infrastructure. It may also have hoped to inspire supporters in North America to freelance local attacks, more in the hope of keeping the US off balance than with any real intention of inflicting major economic damage. It may even be that the psychological effect alone was reason enough to issue the threat.

Whatever al Qaeda's true motives and capabilities, North America's energy infrastructure cannot be taken for granted. Even low-level threats should be taken seriously and that means deploying prudential countermeasures that have been shown to be cost-effective in other parts of the globe. Sooner or later, al Qaeda may supplement its rhetoric with concrete and specific action. If that happens, the continent's energy system should be prepared to deflect the blow.

References

Pavel K. Baev, *Reevaluating the Risks of Terrorist Attacks Against Energy Infrastructure in Asia*, China and Eurasia Forum Quarterly, Volume 4, No. 2 (2006) p. 33-38.

Business Monitor International, *Al-Qaeda Targets Canadian Infrastructure***.**, 01 March 2007.

W. Clark, J. Page. *Energy, Vulnerability, and War,* New York, 1981, WW Norton. 251 pp.

Dow Jones Newswires, 16 August 2006.

East-West Institute, *Report on Seminar on Specific Proposals for Strengthening Partnerships between Governments and Businesses to Counter Terrorism,* October 11, 2006, Moscow.

Alexander E. Farrell, Hisham Zerriffi, and Hadi Dowlatabadi, *Energy Infrastructure and Security,* Annual Review of Environmental Resources. 2004. vol. 29:pp 421–69.

Alexander E. Farrell, Lester B. Lave, and Granger Morgan, *Bolstering the Security of the Electrical Power System*, Issues in Science and Technology, Spring 2002.

ICF Consulting Perspectives, *International Oil Facilities Are a Top Infrastructure Target of Terrorists,* Summer 2004.

Inside the Navy, 27 November 2006, Vol. 19, No. 47.

Alexander Jung, *Snow White's Liquid Gold: Gas from Norway Could Reduce Dependency on Russia,* Spiegel Online, January 3, 2007.

Mark Lindsay, *The Security Threat to Oil Companies in and out of Conflict Zones* Business Briefing: Exploration & Production: The Oil and Gas Review 2005, Issues 2.

Gal Luft and Anne Korin, *Terror's next target,* The Journal of International Security Affairs, December 2003.

Oil Daily, September 18, 2006, p.8.

Ottawa Citizen, 14 February 2007, CanWest News Service.

Inggrid Panontongan, *Energy Industry and Terrorism in Indonesia,* IDSS Commentaries (73/2006), July 28, 2006.

The Middle East. 1 February 2007, The Gale Group.

The Oil Daily, 15 November 2006.

United States Government Accountability *Office, Security Assistance: Efforts to Secure Colombia's Cano Limón-Covenas Oil Pipeline Have Reduced Attacks, but Challenges Remain*. September 2005 (GAO 05-971).

Yergin, Daniel. *Ensuring Energy Security*, 1 March 2006 Foreign Affairs.