Bombs and Keystrokes: Asymmetric Threats to the Petroleum Supply of the United States

Stealth bombers and cruise missiles bombarding Saddam Hussein's Baghdad strongholds; massive convoys of tanks and armored vehicles rolling into the city to topple statues of the deposed dictator; helicopters full of Navy Seals launching a surprise attack and succeeding in eliminating their target, Osama bin Laden: these are but some of the images which define American military power in the modern era. Behind them, waves of unnoticed trucks, ships, and cargo planes transport personnel and equipment at unprecedented speeds. This ability to rapidly exercise overwhelming power, with a massive supporting logistical force, likewise is reflected in the American economic system. Every day, tons of goods numbering in the hundreds of thousands, and at least as many people, enter, cross, or leave the United States via container ships, airliners, trucks, freight trains, and automobiles, in millions of business transactions. The aggregate sum of these transactions is the largest and most prosperous economy on the planet, funding the most powerful military force in human history. However, this power is vulnerable to a weakness which could be exploited by its enemies employing asymmetric warfare tactics: a dependence on cheap, petroleum-based fuel.

The immense consumption of energy that drives American military and economic might is based on liquid fuels. These liquid petroleum (oil) based fuels are in the form of gasoline, jet fuel, and diesel fuel. If supplies of oil are catastrophically interrupted, especially for extended periods, and production or importation of these fuels is stopped, American power is severely constrained. This paper seeks to explore the weakness of American dependence on oil – who may exploit it, how, and how effectively, and furthermore, what the United States can do to address these presented national security concerns: it will do so in five sections of inquiry.

Section One will provide some basic contextual information on the levels of American oil consumption, where that oil comes from, and where it goes to be processed before usage on the market, with emphasis on the oil-exporting infrastructure of Saudi Arabia, and the oil importing and processing infrastructure within the United States. Section Two focuses on Saudi Arabia, and the sources and manifestations of asymmetric threats presented to its oil industry, principally by Al Qaeda. Section Three turns to the United States, and the cyber-warfare threats posed to its oil refining industry by both Al Qaeda and potentially hostile nation-states like China and Russia. Section Four studies the threat of so-called *cyber-proliferation*, and creates a scenario in which Al Qaeda launches a devastating attack against the oil supply of the United States. Finally, Section Five inspects how prepared the United States is for asymmetric threats to its oil supply, and what measures, if any, can be further taken to provide adequate security. The ultimate conclusion of this investigation is that asymmetric threats posed against the oil supply of the United States, while very real and able to cause significant damage, are for now overblown and can be effectively mitigated.

An Intravenous Petroleum Drip: American Demand for Oil, and How It is Satisfied

According to the United States Energy Information Agency, or U.S. EIA, the United States uses 19.1 million barrels of oil per day (2011, How dependent, para 1). Some of that is used to generate electricity, particularly in the state of Florida, but the vast majority of it is used to produce petroleum-based fuels: gasoline, jet fuel, and diesel fuel. According to L. Daniel (2010), the Defense Department uses 300,000 barrels a day, 70 percent of which is shipped overseas (para 5). These 300,000 barrels cost $13.4 billion, representing 80 percent of the federal government's energy expenditures. With transportation costs added, a $3 gallon of domestic

U.S. gasoline can cost upwards of $20 in Afghanistan (Daniel, 2010, paras 5, 6, 11). Regardless of exactly how it is consumed, the United States is by far the largest consumer of oil in the world.

The United States has significant petroleum reserves in Alaska, Texas, and offshore along the Gulf Coast, and new technologies like hydro-fracking promise to expand previously untapped reserves. Until the widespread use of these technologies is implemented, or there is a drastic downward change in consumption levels, however, these reserves are not enough to supply American demand. As of 2010, the United States imported 11.8 million barrels of oil per day (U.S. Energy Information Agency, 2011, How dependent, para 2). This represented 49.3 percent of U.S. consumption, which was down from an all-time high of 60.3 percent imported in 2005 (U.S. Energy Information Agency, 2011, U.S. oil import dependence, para 2). The five main sources of these oil imports, in terms of total percentage of U.S. oil consumption were Canada (25 percent), Saudi Arabia (12 percent), Nigeria (11 percent), Venezuela (10 percent), and Mexico (9 percent) (U.S. Energy Information Agency, 2011, How dependent, para 5). Although Canada may be the largest source of American oil imports, Saudi Arabia remains the largest source of oil globally, and therefore has immense influence on the oil market, OPEC membership aside.

This status warrants a closer examination of Saudi Arabia's oil-exporting infrastructure, starting with its processing facilities. Abqaiq is the most important, handling two-thirds of Saudi crude extracted from the country's oil fields (Luft, 2006, p. B02). From Abqaiq, the oil is sent via pipeline to the main Saudi oil seaports: Ras Tanura on the Persian Gulf, and Yanbu on the Red Sea. According to the U.S. EIA's profile of Saudi Arabia (2011), Ras Tanura has a 6 million barrel exporting capacity, 2.5 million barrels of which can be loaded onto oil tankers at

any one time via the world's largest offshore oil loading platform: this facility represents more than 75 percent of Saudi export capacity (para Major Ports). Yanbu handles most of the other 25 percent, with around 4.5 million barrels in capacity (U.S. Energy Information Agency, 2011, Saudi Arabia, para Major Ports). Wherever it comes from, the oil imported by the United States via ocean-going tanker is in turn received and processed in a limited number of locations.

These locations are principally Texas, Louisiana, and California. Although there are other major oil seaports along the coasts of the continental United States, these three states alone "account for over half of the [n]ation's operating crude oil [refining] capacity" (U.S. Energy Information Agency, 2011, U.S. States). Oil is delivered to where it is refined, and with 27 refineries with a capacity to process 4.7 million barrels of crude oil a day – one-quarter of total U.S. capacity – Texas is the number one recipient of imported oil, as well as number one producer of domestically extracted crude (U.S. Energy Information Agency, 2011, Texas). All of this data becomes relevant within the context of asymmetric threats.

The main takeaway of this energy and infrastructure data in terms of military strategy is that the United States is heavily dependent on cheap oil in large quantities, and moreover, this volume of oil is primarily processed, exported, imported, and re-processed in a limited number of locations. Each one of these locations can be made a chokepoint within the system of supply and delivery: force one to become inoperable, and the stream of deliveries slows down, driving up the price of oil. This has not gone unnoticed either. Saudi Arabia, the United States' number two oil supplier and the world's main price setter, has proven particularly vulnerable to the actions of Al Qaeda, whose goal in these operations is to strike at the West by driving up the price of its petrochemical lifeblood.

Burning Sands: Al Qaeda Operations against Saudi Arabian Oil-Exporting Infrastructure and Implications for the United States

Al Qaeda's aim to cause havoc in the Saudi Arabian oil industry, largely unrealized and likely to remain so for reasons which will be explored, stems from the words of its founder, deceased Osama bin Laden. M. Scheuer (2006) describes an interview Osama bin Laden gave in 1997, in which the Al Qaeda leader said "the deliberate damage done to the *ummah* (the Muslim community) by Washington's ability to control oil prices … has been a primary theme in [A]l Qaeda's consideration of the oil target" (p. 7). This is not a mere conspiratorial delusion by bin Laden, but rather a well-thought out argument (plausibility and validity aside). In the words of bin Laden, "'Since 1973, the increases in the price of oil have only been eight dollars per barrel, while the price of other commodities has gone up three fold. Oil should have gone up by the same rate, but that did not happen'" (M. Scheuer, 2006, p. 7). Bin Laden explained this as "because the U.S. is holding a gun against the forehead of the Arab countries" (M. Scheuer, 2006, p. 8). Bin Laden went even further than this, however: he came up with a mathematical justification for his terrorist activities.

As the interview progressed, bin Laden calculated what the United States "owed" the Muslim world, based on what he believed it should have been paying for oil over the previous years. His proposal:

> "During the last thirteen years [preceding 1997], the U.S. has cost us a loss of eleven hundred billion dollars. It is important that we get this … back from the U.S. … eleven hundred billion dollars could be distributed among the Muslims at the rate of ten thousand dollars per family. Muslims around the world are dying from hunger and the U.S. is stealing our oil. The U.S. buys cheap oil from us and then sells us its own tanks and aircraft … '[on the basis of]' the threat from Israel. This is how the U.S. takes its own money back from us" (M. Scheuer, 2006, p. 8).

Bin Laden conveniently excluded from his argument the means by which he aimed to solve the proposed problem: violence, often targeted against the Muslims he set to extend charity to as a

Robin Hood figure. Nonetheless, this does not change the zeal behind bin Laden's words, zeal which has been transferred into the lower ranks of Al Qaeda to members eager to carry out bin Laden's revenge against perceived unjust American oil dominance, which the Saudi royal family so eagerly serves.

This violent bloodlust has manifested itself numerous times against the Saudi Arabian oil industry, and it has had immediate effects on the price America pays for its oil. Al Qaeda has avoided directly attacking oil wells, not wanting to "cripple the ummah's economic power" and generate too much political flak against Al Qaeda in its crusade against the West (M. Scheuer, 2006, p. 8). Instead, to strike at America without egregiously harming Muslims' livelihoods, bin Laden "settled on plans that … [called] for attacks on the infrastructure needed for refining and transporting oil" (M. Scheuer, 2006, p. 8). No aspect of this side of the industry has escaped untouched: processing facilities, worker housing complexes, and tankers have all been targeted.

In 2006, Al Qaeda attempted to bomb Abqaiq, the facility which processes two-thirds of Saudi oil before sending it off to exporting ports, using two trucks loaded with explosives. G. E. Howard (2006) informs that the attack was largely a failure: while the two trucks exploded, "Saudi security forces were able to prevent the [A]l-Qaeda operatives from penetrating the perimeter … Nevertheless, the fact that the [facility] was targeted by al-Qaeda during a time of record-high oil prices caused instability in the global energy market, instantly inflating oil prices after the attack by $2 per barrel" (p. 5). These speculative fears were warranted: G. Luft (2006) explains that "if the car bombers had succeeded at Abqaiq … [they] would have removed 4 million to 6 million barrels a day of supply from [the] oil market. That loss would have exceeded all of the oil taken off the market by [OPEC] during the 1973 Arab oil embargo" (p.

B02). Although the Abqaiq attack was a bullet dodged, Al Qaeda has unfortunately been both more persistent and successful than one failed bombing attempt.

In 2004, twin attacks on foreign oil worker housing complexes, within a month of one another, also had major ramifications on the oil market. The first was an attack in May in the oil-exporting port city of Yanbu, in which five Western oil workers and a Saudi security officer were shot and killed by Al Qaeda terrorists (N. Banerjee, 2004, para 5). The next came later that month: 22 people – foreign oil workers (including one American), children, and Saudis – were murdered in attacks and an ensuing hostage crisis in foreign oil worker compounds in the city of Khobar (O. Bowcott, 2004). After news of the massacre in Khobar by Al Qaeda broke, the combined market response to the two attacks on the Peninsula was a one day 6.1 percent jump in crude oil prices on the New York Mercantile Exchange, which at the time set a record of over $42 a barrel (N. Banerjee, 2004, para 5). Al Qaeda has also targeted ocean-going tankers transporting Saudi oil abroad.

There have been two such attacks: one on the tanker *Limburg* in 2002, and the *M. Star* in 2010, each one consisting of a suicide mission implementing boats filled with explosives, in the vein of the 2000 *U.S.S. Cole* bombing – also an Al Qaeda operation. *Limburg* was a French tanker: when bombed, its hull suffered a major breach, spilling 90,000 barrels of oil into the Gulf of Aden and igniting a large fire which caused additional damage to the ship (K. Wassef, 2010, para 11). One crew member was killed, and the damage to the tanker was estimated at $45 million (K. Wassef, 2010, para 11.) The *M. Star*, a Japanese tanker, bombed in 2010 by an Al Qaeda-affiliated group, the Abdullah Azzam Brigades, was more fortunate – its hull being indented by the force of the explosion, but not breached (K. Wassef, 2010, para 4). These attacks, however, failed to significantly affect world oil prices.

While all these attacks certainly killed many persons and caused significant economic damage both directly and indirectly, they have failed to be as spectacular and devastating as the September 11, 2001 attacks in the United States. However, the possibility for such an attack remains feasible for Al Qaeda. Vulnerabilities in the Saudi oil industry yet to be exploited are the major exporting ports and the pipelines which connect them to facilities like Abqaiq. As J. C.K. Daly (2006) writes, "a [hijacked] jetliner crashing into the Ras Tanura facility could remove 10 percent of the world's energy imports in one shot," and the pipelines feeding Ras Tanura and Yanbu with oil "[depend] on 30 pumping stations, powered by six generators, which would shut down the flow if destroyed" (p. 2). While these vulnerabilities remain, the likelihood of them being exploited by Al Qaeda any time soon is increasingly unlikely.

This is because of recent setbacks in the organizational leadership structure of Al Qaeda. There is the 2011 killing of Osama bin Laden by U.S. Navy Seals in Pakistan, but there have also been arrests and killings more pertinent to operations on the Arabian Peninsula and in the Persian Gulf. In 2007, a huge sweep of arrests in Saudi Arabia turned up 172 Al Qaeda fighters from seven armed cells, along with explosives, firearms, ammunition, and over $5 million cash (Fox News, 2007, para 2). Along with Osama bin Laden, Anwar al-Awlaki, leader of Al Qaeda in the Arabian Peninsula, was killed in 2011 by a U.S. drone strike, decapitating that branch of the organization. With these major setbacks, combined with a continued crackdown against Al Qaeda around the world, the Arabian Peninsula is quiet, and the Saudi oil industry safe, for now.

Terrorism at the Speed of Light: Cyber-Warfare Threats Posed against Oil Infrastructure within the United States

Al Qaeda is no longer constrained to exclusively physical attacks in one geographic region, however. The digital age has opened up numerous opportunities for long-range, out-of-

the-shadows terror to be exploited by those with ill will against the United States, from terrorist groups to rogue states. We will see reasons why these vulnerabilities have not been exploited, though. Al Qaeda specifically has dabbled in operations on the new cyber battlefield under the guidance of only a few select members. These members have included Imam Samudra, Younis Tsouli, and Fazul Abdullah Mohammed.

Samudra and Tsouli dabbled in the financial dimension of cyber-warfare. Imam Samudra – more infamously known by "masterminding the 2002 nightclub bombings in Bali, Indonesia, that killed 202 people" – wrote his autobiography in prison after his capture by Indonesian police (K. Koch, 2009, p. 300). In it, he included "a rudimentary outline of how to commit online credit-card fraud," (K. Koch, 2009, p. 300) the purpose of which was to raise money for terrorist operations "against infidels, 'especially now the United States and its allies'" (A. Sipress, 2004, quoted in K. Koch, 2009, p. 300). Meanwhile, Younis Tsouli, a young Moroccan immigrant in London who made contact with Al Qaeda online, along with two associates, raised $3.5 million to buy "hundreds of prepaid cellphones and more than 250 airline tickets" for Al Qaeda, using stolen credit card information (K. Koch, 2009, p. 300). Tsouli also used this stolen information, in conjunction with computer viruses, "to set up a network of communication forums and Web sites that hosted 'everything from tutorials on computer hacking and bomb making to videos of beheadings and suicide bombing attacks in Iraq'" (D. Lormel, 2008, quoted in K. Koch, 2009, p. 300). None of this adds up to spectacular attacks against the United States, however, and it certainly does not reflect Osama bin Laden's stated desire to manipulate the international oil market to America's disadvantage.

While Tsouli's dubious accomplishments are notable, he remained a low-level member within Al Qaeda. Samudra, on the other hand, was a major player, yet all he did to advance Al

Qaeda's cyber-warfare capability was to give instructions on how to steal credit card numbers. Both men were eventually arrested before much more could become of their technical know-how. Likewise, Fazul Abdullah Mohammed, "one of the last [A]l Qaeda leaders expert in computers" (S. Borg, 2011, para 8), also planner of the 1998 African U.S. embassy bombings, and military commander of Al Qaeda-affiliate Al Shabaab in Somalia (the group behind the 2010 Uganda bombings), was killed in a shootout with Somali security forces in June 2011, before his skills, whatever they were, could be manifested (T. Peter, 2011). It can be reasonably assumed that none of these men or their work posed a significant, direct, cyber threat to the United States.

Al Qaeda, as a whole, is growing increasingly competent technically. G. Weimann (2005) writes that "when U.S. troops recovered Al Qaeda laptops in Afghanistan … [t]hey discovered structural and engineering software, electronic models of a dam, and information on computerized water systems, nuclear power plants, and U.S. and European stadiums" (p. 143). However, "the evidence did *not* suggest that Al Qaeda operatives were planning cyberattacks, only that they were using the Internet to communicate and coordinate physical attacks" (G. Weimann, 2005, p. 143). Again, for now, the Al Qaeda threat on this front appears to be nil: Al Qaeda simply lacks the technical skill among the organization's members to launch a serious cyberattack against any major infrastructure target, including oil facilities. However, there are other parties in cyberspace who are technically capable, and have in fact, already infiltrated the networks required to bring down America's oil supply system.

Those parties are nation-states with major cyber-warfare programs, namely China and Russia, although Iran and North Korea may join that list, if not on it already. According to S. Gorman (2009), Chinese and Russian spies have already infiltrated the electrical grid control systems of the United States, not seeking (for the moment) to cause any damage, but simply to

map the system, and save that knowledge for a time when either state may deem it necessary to act upon it (paras 2, 3). What does the power grid have to do with oil supplies?

The answer to that question leads back to the refineries which are necessary to process crude oil into usable transportation fuels. This process requires electricity – a lot of it – to run the necessary machinery and chemical processes. In other words, an asymmetric opponent does not even have to directly attack oil refineries in the United States to severely affect the country's supply, and hence, the price it pays. Instead, all that is necessary is to knock out the refineries' power supply for an extended period of time, curtailing production. It has proven frighteningly easy to disable a power grid: two apparent cyberattacks in Brazil caused extensive blackouts there in 2005 and 2007 (G. Messick, 2010, p. 1). Vulnerabilities exist in the systems of the United States, as well.

If someone wanted to disable the power grid, they would first hack into the grid's control system. G. Weimann (2005) explains why this first step has become increasingly easier to accomplish in recent years:

> "Deregulation and the increased focus on profitability have forced utilities and other companies to move more … of their operations to the Internet as a means of improving efficiency and reducing costs. The energy industry and many other industrial sectors have opened their enterprises to a vast array of cyberdisruptions by creating inadvertent Internet links (both physical and wireless) between their corporate networks and the digital crown jewels of most industrial processes: the supervisory control and data acquisition (SCADA) systems. These systems manage the actual flow of electricity and natural gas and perform other critical functions in various industrial control settings, such as chemical processing plants, water purification and delivery systems, wastewater management facilities, and a host of manufacturing firms" (p. 139).

Once inside a grid's SCADA system, an attacker can proceed in one of two ways, or both simultaneously: overload generators at power plants or overload large electrical transformers at power substations.

In a U.S. government experiment in 2008, codenamed "Aurora," scientists and engineers were able to digitally instruct a 27-ton power generator to self-destruct – a highly problematic ability, given that such generators require months to replace if damaged or destroyed (G. Messick, 2010, p. 5). Electrical transformers are similarly vulnerable, perhaps requiring "a year or more to manufacture," delivery times from production plants in developing nations aside, if they were to be damaged or destroyed by a cyberattack-induced electrical surge (A. E. Farrell, et al, 2004, pp. 449-450). Even oil facilities themselves may be vulnerable, without these vulnerabilities in U.S. power grids: W. Safire (2004) relates a story from the Cold War of how corrupted software the U.S. allowed the KGB to steal led to a 3 kiloton yield-equivalent explosion in a natural gas pipeline in Siberia, caused by the software commanding pumps and valves to over-pressurize the pipe (p. A25). A would-be hacker could, in theory, inflict similar damage remotely upon an oil refinery or oil off-loading tanker terminus using a computer virus.

Once again, however, a familiar pattern reasserts itself: while there are gaping holes in the security guarding the domestic U.S. oil infrastructure, no major players have taken advantage of them. Al Qaeda lacks the technical skills, and China and Russia, while more than capable of launching a devastating attack, are not presently threatened or motivated enough to do so. Iran and North Korea, like Al Qaeda, have not caught up in terms of technology to match what fervor they may have.

Pandora's Box and an Explosive Playground: The Threat of Cyber-Proliferation?

A potential nightmare scenario is foreseeable out of this uneasy stability, however: what if a group like Al Qaeda, with the desire to inflict serious damage upon the United States' oil infrastructure, somehow received the technical resources of China or Russia? This is the fear

behind so-called *cyber-proliferation*, relation to its feared nuclear cousin. As with classical nuclear proliferation, the concern is that valuable and dangerous technology, this time involving cyberspace, will slip out of the hands of large nation-state programs and end up on the black market, where it can change hands and eventually be received by terrorists or rogue states to use as weapons of mass *disruption*.

In many respects, such a cyber-proliferation process would be far easier than nuclear proliferation. Kristin Lord, vice president at the Center for a New American Security, says in E. Walsh (2011), "This isn't like missiles, which require transporting large materials that can be detected. We are talking about knowledge and code" – intangible things which exist within the small space of a laptop or a human brain (para 2). And, like nuclear technology and technique passing from Pakistan to Iran and North Korea, cyber-warfare applicable knowledge is already proliferating across the globe. In China, for example, Captains S. W. Dilworth and P. A. Stempel, USAF (2010), report that "hacking is now popular sport…The hacker hero is alive and well in Chinese popular culture and fiction…hacker websites include discussion forums where hackers compare accomplishments and describe how to hack certain networks" (pp. 42, 40). Despite what knowledge might be accumulating for potential hire in countries like China, the odds of an organization like Al Qaeda working directly with the Chinese, or Russians, is highly unlikely.

G. Giacomello (2004) reminds that "most committed terrorists do not like and, more importantly, do not *trust* mercenaries. Contemporary terrorists tend to be increasingly true believers who have an unmasked contempt for those that might not share their same commitment" (p. 401). It is unlikely that Al Qaeda terrorists would trust hired hands with an operation as expensive and time-consuming as launching a major cyberattack against the United

States, especially if the hired hands are current or ex-communists like the Chinese or Russians! Moreover, the accumulated *knowledge* of all of China's cyber-punk teenagers does not compare to the *resources* of professional cyber-warfare programs of the Chinese government. Al Qaeda would not be looking to acquire advanced technical skills to write its own cyber-warfare codes, but would want to be able to use the limited technical skills it already possesses to run a program that has already been created by another. In other words, Al Qaeda would not dream of working with the Chinese, but, it would not be above stealing from the Chinese military or buying on the black market access to the Chinese cyber-sleeper programs already in place within the American power grid system.

Which cyber-sleeper program would Al Qaeda be particularly interested in? The logical answer is Texas. One only need to refer to the data in Section One to realize that disabling the Texas power grid would take down one-quarter of the United States' crude oil refining capacity, some of its biggest oil-importing seaports, and its largest continental production fields. Given Al Qaeda's penchant for flashy, high-casualty attacks, simply turning off the lights would probably not be enough: a concurrent, physical, suicide terrorist attack upon a major oil facility in the United States or elsewhere would be likely, or at least highly desired, by Al Qaeda. If an oil infrastructure-crippling cyberattack in Texas, Louisiana, or California were combined with a catastrophic bombing of Ras Tanura's offshore tanker-loading terminus, for example, or even worse, a domestic U.S. target, oil prices would skyrocket into completely unprecedented territory. No one can be certain how high prices would go exactly, but there could only be degrees of devastation to the economy of the United States, not a possibility of escaping unscathed.

Lessons from the Storm: Countermeasures to Asymmetric Threats to the U.S. Oil Industry

Such a nightmare scenario is just that – a nightmare, a bad dream not yet realized. However, while the United States has the upper hand – while it can enjoy relative assurance about the lack of threat to the international oil structure it depends on, at least from the very specific threats presented in this paper – *now* is the time to get ahead and invest in security and system redundancy. How exactly the United States should do that is a matter more open for discussion, but there are precedents of effective countermeasures. Additionally, these specific threats are not as terrible as they seem.

Some argue that a complete overhaul of the system is unnecessary, and actually counterproductive. Those like Counc. Compet. (2002) state, "'[t]op-down, prescriptive security standards could drain productivity and dampen growth prospects, putting [the] U.S. … at a disadvantage vis-`a-vis [its] foreign competitors. Only the private sector is able to design integrated security solutions to protect productivity and competitiveness'" (quoted in A. E. Farrell, et al, 2004, p. 442). Moreover, many "Private owners of critical infrastructure are reluctant to provide information that may have security or commercial value to the government for fear of it falling into the wrong hands under provisions like those of the federal *Freedom of Information Act"* (A. E. Farrell, et al, 2004, p. 442). No one wants to divulge costly cyber-secrets, even if that means leaving the system vulnerable to potential attack. However, even if the system was devastatingly attacked, whatever would be broken at that point is more than capable of being fixed: as G. Weimann (2005) reminds, "the employees of companies that handle power grids [and] oil and gas utilities … are well rehearsed in dealing with the fallout from hurricanes, floods, tornadoes, and other natural disasters" (p. 144). Natural disasters also provide

us with a model useful for examining how the United States would cope with a massive intentional strike upon its oil infrastructure.

Gulf Coast hurricanes have devastated the oil industry and provoked crisis response and recovery in recent history. Drs. M. Mihalka and D. Anderson (2008) recall that in 2005, "Hurricanes Rita and Katrina shut down about 1.3 million barrels of refining capacity, about 8 percent of the U.S. national total" (p. 4). D. Yergin (2006) estimates an even more devastating total: "Hurricanes Katrina and Rita shut down 27 percent of U.S. oil production (as well as 21 percent of U.S. refining capacity). As late as January 2006, U.S. facilities that before the hurricanes had produced 400,000 barrels of oil a day were still out of operation" (p. 74). The U.S. Coast Guard (2011) reports that Hurricane Katrina alone created "nine major and medium [oil] spills totaling more than 7.1 million gallon[s] … as well as approximately 35 minor spills of less than 10,000 gallons" (para 10). This incredible destruction to the U.S. oil supply, it must be remembered, was also on top of the apocalyptic destruction done to coastal communities along the Gulf Coast by the same record storm surge which affected the industry so much. Yet, the nation made it through this oil crisis.

The effects of these hurricanes were mitigated by several important measures. D. Yergin (2006) describes that "emergency supplies from the U.S. Strategic Petroleum Reserve…were released, sending a 'do not panic' message to the market. At the same time, two critical regulatory restrictions were eased" (p. 80). These restrictions were the Jones Act, "which bars non-U.S.-flagged ships from carrying cargo between U.S. ports…waived to allow non-U.S. tankers to ship supplies bottlenecked on the Gulf Coast" and *boutique gasoline* regulations "that require different qualities of gasoline for different cities … temporarily lifted to permit supplies from other parts of the country to move into the Southeast" (p. 80). These same measures could

easily be taken again if either domestic or Saudi oil infrastructure was hit by an asymmetric opponent. None of them individually, or even in conjunction, is a permanent solution, especially if power to U.S. refineries were to be knocked out for an extended period of time, but they would significantly ease any oil market price shock.

Cyber-security and post-crisis mitigation measures aside, in terms of physical, preventative security, Saudi oil infrastructure is actually well-protected, despite Al Qaeda's grim track record. K. Al-Rodhan (2006) writes that "[a]t any given time, there are an estimated 25,000 to 30,000 troops protecting the Kingdom's infrastructure. Each terminal and platform has its own specialized security unit, comprised of 5,000 Saudi Aramco security forces, and an unknown number of specialized units …The Coast Guard and components of the Navy protect the installations from the sea" (p. 3). Of course, no security system of any kind working against any manner of threat is perfect. However, even in the event of a worst-case scenario, all is not lost.

K. Crane, et al (2009) explains that "In the event of an abrupt reduction in the global supply of oil … U.S. consumers would have to pay the higher market price, which would lead to a fall in consumption. By the same token, as long as the U.S. military is willing to bid high enough, it will have access to fuel" (p. 18). In other words, every potential oil crisis has a built-in safety mechanism, or relief valve: once the price of oil gets too high, people will simply stop buying it, and the price will slowly return to acceptable levels in response to these demand trends. Whoever can afford the price of oil, the U.S. military included, will pay for it if they need it. This is still bad news for the U.S. economy, but comforting in the sense that no act of man or nature can permanently disrupt our access to the world's global reserves. In the end, it is the

feature of the oil market that most makes asymmetric threats to the national security of the United States unreliable weapons.

Short terms events, however catastrophic, do not define markets in the long term. While U.S. economic health is acutely threatened by such short term events, long term American military and economic supremacy is not chronically. Purely in terms of efficient military strategy, using American oil-dependence as an asymmetric weapon fails: damage does not count as defeat. Combined with the facts that Al Qaeda is on the run and has not conducted any oil infrastructure attacks in years, the Chinese and Russians – while poised – have no motivation to launch a cyberattack, and cyber-proliferation, while a very real fear, is not yet realized, the determination can be made that asymmetric threats to U.S. oil infrastructure are overblown. Fear is always the greatest source of volatility in the oil market, so overcoming destructive speculation based on imagined threats is a very important step towards security, along with mitigating actual threats as they arise.

This being stated, asymmetric threats must still be taken seriously. What is true today may not be tomorrow, and constant vigilance is a necessity against any threat. Climate change, peak oil, threats from Iran of cutting off sea-access to the Persian Gulf, and political instability in the wake of the Arab Spring are examples of other concerns to keep in mind regarding American oil dependence too. For now, the United States can rest easy without fear of terrorist bombs or malicious keystrokes attacking its energy lifeblood, but it may not eventually even be bombs or keystrokes that do us in after all – instead, our belief we can continue to consume beyond our means without consequence.

Works Cited

Al-Rodhan, K. (2006). The impact of the Abqaiq attack on Saudi energy security. Center for Strategic and International Studies: Washington D.C.

Banerjee, N. (2004). Oil prices set another record, topping $42. *New York Times*, June 2, http://www.nytimes.com/2004/06/02/business/02oil.html.

Borg, S. (2011). Why Al Qaeda has failed at cyberwarfare. *Scientific American*, Jul. 12, http://www.scientificamerican.com/article.cfm?id=al-qaeda-and-the-internet.

Bowcott, O. (2004). 'They killed two security guards then shot at the school van': Targets witnesses describe how militants singled out westerners and their families. *The Guardian*, Sunday, May 30, http://www.guardian.co.uk/world/2004/may/31/saudiarabia.oil2.

Counc. Compet. (2002). *Creating opportunity out of adversity*. Presented at Natl. Symp. Compet. Secur., Pittsburgh, PA. In A. E. Farrell, et al (2004), Energy infrastructure and security, *Annual Reviews of Environmental Resources*, 29, 421-469.

Crane, K., et al. (2009). *Imported oil and U.S. national security*. RAND Corporation: Santa Monica, CA; Arlington, VA; Pittsburgh, PA.

Daly, J. C.K. (2006). Saudi oil facilities: Al Qaeda's next target? *Terrorism Monitor*, 4(4).

Daniel, L. (2010). New office aims to reduce military's fuel usage. American Forces Press Service. http://www.defense.gov/news/newsarticle.aspx?id=60131. July 22.

Dilworth, USAF Captain S. W. and Stempel, USAF Captain P. A. (2010). The art of cyber war. *The Reporter*, 37(3), 36-42.

Farrell, A. E., et al. (2004). Energy infrastructure and security. *Annual Reviews of Environmental Resources*, 29, 421-469.

Fox News. (2007). 172 militants planning attack on oil fields arrested in Saudi Arabia. April 27, http://www.foxnews.com/story/0,2933,268941,00.html.

Giacomello, G. (2004). Bangs for the buck: A cost-benefit analysis of cyberterrorism. *Studies in Conflict & Terrorism*, 27(5), 387-408.

Gorman, S. (2009). Electricity grid in U.S. penetrated by spies. *Wall Street Journal*. http://online.wsj.com/article/SB123914805204099085.html. April 8, 2009.

Howard, G. E. (2006). Foreword. In M. Scheuer, S. Ulph, and J. C.K. Daly, *Saudi Arabian oil facilities: The Achilles heel of the Western economy*, (2006), The Jamestown Foundation: Washington D.C., 5.

Koch, K. ed. (2009) Terrorism and the internet. *CQ Researcher*, 3(11), 285-310.

Lormel, D. (2008). Terrorists and credit card fraud . . . A quiet epidemic. CounterterrorismBlog, Feb. 28, 2008, http://counterterrorismblog.org/2008/02/terrorists_and_credit_card_fra.php. In K. Koch, ed., Terrorism and the Internet (2009), *CQ Researcher,* 3(11), 285-310.

Luft, G. (2006). An energy Pearl Harbor? A near miss in Saudi Arabia hints at future shocks. *The Washington Post*, Mar. 5, B02.

Messick, G. (2010). Sabotaging the system. *60 Minutes*, CBS, http://www.cbs.com/shows/60_minutes/video/1521067910/cyber-war. Transcript. http://www.cbsnews.com/2100-18560_162-6568387.html.

Mihalka, Dr. M. and Dr. D. Anderson. (2008). Is the sky falling? Energy security and transnational terrorism. *Strategic Insights*, Center for Strategic Conflict: Monterrey, CA.

Peter, T. A. (2011). Somalia kills Fazul Abdullah Mohammed, widening Al Qaeda power vacuum. *The Christian Science Monitor*, June 12, http://www.csmonitor.com/World/terrorism-security/2011/0612/Somalia-kills-Fazul-Abdullah-Mohammed-widening-Al-Qaeda-power-vacuum.

Safire, W. (2004). The farewell dossier. *New York Times*, Feb. 2. p. A25.

Scheuer, M. (2006). Al-Qaeda and the oil target. In M. Scheuer, S. Ulph, and J. C.K. Daly, *Saudi Arabian oil facilities: The Achilles heel of the Western economy*, (2006), The Jamestown Foundation: Washington D.C., 7-12.

Sipress, A. (2004). An Indonesian's prison memoir takes holy war into cyberspace. *The Washington Post*, Dec. 14, 2004, p. A19, www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html. In Koch, K. ed. (2009) Terrorism and the internet. *CQ Researcher*, 3(11), 285-310.

U.S. Coast Guard. (2011). District 8: Guardians of the heartland. http://www.uscg.mil/d8/d8facts.asp. Last updated April 29, 2008.

U.S. Energy Information Agency. (2011). How dependent are we on foreign oil? http://www.eia.gov/energy_in_brief/foreign_oil_dependence.cfm. Last updated June 24, 2011.

U.S. Energy Information Agency. (2011). Saudi Arabia. http://www.eia.gov/countries/cab.cfm?fips=SA. Last updated Jan. 2011.

U.S. Energy Information Agency. (2011). Texas. http://www.eia.gov/state/state-energy-profiles.cfm?sid=TX. Last updated October 2009.

U.S. Energy Information Agency. (2011). U.S. oil import dependence: Declining no matter how you measure it. http://www.eia.gov/oog/info/twip/twiparch/110525/twipprint.html. Released May 25, 2011.

U.S. Energy Information Agency. (2011). U.S. States. http://www.eia.gov/state/. Last Updated Jan. 2011.

Walsh, E. (2011). The cyber proliferation threat. *The Diplomat*, Oct. 6. http://the-diplomat.com/new-leaders-forum/2011/10/06/the-cyber-proliferation-threat/.

Wassef, K. (2010). UAE: Al Qaeda responsible for Japanese tanker attack. CBS News World Watch. http://www.cbsnews.com/8301-503543_162-20012890-503543.html. 6 August 2010.

Weimann, G. (2005). Cyberterrorism: The sum of all fears? *Studies in Conflict & Terrorism*, 28(2), 129-149.

Yergin, D. (2006). Ensuring energy security. *Foreign Affairs*, 85(2), Mar.-Apr., 69-82.