

February 15, 2007

Vulnerabilities in energy supply chain and infrastructure

Threats arise from terrorists, uranium, nature and complacency

Several years ago the distinguished author Thomas Clancy wrote a prescient novel, The Sum of All Fears, portraying a scenario in which a group of Middle Eastern terrorists fortuitously acquired a nuclear weapon, and planned to attack the Super Bowl causing a catastrophe with innumerable casualties. Although this popular novel was considered pure fiction only 16 years ago, all the ingredients are now in place wherein fiction could become reality. A terrorist group exists swearing to attack the United States and its allies with the goal of inflicting large numbers of casualties to provoke a wider conflagration of forces, causing what some pundits have described as a "clash of civilizations." To date, al-Qaeda and its inspired horizontal affiliates have wreaked havoc on transportation systems in Madrid, Mumbai, Moscow and London in addition to other vulnerable targets that attract large numbers of people. To date, however, conventional explosives have been utilized and there has been thankfully a noticeable absence of weapons of mass destruction. Recently the world was alarmed by the information emanating out of the former Soviet Union, indicating the possibility that somewhere there is a leakage of weapons-grade uranium.

Last January a Russian crossed into Georgia and traveled to Tbilisi by car along a high mountain road. In two plastic bags in his leather jacket, Georgian authorities say, he carried 100 grams of uranium so refined that it could help fuel an atomic bomb. The Russian had come to Tbilisi to meet a buyer who he believed would pay him a million dollars and deliver the material to a Muslim man from "a serious organization." The uranium was a sample and the deal a test. The Russian claimed he had access to approximately six pounds in his apartment in southern Russia, which, in expert hands, is enough to make a small bomb. Fortunately his "contact" was an agent of the Georgian security services who arrested him and confiscated his merchandise. The case has alarmed officials because it was thought that

new security precautions had disrupted the nuclear black market that developed in the 1990s, after the Soviet Union collapsed. The United Nations' nuclear watchdog group, the International Atomic Energy Agency (IAEA), confirmed there have been sixteen attempted sales of weapons-grade nuclear material broken up by authorities since 1993. The largest occurred in 1994 when police in the Czech Republic intercepted six pounds of highly enriched uranium. When the uranium recently confiscated in Georgia was analyzed by the United States Department of Energy, it was found to have a U-235 purity "suitable for certain types of research reactors, as a source material for medical isotope production, and for military purposes including nuclear weapons." This case, along with a similar case in 2003, was centered on material in large enough quantities that could provide a terrorist with an instant solution to the biggest challenge to making a nuclear weapon, obtaining the fuel. This region, southern Russia and the northern Caucasus, is plagued with political instability and rampant corruption, providing a fertile breeding ground for illicit commerce in atomic materials.

Black market spurs a global emergency

During the 1990s almost all the illicit sales of nuclear materials involved scams. Small amounts were made available for sale with the promise of larger amounts at a later date to be paid for up front. According to American government reports virtually all the nuclear materials seized since the Soviet breakup are believed to be Russian in origin. These seizures in Georgia contradict the belief that the situation has improved and suggests the trade in nuclear materials may simply have gone under the radar.

United States Homeland Security Secretary Michael Chertoff may have been thinking about the aforementioned events when he

(continued on next page)

Vulnerabilities in energy supply chain and infrastructure

Threats arise from terrorists, uranium, nature and complacency

recently addressed a prominent terrorism panel at the World Economic Forum in Davos, Switzerland. He warned that the specter of terrorism “is only going to get worse” in the years to come. As Chertoff said, “what we face in the 21st century is the ability of even a single individual, and certainly a group to leverage technology in a way to cause a type of destruction and a magnitude of destruction that would have been unthinkable a century ago.” He added that the magnitude of future terrorist attacks could make the September 11 attacks seem miniscule by comparison. Consequently the world must do everything in its power to keep terrorists from acquiring nuclear weapons. Meanwhile, on the same day that Chertoff addressed the World Economic Forum, a videotape from Ayman al-Zawahiri, al-Qaeda’s number two leader, surfaced on the Internet warning that the United States must change the way it deals with Muslim countries or else Americans will face a fate “far worse than anything they have seen.” Experience has shown these are not idle threats.

Private sector must protect infrastructure

Because a staggering 85 percent of the U.S. critical infrastructure is in the hands of the private sector, business leaders must be aware of their responsibilities to assist in protecting this critical infrastructure. Consequently the private sector, in the absence of regulations, should volunteer to cooperate with the authorities to erase the vulnerabilities that could become opportunities for terrorists to attack. Business leaders in the nation’s 17 critical infrastructure sectors should also work to identify sleepers who could pose threats to the U.S. infrastructure.

The National Infrastructure Advisory Council is a group of private sector executives and state and local government leaders who meet four times a year to advise the White House on keeping crucial facilities secure. This group was recently tasked to establish a subcommit-

tee to explore the insider threat to critical infrastructure systems to identify “sleepers who could be the source of the threats.” Internal threats are a risk in all 17 critical infrastructure sectors and represented the next logical step for the Council to explore following threat assessments at the entrances and perimeters of facilities.

The Department of Homeland Security identifies the 17 critical infrastructure sectors as follows: water, energy, transportation, communications, chemical and hazardous materials, commercial facilities, dams, defense industries, emergency services, financial services, food and agriculture, government facilities, information technology, national monuments and icons, nuclear power plants, postal and shipping and public health and health care. To date, the transportation sector has been the hardest hit because it is the most vulnerable and the nature of this sector is to move the largest number of people possible from point to point as fast as possible, with minimum inconvenience. It would not be practical to screen subway riders in New York or London in a manner similar to the screening at airports, and therein lies the issue of vulnerability.

The aforementioned “sleeper study” is timely in view of recently developed information revealing that al-Qaeda in Iraq plotted to send operatives into the United States through the student visa program. It was not coincidental that most of the 9/11 hijackers were from Saudi Arabia. Prior to 9/11 it was easier for Saudis to obtain visas to the United States than it was for citizens of any other Arab country in the Middle East. Al-Qaeda took advantage of this vulnerability.

Since then the visa process has been tightened, but the United States is faced with a dilemma because as a nation we still welcome foreign

students to study here. There are many advantages to welcoming foreign students, but the program can be exploited if not closely supervised. The student visa program was used by one of the 9/11 hijackers, Hani Hanjour, to get into the United States and some of the hijackers were attending schools to take flying lessons in Florida and Arizona. Al-Qaeda was considering in 2006 to use the student visa program to infiltrate about a dozen operatives into the United States to carry out attacks. A raid conducted on a militant hideout in Iraq uncovered a list of operatives and initial plans exploiting the weaknesses in the student visa program. This plan was most definitely the result of instructions from al-Zawahiri to the former al-Qaeda leader in Iraq, Abu Musab al-Zarqawi, to marshal his resources to carry out terrorist attacks beyond the borders of Iraq as witnessed by the attack on hotels in Amman, Jordan on November 9, 2005.

“Home grown terrorists”

Prior to the July 7, 2005 suicide bombings on the transportation system in London that killed more than 50 people, several British intelligence authorities were on record to assure citizens that there was not a terrorism threat in the United Kingdom. This false sense of security was shattered overnight and then again when a second wave of attacks targeted the transportation system only two weeks later. A year later another cell was discovered planning to blow up jumbo jets traveling to the United States. During January 2007, while six individuals were on trial in London for the second wave of bombings, the British authorities arrested nine individuals in Birmingham, England on terrorism charges. This group had been under investigation for some time and was in the penultimate stage of kidnapping a British Muslim soldier and beheading him, and then posting a video of his torture and gruesome death on the Internet. Top security sources in the United Kingdom claimed the al-Qaeda leaders in Pakistan and Iraq have ordered terrorist cells in the United Kingdom to adopt the decapitation tactics used by the former al-Qaeda in Iraq leader Abu Musab al-Zarqawi. Despite the simplicity, a gruesome attack of this nature would be as effective as a subway

or airplane bombing in spreading fear among the population. If the plotters had been successful, and the tactics had been adopted by other cells, the discovery of headless bodies at random locations could easily lead to mass hysteria.

Two years after the initial wave of attacks, the security service MI5 was “working to contend with some 200 groupings or networks, totaling over 1600 identified individuals.” Experts say Europe’s major problem in 2006 was “home grown terrorism.” This problem of the home grown terrorist has not surfaced in the United States and experts contend for a variety of reasons, social, political and economic, that the threat would more likely come from operators recently infiltrated into the United States. Also the American intelligence and law enforcement community deserves some credit in making the United States a difficult target, neutralizing and preventing some of these threats in their early stages. Nevertheless, as witnessed in the United Kingdom we cannot afford to be complacent.

Threats are numerous and varied

The three threats to the critical infrastructure are: international and domestic terrorists, Mother Nature and the third could be described most succinctly as incidents of incredible stupidity. “The best defense might just be a good defense,” especially when dedicated to preventing the catastrophes associated with these threats. Studying the importance of physical security surveys to assure perimeter security at critical infrastructure facilities in addition to the insider threat are logical and necessary steps to protect people and property. Cameras, lighting, control points and metal detectors are important to control the individuals who enter and leave a facility, but the human factor is also very important. The best equipment in the world is no better than its operator. No strategy, however well conceived, can prepare the personnel of sensitive sites for every contingency. The protective force will depend on professional skills as situational awareness, strength of mind, mental readiness,

(continued on next page)

Vulnerabilities in energy supply chain and infrastructure Threats arise from terrorists, uranium, nature and complacency

boldness, self-reliance, intuition and a willingness to take calculated risks. These traits were recently evidenced in Pakistan when the heroic actions of vigilant security officers prevented suicide bombers from even entering the premises of their targets, saving numerous lives at the Islamabad Marriott Hotel and the Islamabad airport. Due diligence investigations, providing thorough reviews of each individual's background, are essential to manage, and potentially eliminate, threats from the inside.

A 9/11-scale terrorist attack or a major natural disaster does not have to have catastrophic consequences, but the danger grows as long as we fail to face up to the fact that these events can occur and the proper security and safety procedures are not implemented. A recent study claims that "the source of our vulnerability to manmade and natural perils is rooted in our ongoing neglect of the physical infrastructure." The predicament arises from our failure to invest in pragmatic measures that would better prepare us to respond and recover when things go wrong. Additionally, in preparing for the kinds of hazards that Mother Nature will periodically unleash on us, our society will become a far less attractive target for those who might contemplate acts of terrorism as a means of warfare directed against the United States. This is especially relevant now because it has never been easier for individuals and groups to find money and weapons, or to spread their ideas – including violent anti-Americanism.

The Time for Urgency is Now®

On the industrial front, the Homeland Security Agency is concerned about the nation's chemical, petrochemical and nuclear facilities, perhaps the most lethal and vulnerable of all our manufacturing complexes. Recently the public has displayed a heightened awareness of this vulnerability, and many chemical firms have been good citizens and have invested significant effort and money to improve security and safety. However recent events portend that more must be done. With threats coming from so many directions, the corporations that con-

trol the nation's chemical industry and the 16 other important infrastructure sectors must be continuously innovative, testing protection systems to ensure such precautions will thwart attacks by terrorist groups, who strive for innovation as well, and disasters and accidents that arise with little or no warning. There is no doubt al-Qaeda is still aggressively looking for the weakest link in the supply chain, and standards across the industry would preclude a weak link. The companies who control the country's infrastructure must evolve faster than the threats that surround them, as well as anticipate future threats. This is no small task and requires serious dedication of corporate resources.

Companies should realize that despite increased board-level scrutiny of financial affairs in the wake of the Enron scandal, businesses face other grave risks and at industrial companies safety and security are primary considerations. Executives and non-executives need to start asking the right questions. Senior executives need to protect themselves, their people and their plants. This involves leadership at all levels, partnerships and trust and a plan to effect regulations, best practices and standards. These ingredients are necessary to prevent the fictional Sum of All Fears scenario from soon becoming a reality.



The Lipman Report Editors