

March 15, 2006

Global and National Security Threats

Sense of urgency needed to combat variety of dangers

Global and national security threats are dynamic. Significant transitions in key states and regions throughout the world, the continued existence of rogue states and terrorist groups, rapid technological development and proliferation and emerging global health challenges all foster a complex and dangerous global security environment that will spawn crises. In the years following the attacks of September 11, 2001, these dangers have passed in and out of the mass media and the public consciousness. The threats, though, are always present. This edition of The Lipman Report examines some of the most serious current threats to global and national security.

The Nuclear Threat

The results of a nuclear attack, whether from a rogue state or from a terrorist organization that has managed to acquire or build a portable, or “suitcase,” nuclear device, would be catastrophic. Such an attack could cause thousands of fatalities along with numerous other consequences. Damaged buildings, downed power and phone lines, leaking gas lines, broken water mains and weakened bridges and tunnels are only some of the dangerous conditions and devastation that would be caused by such an event. Depending on the type of industries present in the area of the blast (such as chemical or petroleum production, industrial storage facilities, and manufacturing operations), there also may be significant releases of hazardous materials.

Approximately 30,000 nuclear weapons in the arsenals of the nuclear states and hundreds of tons of fissile material (either enriched uranium or plutonium, the ingredients needed for such bombs) are dispersed throughout more than 40 countries around the world. According to terrorism experts, security for many nuclear stockpiles is inadequate. These weapons and materials are vulnerable, and a terrorist group may acquire them through theft or purchase.

The bulk of the most vulnerable nuclear material is in Russia and in some countries that constituted the Soviet Union. For this reason, the United States, in the early 1990s, embarked on a program of financial and technical support to aid Russia and other former Soviet republics in

accounting for and securing their nuclear weapons and materials. Much remains to be done, however. At the present pace it will take more than a decade before all of Russia’s nuclear stockpiles are adequately secured. The United States needs to build an effective global nuclear security partnership, develop a global nuclear security standard and assist any state willing to meet the standard but lacking the means to do so.

Radiological Attack (“Dirty Bomb”)

A radiological weapon, or “dirty bomb,” is a conventional explosive such as dynamite packaged with radioactive material that scatters when the bomb detonates. A “dirty bomb” kills or injures through the initial blast of the conventional explosive and with airborne radiation and contamination. People in the immediate vicinity would likely die from the conventional explosion itself with some survivors dying of radiation poisoning in the weeks afterward. Such bombs could be as small as miniature, easily concealable devices or as large as a truck bomb, killing hundreds immediately and exposing thousands more to radioactive material.

It would not be substantially more difficult to construct a radiological weapon than it would be to build a conventional bomb. The challenge for terrorists would be to acquire the radioactive material to be packed into the device. Unfortunately, the International Atomic Energy Agency notes that virtually every country possesses radioactive substances that could be used to make a “dirty bomb” and that some countries do not guard these materials adequately. Experts warn that organized crime gangs in Eastern Europe may be able to acquire this material through theft or on the black market.

Port security, though, may present the biggest challenge to preventing a “dirty bomb” attack. Terrorists could smuggle in radiological materials or an already constructed radiological bomb in one of the 11 million containers that enter the ports of the United States every year. Currently, only about five percent get proper scrutiny. Such an event could cause ports to be shut down,

(continued on next page)

Global and National Security Threats

Sense of urgency needed to combat variety of dangers

(continued from preceding page)

throwing the entire global shipping system into chaos. Port security must be improved and cargo entering the United States must be inspected and monitored more closely. While funding for port security has increased significantly since 9/11, much remains to be done. A troubling recent report, for example, indicated that many of the government's mobile radiation detectors work only half of the time, raising serious security concerns.

Chemical Attack

The difficulty of obtaining or developing chemical weapons has made their use rare, but these weapons have been used for terrorism. Sarin, a chemical nerve agent, was used in the Tokyo subway system in 1995 and resulted in twelve deaths and hundreds of injuries. Previously, it had been thought that the difficulties of developing, weaponizing and disseminating chemical weapons provided high barriers to their use by terrorists and other non-state actors. Advances in chemistry and engineering, however, have increased the ease by which chemical compounds can be manufactured and experts believe that the technological barriers to chemical weapon use have significantly decreased. Chemical weapons formulas have been publicly available for decades and the ingredients and equipment needed to produce these agents are readily available because they are the same items used commercially every day.

Chemical plants also provide another potential target for a terrorist attack. The Department of Homeland Security has identified 3,400 chemical facilities that, if attacked, would pose the greatest hazard to human life and health. The department has initiated programs to assist industry and local communities in protecting facilities, but has yet to complete a chemical sector-specific security plan.

While voluntary efforts are under way, the chemical industry faces challenges in preparing facilities against terrorism, including high costs and limited guidance on what constitutes adequate security. Chemical companies and indus-

try associations agree that additional legislation placing federal security requirements on facilities is needed, but have not yet reached consensus on the contents of such legislation.

Biological Threats

A biological attack is the deliberate release of germs or other substances that can induce illness. Many agents must be inhaled, absorbed through cuts in the skin or ingested to make one sick. Other biological agents, like the smallpox virus, can result in an illness that can be contagious. Additionally, because biological pathogens multiply within victims, a small initial amount of pathogen is sufficient to cause infection. As a consequence, biological weapons require much less material than chemical weapons to produce equivalent casualties.

Unlike an explosion, a biological attack may not be immediately obvious. While it is possible that individuals might see signs of a biological attack, as was the case with the anthrax mailings, it is more likely that local health care workers will report a pattern of unusual illness or there will be a wave of sick people seeking emergency medical attention. If such a weapon were disseminated widely, especially in the case of a contagious pathogen, there might be government intervention to quarantine individuals or groups of individuals. Use of a biological weapon also could lead to panic by the public and could have large secondary effects on economic markets.

Regional Transportation Systems

Between 1998 and 2005, there were approximately 180 attacks on trains and related rail targets such as depots, ticket stations and rail bridges. Attacks have occurred all over the world and have resulted in nearly 500 deaths and thousands of injuries. Bombs were the most frequently used weapon in these attacks, although firearms also have been used. The 2005 London train bombings that killed 56 and the 2004 bombings in Madrid that killed 191 were among the most sophisticated rail terrorist attacks.

Passenger rail facilities present potentially inviting targets for terrorists for a variety of reasons. They are easily entered and frequently have high concentrations of people. The logistics of a passenger rail attack are relatively simple and substantial casualties can be inflicted with a backpack-sized bomb. Also, terrorists may perceive psychological benefits to attacking passenger transportation networks. An attack is likely to leave passengers reluctant, at least temporarily, to travel on passenger rail systems.

There is a need for a coordinated federal policy on rail security. Compared to other transportation sectors, decision-making is decentralized among a number of federal, state, local and private concerns leading to inconsistency in security measures. A coordinated approach for counterterrorism measures in the rail transportation system should undertake three tasks. First, it should define the federal role in preventing or mitigating such attacks. Second, it should prioritize investments needed for preventing attacks against rail transportation systems with those needed to prevent attacks against other transportation systems. Third, it should define the roles and responsibilities of federal, state, and local agencies and transportation companies in preventing terrorist attacks against rail systems and in responding to their consequences.

Energy Supply Attacks

An electricity blackout in 2003 affected 50 million people in the northeastern and midwestern United States and Canada. Typically, blackouts are caused by severe weather damage or facility equipment failures, most of which can be repaired quickly. Destruction of electricity facilities by terrorist attacks, however, would create a much more serious situation. The blackout of 2003, though not itself the result of a terrorist attack, underscores the vulnerability of electric power transmission lines to such attack.

The electric utility system is vulnerable to outages caused by a range of activities, including system operator errors, weather-related damage and terrorist attacks. The main risk from a successful terrorist attack against the electric power

industry would be widespread power outages lasting for an extended period of time. While the electric power industry has the primary responsibility for protecting its assets, federal and state government agencies also have been addressing physical security concerns. The potential for terrorist attacks on the electric system has pushed secure operation of the power grid into the federal policy arena from its traditional position as an industry responsibility.

Cyberterrorism

Tighter physical and border security may encourage terrorists and extremists to attempt to use other types of weapons to attack the United States. Persistent Internet and security vulnerabilities may gradually encourage terrorists to develop new computer skills, or develop alliances with criminal organizations and consider attempting a cyberattack against the U.S. critical infrastructure.

Usually, a cyberattack is difficult to detect until after it is well underway, and may involve hundreds or thousands of compromised computers that are directed by a cybercriminal to attack as a swarm from all parts of the globe. If the attack is against a yet undisclosed, or newly discovered security vulnerability, the targeted computer systems may be at a significant disadvantage. A new and unique type of attack against computers may encounter inadequate, untested or non-existent defenses.

Cybercrime increased dramatically between 2004 and 2005 and reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals in the international movement of money and in the smuggling of arms and illegal drugs. These links with hackers and cybercriminals may be adding to terrorists' computer skills, and finances obtained through drug trafficking also may provide terrorists with access to skilled computer programmers. The July, 2005 bombing in London also indicates that extremists and their sympathizers already may be embedded in societies with a

(continued on next page)

Global and National Security Threats

Sense of urgency needed to combat variety of dangers

(continued from preceding page)

large information technology workforce.

The United States and the international community have taken steps to coordinate laws to prevent cybercrime. Recently, the Department of Homeland Security completed Cyber Storm, the first full-scale government-led cyber security exercise to examine response, coordination and recovery mechanisms to a simulated cyber-event within international, federal, state and local governments, in conjunction with the private sector. The exercise simulated a sophisticated cyberattack through a series of scenarios directed against critical infrastructures. One of the scenarios simulated an incident where a utility company's computer system is breached, causing numerous disruptions to the power grid.

Computer security experts disagree about whether a widespread coordinated cyberattack by terrorists is a near-term or long-term possibility. However, terrorists have repeatedly demonstrated a willingness to plan and launch conventional attacks against targets that have easy accessibility and numerous vulnerabilities. Internet and computer system vulnerabilities are persistent and widely publicized. As technology continues to advance, the capability, reliance, and interdependent nature of computer systems likely will be more vulnerable to cyberattack tools that are becoming faster and more sophisticated.

Global Pandemic

As Hurricane Katrina demonstrated, terrorism is not the only threat to national security. Natural phenomena, whether in the form of a hurricane-like disaster or in the form of a global pandemic, have the potential to cause even greater damage than terrorism. The human and economic impact of a global pandemic could be devastating.

The World Bank estimates that a two percent drop in global GDP during an influenza pandemic, such as that caused by SARS in East Asia during the second quarter of 2003, would represent a loss of about \$200 billion in output

in one quarter or \$800 billion over a year. The Centers for Disease Control and Prevention estimates that direct medical costs alone in the United States could top \$166 billion.

Influenza pandemics present unique national security challenges because they are not singular events like terrorist attacks. Pandemics unfold over time, re-circulate in waves, continually mutate and persist for months or years. Planning must appreciate the difference between emergency response and long-term disaster planning for shortages of food, medical supplies and other essentials. Few cities and states have thought this through and developed a clear understanding of which individuals will be in charge of various aspects of pandemic response.

Planning must emphasize organizational issues, chains of command and international cooperation. Investments must be made in diagnostics, vaccines and antiviral drugs and in research and development of new flu vaccines. Most importantly, the public and private sectors must work together to combat this and plan for the worst-case scenario.

Security threats from terrorists and natural phenomena are always present. Complacency must constantly be guarded against so that the greatest sense of urgency can be brought to meeting and defeating the unique challenges that each danger may bring.

Businesses, governments and private citizens must all prepare for the worst. Those who are prepared and who have carefully planned for security dangers will not only be more likely to prevent such threats, but will also be capable of responding to a crisis effectively to minimize human and economic costs.



The Lipman Report Editors