Chapter 2

THE ECONOMIC IMPACT OF A TERRORIST ATTACK

We can be a safer, more secure country if we expand our thinking in ways that some might never have considered. In this chapter, I will show you the economic costs of 9/11, and I'll compare that tragic day with other national and international disasters. I'll also ask you to help prevent a future we hope never occurs by contemplating what could go very wrong. I believe that's the best way for us to begin thinking and acting now to prevent major catastrophes.

UTILITY INDUSTRY–PRIME TARGETS FOR TERRORISTS

There are a variety of significant threats to our nation's utility/energy infrastructures. These threats come from several sources, although the most damaging would be from terrorists:

- New hires: It is extremely important to prescreen new employees by running background criminal checks to ensure that they are who they say they are.

- Vendors/contractors: Because of deregulation in the utility/energy industry, companies are downsizing and contracting out services. Due-diligence checks that include terrorism affiliations need to be done on contractors and security checks need to be conducted on their employees.
- Disgruntled employees: They could be knowledgeable about particular energy facilities, and they could get past gates and guards to damage infrastructures. If they also are familiar with cyberspace, disgruntled employees can hack into a utility's computers to cause damage. An employee who was fired from his job at a hotel sought revenge that would offend lots of people. He invaded a nearby utility's computer and caused tons of raw sewage to flow on the hotel's grounds.
- Computer hackers: Some seek to infiltrate large systems just to prove that they are more skilled than the system's designers. Others could be funded by angry stockholders who face major losses if corporate fraud were to occur at any utility/energy companies.
- Game players: Seemingly innocent players of computer games have broken through firewalls to access the more powerful computers in energy facilities. In some cases once inside the power plant's computers, these hackers have found a new game: shutting down utility boilers. Why do they do it? Just to show they can.
- Islamic terrorists: They pose by far the greatest threats. Just as the perpetrators of the 9/11 hijackings went to flight school to learn how to navigate commercial airliners, today thousands of computer-science students from countries that harbor terrorists are enrolled in American universities. Of course this doesn't necessarily mean that any or many of these students will become terrorists. But we should definitely be alert and far better prepared for actions that terrorists might take.

Except when there's damage from a hurricane or tornado or during disruptions such as blackouts, we take our nation's utility/energy infrastructures for granted. Yet these most fundamental infrastructures in our nation carry electricity throughout the country from our electric-power systems. After 9/11 we significantly increased airport and seaport security. That was and continues to be necessary, but it is not sufficient.

Security at our air and seaports is dependent upon electricity. Of course, these security operations have backup energy generators, but they only operate for a specified amount of time before they need to be replen-

ished. I also wonder how many of these backup systems are checked regularly to ensure they that will start when needed.

Beyond the security systems that help screen airplane passengers, we have approximately 6,000 commercial flights per day all over the United States. The air-traffic-control systems that manage all these flights depend upon electricity. We and every other nation in the world are vulnerable to attacks on our power-generating infrastructures.

But if you think that's troubling, let me be straightforward: The situation is far worse than simply being vulnerable. Our nation's utility/energy infrastructure can be used against us. The threat is similar to the commercial aircraft that the 9/11 terrorists transformed into bombs that crashed into our buildings.

MAJOR TYPES OF THREATS

There are five major types of threat to our nation's utility/energy infrastructures. The first threat is a direct attack on the infrastructures. These assaults could be on the ground, using suicide bombers and trucks laden with explosives, or through the air, even using single-engine planes that fly from small airports with far less security than the major hubs. A direct attack could take down a local area, a vast region, or a major portion of the country, even the entire electric grid.

Use the Infrastructure as a Weapon Against Us

The second threat is to transform the infrastructures into weapons used against us. For example, terrorists could dump chemical or biological materials into a power plant's operating system, which could result in contaminating a large area via the cooling towers.

Create Power Surges

The third is to create power surges through the grid. These surges can ruin computers and cause major damage to telecommunications systems and related technologies. If these systems are interrupted, communications will be lost and financial transactions of all sorts will stop.

Cyber Attack

The fourth is a cyber attack. Hackers located anywhere in the world could break into the computer systems that control the utility/energy

Ness Group International
Professional Loss/Risk Consulting

Larry Ness
President/Owner
Ness Group International – Dallas, TX
WWW.NESSGROUP.COM
LNESS@NESSGROUP.COM
214.415.9687 Office

EMPLOYEE BACKGROUND SCREENING POLICY

Effective August 1, 2002, _____ will introduce new policy guidelines that will identify the process for verifying information given to _____ by prospective employees.

The purpose of the policy is to provide management with guidelines to insure consistency in the verification process and to insure compliance with the provisions of the Federal Fair Credit Reporting Act and other applicable State and Federal Guidelines.

The following is an overview of the policy and process, which will be administered and managed by the Corporate Security Director.

All applicants who are interviewed, either in person or via telephone, must be informed at the time of the interview that _____ will conduct a background check **after an offer has been tendered and accepted.**

The background check will consist of the following:

- Verification of the information given to _____ on the applicant's resume and/or employment application, e.g., work history and education,
- Social Security Number verification,
- Criminal history check and,
- Driving record verification (Applicable to those who are responsible for driving company owned or leased vehicles. This does not apply to vehicle rental while on business travel).

Applicants must also be informed that, if selected, they will be required at the time of hire to sign a **Notice and Consent form,** which authorizes _____ to conduct the background check, and

Figure 2.1 Employee background screening policy *(continued on next page)*

Release of Liability form.

The Notice and Consent and release of liability forms need only be given to applicants who **are offered and accept** a position with _____. To clarify, all applicants who are interviewed must be notified that _____ will conduct background checks if and when they receive and accept an offer of employment, but only those for whom an offer is tendered and accepted will Notice and Consent and Release of Liability forms be presented for signature.

After accepting an offer for employment, the New Hire will receive the following documents:

- Notice and Consent (Must be signed)
- Release From Liability (Must be signed)
- Prescribed Summary of Consumer Rights
  - The *Notice and Consent* form notifies the New Hire that a background check will occur and the signature gives _____ consent to proceed.
  - The *Release from Liability* must be signed and filled out with date of birth and Social Security number. **Note: It is important that the date of birth and social security number be accepted only after an offer and acceptance of employment.**
  - The *Prescribed Summary of Consumer Rights* form explains the employee's legal rights under the Fair Credit Reporting Act. Under certain circumstances, this form must be given three times: once in the initial offer and acceptance, prior to rescinding any offer as a result of information received during the background check and again if the offer is rescinded at a later date as the result of information received during the background check.

The New Hire must also be notified prior to the date on which the background report is first requested.

Once the background check is completed, Human Resources and the Hiring Manager will be notified. If the background contains adverse information, the Human Resources Department and the Hiring Manager will review the information and make the decision for continued employment or to rescind the offer of employment based in whole or in part on the results of the background check. If the offer for employment is rescinded, the Hiring Manager and Human Resources must:

Figure 2.1 Employee background screening policy *(continued on next page)*

- Present the employee with a copy of the background report;
- Give the employee an additional copy of the *Prescribed Summary of Consumer Rights form;* and
- Give the employee a reasonable amount of time (three business days) to dispute the accuracy of the report.

If the employee does not dispute the accuracy of the report, fails to respond within a reasonable time (three business days), or fails to provide feedback to the Human Resource Department and the Hiring Manager within the time period specified, the offer of employment shall then be rescinded. The employee must then be provided with the following:

- Oral, written or electronic notice of the adverse action,
- Name, address and telephone number of the consumer reporting agency that furnished the report,
- Statement that the consumer-reporting agency did not make a decision to take adverse employment action and is unable to explain the specific reasons behind the decision and
- The *Prescribed Summary of Consumer Rights form.*

Any questions or concerns relative to this policy should be submitted to the Director, Corporate Security.

Figure 2.1 Employee background screening policy *(continued)*

infrastructures. The results at electric-generating plants, for instance, could vary from power losses to power surges. For water facilities, the pipelines could be closed to prevent distribution or opened to cause flooding. For sewage plants, the offal could be dispersed into reservoirs that would become polluted. For nuclear facilities, an attack could result in deadly fallout in metropolitan areas.

Lack of Vital Spare Parts

The fifth is a lack of vital spare parts. Core components of our nation's utility/energy infrastructures were built forty or more years ago, yet we do not stockpile the most important large spare parts. If and when key power-generating turbines wear out or are destroyed, for example, it could take six or more months to get replacements built and shipped from overseas, where most of them are manufactured.

TERRORISTS' GOALS

Despite this focus on infrastructures, please don't think that Islamic or other terrorists simply target systems. Instead, they target people, masses of people. They use systems to kill people and, ultimately, to cripple economies. Two tragic examples are the hijacked planes used to attack thousands of people in office buildings during 9/11 and the railroad cars carrying hundreds of people that they blew up in Spain during 2004.

But this strategy of attacking enemies is not new. Islamic extremists began that tradition in the 11th century. The terrorist threat to our nation's utility/energy infrastructures is real. Here's a brief historical perspective.

Jihadism Began in the 11th Century

Let us use Islamic history as an example of the historical development of terrorist activities. According to Elizabeth Cobbs Hoffman, the Dwight Stanford Professor of American Foreign Relations at San Diego State

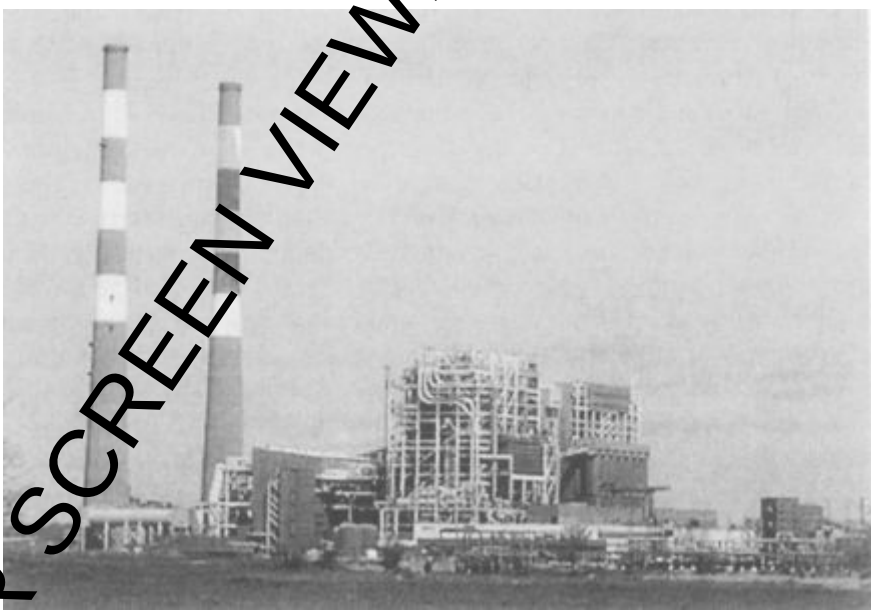

Figure 2.2 LaCygne power plant

University, martyrdom was an expression of political terrorism as early as the 11th century. At that time a religious leader, an imam called Hassan, established a ruthless cult that became known as the Assassins. He inspired passionate devotion with extreme interpretations of the Koran and a strict requirement of obedience.

To prove their devotion, cult members were required to undertake suicide missions with the goal of murdering the enemies of the imam. "Terrorism was a political act and a sacred religious duty," Professor Hoffman stated. "Angels would carry the broken bodies of the Assassins to Paradise."

The first Islamic jihad, or Holy War, developed in the early life of Islam. The teachings of Mohammad, who died in 632 CE, incorporated both Jewish and Christian teachings. There was one God, Allah, and Muhammad was His Prophet, as was Jesus and the pre-Christian Jewish prophets of the Torah, the Jewish Bible. Both Jesus and the prophets were called "children of the book," and the book was the Koran. It replaced both the Old and New Testaments, spreading in all directions from the Saudi Arabian peninsula.

During this first Islamic jihad, Islam met with little resistance as it firmly established the religion on the Iberian peninsula. Charles Martel of France, the father of Charlemagne, stopped the onward march at the battle of Tours in France. Islam was finally driven out of Spain in 1492 at the battle of Granada, which ended the first jihad.

The Ottoman Turks carried out the second Islamic jihad. That empire caused the downfall of Constantinople as a Christian stronghold and brought an end to Roman hegemony in its various forms. Although the Ottoman Empire was a most successful expansion of Islamic territory, the religion became fractured into warring sects and bitter rivalries. By 1683 the Ottomans had suffered many defeats on land and sea. When they failed to capture Vienna, further territorial ambitions were diminished. Islam shrunk into various sheikhdoms, emir-dominated principalities, and roving tribes of nomads.

By this time, however, a growing anti-Western sentiment became part of the Islamic fundamentalist dogma. Internal failures were blamed on others, particularly Westerners. The new sect that predominated during this new revival was called Wahhabism. Shortly before the beginning of World War I, it came into full bloom under the House of Saud on the Arabian peninsula. This Wahhabi version of Islam has infiltrated the religion itself, now finding adherents in almost all branches and sects,

especially the Shiites. What this sect calls for is the complete and total rejection of anything and everything not based in the original teachings of the Prophet.

Wahhabism finds its most glaring practice in the policies of the Afghani Taliban and the Shiite practices of Iran's late Ayatollah Khomeini. Its Field Marshall is Osama bin Laden. He is the leader of the third Islamic jihad. In 1983, this movement got worldwide attention through actions of an Islamic terrorist organization funded by Iran and Syria named Hezbollah. In April of that year, a suicide bomber exploded a truck in front of the American embassy in Beirut, Lebanon. 63 employees were killed and 120 were wounded. In October 1983, 241 U.S. Marines were killed and 81 more were wounded when another Hezbollah suicide bomber blew up an American barracks at Beirut's airport. That December, the American embassy in Kuwait was bombed.

In 1984, the CIA station chief in Beirut, William Buckley, was kidnapped and murdered. During September 1984, an annex to the U.S. Embassy near Beirut was bombed. In June 1985, Hezbollah hijacked an American airliner and made the pilots fly to Beirut, where they held the pilots and passengers for more than two weeks. The jihadists killed an American naval officer who was on the plane and threw his body on the tarmac.

Later that year an Italian cruise ship, the *Achille Lauro,* was hijacked by a group led by Abu Abbas of the Palestine Liberation Organization (PLO). An elderly American passenger who was confined to a wheelchair, Leon Klinghoffer, was thrown overboard.

After several terrorist incidents in Rome, Vienna, and Berlin that were tied to Libya's leader, Muammar Qaddafi, left many Americans dead, the U.S. attacked Libya. Three U.S. citizens who worked in Beirut were killed in retaliation by Palestinian terrorist Abu Nidal.

In December 1988, Pan Am flight 103 blew up over Lockerbie, Scotland, killing more than 270 people, mostly Americans. Two Libyan intelligence officers were tried for planting the bomb; one was convicted, the other acquitted.

I am purposely not focusing on which U.S. President did how much—or how little—after which terrorist action, because I don't want to deflect from a focus on terrorism. I have no desire to even appear to favor Republican or Democratic administrations. Instead, I am trying to provide brief, solely factual summaries of terrorist incidents that occurred during the administrations of Presidents Ronald Reagan, George Bush, Bill Clinton, and George W. Bush.

Terrorism in America

Terrorist action came to the continental U.S. early in 1993. On February 26 a truck bomb exploded in the parking garage of the World Trade Center in New York City. Six people were killed and more than 1,000 were injured. Six Muslim terrorists were convicted and sent to prison.

We subsequently learned that a terrorist Islamic networked named al Qaeda was behind the World Trade Center bombing of 1993 and its leader was Osama bin Laden. During the next two years, Islamic terrorist acts occurred in Israel, Lebanon, Pakistan, Saudi Arabia, Turkey, and Yemen. In Pakistan during 1995, for example, two American diplomats were killed, and in Saudi Arabia that year, five Americans died when a car bomb exploded.

In June 1996, a truck bomb detonated at a building in Saudi Arabia, killing 19 Americans and wounded 240 more. Two years later, American embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, were bombed, leaving more than 200 dead, including many Americans. Al Qaeda claimed credit for the bombings, both of which occurred on August 7. On October 12, 2000, bin Laden attacked the USS Cole, a destroyer that had been docked in Yemen. The team of suicide bombers killed 17 American sailors and wounded 39 others.

No Stopping Terrorism

This is a brief summary of terrorist actions largely against the United States that led up to the events of September 11, 2001. My purpose in presenting this overview is to show a continuum of jihadist actions. They began in the 11th century, and over the last twenty years, many of them have been directed against American interests.

These attacks by Islamic extremists are continuing. And they will persist. Please don't think otherwise, or you will be helping to put yourself, your family and our country at risk.

Here is my most important point: We cannot stop terrorism. But we can and we must be alert to the continuing threat, and we can and we must develop a variety of effective ways to make our most important targets far less vulnerable. By hardening our many targets that are at risk, we can make jihadist acts harder to complete, and we can convince some terrorists to try other, softer targets in far-off parts of the world.

There's been much speculation in the media and years of debate in Congress about increased security in response to perceived threats. Here's just one much-discussed example. There is a possibility that terrorists could assemble a dirty atomic bomb, steal a Scud missile, place both on a

boat that runs near one of our coastlines, and then shoot the dirty bomb high into the earth's atmosphere. The result could trigger an electromagnetic pulse (EMP) attack.

The pulse generated by the blast would destroy electronics and satellites in its field of vision. A well-executed blast, for example over the Midwest, would not kill people, but it could cause great damage to telecommunications and electronics, including our electric grid, with disastrous consequences. This could happen. My point is not to discount this horrible, possible act, but to focus us in a different direction: The national electric grid and other vital portions of our utility/energy infrastructures can be knocked out much more easily than through an EMP attack.

Similarly, it would be much easier for jihadists to hijack planes that are then crashed into financial centers, government buildings, or sports events where tens of thousands of Americans have gathered. And terrorists would find it easier, far quicker, less costly, and much more likely to succeed if they set their sights on our utility/energy infrastructures. They could accomplish any one of these actions:

- Physically enter one or a number of our inadequately protected chemical, biochemical, electricity-generating, or water-treatment plants and release fluids or pulses that would create havoc over wide areas.
- Dump highly-toxic chemicals into reservoirs that serve any number of the nation's major cities.
- Use the Internet to hack into computer systems that control energy-generation plants, water supplies, oil and natural-gas distribution lines, chemical pipelines, and much more. This cyber warfare can be done from thousands of miles outside the U.S. by people with basic computer knowledge. It's already happening many thousands of times every day as outsiders seek to hack into computers housed at the Department of Defense (DOD) and other military installations. Our military facilities are prepared for this. Most civilian organizations managing our nation's utility/energy infrastructures aren't.

Please note that nothing in this list is news to terrorists. This and all other information in this book is publicly available.

IMPACT COMPARISONS VERSUS OTHER CRISES

We are all still too painfully aware of what happened on 9/11. But please take a moment to think back in time. What if someone had come to you on September 10 and said, "I'm worried that terrorists could

hijack some large passenger planes and crash them into skyscrapers and government buildings!"

What would you have said to that person? Beyond what you would have said, more importantly, what would you really have thought about him or her? I think I know your answers. Since 9/11, you and everyone else in the United States have had to adjust his or her thinking. We as a nation not only have begun to think differently; we have also had to change what we plan and how we act.

Now we must do more. We must act more defensively to provide greater protection to our country. So I'm asking you to think about the possibility of a catastrophe in America that makes 9/11 seem as if it's only the first act. Open your mind to the potential misuse of our nation's utility/energy infrastructures by terrorists so that tens of thousands of people are killed and hundreds of billions of dollars are lost.

This thinking can help ensure that the worst-case scenarios won't occur by recognizing the natural and man-made disasters that have happened both here and abroad. The terrorist attacks of September 11, 2001 resulted

Figure 2.3 Transmission substation

in a massive loss of life, destruction of property, and shocks to various economic systems. Although the attack on the World Trade Center ranks as one of the most fatal disasters in U.S. history with 2,976 fatalities, it is half the loss of life that occurred during the Galveston Hurricane of 1900, which took over 6,000, lives or, in another part of the world, the 1991 Bay of Bengal cyclone that killed 139,000. In fact, the 9/11 death toll does not even make the top 100 list of worldwide disasters in the last 100 years.

On a global basis, even more significant in terms of death toll and persistence has been the genocide occurring within Burundi and Rwanda. Approximately 1.2 million people have died in at least six distinct Hutu-Tutsi ethnic exterminations since 1965, most notably 800,000 in Rwanda in 1994.

Terrorism is more of a clandestine process designed to allow small organizations or networks with limited resources to wage war against more powerful governments and nations over long periods of time. As such, attacks range from small to large in magnitude and usually occur in an unpredictable, almost random fashion. The negative economic impact of such a nefarious process is long-term, sustained by not only the actual acts of destruction but also the pure fear of the when, where, and how of that next attack.

IMPACT ON THE UNITED STATES ECONOMY

It's certainly important to study the historical effects of massive outages. But how can we use this information to understand the short- and long-term economic and social impacts if we lose the entire grid for an extended period of time?

When we think about massive outages from a conventional point of view, there is a tendency to point to the following types of widespread yet still localized examples:

- 1965, 1977, and 2003 blackouts in New York City and neighboring areas, with cost estimates of the most recent event ranging up to $10 billion
- August 10, 1996: 7.5 million customers across 11 western states and two Canadian provinces lose power, some for several hours. The estimated economic losses are $2 billion
- August 13, 1999: Downtown Chicago blackout, which shut down about 3,000 businesses in the Loop and caused $100 million in estimated economic losses

- March 18, 2000: 550,000 customers in New Mexico lose power due to grass fire, rendering a key transmission line to be inoperable.

A joint undertaking of Mirifex, a regional business-technology consulting firm, the Center for Regional Economic Issues at Case Western Reserve University's Weatherhead School of Management, and CrainTech measured the economic impact of the 2003 blackout. The event continues to have far-reaching, long-term implications for businesses in the affected region.

Study findings incorporate the input from 129 executive-level managers in Ohio, New York, Pennsylvania, Michigan, Wisconsin, and southern Canada. The key findings are:

- 11 percent of firms say that the blackout will affect their decision-making with regard to either growth or relocation.
- As a consequence of the blackout, over one-third of businesses surveyed (38 percent) said they would be somewhat or very likely to invest in alternate energy systems.
- More than one-third of firms surveyed (34 percent) have no risk management or disaster recovery plan in place.
- Nearly half (46 percent) of the businesses surveyed will invest more in risk management, business continuity, and/or disaster recovery in the future.
- More than a third of the businesses surveyed (35 percent) felt that it was somewhat or very likely that the region's image would suffer as a result of the blackout.
- Two-thirds of the businesses surveyed (66 percent) lost at least a full business day due to the blackout.
- One quarter of the businesses surveyed (24 percent) lost more than $50,000 per hour of downtime—meaning at least $400,000 for an 8-hour day. And 4 percent of businesses lost more than $1 million for each hour of downtime.
- Nearly half the businesses surveyed (46 percent) said that lost employee productivity was the largest contributor to losses suffered due to the blackout.
- Production/manufacturing and customer sales/service were the areas of business hardest hit by the blackout.

How vulnerable is the grid itself? Reka Albert, assistant professor of physics at Pennsylvania State University, has studied the topology of the grid structure and concluded that, although the grid has been designed to withstand random losses of generators and/or substations, its overall integrity may depend on a few key elements. "Our analysis indicates that major disruption can result from loss of as few as two percent of the grid's substations," says Albert, whose research team includes Istvan Albert, research associate in the Bioinformatics Consulting Center at Penn State, and Gary L. Nakarado at the National Renewable Energy Laboratory. One implication of the research is that the identification of a few strategic points in the grid system can bring down the system.

The study, titled "Structural Vulnerability of the North American Power Grid," was published in a recent issue of the journal *Physical Review E.* The researchers constructed a model of the entire transmission grid with over 14,000 "nodes" which include generators, transmission substations, and distribution substations, and more than 19,000 "edges," corresponding to the high-voltage transmission lines that carry power between the nodes. They measured the importance of each substation node based on its "load," or the number of shortest paths between other nodes that pass through it. "While 40 percent of the nodes had a load below one thousand, the analysis identified 1 percent of the nodes—approximately 140—that has a load higher than one million," Albert says.

This high degree of connectivity in the grid system allows power to be transmitted over long distances, but it also allows local disturbances to propagate across the grid. "There are systems to protect the nodes from overload, such as a controlled shutdown to take a substation out if it overloads or to shut off a generator. In general, these systems do a good job of protecting the nodes," says Reka Albert. "What this model really looks at is the effect of losing a number of nodes in a short period."

If the nodes are removed randomly, the effect on the system is roughly proportional to the number of generators or substations removed. However, the grid quickly becomes disconnected when the high-load transmission substations are selectively removed from the system—if the nodes that have the highest load are removed first, followed progressively by the nodes with successively lower loads. According to the model, a loss of only 4 percent of the 10,287 transmission substations results in a 60 percent loss of connectivity. During a cascading failure, in which the high-load substations fail in sequence, the model shows that the loss of only 2 percent of the nodes causes a catastrophic *failure of the entire system.*

An attack on poorly protected elements of substation automation systems could achieve disastrous effects for the overall grid. In fact, over one-half of the electric utility personnel who responded to a recent Electric Power Research Institute (EPRI) survey believed that a cyber intruder in the information and control systems at an electric utility could cause serious impact on their regions and beyond for more than 24 hours. Easily available resources such as Federal Energy Regulatory Commission (FERC) filings, electricity industry publications, transmission and distribution maps, and the Internet provide ample information on the most critical transmission lines and substations in the power grid. Relatively simple hacking techniques could then be used to locate ports to these points that trigger outages.

Let's turn from attacks on the nation's electric grid to the possibility of a terrorist attack on a nuclear power plant. In 2004, Edwin S. Lyman, Ph.D., of the *Union of Concerned Scientists* conducted a study entitled "Chernobyl on the Hudson? The Health and Economic Impacts of a Terrorist Attack at the Indian Point Nuclear Plant." It reported the following quoted findings:

- The current emergency-planning basis for Indian Point provides insufficient protection for the public within the 10-mile emergency-planning zone in the event of a successful terrorist attack. Even in the case of a complete evacuation, up to 44,000 early fatalities are possible.
- The radiological exposure of the population and corresponding long-term health consequences of a successful terrorist attack at Indian Point could be extremely severe, even for individuals well outside the 10-mile emergency planning zone. Lyman calculated that over 500,000 latent cancer fatalities could occur under certain meteorological conditions. A well-developed emergency plan for these individuals, including comprehensive distribution of potassium iodide throughout the entire area at risk, could significantly mitigate some of the health impacts if promptly and effectively carried out. However, even in the case of 100 percent evacuation within the 10-mile EPZ and 100 percent sheltering between 10 and 25 miles, the consequences could be catastrophic for residents of New York City and the entire metropolitan area.
- The economic impact and disruption for New York City residents resulting from a terrorist attack on Indian Point could be immense, involving damage from hundreds of billions to trillions of dollars

and the permanent displacement of millions of individuals. This would dwarf the impact of the 9/11 attacks. The economic damage within 100 miles would exceed $1.1 trillion for the 95th percentile case, and could be as great as $2.1 trillion for the worst case evaluated, based on Environmental Protection Agency guidance for population relocation and cleanup. Millions of people would require permanent relocation.

- The potential harm from a successful terrorist attack at Indian Point is significant even when only the mean results are considered and is astonishing when the results for 95th and 99.5th meteorological conditions are considered. Given the immense public-policy implications, a public dialogue should immediately be initiated to identify the protective measures desired by the entire affected population to prevent such an attack or effectively mitigate its consequences should prevention fail. As this study makes abundantly clear, this population extends far beyond the 10-mile zone that is the focus of emergency-planning efforts today.
- To better understand the amount of loss this nation might sustain, experts conduct modeling efforts. A terrorist attack can lead to significant economic loss, both as a direct consequence of the attack as well as through the secondary or ripple effects felt around the affected region.

Costs of Recovery

A White House report, *The National Strategy for Physical Protection of Critical Infrastructures and Key Assets,* calls for efforts to "develop economic models of near- and long-term effects of terrorist attacks." The report highlights the temporal and cross-sector complexities of modeling such economic damages because the ripple effects across sectors and geographical areas may be significant although difficult to predict. ICF Consulting, in collaboration with Regional Economic Models, Inc. (REMI), explores methodologies and models to measure such potential economic damages.

As part of this effort, the report modeled economic changes resulting from hypothetical terrorist-attack scenarios. It analyzed the impact of a coordinated attack on the electricity- transmission grid in California, for example, resulting in a sizeable loss in electricity supplied to the state. The modeling focused on the economic damages of these attacks, avoiding issues related to measuring the human toll. ICF Consulting examined the

scenarios to estimate direct costs on affected industries and calculated the ripple effects on other industries and the economy as a whole. This study revealed the magnitude of the losses and helped determine the best strategies for policymakers to prepare for and mitigate damages.

Another way to estimate the impact on our economy is to simulate an attack. One simulation focuses on a California transmission grid. Based on ICF Consulting's expertise in the energy-transmission and homeland-security sectors, it was hypothesized that the simulated attack on the electric grid caused a severe disruption in the power supplied to California and led to a 25 percent reduction in the availability of electricity. This initial loss resulted in significant economic damage but for a very short period of time.

During the day of the simulated attack, authorities were able to reoptimize the grid and restore power to certain prioritized sectors. This incomplete restoration led to rolling blackouts for an extended period of time. The gradual ramp-up was assumed to continue for two weeks, after which the system was back to its pre-attack state. The economic damage from this attack was calculated for this two-week period. Significant damage resulted from this terrorist attack, leading to a total direct cost of approximately $11 billion.

This initial direct damage predicted by this model had a ripple effect and led to another $7 billion in secondary impact on the state's economy. The total loss of about $18 billion was approximately 1.3 percent of the gross state product of California. The significant negative shocks of this model led to more than 122,000 lost jobs in that state.

To help understand the economic costs of a terrorist attack in the future, we can more closely examine the direct and indirect costs and the timing, both immediate and long-lasting, from the 9/11 attack.

Direct Impacts

Various accounts of the aftermath of 9/11 list well-known statistics, such as the facts that lower Manhattan lost about 30 percent of its office space and that a significant number of businesses ceased to exist. About 200,000 jobs disappeared or fled New York City. Destroyed tangible assets amounted to $14 billion for private enterprises, $1.5 billion for state and local government concerns, and $700 million for federal agencies. Total immediate cleanup and other recovery costs have been estimated in the range of $11 billion. These figures add up to a staggering total direct cost of $27.2 billion.

Indirect Impacts

The security-conscious culture immediately instilled as a direct reaction to 9/11 has had a significant impact on several key industries, including insurance, airlines, tourism and travel, and defense. Let's take a look at each of these industries.

Insurance

Losses from 9/11 have been estimated at between $30 and $58 billion. By comparison, Hurricane Andrew's 1992 ravage of the state of Florida caused about $26.5 billion in losses. The federal government has slated $11.6 billion to help Florida and other eastern states rebuild from the cumulative effects of the four hurricanes that occurred in 2004.

Most insurers increased terrorist insurance premiums at least 30 percent almost immediately after 9/11, and others just dropped that type of coverage completely. These increases have negatively impacted many industries, such as airlines, transportation, construction, tourism, and energy.

Airlines

The airline industry was hit particularly hard. Routes were curtailed or eliminated due to lower passenger traffic, higher fuel costs, and the hassle factor of flying in general. For many short routes, it's just as fast to drive when taking into account increased airport-security measures. The U.S. airline sector lost 40 percent of its value when the market reopened after 9/11 and has never fully recovered. Other related industries that have also been negatively impacted include tourism, automobile rentals, and commercial-aircraft manufacturers.

Defense Spending

The Congressional Budget Office (CBO) recently estimated the cost of occupying Iraq and other operations associated with the global war on terrorism for fiscal year 2005. Assuming current levels of effort, CBO projects that the Department of Defense (DOD) will likely require $55 billion to $60 billion in a new budget. This estimate includes only the costs above amounts budgeted for routine military operations. It does not include any of the cost for reconstruction activities carried out by DOD or other governmental agencies. CBO has estimated the 10-year (2005-2014) cost of the occupation of Iraq and other operations (Noble Eagle, Enduring Freedom, classified activities, coalition support, and activities that cannot be allocated to specific operations) to be between $182 billion and $393 billion.

Some of the immediate economic impacts resulting from 9/11 have been lessened to varying extents, but there are permanent losses that will never be recovered. For example, the diminution of terrorism-related insurance coverage will stymie investment of capital in businesses more vulnerable to terrorist acts due to higher potential risks. Another example is the additional deficits due to accelerating defense needs imposed on the federal budget, which can hamper growth and productivity.

Longer Term Impacts

The ever-present threats of potential terrorism can be analyzed by looking at the components making up productivity—output divided by input. Let's take a look at how these components are affected.

- Most industries will have increased operations and maintenance expenses due to higher spending levels for physical and cyber-security needs, insurance requirements, and corporate taxes. Many high-tech product-development costs will be larger due to increased security features.
- Many firms hold larger amounts of inventory due to increased risk of shipping, including air, rail, and trucking. For example, immediately after 9/11, industries that depended on supplies from foreign countries learned a lesson because they had production interrupted by security-related delays.
- In addition to higher debt-financing costs due to increased business risk, most companies have experienced demand for higher returns from their stock to attract needed equity investment. This in turn has raised the cost of equity capital for business-expansion purposes.
- In order to combat terrorism head on, governmental research and development (R&D) resources have been shifted away from civilian applications to military use. As a result, more of a financial burden is being placed on private enterprises to make up the difference.
- Firms tend to invest closer to home under the potential threat of terrorism, mainly due to increased transaction costs—higher insurance premiums, shipment delays caused by increased security checks, and fear of unstable political situations, reducing the ability of businesses to expand to global markets.
- If and when there is a terrorist attack with long-term consequences, a recent study reported that 40% of Fortune 1000 companies will not survive two years after the attack, unless they are properly prepared.

According to a report prepared by IFC Consulting in Fairfax, Virginia, the cost of the 2003 blackout was between $7 and $10 billion for the national economy "and would been significantly higher had it been caused by a terrorist attack." This study points out that beyond grid malfunctions, there is a "hangover effect... the most significant burden was borne by the tourism industry as people became nervous and avoided travel."

If we talk about the costs of recovery proactively instead of reactively, we change the subject to ways that utilities get reimbursed for security improvements. New legislation and regulatory proceedings in some states have been developed to achieve cost recovery, often involving rate case proceedings. In Michigan, for example, Jeff Pillon is the Chairman of the Energy Data and Security Committee of the National Association of State Energy Officials (NASEO). "Utilities in Michigan are not reluctant to take upfront actions that improve the security of their critical infrastructures, then petition the state for cost recovery," he says. "Commissions here are predisposed to approve these investments. Some utilities take the defensive perimeter approach; others are more aggressive in their pursuit of security by, for instance, building in redundancy that leads to greater reliability. The latter group anticipates all-hazards protection in terms of terrorists who could blow it up or hurricanes that could blow it down."

Michigan is one of the leading states. A July 2004 report prepared for the National Association of Regulatory Utility Commissioners (NARUC) Ad Hoc Committee on Critical Infrastructure concludes, however, that "Most states have not received security-specific cost-recovery requests."

California, Florida, Iowa, Michigan, New Jersey, New York, and Oklahoma are the examples for other states to follow. Chapter 3 presents important initiatives by these states, the federal government, the utility/energy industry, and private enterprise that help to protect the utility industry.