Energy Infrastructure and Security

Alexander E. Farrell[1], Hisham Zerriffi[2], Hadi Dowlatabadi[3]
[1]*Energy and Resources Group, University of California Berkeley, 310 Barrows Hall, Berkeley, CA 94720-3050; email: afarrell@socrates.berkeley.edu*
[2]*Department of Engineering and Public Policy, Carnegie Mellon University, 129 Porter Hall, Pittsburgh, PA 15213-3890; email: hisham@cmu.edu*
[3]*Sustainable Development Research Initiative, University of British Columbia, 216, 1924 West Mall, UBC Vancouver, BC Canada V6T 1Z2; email: hadi@sdri.ubc.ca. University Fellow, Resources for the Future.*

Key Words energy security, critical infrastructure protection, terrorism

Abstract Concerns about how to safeguard key infrastructures (energy, communications, banking, roads, etc.) from deliberate attack are longstanding, but since the end to the cold-war, emphasis has turned to the possible impacts of terrorism. Activities to address these concerns are sometimes called Critical Infrastructure Protection (CIP), which is somewhat different from the longstanding concept of 'energy security,' which focuses on politically and economically motivated supply interruptions. Different elements of the energy infrastructure are characterized by distinct vulnerabilities. Breaches of security in nuclear plants can lead to large scale environmental disasters – but the infrastructure is concentrated and relatively easy to guard. Oil and gas production, transportation and refining infrastructures are often spatially concentrated, and disruptions can lead to shortages if supply is not restored before stored reserves are exhausted. Traditional electricity infrastructures suffer from requiring system-wide integrity for supply reliability, having critical facilities spatially concentrated (substations) and insignificant storage capacity for emergency supply. This review discusses how energy infrastructure and security are related, how it differs from most traditional energy security terms, and what it may mean for private and policy decisions. Key concepts include redundancy, diversity, resilience (or security), storage, decentralization, and interdependence. The concept of CIP is still relatively new and is likely to evolve over time, possibly away from a 'guards, gates, and guns' defensive approach and towards a design approach that yields systems that are inherently harder to successfully attack. Such survivable systems may feature distributed intelligence, control, and operations.

1 INTRODUCTION

Conflict over resources stretches far back in human history and energy infrastructures have long been subject to deliberate attacks. For instance, the New World Liberation Front (NWLF) bombed assets of the Pacific Gas & Electric Company (PG&E) over ten times in 1975 alone. Members of the Ku Klux Klan and San Joaquin Militia have been convicted of conspiring or attempting to attack energy infrastructure (1 pp. 5-7, 2). Organized paramilitaries have had very significant impacts in some countries. For example, the Farabundo-Marti National Liberation

Front were able to interrupt service in up to 90% of El Salvador at a time, and even produced manuals for attacking power systems (3). Other examples of conflicts that have resulted in significant damage to electricity systems include the civil war in Bosnia-Herzegovina and the conflicts in Lebanon. Less direct attacks have occurred as well such as the delivery of anthrax to the British Petroleum (BP) office in Ho Chi Minh City, Viet Nam in 2001 (4 pp. 5-12). Oil and natural gas infrastructures in Colombia and Nigeria have experienced numerous attacks. Recent wars have involved attacks on other energy infrastructures. For instance, the United States, operating under NATO auspices, destroyed portions of the Serbian electric power infrastructure in 1999. During the Iran-Iraq war, Iran seized all of the offshore oil production platforms of the Dorra field in the Persian Gulf. When Iran retreated at war's end in 1988, several platforms were destroyed. Several years later Iraq spectacularly set fire to the Kuwaiti oil fields during retreat in the Gulf War in 1991.

These events and especially the rise of catastrophic terrorism in industrialized countries, like the September 11, 2001 terrorist attacks, have heightened attention on the security of energy infrastructures. Concerns include the vulnerability of energy infrastructures to deliberate attack, the consequences of such attacks, and means of preventing or mitigating their effects.

Terrorist groups have differing goals and capabilities and it is not clear if a highly successful physical attack on an energy infrastructure would have the same social effect as terrorist attacks that claim lives or focus on symbolic targets. Responses would likely include outrage and a sense of vulnerability, but evidence from recent large-scale blackouts indicates that panic and shock do not generally ensue. Recent war game exercises have shown that in the U.S., attacks on the chemical sector may pose far larger risks than those on the energy sector (5). Nonetheless, several groups have attacked energy infrastructures in the past and can be expected to do so in the future.

We consider four main energy supply infrastructures; oil, gas, electricity, and nuclear power; but also mention end-use, where efficiency and storage (e.g. batteries in portable devices) are possible responses. Clearly, vulnerability of the primary source of energy is a common concern across oil, gas and electricity, hence renewable energy supplies are a recurring theme. In this review, we first provide some background; next present key concepts and discuss Critical Infrastructure Protection (CIP) efforts; then discuss oil and gas, electricity, and nuclear power infrastructures individually; and address prevention and response. We close with some brief conclusions.

1.1 Background

The modern idea of 'energy security' emerged in the 19th century as warfare became mechanized and began to require substantial fuel inputs, first as coal for warships and trains (6). The decision of the British Admiralty prior to the First World War to switch from coal-fired to oil-fired vessels marked the start of the now traditional link between petroleum and security (7 pp. 155-6, 8 pp. 2-3, 9 pp 29-31, 10 pp. 2, 391). Today, the term energy security and oil supplies are implicitly linked. The links between energy security and resource depletion (11-13), and geographic concentration of resources (e.g. oil in the Persian Gulf region) are also important themes (9, 14-17), but they are beyond the scope of this review. This review is focused on the issue of intentional acts aimed at disruption of an energy infrastructure and measures to reduce

their occurrence and impact, so while the concepts of scarcity and geopolitics may accentuate infrastructure security concerns, they are not central.

1.2 Early Analyses

The theme of energy infrastructure and security appears in more general studies of national security and warfare. During the Second World War, the Allies missed a significant opportunity to shorten hostilities by failing to target Germany's energy infrastructure (18 pp. 49-55). A similar failure to attack Japan's energy infrastructure was less important because it was highly decentralized and thus would have been very difficult to damage. An analysis of strategic attack of electric power systems during the Korean, Vietnam, and First Gulf War showed that such efforts were not highly effective in affecting public morale, economic activity, or war-fighting capability (19). Moreover, this study argues that the requirements for international support during the prosecution of a contemporary limited war would likely make strategic attack on energy infrastructure an unattractive option. However, there may be underlying issues for the lack of success of such attacks, such as little dependence on electricity on the parts of the Koreans and North Vietnamese, and significant preparations on the part of the Iraqis. Further, the successful attacks by U.S. forces operating under NATO auspices on the Serbian electric power system during May, 1999 suggest military campaigns may continue to feature attacks on electric power systems (20).

Cold War analyses focused on limited or full nuclear exchange between the United States (and its NATO allies) and the Soviet Union (and its client states), and often discussed the potential impacts of such a nuclear exchange on energy infrastructure. We can only guess that much relevant analysis remains classified, but the 1958 U.S. Department of Defense report "Emergency Plans Book" has been published in the open literature (21). Reporting the expected outcome of a large-scale nuclear war, the report predicts that much of the energy infrastructure will be destroyed, but so, too, would much of the demand. Many electricity generators were expected to survive an urban-focused strike, but transmission systems were expected to be largely destroyed, as were petroleum refining and shipping facilities. Local fuel stocks were expected to be consumed relatively rapidly, while massive loss of life, widespread contamination, and destruction of transportation systems were expected to greatly delay recovery. However, the report notes that "With strict rationing, of petroleum products and allocation of coal, the surviving [civilian] fuel production …is sufficient to meet properly time-phased military requirements and minimum essential civilian needs…" (21)

In 1979, the Office of Technology Assessment (OTA) published a study, *The Effects of Nuclear War*, which emphasized the devastation and difficulty in recovering from such an attack (3). One of the cases studied in the report is a strike against oil refineries using 10 missiles with multiple warheads (pp. 64-80). This case was chosen because energy systems were considered to be the most vulnerable sector of the U.S. economy and refineries best met the study criteria of criticality, vulnerability and long recovery times. The conclusion is that most refining capacity in each country (the U.S. and the Soviet Union, or USSR) would be destroyed and both would suffer extensive reductions in industrial productivity and significant changes in socio-economic organization, although differently. For example, the already precarious Soviet agricultural sector was thought to be heavily affected, while in the U.S. the concern was the devastating impact on industrial sectors dependent on refined petroleum products and the socio-economic changes that

would result from living with scarcity (e.g. greatly restricted mobility). The OTA report generally recognizes that decentralization and redundancy could reduce the impact of any of the attack scenarios considered.

Two reports commissioned by the US government greatly sharpened the focus on decentralized energy technologies to mitigate security concerns.[1] The first, later republished as a book, *Energy, Vulnerability, and War,* provides a fairly detailed examination of the existing energy infrastructure at the time and the effects of a nuclear attack on it (22, 23). After detailing current vulnerabilities, the report reviews potential options including energy efficiency, storage (e.g. superconducting magnets and hydrogen), and renewable energy sources. *Energy, Vulnerability, and War* discusses Libyan and Soviet-sponsored terrorism and notes that from 1970 to 1980, over 250 terrorist attacks against energy infrastructure were carried out (22, 23).

The report's final chapter ranks technology options in terms of vulnerability, based on their degree of centralization, local fuel supply, local maintenance, cost, lead-time and other criteria. Ethanol, low and medium BTU gas, new domestic petroleum and methanol received the highest ratings (8-10). Diesel, biogas, synthetic natural gas, biomass oils, and coal-derived oil receive medium ratings (5-7). Gasoline (3) and hydrogen (1) receive the lowest ratings. A second ranking for decentralized energy sources was also created. Cogeneration, small fossil plants (<250 MW), small hydro, geothermal and fossil fuel gasification all receive the highest ratings. Next are biomass steam (8), wind and biomass low BTU gas (7). Solar technologies (both thermal and PV) rate between 4 and 5. The lowest ratings are received by fuel cells (3), waves (1) and ocean thermal energy conversion (1).

This report also suggests a fundamental institutional response, the creation of Defense Energy Districts, "which would be administratively responsible for categorizing, inventorying, and coordinating the implementation of dispersed, decentralized and renewable energy resources technologies" (p. 319). While the report describes the potential for decentralized energy technologies to address security concerns, it does not provide a method for quantifying this effect. The report emphasizes civil defense preparedness, not efficiency and renewable energy, per se. Political choices regarding possible trade-offs between conflicting goals (e.g. more security vs. lower prices) are not addressed in *Energy, Vulnerability, and War*, which assumes a unitary decision-maker with a single goal, civil defense.

The second report was reproduced as the ground-breaking book *Brittle Power* by Amory and Hunter Lovins (10, 24). It documents an amazing array of accidents, malicious attacks, and near-misses on U. S. energy systems, identifying the infrastructures for electricity, natural gas, oil and nuclear power as "Disasters Waiting To Happen" (10, Part Two, pp. 87-174). The key factors that make these centralized energy infrastructures "the root of the problem" (10, p. 218) include the use of dangerous materials (fuels); limited public acceptance of centralized energy infrastructure; centralization of fuel sources; little fuel substitutability; the length, operational

[1] The reports were initially commissioned by the Defense Civil Preparedness Office of the Department of Defense. During the time that the reports were being prepared that office became part of a new organization called the Federal Emergency Management Agency (FEMA), a civilian agency established in 1979 that brought together many disparate federal entities that were involved in some aspect of emergency management.

requirements and inflexibility of energy shipment systems; interactions between energy systems; high capital intensity, long lead times; and reliance on specialized skills.

Brittle Power highlights the benefits of efficiency and small-scale renewable energy technologies under routine conditions. In their work, one paper that attempts to model the effect of decentralized energy technologies in abnormally stressful situations is identified (25). Lovins and Lovins argue that the mismatch between the scale of centralized energy system components (large) and the scale of most power consumption (small) is at the core of energy system vulnerabilities, and can be rectified by increasing end-use energy efficiency and using more decentralized renewable energy. This approach, they argue, is cheaper than the centralized approach, in addition to any security implications.

Another key concept in *Brittle Power* is resilience, which is borrowed from ecology (23, 26), and which the authors argue should be designed into energy systems. Elements of a resilient system would include a modular structure, redundancy and substitutability, diversity, possibility of decoupling, and dispersion (pp. 179-182). This discussion is remarkably similar to the concept of 'survivability' that was developed in the computer security field in the late 1990s (27, 28). Lovins and Lovins even use a discussion of mainframe versus distributed computation as an analogy for decentralized energy systems (pp. 208-213). However, *Brittle Power* goes further, emphasizing social factors such as minimizing the need for social control to operate and protect the energy system and understandability of the technology to enhance social acceptance.

Both *Energy, Vulnerability, and War* and *Brittle Power* summarize relevant literature, provide numerous relevant facts and examples, make many logical arguments, and offer compelling visions, but they do not attempt any quantitative assessment of the value of resilience or the comparative values of centralization versus decentralization. Moreover, the details of energy system design, investment and operation are ignored, despite the many examples provided. Crucially, both books (but especially *Brittle Power*) inextricably link the concepts of efficiency, renewability, decentralization and security together, offering little conceptual space for decentralized energy infrastructures based on fossil fuels or small (<250MW) nuclear reactors: "Ultimately, high national levels of end-use efficiency could … allow the entire grid to depend on inherently resilient, largely local energy sources." (*Brittle Power*, p. 281). It is hard to imagine how large concentrations of people or industry could be served this way, even with significant energy efficiency improvements, yet Lovins and Lovins insist their vision does not require "social decentralization" (*Brittle Power*, pp. 219-220).

Thus both books offer an idealized vision with heavy reliance on decentralized renewable energy sources. Unfortunately, when larger renewable energy systems are mentioned, the problems of grids are barely mentioned (e.g. *Energy, Vulnerability, and War* pp. 171-185, 204-215; *Brittle Power* pp. 264-268, 277-282). Both books generally ignore key issues about large-scale, renewables-based energy systems that might be needed for cities and industry, or assume they can be solved relatively easily. For instance, the problems of 'long haul distances' and resulting vulnerability of energy infrastructures are associated with centralized energy systems. This may simply be technological optimism. In addition, some key challenges such as: network coordination, backup power, and line-worker safety continue to pose challenges to distributed generation for which no universal solutions have emerged. Nonetheless, some elements of the

vision outlined in *Brittle Power* are being put into practice, which will provide the lessons and experiences necessary to make progress in resolving issues. If this vision proves accurate in the long term, it changes the nature of the debate on how much energy security a society wants, how best to obtain it, and who should pay for it.

2 CONCEPTS

Several key concepts can be identified with the issue of energy infrastructure and security, some of which are present to one degree or another in the early analysis, but some of which are new.

2.1 Routine Security

Like any other activity, the energy industries have secured their assets and operations against ordinary threats such as theft, low-level vandalism, and commercial espionage. To do so, relatively modest efforts were all that was required, and less-than-perfect prevention was acceptable. That is, the costs of preventing losses had to be balanced with the cost of loss prevention. Typical efforts taken by firms include the use of various methods for monitoring and control of access (e.g. surveillance, fences and computer passwords). These firm-level security measures are embedded in a social setting where security is provided by various government measures: ranging from definition of who has control over property, through policing property from unlawful access and protecting national borders.

Thus, economists would describe routine security as a mixture of private and public good (29).[2] O'Hanlon, et al. provide several reasons for government action in this area, including national sovereignty, economies of scale, and mismatches between public and private goals (30 pp. 79-82). Of course, the level of routine security varies from place to place, but at any level it embodies at least an implicit agreement on adequate levels of routine security and how to pay for it, privately or publicly. Naturally, such agreements on the level and distribution of acceptable security costs are controversial and politics is generally involved in reaching them. What is not clear, however, is if these processes have considered the possibility of achieving functional security through an alternative infrastructure designed to be fault tolerant and hence an unrewarding target for disruption. This approach might have higher costs during routine operation, but lower overall costs when non-routine events are considered.

2.2 Expected Failures

Engineered systems such as energy infrastructures require periodic maintenance and suffer occasional equipment failures. Except for unexpected systematic failures, experience is used to generate reliable expectations of failure rates, as well as information with which to balance the costs of maintenance, failures, and new capital. These expectations are conditional upon 'routine' conditions, such as proper equipment operation and usage rates and the availability of trained repair personnel and supplies. These expectations yield 'normal' outage rates for customer service in various energy infrastructures, which range from extremely rare (e.g. residential natural gas delivery) to several hours per year (e.g. residential electricity service).

[2] Some economists (8, 30) use the concept of externalities, but this seems a less useful approach since many aspects of security are non-exclusive and non-rival, key properties of public goods.

Similarly, labor strikes and bad weather can interfere with the transportation of fuel (e.g. coal) or electric power system operation and cause 'routine' outages that must be planned for.

These issues are more important in electric power systems than in other energy infrastructures due to the inability to economically store energy and the consequent necessity of matching supply and demand continuously. The necessity of dealing with these constraints during normal operations has resulted in a long history of *reliability* planning in the electricity sector, which includes consideration of both normal operation under 'reasonable expectations' of 'intended operating conditions' (*adequacy*) and of limited disturbances due to weather and occasional stochastic equipment failures that are expected but whose occurrence cannot be scheduled (*security*) (31).

Furthermore, large-scale blackouts result from *cascading failures*, which occur when equipment failure or other disruption cause further failures or disruptions in large portions of the power grid (32). These events are relatively rare, but very costly. Normally, reliability planning is more successfully implemented in industrialized than in less-industrialized countries. However, systematic changes in the management of power delivery have been known to overwhelm such planning, resulting in rolling blackouts (e.g., in Eastern Europe of the 1990s, when they sought hard currency and exported to the West during peak demand, and in California in the summer of 2000).[3]

2.3 Attack Modes

The most obvious effect from an attack on energy infrastructures is supply interruption; blackouts and oil embargos figure prominently in the popular and political interpretations of 'energy security'. Supply interruptions are discussed in sections 4 (Oil and Gas) and 5 (Electricity). However, there are a number of other possible attack modes as well. The fuel and waste of nuclear power plants is both radiologically dangerous and can (with significant processing) be used to produce nuclear weapons, as discussed in section 6 (Nuclear Power). Other attack modes can include releasing the stored energy in fuels (e.g. liquefied natural gas, LNG, storage vessels or tankers) or in the water impounded behind hydroelectric dams against life and property (33, 34). We deal with this last group below.

LNG is stored at approximately 150 peak-shaving plants worldwide, and is shipped between 40 terminals in about 150 tankers (35). There is a negligible probability that an attack on an LNG tank (whether on land or afloat) would cause an explosion, although a fierce fire would likely burn for up to an hour. Boiling liquid expanding vapor explosions are not uncommon for liquefied petroleum gas and other chemicals, but none has been observed during experiments or in the thirty years of LNG trade (36-38). Worldwide, approximately 30 tanker safety incidents have occurred since commercial shipping began in 1959, of which 12 involved LNG spillage, but none resulted a fire or explosion. Several significant accidents on land have occurred, including a recent explosion at an LNG terminal in Skikda, Algeria that killed about 30 people and will cost approximately $800million to repair (39). Given the security measures currently in place,

[3] Rolling blackouts, voltage variations and unreliable supply in many less industrialized countries is often due to insufficient generation capacity or fuel and demand outstripping supply and a more fundamental challenge than an issue of poor reliability planning.

possible terrorist attacks on LNG infrastructure may present a smaller hazard to public health and safety than possible attacks on other hazardous materials shipped in large quantities, and may present a greater risk to supply security than to public safety.

Cooling towers at electric power plants could conceivably be used in a deliberate attack as a means of dispersing biological or chemical agents. The magnitude of this threat is not well understood since these facilities have some physical security and the effectiveness of cooling towers to disperse various agents is not well studied.

Hydroelectric dams can store significant amounts of energy in the form of water retained behind them. If they were suddenly breached both property and lives could be lost. It is not very easy to successfully attack most large dams, however, and physical access to them can be controlled relatively easily. One complicating factor is that smaller upstream facilities such as locks or small dams may be more vulnerable to attack. Breeching one or more of these could send a pulse of water downstream, possibly causing a larger dam downriver to fail catastrophically. Physical security (access control) is the primary means of mitigating this threat.

Finally, large electromagnetic pulses (EMP) can induce instantaneous voltages of hundreds of thousands of volts in conductors, creating very large disruptions in electric power systems and destroying electrical equipment components such as motors, backup generators, and -microprocessors (18 pp. 47-49, 67). Concerns about EMP have traditionally been focused on the impact of high altitude nuclear detonations, and there is an extensive body of literature in this area (much of it seemingly written in the seventies and eighties). In addition, relatively simple, inexpensive devices that can deliver an EMP have been designed and tested by the U.S. and other nations.

Recently, concerns have emerged that even crude devices could be deployed with significant localized impacts (40, 41). Such weapons could damage the electric power systems; and also use the electric power system as a conduit to attack other infrastructures (e.g. telecommunications) without physically penetrating facility perimeters. It is not clear how vulnerable the current system is to such an assault, nor what could be done to defend against them. The continued vulnerability of power systems to geomagnetically induced currents as a result of solar activity indicates that power systems have not been hardened against such threats. There are a number of factors that impact how solar flares (which occur on a relatively regular cycle of eleven years) will affect a power system, but the historical evidence indicates the potential for widespread outages is real. For example, a 1989 solar flare resulted in a multi-hour widespread blackout in Quebec (42).

Currently, there is very little information from credible sources on the EMP threat from non-state actors, so this concern is somewhat speculative. It is also unclear how similar such a threat would be to a solar flare or thermonuclear event. One paper that modeled solar and thermonuclear induced currents showed that even these two types of fairly well known events have differing characteristics and potential impacts. The electromagnetic pulse from a nuclear blast is stronger but not as long-lived as the one from the solar flare event. While both can cause the transformer to produce harmonics and become a reactive power load potentially causing the system to try to isolate transformers (and thus possibly resulting in outages), the longer time

scale of the solar events can provide enough time for transformer cores to overheat and lead to greater equipment damage (43). Possible damage to sensitive electronics at the end use is not discussed.

2.4 Diversity

One of the key methods for achieving reliable energy supply and secure energy infrastructures has been through diversity, even if accidentally achieved. This concept was imported to some degree from ecology (10 pp 195-8, 23, 26). Vulnerability due to a lack of diversity was well demonstrated in the first oil crisis. The price hikes in 1973 led to active and successful search for oil reserves away from the Middle East and by non-OPEC countries. The resulting diversity of supply reduced the power of OPEC as an oligopoly. However, non-OPEC production seems to be peaking and demand in China is booming, thus the concentration of reserves and production capacity in the Middle East renews concerns about vulnerability in supply (44-47).

Another form of diversity is not across suppliers of one fuel, but across types of fuels and technologies for their utilization. Diversity of fuel mix often occurs in the production of electricity, and advocates of every fuel can use this term to support policies that could mandate minimum and maximum market shares. For instance, Porter (48) illustrates how diversity in fuel supplies is being sought through renewable energy in the United Kingdom and Lemar shows how it can be achieved in the U.S. through Combined Heat and Power (49). Diversity in technology is also important as a means of reducing vulnerability to a design error leading to wide-spread failures or pre-emptive shut-downs in order to affect repairs. Evans and Hope argue that while standardized designs in nuclear plants improve economies of production, they also increase exposure to the possibility of systematic unknown failures due to that design (50). They stress the need for a range of nuclear plant designs. Taking a longer-term perspective, several researchers have documented the need for diversity in energy research and development in order to assure a broad choice of technologies into the future (51, 52).

In recent times there is evidence that neither political control nor market forces can be counted on to yield diversity in energy systems. For instance, before market liberalization in the United Kingdom (UK) political pressure from coal miners' unions prevented coal-fired plants from being installed near ports because this would open them up to steam-coal imports at a quarter of the prevailing price from UK mines. At the same time, however, the public electricity monopoly in England and Wales (CEGB) included diversity of supply as an operational issue. After privatization, market forces have yielded a singular 'dash to gas'. A strong preference for local fuels is common in electricity generation, as is a preference for whatever the least cost or most fashionable technology happens to be. For instance, in Spain, dirty, expensive local brown coal was used for power generation long after it was economic to do so, largely to preserve local jobs (53). In the U.S., a fairly diverse set of fuels for the electricity sector has come from a century of investment decisions in generation technologies that have been relatively uniform nationwide within each cohort, but have shifted from primary reliance on one technology to another with each pulse of system renewal and expansion starting with hydroelectric, then coal, nuclear, and, now, gas-fired plants. If global oil markets were strictly competitive, much more production in the ultra-low cost Mid-East region might result, although risk aversion by producing firms might cause them to broaden their production portfolio to include other regions, even if a cost premium

was required. However, the balance that would be struck in this way would reflect the interests of the infrastructure owners more than the public's interest.

Such portfolio management approaches are based on a probabilistic framework for quantifying the risks of various technologies and the use of utility maximization or other probabilistic techniques. It has been suggested that such techniques can fail if the uncertainty and risk cannot be adequately characterized and in such cases diversity may yield benefits that would not be captured by such techniques (54). There have been several efforts at formalizing the benefits of diversity, which could include mitigating technological path dependencies for the future, allowing for multiple and contradictory social choices to be met, fostering innovation and hedging against "ignorance" (55, 56).

2.5 Storage

The second key method for achieving reliable energy supply and secure energy infrastructures is storage, which applies most strongly to the oil and gas sectors since electricity cannot be stored readily. A key issue is the amount of storage that might be necessary, especially as compared with demand. Together, these two factors will determine how long normal operations can go on without interruption, and give some indication of how much demand reduction (conservation) might be needed in an emergency to extend the period during which storage can supply vital services.

A major topic in energy policy is the creation and management of strategic petroleum reserves (SPRs), which is discussed in a subsequent section. However, SPR facilities can become a security risk themselves, especially if they are exposed to attack in the form of tank farms. Storage is expensive and consumers may not be willing to pay for it regularly, so socially optimal levels may not be achieved under purely market conditions. For natural gas, regional storage (typically in depleted oil and gas reservoirs) is an important component of the infrastructure system and helps gas utilities deal with high demands in the winter. Such storage areas can also act as buffers in the event of damage to the upstream system, allowing a utility to ride through such a disturbance for days or even weeks depending on when the incident occurs.

Opportunities to store electricity are much more limited. Hydroelectric dams offer some measure of storage capacity that can provide emergency supply for a short-term emergency. Pumped-storage (air and water) schemes (have storage capacity ranging from tens to hundreds of MW-hrs) are also a possibility for even shorter-term supply security. On the user side, the rapid proliferation of portable devices (e.g. laptops and cellular phones) has introduced a few hours of storage capacity embodied in the battery of such devices. This end-user storage capacity does not extend to the vast majority of end-uses supported by electricity, however.

2.6 Redundancy

The third key method for achieving reliable energy supply builds on the concept of planning for expected failure through reserve margins and applies most strongly to the electricity sector. For example, in many locations hospitals are served directly by multiple feeder lines in order to have some measure of security against interruptions to one of the distribution networks. Redundancy in an electricity network would mean significantly larger reserve margins and multiple

transmission and distribution networks. This approach is very costly because much of the infrastructure sits unused most of the time, but it makes supply disruption more difficult since all redundancy for a particular load must be simultaneously rendered inoperative. Only a subset of consumers is willing to pay for such a system.

2.7 Cyber Security

An increasingly important topic in the security of infrastructure, and one that distinguishes current concerns from the primary concerns of the Cold War era is computer, or cyber-security, especially as delivered through the Internet. Traditionally, information technology (IT) in the energy sector has been considered less vulnerable to attack (at least by outsiders) than the infrastructure itself. This is partly because these IT systems often consisted of dedicated systems without interconnection to other computer networks and with built-in redundancies.

Concern about current energy sector IT systems arise because of their use of open protocols, increased use of intelligent devices, and lack of encryption (57). Remote systems receiving control signals from the control center often do not verify such signals for authenticity. Instead of relying on traditional means to protect these systems, information security typically has relied on uncommon, often proprietary protocols and the need for considerable hard-to-obtain knowledge about operating systems and so forth. However, such measures are insufficient, particularly when one considers the insider threat problem. An employee with the proper knowledge could create serious problems and face minimal resistance from the system due to lack of encryption and authorization requirements. Current systems may be more vulnerable to attack due to their increasing use of dial-up modems and the Internet. For instance, in January 2003 an Internet-transmitted computer virus infected and disabled several computers at the Davis-Bessie nuclear power plant, although the plant was shut down for emergency repairs so there were no safety concerns.

In the electricity industry, Energy Management Systems (EMS) monitor and control the production, transmission, and distribution of electrical energy. This includes scheduling and controlling generators and monitoring and analyzing the transmission network in order to provide power while maintaining reliability of the system. Competition is leading to more and more use of electricity markets to make decisions about what power plants will be operated when. Since markets are typically open, it may be impractical (or simply expensive) to verify the identity and reliability of all participants, exacerbating the problem.

A rare public admission of energy-related cyber-warfare was recently described in a news column (58). The U.S. government arranged for the sale of faulty natural gas pipeline operating software to a third party who it knew would illegally resell (pirate) the program to the Soviet Union. The fault was designed to over-pressurize gas pipelines, which led to an explosion of nuclear proportions in an uninhabited area of Siberia in June of 1982, and, more importantly, slowed Soviet scientific and engineering work that was using similarly pirated software.

2.8 Interdependency

A relatively new and crucial concept associated with the security of energy infrastructures is interdependency, which is the reliance of one infrastructure (e.g. electric power) upon another

(e.g. telecommunications) or even mutual reliance of infrastructures upon one another (59, 60). Amin goes so far as to argue that a new 'megainfrastructure' is emerging (61). Interdependency effects have been observed numerous times, such as during the U.S. western states power outage in 1996, which very nearly led to the collapse of the telecommunications system.

Rinaldi, et al. identified six dimensions for understanding infrastructure systems, including infrastructure characteristics such as spatial and organizational scope and environmental characteristics such as the legal/regulatory framework (60). One of those dimensions is the type of interdependency. They have created a classification scheme with four types of interdependencies (physical, cyber, logical, geographic). Other research efforts have focused on developing specific tools to understand infrastructure interdependencies. Longstaff and Haimes' Hierarchical Holographic Modeling technique is one example (62).

Another example of infrastructure interdependency is that some nations rely on petroleum products for a considerable fraction of electricity generation, such as Singapore (65%), Italy (32%), and the Philippines (28%) (63). A significant oil supply interruption could impact the electricity sector in these countries. A final example is provided by Zweifel and Bonomo, who show that simultaneous shortages of both oil and gas lead to different optimal strategic responses than does consideration of singular supply interruptions (64).

2.9 Stress

The reliability planning long used for energy infrastructure investment fairly well describe most conditions in high-income countries, but they do not describe a variety of situations now considered important in both high- and low-income countries (31, 65, 66). In this review, deviations from intended or 'routine' operating conditions is defined as a condition of *stress*, which includes deliberate attacks, multiple failures, persistent failures or attacks, and conditions that make system restoration difficult (e.g. a lack of spare parts) (67-69). Stress differs from the modes of disturbance analyzed in typical reliability planning in several important ways, including events with one or more of the following general characteristics.

1. **Coordination of Attack:** Unlike equipment failures or even extreme weather events, deliberate attacks are not short-term random events. As discussed above, both militaries and terrorists have the capability to co-ordinate attacks and intentionally maximize damage to the system. Attacks can also be repeated as system components are repaired.

2. **Significant Scope of Impacts:** The failure of distribution equipment within 1/2 mile of the customer accounts for about half of electricity outages in the U.S. However, in conflict situations, remote transmission lines, transformer sub-stations, pipeline pumping stations, or oil terminals can also become primary targets or be impacted by indirect damage stresses. The non-conflict stresses discussed above (e.g. poor access to spare parts) would also have a wider scope of impacts.

3. **Persistence of Outage:** Deliberate attacks may not be single events, and they may occur under conditions (or create conditions) that make restoration of service and repair more difficult. Alternatively, conditions could be created that make even routine maintenance more difficult. When outages do occur there are a number of factors that can lead to outages

that persist for days or even longer. Such factors would include: risks to personnel, impeded transportation of personnel and parts, insufficient funds for replacement parts, absence of technical expertise, and the possibility of subsequent sabotage. While long-outages lasting from hours to days are common-place in less industrialized countries, they are so abnormal in industrialized countries that a 'sustained interruption' is generally classified as one that lasts more than one hour. There are no further classifications for longer outages.

2.10 Survivability

The traditional reliability planning approach does not lend itself well to responding to un-expected, deliberate, and potentially very high impact attacks. For one thing, it is very difficult to imagine all possible attack modes or strategies. Even if this problem could be overcome, current practices in reliability analysis allow for essentially only one strategy – provide more reserve capacity – a very costly solution that competitive firms are not likely to implement, and one that may divert resources from other important uses and possibly slow economic growth (70). Thus, supply-side solutions are not likely to be sufficient any longer; more attention will need to be paid to the economic and social implications of end-use disruptions. One concept that may serve to link reliability and security, and also be compatible with competitive energy industries is *survivability*, also known as 'the self-healing grid' or 'the resilient network.' Survivability is similar to the ecological concept of resilience that was applied to energy systems over twenty years ago (10 Ch. 13, 26, 28, 62, 63, 67, 68, 71, 72).

Survivability is the ability of a system to fulfill its mission in a timely manner, despite attacks, failures, or accidents.[4] It can be contrasted with the current 'fortress' model of security that tries to prevent or counter all attacks but has disastrous outcomes (e.g. cascading failures) when it does inevitably fail. A fundamental assumption of survivability analysis and design is that no individual component of a system is immune from attacks, accidents, or design errors. Thus, a survivable system must be created out of inherently vulnerable sub-units, making survivability an emergent property of the system rather than a design feature for individual components.

Due to the size and complexity of energy system operations, and the speed at which faults can propagate in some of them, it may be difficult to recognize attacks until there is extensive damage. Thus, ways must be found to recognize attack early and isolate the affected area in order to protect the rest of the system. Survivable systems must be able to function autonomously and maintain or restore essential services during an attack, and recover full service after the attack. Thus, the system must 'fail gracefully,' shedding low priority tasks and later resume tasks in a priority ordering during recovery. Our current energy systems are optimized for operation in routine conditions and cannot do this. The prolonged outage (in many locations as long as 5 days) of power delivery in Ontario in the aftermath of the August 2003 blackout was primarily due to system stability concerns when energizing a grid that would immediately have to meet peak demand conditions from air conditioners that could not be remotely shut down.

For example, in most cities, traffic signals are powered by the same circuits that provide service to much less critical loads like billboards. During blackouts, injury and property loss may occur due to blank traffic signals. Worsening the problem, blackouts cause gridlock that hinder police

[4] Some find the phrase 'in a timely manner' redundant in this definition.

and emergency response crews from reaching their destinations. This demonstrates the fortress aspect of traditional reliability planning – it creates a system in which frequent or large-scale blackouts are not supposed to occur, but when they do, the consequences are severe. In contrast, a system designed around survivability concepts might use low power Light Emitting Diode traffic lights with battery backup to ensure that a blackout does not interrupt traffic flow.

2.11 Centralization

A key theme in the literature on energy infrastructure and security is centralization, particularly as it applies to the electricity sector. Several observers have documented how the combination of technological innovation and social (political and financial) forces has led to ever larger centralized electricity generation plants connected by ever larger synchronized grids throughout the 20th century (73, 74 Ch. 3, 75 Ch. 19). Even a quadruple crisis in the late 1970s that led to fundamental change in the electric utility industry (the introduction of competition) failed to completely arrest this process.[5] Centralization also affects oil and gas infrastructures due to the number and location of key parts of the supply chain, including facilities for production, gathering, shipping, processing, and delivering raw materials and products (4, 10). Given the geographic concentration of petroleum and gas deposits in a relatively small number of locations worldwide, and the need to ship petroleum through constrained corridors, the potential for decentralization in this sector seems slight. In addition, it is not clear that resilient technologies for these sectors exist other than those that result in more efficient use of fuels.

Critics of centralized energy systems argue that they are 'brittle' and prone to failure, while decentralized systems can be resilient (10, 76, 77). Resilient technologies are argued to include efficiency improvements, electricity generation near point-of-use, responsive demand, and renewables (which require no fuel supply). Supporters of these approaches also claim other benefits, such as lower costs, lower environmental impact, and, sometimes, more decision-making power in local (not federal or corporate) hands (78). One of the main promoters of such concepts, Amory Lovins, claimed that "[t]he distinction between the hard and soft energy paths rests not on how much energy is used but rather on the technical and political *structure* of the energy system." (79 p. 38)

In contrast, supporters of centralized electricity systems focus on the need for a sufficiently large grid in which to embed higher-efficiency centralized plants and the ability of a grid to capture the time-diversity of demand allowing the integrated system to have a higher load factor. The reliability benefits of large, coordinated systems are only visible by looking at unexpected flows on transmission lines during partial network failures, which is uncommon outside of the electricity industry. Thus, supporters of large, centralized systems tend to support technologies that will make electric power grids connecting large, centralized plants 'smarter' (increased automation and computation), more 'aware' (more and better sensors and communications), and faster to react (power electronics instead of electromechanical controls) (80-82).

For instance, the recent National Transmission Grid Study includes "targeted energy efficiency and distributed generation" as one of ten approaches to 'relieving transmission bottlenecks', not

[5] The four horsemen of this "apocalypse" were technological failures, fuel price shocks, environmental control costs, and unexpected interest rate increases.

as a central organizing paradigm to be applied widely. Similarly, the United States Energy Association's National Energy Security Post 9/11 is asymmetrical in the treatment of centralized energy supply and of efficiency, renewables and decentralized supply (82). Strong policies to support centralized supply are recommended without reservation (e.g. "Allow refiners and other energy producers to recapture the full cost of meeting new environmental regulations."), while policy recommendations on efficiency are limited to research and development, and policy recommendations for renewables are weak and contingent (e.g. "Encourage deployment of renewable energy supplies when doing so will strengthen the energy infrastructure and/or increase U.S. energy security") (82).

Government efforts to support improved security of energy infrastructure generally ignore these issues as well, generally leaving decisions regarding technology choice to the private sector. The cost of government efforts tend to be socialized by being supported by general revenue, not by the infrastructures that create concerns. This approach may yield more infrastructure and more infrastructure security activities than would an efficient market outcome and would tend to subsidize technologies with greater concerns over those with fewer (83). This would likely be both inefficient and unfair, as those that impose security burdens are not required to pay for them (30 pp. 77-97).

More recently, von Meier used the term 'supple' electric power technologies to identify technologies that promote decentralization without regard to renewability, which characterized prior analyses from the 1980s (84). Supple technologies are modular, suited to dispersed siting, and fuel-flexible, and include reciprocating engines, microturbines, and fuel cells. She notes other important differences, including the fact that the current energy system can no longer be characterized as purely hard, energy efficiency improvements and smaller scale generation are now more common and accepted.

However, von Meier notes that the fundamental political changes Lovins and others sought in order to achieve widespread adoption of soft technologies have not been accomplished. Instead, technological improvements in decentralized technologies have had an effect, and, more importantly, market forces have come to the fore. von Meier argues that "the ensemble of supple technologies does not support a natural monopoly in … electricity" (p. 213). This may not be strictly true; Strachan and Dowlatabadi document the very successful deployment of decentralized energy technologies in the Netherlands by incumbent utility companies once proper incentives were provided (85). However, the potential antagonism between the interests of large, incumbent energy firms operating a centralized infrastructure and the deployment of decentralized energy technologies may be a significant limit to their potential contributions to the security of energy infrastructures. Ample evidence in the U.S. supports the claim that large, incumbent energy firms tend to be antagonistic to decentralized energy (86).

3 CRITICAL INFRASTRUCTURE PROTECTION (CIP)

As noted above, concerns about the security of energy and other infrastructures faded with the Cold War in the late 1980s. However, the rise of catastrophic terrorism within industrialized countries (e.g. the truck bombing of the World Trade Center in 1993), the Western States power outage in 1996, and the realization in the mid-1990s that the transition from 1999 to 2000 might

cause significant disruptions led to a renewed concern about the potential vulnerability of key infrastructures. The response to these developments has come to be termed Critical Infrastructure Protection (CIP), which links energy and other infrastructures with national security (87, 88). Many nations have undertaken CIP activities in the last several years, especially the United States (89).

3.1 Definitions

Definitions of CIP vary somewhat. For instance, Section 1016(e) of the USA PATRIOT Act defines critical infrastructure as

> "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters." (90)

The White House subsequently highlighted the symbolic value of critical infrastructures, which

> "provide the foundation for our national security, governance, economic vitality, and way of life. Furthermore, their continued reliability, robustness, and resiliency create a sense of confidence and form an important part of our national identity and purpose." (91 p. viii)

However, international agreement on a definition of CIP does not exist, for instance, some would add maintaining ecological health (87). However, despite the specific definition of critical infrastructure, all nations that use this term include energy systems (or networks) in this categorization. Other sectors usually include Banking and Finance, Communications, Transportation, Water Supply, Emergency Services (Police, Fire, etc.), Law Enforcement, and Public Health.

Another key issue in defining CIP, and one that distinguishes it from previous analysis, is the role that cyber-security plays in the operation of critical infrastructures (92). All infrastructure systems in industrialized economies are highly computerized and cyber-security is as serious a challenge as physical security. For example, the White House has released one national strategy documents on physically protecting infrastructures and another on securing cyberspace (91, 93).This has occasionally resulted in the terms Critical Infrastructure Protection and cyber-security of infrastructures to be used synonymously. However, it is difficult to determine the likelihood of success or the impact of a cyber-attack on an energy infrastructure, as there is scant historical precedent to analyze.

In an interesting review of definitions, Moteff et al. note that since Executive Order 13010 was signed in 1996, the definition of CIP used in by the federal government in the United States has grown broader (94). They note that an overly broad and overly flexible definition of CIP is problematic since this could lead to vague, ineffective policies and a growing commitment by the federal government. If the list of critical infrastructures continues to change, or multiple lists of critical infrastructures are created, public and private decision-makers may find it more difficult to actually protecting these infrastructures. This problem raises the need for prioritization, and Moteff et al. propose XX approaches focused on different aspects of the problem: the degree of criticality of any infrastructure element, vulnerabilities that cut across infrastructures, interdependencies among infrastructures, key geographic locations where multiple critical infrastructures co-exist, or assets owned by or relied on by the federal government.

3.2 Practice

Australia and the United States were the first nations to address CIP, and we will focus on CIP efforts in the U.S. because they are by far the most comprehensive. The first formal CIP measure in the U.S. was the establishment of the President's Commission on Critical Infrastructure Protection (PCCIP) under Executive Order 13010 (95). This commission's documents, as well as subsequent analyses, highlighted the potentially serious consequences of attacks on critical infrastructure. The commission issued its final report in 1997 which had several key recommendations, including the creation of a national warning center, an idea that was acted on by the creation of a National Infrastructure Protection Center (NIPC, see www.nipc.gov) within the Federal Bureau of Investigation (FBI) in 1998 (96). The PCCIP also identified a large number of gaps in existing capabilities needed for successful CIP and called for a significant research, development, and education initiative (97)

These recommendations were taken up in Presidential Decision Directive 63, which called for a range of activities (98). Among these steps was an enhancement of the NIPC as "a national focal point for gathering information on threats and facilitating government's response to computer-based incidents" and to provide "the principal means of facilitating and coordinating the Federal Government's response to incidents, mitigating attacks, investigating threats, and monitoring reconstitution efforts." (88 p. 8). Since that time, especially after the attacks on the World Trade Center on September 11, 2001, a significant CIP bureaucracy has been developed in the U.S. government, some of which has (or may have) significant impacts on the energy sector. The new Office of Energy Assurance in the U.S. Department of Energy identifies over 60 CIP organizations, ranging from the President to the National Security Council, to the U.S. Coast Guard, to the North American Electricity Reliability Council (NERC) (99).

One of the most significant organizational developments since PDD-63 has been the creation of the new Department of Homeland Security (DHS). Initially a White House Office created by Executive Order, it has now become a government department and has taken over several roles (and organizations) once located in various parts of the federal government (90, 100)

Other new federal organizations include the National Coordinator for Security, Critical Infrastructure, and Counter-Terrorism in the NSC; the Critical Infrastructure Assurance Office (CIAO); the National Infrastructure Simulation and Analysis Center (NISAC); a set of lead agencies for individual critical infrastructures (the Department of Energy, DoE, is the lead agency for the energy sector, although the Nuclear Regulatory Commission (NRC) has a role as well); the Critical Infrastructure Coordination Group; the Department of Energy's Office of Energy Assurance; and several other intergovernmental groups focused on cyber security (90, 100). The key roles of these organizations are to coordinate public sector activities, from the Federal to the local level; conduct research and development; and 'coordinate' and encourage private sector owners of critical infrastructure to help assure its protection. (A large majority of the energy infrastructure in the U.S. is privately owned.) Another important issue is determining the level of control and funding for government activity at the federal, state, and local levels. O'Hanlon, et al. argue that activities with primarily local benefits should be decided upon and paid for locally, while those with national implications should be under the jurisdiction of the federal government (30 pp 77-97).

Coordination between the federal government (through the NIPC) and the private sector is conducted through Information Sharing and Analysis Centers (ISACs), which for the energy sector are coordinated by NERC (www.esisac.com), and the American Petroleum Institute (www.energyisac.com). There is considerable disagreement about the appropriate role of legally binding CIP standards or requirements versus voluntary targets and self-regulation. Naturally, industry prefers less regulation yet the public good nature of CIP makes it unclear that wholly voluntary approaches can yield a socially optimal level of CIP. At the moment, the government has only officially called for "standardized guidelines" for risk assessment and security that would be developed in partnership with industry and other levels of government (91).

The issue of financing overall Homeland Security measures, including critical infrastructure protection, is complex and will remain a mix of both public and private expenditures (30). In the United States, proposed public expenditures for infrastructure protection in 2005 are over $850 million dollars out of a total non-defense homeland security budget of almost $34 billion. There is some concern over the economic impact that expenditures in these areas may have. O'Hanlon, et al. recommend a Homeland Security program that would result in $45 billion of public and $10 billion of private costs per year. Their estimate is that this would result in a 0.3 to 0.5 percent reduction in real output from the economy and reduce growth rates by 0.1 percentage points or less. The National Strategy for Homeland Security states that the federal government will set priorities based on a consistent methodology and an approach that will allow it to balance costs and expected benefits, but does not state what an appropriate methodology or approach might be (94, 101).

The key issues associated with recovering security-related costs in regulated utilities are summarized in a recent NRRI white paper (102). Some of the most important issues include differentiating security-related from competition-related costs, applying tests of 'reasonableness' appropriately to CIP expenditures, and devising cost recovery mechanisms (e.g. rates). A survey conducted by NRRI showed that in 2003, only 17% of state public service commissions either had or were developing guidelines for the prudence of CIP-related expenditures, even though 45% reported that utilities had filed requests for recovery of such costs (103). Of those states reporting such filings, only a small fraction (23%) reported that utility CIP-related expenditures were driven by state or federal regulations.

Some business leaders have raised concerns that the high level of security expenditures in the United States could result in a reduction in international competitiveness and requires a balance between security and competitiveness (70). They argue that "[T]op-down, prescriptive security standards could drain productivity and dampen growth prospects, putting U.S. companies, universities and workers at a disadvantage vis-à-vis their foreign competitors. Only the private sector is able to design integrated security solutions to protect productivity and competitiveness." In contrast, O'Hanlon et al. argue that "in most cases, providers and owners of the property or activity should generally pay for the costs of additional security. Furthermore, in most cases, the action should take the form of performance-oriented mandates on the private sector, perhaps coupled with insurance requirements or incentives, rather than direct subsidies or tax incentives." This approach is thought to discourage risky activities, prevent rent-seeking behavior and promote innovation in anti-terror strategies.

Another particularly important area of disagreement is disclosure of information about critical infrastructures by private owners to the federal government (104).This debate focuses on the reconciliation of two conflicting public goals: the need to share information confidentially for CIP purposes and the need for public access to information to ensure open government. Private owners of critical infrastructure are reluctant to provide information that may have security or commercial value to the government for the fear of it falling into the wrong hands under provisions like those of the federal Freedom Of Information Act (FOIA). Advocates for civil liberties and for changes in regulation (e.g. environmental groups) are concerned that special protection of 'critical infrastructure information' would preclude the ability to obtain information about abusive government practices, cast a veil of secrecy over central DHS activities, possibly allow industry to improperly shield information with policy implications unrelated to CIP, and are unnecessary due to existing FOIA exemptions. Some public interest groups are concerned that such protection would improperly shield infrastructure owners and operators from liability under antitrust, tort, tax, labor, and consumer protection laws (105).

Action in this area has already been taken by many regulatory agencies. In 2003, FERC issued a rule providing definitions for 'Critical Energy Infrastructure Information' (CEII) and procedures besides the FOIA for obtaining CEII information that has been submitted to FERC (106). In addition, the National Regulatory Research Institute (NRRI) found in surveys that the percentage of state public utility commissions offering FOIA protection for sensitive information increased from 42% in 2002 to 82% in 2003 (103).

Nonetheless, concerns about secrecy have lead to bills such as the Leahy-Levin-Jeffords-Lieberman-Byrd "Restore FOIA" proposal. Specific concerns include third-party liability, the lack of anti-trust exemptions for industry-wide information sharing, and the release of competitively sensitive information. These issues will most likely take several years to be resolved by Congress and the courts. However, there have already been some examples identified of public-private information sharing that have been considered successful (one in telecommunications and one in health care) and these could act as models for future activities (107).

Similar, if smaller, CIP activities are underway in many other countries. The idea of a warning center and information-sharing mechanism embodied in the NIPC has been replicated in at least ten countries (Australia, Canada, Germany, Israel, Italy, Japan, the Netherlands, New Zealand, South Korea, Sweden, and the United Kingdom) and over a dozen more have investigated the concept (87, 108, 109). Many, such as New Zealand's Center for Critical Infrastructure Protection, formed in August 2001, and the United Kingdom's National Infrastructure Security Co-Ordination Centre, focus on cyber attack.

3.3 Research

Research into CIP has begun to appear in the literature, although it is likely that a considerable amount of such activities will remain classified or proprietary. The U.S. National Academy of Sciences produced a comprehensive survey of, and strategy for, research and development in support of counter-terrorism (110). This effort stressed the vulnerabilities of the electric power infrastructure, and recommended research into tools for identifying and assessing infrastructure vulnerabilities, improving monitoring, hardening energy infrastructure from attack, enabling

faster recovery, preventing cyber-attack, and deploying an 'intelligent, adaptive power grid'. Related research is also going on outside the U.S., some of it oriented towards survivability concepts (111).

Several themes have emerged from this research so far. A fundamental goal of these research efforts has been to better understand the specific vulnerabilities of infrastructure systems. There have been significant research efforts underway in academia, government and private industry in this area. A corollary to this effort has been research on robustness and survivability of current and alternative infrastructure systems. The goals of such efforts have included gaining a better understanding of the vulnerability of individual infrastructure systems, specific interdependencies between infrastructure systems, survivable systems and the larger economic impacts of infrastructure failures.

Another major focus of research has been to develop modeling, simulation and analysis tools to analyze infrastructures. Several of the U.S. National Laboratories have taken on this role. Sandia National Laboratory has recently created NISAC in order to apply the largest scale computational capabilities to model and analyze infrastructure vulnerabilities and provide support to government and industry (112 and see also www.sandia.gov/CIS/NISAC). Modeling and the development of energy infrastructure test beds are under development at the Idaho National Engineering and Environmental Laboratory (see www.inel.gov/nationalsecurity/infrastructure_protection). One of the key strengths of modeling and simulation is that it can shed light on infrastructure interdependencies that are otherwise very hard to quantify (112, 113).

In many cases, the questions that have been asked over the last five to ten years could not be analyzed with the tools available (in some cases, simply because the problem has been posed in a slightly different manner). Combined with improvements in computational capabilities (including the development of new super-computers for the national energy laboratories), this has led to significant advances in modeling capabilities. This includes the improvement of traditional risk, vulnerability and engineering methods, as well as the application of more recent modeling methods (such as agent-based models) to the infrastructure protection problem.

Another tool being used to understand the vulnerability of energy infrastructure systems are simulation exercises, similar to those used in military war-gaming or in disaster response preparation. In the United States these have included the Blue Cascades (focused on the Pacific Northwest) and the Silent Vector (focused on how to deal with a potential terrorist strike) exercises (5). These exercises have highlighted a number of issues related to the coordination of protection efforts, risk communication, differences between the public and private sector, and vulnerability of different infrastructure and economic sectors to disruption.

4 OIL AND GAS

The vast majority of the literature on 'energy security' focuses on oil imports and on possible interruptions of petroleum supply (e.g. 8, 46, 114). Figure 1 illustrates the reasons; the major economic powers, the U.S., Europe and Japan, import huge amounts of oil, while the Middle East holds about two-thirds of proved oil reserves (115, 116). Current production trends suggest

production will tend to concentrate (centralize) further in the Middle East. An important counter-trend is in the discovery and production of non-conventional oil, such as deposits deep off-shore or formations like the Alberta tar sands, or even synthetic petroleum from gas or solids (117). Technological innovation tends to make these resources more economical, raising effective petroleum reserves, and decentralizing them as well. This effect is non trivial, the Alberta tar sand deposits may hold the equivalent of over one third of Middle East conventional oil reserves.

The dependency of major oil producing nations on the income from petroleum sales, coupled with the availability of alternative supplies at only slightly higher prices may limit the potential for oil supply interruptions caused by national governments (14, 15, 17, 118). In addition, the flexibility demonstrated by global oil markets may limit the damage to oil importing countries (119, 120). However, some terrorists may find this adds to the attractiveness of oil-production facilities as a target, since destabilization of current Middle Eastern regimes may be among their goals. Thus, deliberate attack on oil supply infrastructure may be one of the more likely causes of supply interruptions. However, given market structures like those in use today, the outcome will be increased prices, not physical scarcity.

The most important vulnerabilities are in refineries and pipeline pumping stations, only a limited number of which typically supply any particular region (2, 4, 10). An additional problem is that several chokepoints vulnerable to mines or other types of attack exist on ocean petroleum shipment routes, including the Straits of Malacca, Bosporus Straits, and Straits of Hormuz. Although petroleum production (wells) and shipping (tankers) can and have been attacked, they are numerous and operate through a global market, so substitutes may be relatively readily found. One possible limitation is the time it takes to bring new petroleum production capacity on stream, especially non-conventional sources. Increasing imports of oil and gas by East Asian nations has created new concerns about energy security in these countries, which may force some of these nations to take more active roles in international affairs and heighten their interest in combating terrorism (47, 121-123).

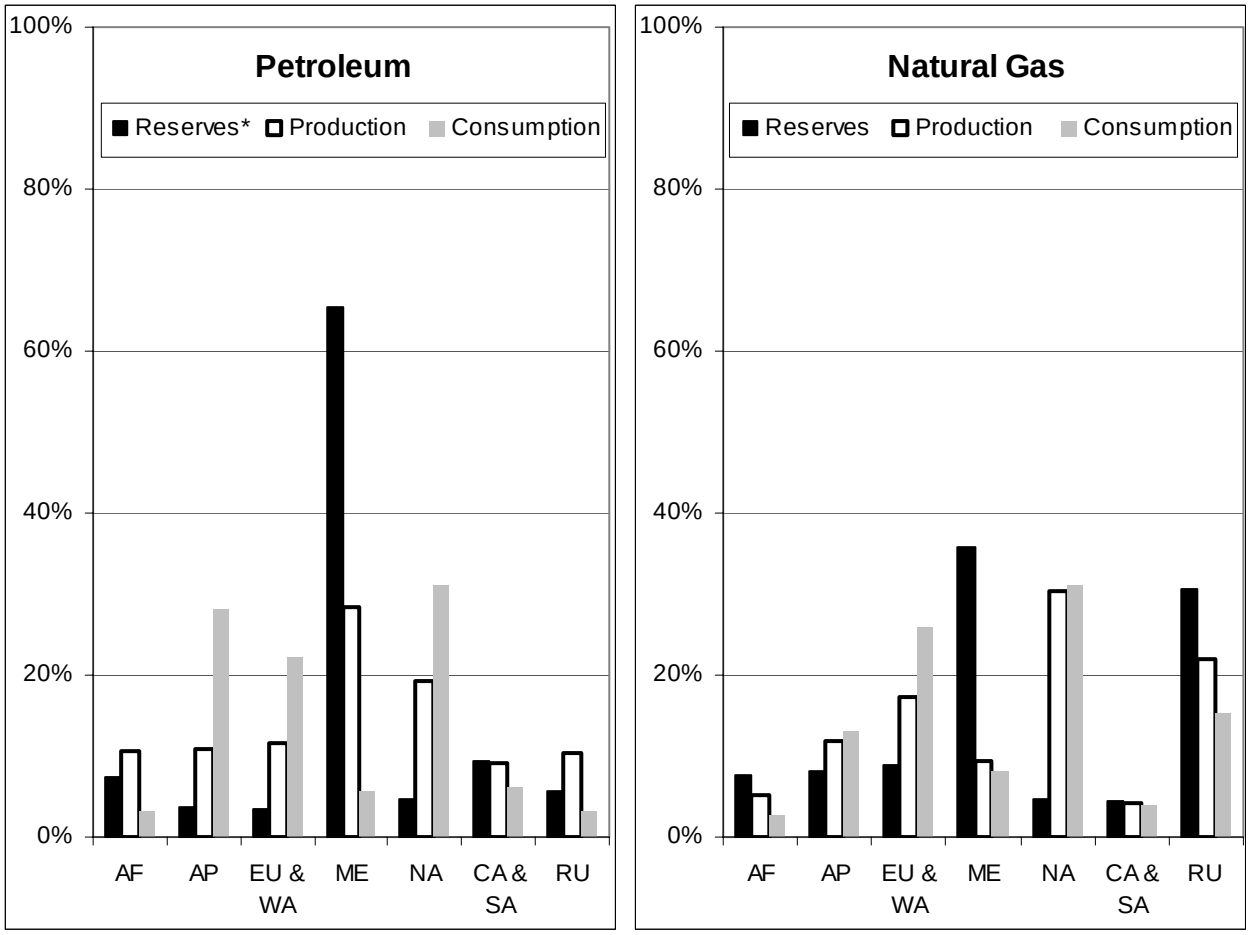
Much of the early work on likely effects of oil supply interruptions is summarized in a report published by the Oak Ridge National Laboratory, which examines both the costs and benefits of petroleum imports (44). This and subsequent work by the same authors identified 24 oil supply shocks from 1950 to 2003, averaging eight months in length and 3.7% of global supply (124). This study also characterized two types of costs associated with oil supply interruptions, increased payments for imports and macroeconomic adjustment losses (pp. 37-51).

The concept of increased payments for higher-priced oil imports is straightforward, but it is important to note that while futures markets and other mechanisms can hedge against the private costs, they cannot hedge against social losses (125). Thus, even improvements in oil markets will not mitigate the effects of increased prices for oil in the case of a successful attack on the supply infrastructure.

Energy is universally acknowledged as a key element of the modern industrial economy. However, two schools of thought have emerged on the relationship between energy prices and economic growth in the wake of oil price shocks of 1973 and 1979. Some see high energy prices as having led to the rapid reduction in economic growth (e.g. 126). Others have argued that it

was not higher energy prices but restricted money supply that led to a slower pace of capital investment and technical change (e.g. 127). These two perspectives lead to very different policy prescriptions. If the former analysis is correct, it is advisable to have policies that keep energy prices steady. If the latter is correct, it is advisable to have good macro-economic policies in place to minimize the impact of energy price fluctuations. The studies discussed in the next few paragraphs assume oil prices are the main effect.

Figure 1: Percent shares of conventional petroleum and natural gas



Source: (116).KEY: AF – Africa, AP – Asia Pacific, EU & WA – Europe and West Asia (e.g. Kazakhstan), ME – Middle East, NA – North America, CA & SA – Central and South America, RU - Russia
* Does not include non-conventional oil, so, for instance, Albertan tar sands and methane hydrates are excluded.

Macroeconomic adjustments are changes in labor and capital utilization to reflect the new, higher prices relative to other goods and services. These changes take time due to, for instance, labor contracts and sunk capital. Although Bohi and Toman (119) find no stable estimates of these effects, a significant amount of subsequent research has found that they do exist in many countries (124, 128). Several key findings emerge. First, the effect is asymmetric, price increases have greater negative effects than decreases have in speeding an economy. Second, the effect is non-linear and may have a threshold that moves over time. Third, the best (linear) estimate of the

effect of doubling the price of oil for one year on gross domestic product for eleven countries, including the U.S., France, Thailand, and others, averages -6.5% for two years. Generally, this work finds that the use of strategic petroleum reserves (SPRs) can be quite effective in managing short- and mid-term supply interruptions, but that current policy in the U.S. and elsewhere does not take significant advantage of these opportunities.

In related work, LaCasse and Plourde find that SPRs are more effective against random, short-term supply interruptions, not longer increases in price (129). This suggests that strategic oil reserves might be a reasonable precaution against possible attacks on the petroleum infrastructure. Of course, such reserves become part of the infrastructure and a potential target themselves. Greene et al. model a two-year oil supply reduction similar in magnitude to those in the 1970s and find that OPEC's revenues increase substantially, paid for by importing countries (45). They find strategic SPRs to be ineffective in this longer scenario, highlighting the importance of considering the duration that energy storage can meet end use demands as discussed previously.

Figure 1 shows that the concentration (centralization) of natural gas supplies is less than that of petroleum, but this is largely due to extensive proved reserves in one country, Russia (130). Again, non-conventional sources could dramatically change this picture. Methane hydrates may be an order of magnitude or more larger than conventional resources. However, the gas supply infrastructure is more vulnerable to deliberate attack than the petroleum infrastructure, but less so than electricity.

The natural gas supply infrastructure is more vulnerable to attack than the oil infrastructure for a simple reason, gas requires compression or cryogenics to store and move. Natural gas systems consist of production facilities, transmission pipelines, storage areas, city-gates and sub-transmission mains, distribution vaults and distribution pipes. High pressure pipelines or liquefied natural gas (LNG) tankers are required to transport gas, which may make them more fragile, and perhaps more vulnerable to attack although in routine service they have been quite reliable (131). In addition, LNG facilities are much more expensive and time consuming to construct than oil handling and shipping facilities, which would be disadvantageous in the case of a deliberate attack (132).

Gas supply infrastructure is less vulnerable than the electricity infrastructure because it is mostly buried underground, it can be used to store gas (line pack) and it can use relatively secure depleted oil and gas wells for storage (63). Like the electricity industry, companies in the gas business have long recognized and effectively planned for contingencies that mitigate terrorism risks. Spare parts are generally kept on hand to effect quick repairs. However, the potential vulnerabilities in the gas supply system are illustrated by the August 2000 rupture and explosion caused by corrosion in a 30-inch gas pipe near Carlsbad, NM, killing 12 people. This explosion led to significant increases in gas prices in California, exacerbating the electricity crisis there, an example of infrastructure interdependency.

5 ELECTRICITY

An attack on the electric power system that led to a supply disruption would be hard to distinguish from a blackout caused by more typical events, so there is much to be learned from the study of past outages (133, 134). Contingency planning, spare equipment pre-placement, emergency preparedness training, and temporary personnel transfers tend to be the keys to recovery from large outages. Power companies often loan trained workers in emergencies under fairly informal arrangements, knowing that they are likely to need to make such requests themselves someday. Several aspects of successful management of electric system outages have been identified: planning, training, analysis, and communications (31). However, communication during and after an event might be difficult, especially if the attack is not on the physical part of the electricity infrastructure but on the associated information technology (IT) infrastructure.

The 1990s saw utility privatization in many countries, followed by mergers and acquisitions that often concentrated the electricity industry in international holding companies. In the United States the formation of large electricity markets among power systems that were formerly interconnected, but operated largely independently, has contributed to this trend. However, such markets have been inconsistently developed across the country and the future of Regional Transmission Organizations (RTOs) that would create even larger areas of central control is uncertain.

5.1 Prior Experience With Outages

The experience of several high-profile outages reinforces the need for planning and leadership, no matter the ownership structure. While the memories of the great blackout of 2003 are still fresh, 38 years earlier a similar event, in this case affecting interconnected systems owned by local monopolies, plunged New York, as well as much of Ontario and New England into darkness following an equipment failure. New York City was blacked out for an entire night, and about 30 million people were directly affected. The National Opinion Research Center studied this event and found that:

> "An outstanding aspect of public response to the blackout was the absence of widespread fear, panic, or disorder. There is probably little question that this absence is largely due to the ability of individuals to interpret their initial encounter with power loss as an ordinary event . . .. Of equal importance in maintaining order was the rapid dissemination of information about the blackout." (135).

A smaller outage in New York City in July 1977 was far more troubling (136, 137).Although outright panic did not emerge, there was considerable looting in some parts of the city. At the time, crime had been increasing and there was a general sense of insecurity in New York City. Some of the looting occurred due to poor response by the police, leaving some areas of the city more vulnerable. The 1977 blackout was frightening in ways that ordinary electricity outages are not, suggesting that there *can* be troubling social responses to turning out the lights.

There is some experience with widespread physical damage from natural forces. For example, in January 1998 an ice storm struck southeastern Canada, New York and New England, felling 1,000 transmission towers and 30,000 distribution poles while sending thousands of tree

branches into power lines. This event left 1.6 million people without power, some for more than a month. Almost a quarter-million people had to leave their homes to take shelter and at least a dozen people died (mostly due to loss of heat or suffocation from faulty temporary heating setups). Insurance claims reached approximately $1 Billion Canadian. This event, although massively destructive, did not cause panic or shock.

It is difficult to imagine a terrorist organization amassing the capability to accomplish damage on this scale, but a terrorist attack could nonetheless be larger and more long lasting than typical equipment- or weather-related problem, and multiple attack modes could be coordinated for maximum effect. Critical points exist in the electricity infrastructure (especially among transmission and sub-station assets) where attacks could cause more damage. A recent U.S. National Research Council panel found that "a coordinated attack on a selected set of key points in the system could result in a long-term, multi-state blackout," (110 p. 181) Furthermore, the ability of the electric power sector to deal with coordinated attacks on the system is lacking. As noted by NERC, "most (electricity sector) members do not have in place business recovery plans that include procedures for dealing with widespread, well-planned attacks on physical facilities. Likewise, they do not include procedures for dealing with deliberate attempts to hamper repair and restoration activities." (138 p. 36)

5.2 Transformer Vulnerabilities

High voltage transformers have been long identified as a key vulnerability in electric power infrastructure, but due to the cost of stockpiling, few spares are available. It might be possible to develop modular, flexible transformers, but this goal is frustrated by the tendency of different power companies to insist on unique standards and often on customized equipment for every situation. The current trend towards restructured markets may exacerbate this problem, "[d]eregulation has encouraged efficiency, invested-cost utilization and return on investment rather than redundancy, reliability and security. For the same reasons, power companies keep fewer spares on hand" (110). Other problems have also been identified. Spares are often kept at the substation site, increasing the possibility that an attack will also result in damage to the spares. If spares have to be ordered from the manufacturer, the customized nature of the transformers may mean the units could take a year or more to manufacture. Delivery could also be lengthy given that transformers are increasingly manufactured in a small number of low-cost countries (e.g. China and India).

5.3 Impact of an Outage

Estimates of the cost of a successful attack on the electricity infrastructure could be based on estimates of the costs of longer blackouts, which a successful attack would probably be similar to, or on estimates of the cost of short outages and associated estimates of the value of reliability. The duration of the disruption caused by the attack could then be associated with supply disruptions that range in their impact from merely a nuisance, to interruption of work and leisure activities, to disruption of vital services (e.g., health services and water supply) to loss of life and permanent damage to capital infrastructure (e.g., blast furnaces).

The literature on blackout costs is sparse and appears to be based on ad-hoc techniques. Generally, estimates of the costs of specific blackouts are found only in post-outage reports or articles in the popular press. The aggregate economic impacts of such events can vary widely, with the largest such blackout events having costs that reach into the billion dollar range. For instance, the 1998 blackout in Auckland, New Zealand left some of the downtown without power for up to two months, with an estimated cost of approximately $50 million (1998 US dollars), while a relatively short outage in New York in 1990 reportedly cost Citicorp $100 million (139 p. 15). On the other hand, estimates of the 1977 blackout in New York City are about $1Billion in current dollars (137, 140 p. 23, both adjusted to 2002$). The cost of the January 1998 ice storm in Canada was approximately $2Billion (U.S.) and at least 25 deaths, although not all of this is due directly to the ensuing power outage (141). The losses due to the Northeast blackout of 2003 are variously estimated in the range of $2-$10Billion, as summarized in a recent report by an group representing industrial electricity consumers (142).

The literature on the value of reliability was surveyed recently by Eto, et al., who found over 100 studies based in the U.S. alone (139). They found multiple methods to estimate costs and that a large number of studies focused on different aspects of the problem. Perhaps the most common method is to conduct surveys that cover different categories of losses, customer classes and severity of reliability events (143). These surveys can either elicit costs based upon experienced outages or use contingent valuation techniques to determine the willingness to pay (to avoid outages) or willingness to accept (compensation for experienced outages). Another method is to find an economic indicator that can act as a proxy for the overall cost of outages (for example, the value of lost production using sectoral economic data). A third common method is to use consumer's participation in markets (e.g. for interruptible power supply) as an indicator of the value of reliability. Eto, et al. also found that there were few comprehensive studies and few systematic studies of large outages. The few aggregate estimates of the annual costs to the U.S. economy of typical outages and poor power quality ranged over two orders of magnitude, from $5Billion to $400Billion.

5.4 Analyses of Power Systems Under Stress

There are few analyses of electric power systems under stress. An early analysis by Kahn compared two mixed systems, one with intermittent renewable generation plus hydroelectric dams that provide storage capacity and one with central station generators plus hydro (25, 144). This study looks only at generation adequacy and is somewhat abstract, but it finds that the excess storage capacity that the intermittent-based system needs for ordinary reliability purposes makes that system more resilient in the face of exogenous uncertainty (stress). A more detailed study compared a centralized system (based on the Reference Test System of the Institute of Electrical and Electronics Engineering), which includes multiple generator types and a stylized representation of a transmission system, with a very similar system that used distributed, gas-fired engines, including the necessary gas distribution system (67, 69). This research finds the distributed system is much more reliable, requiring virtually no excess capacity to match the performance of the centralized system. It is also much less sensitive to stress. The costs of the distributed system are higher if only electricity supply under typical conditions is considered, but

if heat recovery is possible, the distributed system is less expensive even under routine conditions. Under stress conditions, the distributed system is always far less costly, according to this study.

One modeling study compared two terrorist scenarios, one involving a sequence of small supply interruptions over the course of a year due to attacks on substations, the second a single, large-scale attack on generation and transmission assets (107). Although the year-long scenario involved only half the destruction, it involved significant damage to generation and subsequent damage to transmission assets that made recovery difficult. This smaller, but lengthy, scenario was five times more costly than the big, one-time attack and had a long-term effect as well. This model showed how series of small disruptions can give a strong signal about increased risk and drive business away.

Thus, it is not surprising that in places where deliberate attacks on the power system and interruption of service are frequent, both everyday life and economic development can be damaged (63). However, it is not clear if an attempt to turn out the lights would permit terrorists to create widespread panic or the shock associated with violent attacks on symbolic objects that cause loss of human life. Electricity customers in most industrialized countries lose power for an average of a couple of hours per year. For the most part, individuals and society cope with these outages well. Power companies respond rapidly to restore service, and facilities that have special needs for reliability (e.g. hospitals and airports) typically have backup generators.

5.5 Fuel Supply Disruptions

Electric power systems vary in how vulnerable they are to fuel supply disruption. In addition to oil, gas, and nuclear fuels (discussed in separate sections), electricity can also be generated with renewable energy sources, which is discussed in section 2.11 on Centralization, and below in section 7.4 on Renewables, and with coal, which is discussed here.

Coal is the fuel least vulnerable to deliberate attacks because it is produced in many locations, can be shipped by multiple means, and can be easily stored. In addition, coal supply systems are made up of large and relatively robust capital equipment (122, 123, 145). Coal is transported by a variety of means. Rail dominates, and other major modes include river barge and truck. Coal-fired power plants may often have multiple supply routes available to them, although one mode will tend to dominate and generally only that mode will have coal-handling capacity sufficient for long-term supply. Coal can be readily stored on site and coal-fired power plants typically have four to twelve weeks of fuel supply on hand. For power plants built at coal mines, fuel security is largely irrelevant, although these plants may require more transmission assets.

6 NUCLEAR

Unlike other energy sources, nuclear fuel and waste are intrinsically dangerous both in terms of their radiological and chemical hazards and as a potential resource for construction of weapons. Radiological material, released by any explosion creates a “dirty bomb.” Thus potential attacks

against various segments of the nuclear power infrastructure (fuel production, reactors, waste handling, and reprocessing facilities) are of concern.

The consequences of an attack against a nuclear facility is considered serious enough that this sector is considered to be one of vital national security and generally treated somewhat differently than other parts of the electric power sector (91 p. 83). This is, in some ways, simply a continuation of how the nuclear industry is treated in general, with its own regulatory bodies, like the U.S. NRC, due to the highly technical nature of the required regulations and the particular risks posed by the technology (146). As a result, there already exist numerous regulations and standards in this industry that are meant to help in both protecting these plants and operating them safely. However, one area of open inquiry is whether the existing set of regulations and standards is sufficient or properly focused to address new and changing risks.

Typically, the costs of mitigating the CIP risks of nuclear power plants, and other security risks such as proliferation, are not fully included in the cost of electric power these plants produce. For instance, after the terrorist attacks of September 11, 2001, many Governors in U.S. states put National Guard troops at nuclear plants, so the taxpayer in effect subsidized electricity consumers. As the owners of nuclear power electricity facilities have begun to face competition and the bottom line becomes more important, the costs of security are likely to receive greater scrutiny.

6.1 Fuel

Although refueling is infrequent (every 18 months or so for most reactors) it does involve risks of deliberate attack associated with production and shipping. The top seven countries ranked in order of nuclear contribution to electricity generation have no uranium resources whatsoever (e.g. France, Ukraine, Korea, Germany, Japan, Spain, UK). However, uranium deposits exist in many countries and are available in significant quantities in several stable democracies (e.g. Australia, Canada and the U.S.). Production of nuclear fuel is typically conducted by the national government under relatively tight security arrangements, or is closely supervised by the national government, as is trade and shipping.

6.2 Reactors

The most obvious threat is a direct attack upon nuclear reactors themselves. One possible attack mode is by airplane. Most nuclear reactor containment buildings are massive structures designed to withstand significant impacts (exceptions include plants like the Chernobyl facility in the Ukraine). Design studies for these structures typically examined massive accidents, such as earthquakes and unintentional airplane crashes. Seismic events do not appear to be relevant to understanding deliberate attacks, but airline crashes obviously are. The design studies typically considered a large commercial plane for the time, a Boeing 707 traveling at a moderate speed, or a military jet (e.g. a Phantom II) traveling much faster, but without weapons. In both cases, the critical factor is the ability of a turbine shaft to penetrate the multiple layers of containment that surround the reactor core. Although some questions remain regarding the effects of a deliberate aircraft attack on a nuclear power plant, these events would not likely present more severe stresses on reactor containment systems than those originally used as the design basis (147-150).

Higher impact speeds tend to reduce the probability that a large aircraft could be flown into a specific point on a power plant, reducing the risk somewhat (151). However, an attack on a nuclear power plant, no matter how it was carried out, could reveal systemic flaws or common-mode failures, which could lead regulators to order an immediate shutdown of numerous reactors (50).

The possibility of an armed assault on a nuclear facility itself has also been a concern and contingency measures are supposed to be in place to protect these facilities from being taken over by a hostile force that could damage the plant. These concerns about direct attack by truck bombs or commando squads have led to physical barriers and armed guards that protect all nuclear power plants. However, it is not clear how effective these steps are, a 1999 review by the NRC found significant weaknesses in 27 of the 57 plants evaluated (152).

Another concern is the number of relatively less well defended research reactors. These exist in many more countries than do power reactors and are often sited at facilities such as universities and research institutes that may be in highly populated areas and may not have adequate security measures. Research reactors are low power reactors used to study reactions, create isotopes and carry out a variety of research projects. These reactors do not have the same amount of radioactive materials in them, but it may be easier for a terrorist to successfully attack one of these facilities and disperse radioactive materials (153)

6.3 Waste

After removal from nuclear reactors, spent fuel rods are highly radioactive. These spent fuel rods are first placed in pools to help dissipate the heat due to radioactive decay of fission products and then can be placed in "dry storage" awaiting disposal. At the moment no country with a nuclear program has begun operation of a waste repository for spent nuclear fuel, which must remain isolated from the environment for thousands of years (154). As a result, there are "temporary" spent nuclear fuel storage areas at reactor sites all over the world. Currently, the vast majority of these spent fuel storage facilities are special pools that are cooled to dissipate the heat. However, a growing amount of spent nuclear fuel is being stored in massive 'casks' without cooling water.

Standards for both wet and dry storage of spent nuclear fuel vary significantly from country to country. Dry cask storage in Germany, for instance, is either in a pool that is inside a containment vessel or stored in massive casks that have successfully resisted penetration by simulated turbine shafts moving at near-sonic speeds, and the casks themselves are held in massively reinforced structures to prevent damage by missile attack (155, 156).

In contrast, spent nuclear fuel in the United States is far less well protected (157, 158). Due to the lack of a final repository for spent nuclear fuel, some spent fuel pools are being packed with fuel rods at a much higher density than originally envisioned and boron has been added to the pool water to absorb neutrons and prevent criticality accidents. These densely-packed storage pools are not inside of containment buildings, and many are elevated well above ground level. The concern about such sites is that they are more vulnerable than reactors that sit inside massive containment buildings, and that a loss of the coolant as a result of sabotage or terrorist act could

result in a nuclear accident. A loss of coolant could result in rapid heating resulting in the outside shell of the fuel rods (called the cladding) catching fire. The result could be significant dispersal of the highly radioactive fission products such as Cs-137. Using a variety of studies conducted for the NRC by various national laboratories and other sources, Alvarez et al. argue that it would be wise to move a significant amount of spent nuclear fuel at reactor sites in the United States to something like the massive-cask-plus-massive-building storage as in now in place in Germany.

As with the issue of breaching reactor containment structures, there is disagreement as to both the possibility of a problem and the potential impacts should there be an incident at a nuclear waste facility. Recently, the NRC argued that the analysis by Alvarez et al. was overly conservative (159). However, this rebuttal is based on classified research, and so is impossible to evaluate (160)

6.4 Reprocessing

Reprocessing facilities are used to process spent nuclear fuel rods in order to separate plutonium from the rest of the highly radioactive fuel. These facilities have been used for both military purposes (and are necessary for all modern nuclear weapons) and for civilian purposes in an effort to create so-called "closed" fuel cycles that re-use the plutonium as a reactor fuel. For both of these uses the reprocessing is done primarily through chemical processes resulting in large quantities of liquid waste that is highly radioactive (due to the other materials in the spent fuel rod). Reprocessing facilities pose two risks from the infrastructure security point of view. The first is that, like reactors and spent fuel storage pools, the waste facilities at reprocessing sites contain large quantities of highly radioactive material that could potentially be dispersed. The second concern is that materials from these sites could be stolen for use in either a nuclear or radiological weapon. In particular, separated plutonium for use in a nuclear weapon would make such sites attractive. However, like reactors, there are strict national and international standards for the protection of these sites against assault. It is not readily apparent if the testing record of these facilities is better or worse than that of power reactors.

6.5 Proliferation

Nuclear power plants also present a unique threat labeled 'proliferation,' which is the potential for nuclear fuel (or waste) to be used in creating nuclear or radiological weapons. Materials might be obtainable from fuel production, fuel storage at power plants, waste reprocessing operations, or from waste storage. One of the major impediments to the terrorist use of a nuclear or radiological weapon is both the technical skills necessary to design a weapon and access to materials. However, designing a crude nuclear device is not necessarily considered to be difficult and material access may in fact be the main impediment (161).

There are a number of means by which one could obtain the necessary nuclear materials to build a nuclear or radiological weapon. Nuclear fission weapons require fissile materials that can sustain a chain reaction (either highly enriched uranium or plutonium), which could be obtained either already in the form of a weapon or as a raw material. Separated plutonium would be the result of spent fuel reprocessing in either military or civilian nuclear programs and plutonium

stockpiles are orders of magnitude larger than what is necessary for a single weapon (162). One source of highly enriched uranium to make a weapon would be the many operating and closed research reactors that are fueled with highly enriched uranium (HEU). Though the United States did replace the HEU in most domestic research reactors with low enriched uranium and did embark on a program to replace the HEU it sent to overseas research reactors, there are still a large number of reactors in existence that use HEU (153).

A radiological weapon does not require fissile material, instead relying on conventional explosives to disperse radioactive materials. In this case, the goal would likely be to disperse highly radioactive fission products rather than fissile materials such as uranium or plutonium. Such materials could either come from sources such as spent fuel rods (which would contain both fissile materials and fission products) as well as the reprocessing waste from the separation of fissile materials from spent fuel. New reactor designs that are more resistant to physical assault or require no refueling might be developed, but the cost of doing so is unclear.

Another risk that has been raised and is also the subject of debate is the transportation of the spent fuel rods from the spent fuel pools at the reactors to an eventual waste repository. There is concern that the fuel rods could be intercepted and the materials used for a radiological dispersal weapons (163). One method to deal with the threat of proliferation of nuclear materials is to improve and strengthen international standards for material accounting and protection (153).

6.6 Public Reactions

Attacks on nuclear facilities, even if there is little direct impact, could raise public alarm and lead to a variety of negative consequences. Due to the dread the public has of nuclear radiation (whether scientifically supported or not), it might be possible to create significant public distress (or even terror) even with an unsuccessful attack on a nuclear power plant. The core meltdown of the Three Mile Island plant in Pennsylvania in 1976 had a devastating effect on the U.S. nuclear power industry even though no one was hurt and insignificant amounts of radioactivity were released (164 pp. 172-7). Even an unsuccessful attack could lead to panicked publics and political pressure for nuclear plant closures, which could have a significant impact on some electricity systems that rely heavily on nuclear power.

The degree to which this is an issue is unknown as it will depend on both government response to an incident (including how risk is communicated) and the public's response to an extreme situation. Civil defense preparedness has been an important government function for a long time and emergency procedures are in place for a variety of contingencies. The question does remain whether the radioactive nature of the incident would result in behavior that could hamper the response efforts. Panic is a widely expected behavior under those circumstances. However, evidence from response to the World Trade Center attacks and other historical events shows it may not be the overwhelming reaction (165). Surveys on responses to terrorism indicate issues with risk communication that may help in shaping an appropriate public response (166).

7 PREVENTION AND RESPONSE

7.1 'Guards, Gates, and Guns'

One approach to dealing with these issues is to assess, and if necessary and justified, improve the physical security of energy infrastructure. For instance, following the September 11, 2001 attacks a number of energy facilities owners did increase their security (particularly nuclear power plants). Some companies have begun to hire trained counter-terrorism officers and obtained waivers from the state for their protective force to carry heavier arms. This approach also probably requires relying on surveillance technologies to detect attack, ranging from manned surveillance to automated sensors to detect intrusion. The primary purpose of such technologies is to detect an attack and mobilize the resources (i.e. private security force, local police, military) to repel the attack and prevent damage. A secondary purpose would be to collect evidence to be used in the investigation of any attack. Improved physical security (including surveillance) is particularly important for the electricity infrastructure due to its exposure and geographic extent. While there exists a wide variety of monitoring and surveillance technologies, they are not considered adequate for protecting the electricity infrastructure. In the case of remote facilities, such as transformers and powerlines, monitoring technologies may not be of use in preventing an attack if the response time of an intervention force is too long.

Unfortunately, any technology used for monitoring or surveillance has the risk of failure. Another problem has to do with nuisance alarms. Surveillance and monitoring systems are not always able to distinguish between an intruder and an animal or between a line being deliberately cut and one that has been struck by a falling tree. Guarding against failures and false positives may require back-up systems or complementary technologies that can confirm or deny events, increasing costs (110).

7.2 Emergency Response and Restoration

As there is no guarantee that an attack can be prevented or will be unsuccessful, emergency response and restoration plans for each energy sector must be, and are, in place. The nature of those response plans will vary quite widely depending on the particular energy infrastructure in question and the extent of the problem. In the event of a nuclear accident or radiological weapon, the immediate problem will be issues such as risk communication to avoid panic and exacerbation of the problem, possible evacuation, and medical treatment. Longer term problems would include decontamination and repair, health monitoring and continued risk assessment.

For the oil and gas industry, consider supply and demand responses. Suppliers face two distinct challenges: a) the immediate process of damage containment (e.g., control of spills and fires, evacuation of personnel and public), and, b) the process of restoration of service (e.g., repairs to affected infrastructure and resources). From an end-user perspective, the time to restoration of supply following an attack or accident is critical to their needs. On-site fuel storage can easily allow end-users to experience no significant impact from a supply disruption if the disruption lasts for a period shorter than the rate at which stored fuels are depleted. However, if the resumption of supply is expected to take longer than available storage, end-users need to weigh the relative costs of curtailment of activities and alternative sources of supply, even alternative energy sources.

The rich and highly technical literature on the restoration of power systems shows how valuable the ability to fail softly or graceful could be (134, 167). Restoring a power system after a blackout can be a complicated process, even when the physical infrastructure itself has not been damaged. Both load and generation have to be brought back on-line while maintaining the various parameters of the system within pre-specified bounds (e.g. voltage and frequency). A number of tools have been developed to aid in the process ranging from training simulators to computer aided restoration employing knowledge based systems.

However, these analyses assume demand is fixed and cannot be controlled at all, unlike the example discussed earlier involving traffic lights. Considering the demand side, and especially possible tradeoffs between curtailment of activities and alternative energy supplies during a prolonged outage, firm level experience with these issues is more widespread that is often recognized as many electricity and gas utilities have long offered 'interruptible supply' contracts to their larger customers.

7.3 Institutions

As noted in section 2.1, the security of energy infrastructure is at least partly a public good, and so will not be provided in socially desired quantities by market forces alone, government action of one sort or another is needed. Most notable are government regulation and private institutions that have been established to promote reliability in the electric power sector. In the U.S., voluntary coordination councils were set up by the electric utility industry following the 1965 blackout, to avoid government regulation of reliability. State public utility commissions play a role as well. All countries have some form of electricity reliability institution(s). However, industry restructuring is drastically changing current institutional arrangements, leading to serious questions about whether such private approaches will be adequate to ensure reliability, let alone provide adequate security. Following the 2003 blackout in the northeastern U.S., pressures to move towards regulation and mandatory reliability rules mounted.

Institutional issues also play out in apparently purely technical domains. For instance, several studies have shown that barriers are often raised to the interconnection of a distributed source to the grid (86). These barriers could come from market structure issues, the relative roles of DG owners and utilities and from standards that are developed for the interconnection of distributed resources. Similar concerns exist about the incentives for cooperation and investment in new control strategies and technologies.

One of the key challenges for the future is ensuring that institutional solutions to emerging energy infrastructure security are created for whatever new structure the electricity industry takes. This includes looking at threats that go beyond those considered in traditional contingency planning. However, the potential for creating terror through attacks on the electric power system seem limited (with the exception of an attack on a nuclear facility). Loss of power, even if large-scale and frequent, is costly and annoying, and if caused by malicious attacks can be disconcerting, but it pales in comparison with the effect of large-scale loss of life that is often the purpose of terrorist acts.

7.4 Efficiency and Renewables

A great deal has been made of the potential of both efficiency and renewable energy sources to reduce the vulnerability of energy infrastructures, from *Brittle Power* to more recent versions of the same somewhat idealized and vague arguments (168-170). There are two related, but slightly different, arguments about energy efficiency. The first is that improved energy efficiency reduces the impact of a disturbance to the infrastructure. Higher efficiency reduces the burden on the infrastructure, according to this argument, which would be particularly important during a crisis and could allow the system to continue to function, and stored fuels would last longer during an emergency. This argument does have salience when security is defined in traditional terms of concerns about oil imports from the Middle East. However, in this new definition of security where deliberate attacks on supply systems are being considered there is no reason to presume that suppliers would not adjust to greater end-use energy efficiency by maintaining reserve margins (as % of use) at previous levels in order to save money.

A related concept is responsive demand, which is most applicable to the electricity sector (171, 172). Demand response, or "intelligent loads" can respond automatically to signals from the energy supplier to reduce energy consumption. This can help reduce the need for peak capacity, which might typically be used to reduce costs in routine operation but could also be used to cope with supply interruptions.

The second argument for efficiency is that energy efficiency could make the scale of fuel consumption more compatible with local production capacity and make renewable sources a more feasible alternative to large scale and centralized fossil fuel and electricity production and distribution (i.e., it may be infeasible to supply a fleet of pickup trucks and sport utility vehicles with bio-fuels, but it could be possible to produce bio-fuels locally for small, hybrid cars).

The argument for renewables is similar to the argument for high efficiency technologies allowing for reduced demand for vulnerable fuels. Small-scale renewable energy sources have little, if any, fuel supply vulnerabilities. However, large systems such as hydro and wind utilized to service distant urban centers cannot be dissociated with risks to the transmission system. Fortunately, these issues are now beginning to be dealt with more seriously (173). However, if the challenge of energy supply security is serious enough to encourage us to probe fundamental characteristics of our current energy infrastructure, the option of combining efficiency and local renewable resources may be so persuasive as to reshape our landscape.

8 CONCLUSIONS

As noted in section 2.1, the burden of security measures is implicitly divided between energy users, suppliers and the government. In addition, status quo in the energy infrastructure reflects an era where deliberate attacks on the system were largely inconceivable, economies of scale still available and intelligent loads a distant fantasy. Today, the context within which energy is supplied and used has evolved well past the paradigm that has led to the current physical infrastructure and institutional arrangements.

As noted in this review, concerns about deliberate attacks on the energy infrastructure have highlighted many critical questions to which no ready answers exist. For example: How much

and what kind of security for energy infrastructure do we want and who will pay for it? Current CIP efforts tend to ignore this issue entirely, focusing on preventing attacks and protecting whatever energy infrastructure the private sector creates. At the same time, some of the costs of security protection are socialized, favoring certain technologies over others.

Energy security has been one of many battlefields between advocates of fossil resources and advocates of renewable energy sources. At first, economics alone largely drove issues. In the late 19th century whale oil gave way to kerosene for lighting, after which horse fodder, wind, and coal gave way to gasoline as a transportation fuel. Throughout the late 20th century, environmental issues have defined the battle lines between the two camps. Today, concern about critical infrastructures have once again brought into sharp relief the diversity of perspectives on the different paths to a future of greater energy security.

The realization of various economic inefficiencies has already led us to revisit the public policy shaping the institutional infrastructure for energy supply. Perhaps the realization of new security concerns will also lead to the recognition that our options are bifurcated along the lines of: a) increasingly inefficient and ineffective security measures (paid for privately and publicly) used to protect a brittle infrastructure and b) adoption of a new paradigm of security based on a soft-fail infrastructure promoted through appropriate public policies. The latter also opens the door to more innovative approaches to demand management, diversity in resources and conversion technologies.

9 REFERENCES

1. Seger KA. 2003. *Utility Security: A New Paradigm*. Tulsa: PennWell Publishers. 238 pp.
2. Parfomak PW. 2004. *Pipeline Security: An Overview of Federal Activites and Current Policy Issues. Rep. RL31990*, Congressional Research Service, Washington, DC
3. Office of Technology Assessment. 1979. *The Effects of Nuclear War*, U.S. Congress, Washington, DC
4. Adams N. 2003. *Terrorism & Oil*. Tulsa, OK: Penn Well Corporation. 208 pp.
5. Anonymous. 2003. *Silent Vector: Issues of Concern and Policy Recommendations*, Center for Strategic and International Studies, Washington
6. Bucholz A. 1994. Armies, Railroads, and Information: The Birth of Industrial Mass War. In *Changing Large Technical Systems*, ed. J Summerton, pp. 53-70. Boulder, CO: Westview Press
7. Yergin D. 1991. *The Prize: The Epic Quest for Oil, Money, and Power*. New York: Simon & Schuster. 917 pp.
8. Bohi D, Toman M. 1996. *The Economics of Energy Security*. Boston, MA: Kluwer Academic Publishers
9. Klare MT. 2001. *Resouce Wars: The New Landscape of Global Conflict*. New York: Henry Holt and Company. 289 pp.

10. Lovins AB, Lovins LH. 1982. *Brittle Power: Energy Strategy for National Security*. Andover, MA: Brick House Publishing Company. 486 pp.

11. Campbell CJ, Laherrere JH. 1998. The End of Cheap Oil. In *Scientific American*, pp. 78-83

12. Bentley RW. 2002. Global oil & gas depletion: an overview. *Energy Policy* 30: 189-205

13. Rogner HH. 1997. An assessment of world hydrocarbon resources. *Annual Review of Energy and the Environment* 22: 217-62

14. Jaffe AM, Manning RA. 2000. The Shocks of World of Cheap Oil. *Foreign Affairs* 79: 16-29

15. Gause FG. 2000. Saudi Arabia Over a Barrel. *Foreign Affairs* 79: 80-94

16. Gately D. 2001. How plausible is the consensus projection of oil below $25 and Persian Gulf oil capacity and output doubling by 2020? *Energy Journal* 22: 1-27

17. Morse EL, Richard J. 2002. The battle for energy dominance. *Foreign Affairs* 81: 16-+

18. Clark W, Page J. 1981. *Energy, Vulnerability, and War*. New York: W.W. Norton & Co. 251 pp.

19. Griffith TE, Jr,. 1994. *Strategic attack of national electrical systems*, Air University Press, Maxwell Air Force Base, AL

20. Mijuskovic N. 2000. *Serbia Restoration after war damages May-99*. Presented at CIGRE Session 2000, SC 39 Workshop on Large Disturbances

21. Keeney LD. 2002. *The Doomsday Scenario*. St. Paul, MN: MBI Publishing. 127 pp.

22. Energy and Defense Project. 1980. *Dispersed, Decentralized, and Renewable Energy Sources: Alternatives to National Vulnerability and War: Final Report*, Work conducted for the Federal Emergency Management Agency (Contract: DCPA-01-79-C-0320, FEMA Work Unit #2314-F), Washington, DC

23. Clark WC, Jones DD, Holling CS. 1979. Lessons for Ecological Policy Design - Case-Study of Ecosystem Management. *Ecological Modelling* 7: 1-53

24. Lovins A, Lovins LH. 1981. *Energy Policies for Resilience and National Security*, Friends of the Earth, Inc, San Francisco For the Federal Emergency Management Agency (Contract: DCPA01-79-C-0317, FEMA Work Unit #4351-C), Washington, DC

25. Kahn E. 1980. Reliability Planning for Solar Electric Power Generation. *Technological Forecasting and Social Change* 18

26. Holling CS, ed. 1978. *Adaptive environmental assessment and management*. New York: Wiley. 377 pp.

27. Ellison RJ, Fisher DA, Linger RC, Lipson HF, Longstaff T, Mead NR. 1999. *Survivable Network Systems: An Emerging Discipline. Rep. CMU/SEI97-TR-013, ESC-TR-97-013*, Carnegie Mellon Software Engineering Institute, Pittsburgh, PA

28. Lipson HF, Fisher DA. 1999. *Survivability - A new technical and business perspective on security*. Presented at New Security Paradigms Workshop, Caledon Hills, ON

29. Schlager E, Ostrom E. 1992. Property-Rights Regimes and Natural Resources: A Conceptual Analysis. *Land Economics* 68: 249-62

30. O'Hanlon ME, Orszag PR, Daalder IH, Destler IM, Gunter DL, et al. 2002. *Protecting the American Homeland: A Preliminary Analysis*. Washington, DC: Brookings Institution Press. 182 pp.

31. Garces FF. 2004. Electric Power: Transmission Generation Reliability and Adequacy. In *Encyclopedia of Energy*, ed. CJ Cleveland, pp. forthcoming. London: Elsevier

32. Little RG. 2002. Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures. *Journal of Urban Technology* 9: 109-23

33. Keeney R, Kulkarni R, Nair K. 1978. Assesing the Risk of an LNG Terminal. *Technology Review* 81: 64-72

34. Fay JA. 2003. Model of spills and fires from LNG and oil tankers. *Journal of Hazardous Materials* 96: 171-88

35. Parfomak PW. 2003. *Liquefied Natural Gas (LNG) Infrastructure Security: Background and Issues for Congress. Rep. RL30153*, Congressional Research Service, Washington, DC

36. Tan DM, Xu J, Venart JES. 2003. Fire-induced failure of a propane tank: some lessons to be learnt. *Proceedings of the Institution of Mechanical Engineers Part E-Journal of Process Mechanical Engineering* 217: 79-91

37. Planas-Cuchi E, Vilchez JA, Perez-Alavedra FX, Casal J. 1998. Effects of fire on a container storage system - a case study. *Journal of Loss Prevention in the Process Industries* 11: 323-31

38. Leslie IRM, Birk AM. 1991. State-of-the-Art Review of Pressure Liquefied Gas Container Failure Modes and Associated Projectile Hazards. *Journal of Hazardous Materials* 28: 329-65

39. Romero S. 2004. Algerian Explosion Sitrs Foes of U.S. Gas Projects. In *The New York Times*, pp. W1. New York

40. Abrams M. 2003. The Dawn of the E-Bomb. In *IEEE Spectrum*

41. Kopp C. 1998. The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction. In *Air & Space Power Chronicles*, pp. Online Journal: Maxwell Air Force Base

42. Kappenman JG. 1996. Geomagnetic Storms adn Their Impacts on Power Systems. *IEEE Power Engineering Review* 16: 5-8

43. Meliopoulos APS, Glytsis EN, Cokkinides GJ, Rabinowitz N. 1994. Comparison of SS-GIC and MHD-EMP-GIC effects on power systems. *IEEE Proceedings on Power Delivery* 9: 194-207

44. Leiby PN, Jones DW, Curlee TR, Lee R. 1997. *Oil Imports: An Assessment of Benefits and Costs. Rep. ORNL-6851*, Oak Ridge National Laboratory, Oak Ridge, TN

45. Greene DL, Jones DW, Leiby PN. 1998. The outlook for US oil dependence. *Energy Policy* 26: 55-69

46. Salameh MG. 2003. The new frontiers for the United States energy security in the 21st century. *Applied Energy* 76: 135-44

47. Salameh MG. 2003. Quest for Middle East oil: the US versus the Asia-Pacific region. *Energy Policy* 31: 1085-91

48. Porter D, Steen N. 1996. Renewable energy in a competitive electricity market. *Renewable Energy* 9: 1120-3

49. Lemar PL. 2001. The potential impact of policies to promote combined heat and power in US industry. *Energy Policy* 29: 1243-54

50. Evans N, Hope C. 1984. *Nuclear power : futures, costs and benefits*. New York: Cambridge University Press. 171 pp.

51. Margolis RM, Kammen DM. 1999. Underinvestment: The energy technology and R&D policy challenge. *Science* 285: 690-2

52. Gritsevskyi A, Nakicenovic N. 2000. Modeling uncertainty of induced technological change. *Energy Policy* 28: 907-21

53. Farrell AE. 2004. Local-National-International Institutional Linkages in Environmental Policy: Air Pollution in Spain. In *Smoke and Mirrors: Air Pollution in Culture and Politics*, ed. M Dupuis, pp. forthcoming. Albany: State University of New York (SUNY) Press

54. Awerbuch S. 2000. Investing in photovoltaics: risk, accounting and the value of new technology. *Energy Policy* 28: 1023-35

55. Stirling A. 1998. On the Economics and Analysis of Diversity. In *SPRU Electronic Working Papers*. Brighton: Science Policy Research Unit, University of Sussex

56. Stirling A. 1994. Diversity and Ignorance in Electricity Supply Investment - Addressing the Solution Rather Than the Problem. *Energy Policy* 22: 195-216

57. Shea DA. 2002. *Critical Infrastructure: Control Systems and the Terrorist Threat. Rep. RL31534*, The Library of Congress, Congressional Research Service, Washington, DC

58. Safire W. 2004. The Farewell Dossier. In *The New York Times*, pp. A25. New York

59. U.S. Department of Energy Office of Critical Infrastructure Protection. 2001. *Critical Infrastructure Interdependencies: Impact of the September 11 Terrorist Attacks on the World Trade Center (A Case Study)*, U.S. Department of Energy, Office of Critical Infrastructure Protection, Washington, DC

60. Rinaldi SM, Perenboom JP, Kelly TK. 2001. Critical Infrastructure Interdependencies. In *IEEE Control Systems Magazine*, pp. 11-25

61. Amin M. 2002. Editorial: Toward Secure and Resilient Interdependent Infrastructures. *Journal of Infrastructure Systems* 8: 67-75

62. Longstaff TA, Haimes YY. 2002. A holistic roadmap for survivable infrastructure systems. *Ieee Transactions on Systems Man and Cybernetics Part a-Systems and Humans* 32: 260-8

63. Farrell AE, Zerriffi H. 2004. Electric Power: Critical Infrastructure Protection. In *Encyclopedia of Energy*, ed. CJ Cleveland, pp. forthcoming: Academic Press

64. Zweifel P, Bonomo S. 1995. Energy Security - Coping with Multiple Supply Risks. *Energy Economics* 17: 179-83

65. Karki R, Billinton R. 2001. Reliability/cost implications of PV and wind energy utilization in small isolated power systems. *IEEE Transactions on Energy Conversion* 16: 368-73

66. Ubeda JR, Garcia M. 1999. Reliability and production assessment of wind energy production connected to the electric network supply. *IEEE Proceedings-Generation Transmission and Distribution* 146: 169-75

67. Zerriffi H, Dowlatabadi H, Strachan ND. 2002. Electricity and Conflict: Advantages of a Distributed System. *The Electricity Journal* 15: 55-65

68. Farrell AE, Lave LB, Morgan MG. 2002. Bolstering the Security of the Electric Power System. *Issues In Science and Technology* XVIII: 49-56

69. Zerriffi H, Dowlatabadi H, Farrell AE. 2005. Incorporating Stress In Electric Power System Reliability Models. *Proceedings of the IEEE: Special Issue on Energy Infrastructure Defense Systems* under review

70. Council on Competitiveness. 2002. *Creating Opportunity out of Adversity*. Presented at National Symposium on Competitiveness and Security, Pittsburgh, PA

71. Byon I. 2000. *Survivability of the U.S. Electric Power Industry*. M.S. thesis. Carnegie Mellon University, Pittsburgh, PA. 85 pp.

72. Strachan ND, Zerriffi H, Dowlatabadi H. 2002. System Implications of Distributed Generation: Economics and Robustness. In *Critical Infrastructures*, ed. P Herder

73. Hughes TP. 1983. *Networks of power : electrification in Western society, 1880-1930*. Baltimore: Johns Hopkins University Press. 474 pp.

74. Hirsh RF. 1999. *Power Loss: The Origins of Deregulation and Restructuring in the American Utiltiy System*. Cambridge: The MIT Press. 406 pp.

75. Hyman L. 2002. *America's Electric Utilities: Past, Present and Future*. Reston, VA: Public Utilities Reports. 297 pp.

76. Lovins A. 1976. Energy Strategy: The Road Not Taken. *Foreign Affairs* 55: 65-96

77. Cowart R. 2002. *Electrical Energy Security: Policies for a Resilient Network*, Regulatory Assistance Project, Montpelier, VT

78. Martin B. 1978. Soft energy, hard politics. In *Undercurrents*, pp. 10-3

79. Lovins AB. 1978. Soft Energy Technologies. *Annual Review of Energy and the Environment* 3: 477-517

80. Amin M. 2001. Towards Self-Healing Infrastructures. *IEEE Computer Applications in Power*: 20-8

81. Electricity Advisory Board. 2002. *Transmission Grid Solutions Report*, U.S. Department of Energy, Washington, DC

82. United States Energy Association. 2002. *National Energy Security Post 9/11*, United States Energy Association, Washington, DC

83. Kunreuther H, Heal G, Orszaq PR. 2002. *Interdependent Security: Implications for Homeland Security Policy and Other Areas. Rep. Policy Brief #108*, Brookings Institution, Washington, DC

84. von Meier A. 1994. Integrating Supple Technologies Into Utility Power. In *Changing Large Technical Systems*, ed. J Summerton, pp. 211-30. San Francisco: Westview Press

85. Strachan ND, Dowlatabadi H. 2002. Distributed Generation and Distribution Utilities. *Energy Policy* 30: 649-61

86. Alderfer RB, Eldridge MM, Starrs TJ. 2000. *Making Connections: Case Studies of Interconnection Barriers and Their Impacts on Distributed Power Projects. Rep. NREL/SR-200-28053*, National Renewable Energy Laboratory, Golden, CO

87. Luiijf E, Burger HN, Klaver MH. 2003. Critical Infrastructure Protection in the Netherlands: A Quick-scan. In *EICAR Conference Best Paper Proceedings*, ed. UE Gattiker, pp. 19. Copenhagen: EICAR

88. General Accounting Office. 2001. *Critical Infrastructure Protection. Rep. GAO-01-323*, General Accounting Office, Washington, DC

89. Moteff JD. 2002. *Critical Infrastructures: Background, Policy, and Implementation. Rep. RL30153*, The Library of Congress, Congressional Research Service, Washington, DC

90. 2002. Homeland Security Act.

91. President of the United States. 2003. *The National Strategy For the Physical Protection of Critical Infrastructures and Key Assets*, The White House, Washington, DC

92. President's Critical Infrastructure Protection Board. 2002. *The National Strategy to Secure Cyberspace (Draft for Comment)*, The President's Critical Infrastructure Protection Board, Washington, DC

93. President of the United States. 2000. Defending America's Cyberspace: National Plan for Information Systems Protection v1.0. ed. CIA Office. Washington, DC: U.S. Department of Commerce

94. Moteff J, Copeland C, Fischer J. 2002. *Critical Infrastructures: What Makes an Infrastructure Critical? Rep. RL31556*, The Library of Congress, Congressional Research Service, Washington, DC

95. President of the United States. 1996. Executive Order 13010: Critical Infrastructure Protection. pp. 37347 - 50

96. President's Commission on Critical Infrastructure Protection. 1997. *Critical Foundations: Protecting America's Infrastructures*, President's Commission on Critical Infrastructure Protection, Washington, DC

97. President's Commission on Critical Infrastructure Protection. 1997. *Research and Development Recommendations for Protecting and Assuring Critical National Infrastructure*, Department of Justice, Washington, DC

98. President of the United States. 1998. Presidential Decision Directive 63: Critical Infrastructure Protection. In *PDD-63*, pp. 12. Washington, DC: Department of Justice

99. Townsend W. 2002. *The Office Of Energy Assurance*. Presented at 2002 SHOPP Conference

100. President of the United States. 2001. Executive Order 13228: Establishing the Office of Homeland Security and the Homeland Security Council.

101. Office of Homeland Security. 2002. *National Strategy for Homeland Security*, Executive Office of the President, Office of Homeland Security, Washington DC

102. Burns RE, Wilhelm J, McGarvey J, Lehmann T. 2003. *Security-Related Cost Recovery In Utility Network Industries*, The National Regulatory Research Institute, Columbus, OH

103. McGarvey J, Wilhelm J. 2003. *NARUC/NRRI 2003 Survey On Critical Infrastrucuter Security*, The National Regulatory Research Institute, Columbus, OH

104. Stevens GM. 2003. *Homeland Security Act of 2002: Critical Infrastructure Information Act. Rep. RL31762*, Congressional Research Service, Washington, DC

105. Moteff J, Stevens GM. 2003. *Critical Infrastructure Information Disclosure and Homeland Security*, Congressional Research Service, Washington DC

106. Federal Energy Regulatory Commission. 2003. Order 630: Critical Energy Infrastructure Information. pp. 9857-73

107. Robinson CP, Woodard JB, Varnado SG. 1998. Critical infrastructure: Interlinked and vulnerable. *Issues in Science and Technology* 15: 61-7

108. 2002. Statement of Ronald L. Dick, Director of the National Infrastructure Protection Center on Critical Infrastructure Protection. In *Committee on Governmental Affairs*. Washington, DC

109. Stein W, Hammerli B, Pohl H, Posch R. 2003. *Critical Infrastructure Protection (CIP) Workshop - Introduction and Goals*. Presented at Critical Infrastructure Protection (CIP) Workshop - Status and Perspectives, Frankfurt am Main

110. National Research Council. 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington DC: National Academies Press

111. Schmitz W. 2003. *Comprehensive Roadmap: Analysis and Assessment for Critical Infrastructure Protection. Rep. ACIP IST-2001-37257*, ACIP, Copenhagen

112. Robinson DG, Ranade SJ, Rodriquez SB, Jungst RG, Urbina A, et al. 2001. *Development of the Capabilities to Analyze the Vulnerability of Bulk Power Systems. Rep. SAND2001-3188*, Sandia National Laboratory, Albuquerque, NM

113. Rinaldi SM. 2004. *The Role of Modeling and Simulation in Critical Infrastructure Protection*. Presented at 27th Hawaii International Conference on System Science, Honolulu

114. Muller F. 2003. Energy security - Risks of international energy supply. *Internationale Politik* 58: 3-10

115. Energy Information Administration. 2002. *International Energy Outlook*, U.S. Department of Energy, Washington

116. British Petroleum. 2003. *BP Statistical Review Of World Energy*, The British Petroleum Company, plc, London

117. Senden MMG, Punt AD, Hoek A. 1998. Gas-to-liquids processes: Current status & future prospects. *Natural Gas Conversion V* 119: 961-96

118. Ramcharran H. 2002. Oil production responses to price changes: an empirical application of the competitive model to OPEC and non-OPEC countries. *Energy Economics* 24: 97-106

119. Bohi D, Toman M. 1993. Energy Security: Externalities and Policies. *Energy Policy* 93: 1093 - 109

120. Adelman MA. 1995. *The genie out of the bottle : World oil since 1970*. Cambridge: MIT Press. 350 pp.

121. Chang HJ. 2003. New horizons for Korean energy industry - shifting paradigms and challenges ahead. *Energy Policy* 31: 1073-84

122. Larson ED, Wu ZX, DeLaquil P, Chen WY, Gao PF. 2003. Future implications of China's energy-technology choices. *Energy Policy* 31: 1189-204

123. ZhiDong L. 2003. An econometric study on China's economy, energy and environment to the year 2030. *Energy Policy* 31: 1137-50

124. Jones DW, Leiby PN, Paik IK. 2004. Oil price shocks and the macroeconomy: What has been learned since 1996? *Energy Policy* forthcoming

125. Newbery DM, Stiglitz JE. 1981. *The Theory of Commodity Price Stabilization*. New York: Oxford University Press

126. Jorgenson D. 1988. Productivity and economic growth in Japan and the United States. *American Economic Review* 78: 217-22

127. Denison EF. 1985. *Trends in American Economic Growth, 1929-1982*. Washington, DC: The Brookings Institution. 141 pp.

128. Hamilton JD. 2003. What is an oil shock? *Journal of Econometrics* 113: 363-98

129. LaCasse C, Plourde A. 1995. On the Renewal of Concern for the Security of Oil-Supply. *Energy Journal* 16: 1-23

130. Rempel H. 2002. Natural gas for Europe - Present state and predictions for a stable supply in the future. *Energy Exploration & Exploitation* 20: 219-37

131. Anonymous. 2000. A Brief History of U.S. LNG Incidents. CH-IV Coporation,

132. Jensen JT. 2003. The LNG Revolution. *The Energy Journal* 24: 1-45

133. Friedlander GD. 1966. The Northeast Power Failure--A Blanket of Darkness. *IEEE Spectrum*: 54-73.

134. Knight UG. 2001. *Power Systems in Emergencies: From Contingency Planning to Crisis Management*. New York: John Wiley & Sons. 378 pp.

135. National Opinion Research Center. 1966. *Public Response to the Northeastern Power Blackout*

136. Wilson GL, Zarakas P. 1978. Anatomy of a Blackout: How's and Why's of the series of events that led to the shutdown of New York's power in July 1977. *IEEE Spectrum*: 39-46

137. Congressional Research Service. 1978. *The Cost of an Urban Blackout: The Consolodated Edison Blackout, July 13-14, 1977. Rep. 95-54*, U.S. Congress, Washington, DC

138. North American Electric Reliability Council (NERC). 2001. *An Approach to Action for the Electricity Sector*, North American Electric Reliability Council (NERC)Working Group Forum on Critical Infrastructure Protection, Princeton, NJ

139. Eto J, Koomey J, Lehman B, Martin N, Mills E, et al. 2001. *Scoping Study on Trends in the Economic Value of Electricity Reliability to the U.S. Economy*, Prepared for EPRI by Energy Analysis Department Environmental Energy Technologies Division E. O. Lawrence Berkeley National Laboratory, Palo Alto, CA

140. Office of Technology Assessment. 1990. *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage. Rep. OTA-E-453*, U.S. Congress, Washington, DC

141. Kerry M, Kelk G, Etkin D, Burton I, Kalhok S. 1999. Glazed over: Canada copes with the ice storm of 1998. *Environment*

142. ELCON. 2004. *The Economic Impacts of the August 2003 Blackout*, Electricity Consumers Resource Council, Washington, DC

143. Morgan AJ. 1987. *A quantification of the effects of electricity supply interruptions*. Cambridge University, Cambridge

144. Kahn E. 1979. Compatibility of Wind and Solar Technology with Conventional Energy-Systems. *Annual Review of Energy* 4: 313-52

145. Office of Coal N, Electric and Alternate Fuels. 1998. *The Changing Structure of the Electric Power Industry: Selected Issues. Rep. DOE/EIA-0620*, Energy Information Agency, Washington, DC

146. 1999. Briefing on Existing Event Response Procedures (Including Federal Response Plan and Coordination Of Federal Agencies In Response To Terrrorist Activities). In *Nuclear Regulatory Commission*. Rockville, MD: NRC

147. Chapin DM, Cohen KP, Davis WK, Kintner EE, Koch LJ. 2002. NUCLEAR SAFETY: Nuclear Power Plants and Their Fuel as Terrorist Targets. *Science* 297: 1997-9

148. Brenner DJ. 2003. Revisiting Nuclear Power Plant Safety. *Science* 299: 201-3

149. Chapin DM, Cohen kp, Davis WK, Kintner EE. 2003. Revisiting Nuclear Power Plant Safety. *Science* 299: 201b-3

150. von Hippel FN. 2003. Revisiting Nuclear Power Plant Safety. *Science* 299: 201b-3

151. Swiss Federal Nuclear Safety Inspectorate. 2003. *Postion of the Swiss Federal Nuclear Safety Inspectorate regarding the Safety of the Swiss Nuclear Power Plants in the Event of an Intentional Aircraft Crash. Rep. HSK-AN-4626*, Wurenlingen, CH

152. Travers WD. 1999. *Recommendations Of The Safeguards Performance Assessment Task Force (WITS 199800188)*, Nuclear Regulatory Commission, Washington, DC

153. Bunn G, Braun C. 2003. Terrorism Potential for Research Reactors Compared With Power Reactors: Nuclear Weapons, "dirty Bombs," and Truck Bombs. *American Behavioral Scientist* 46: 714-26

154. Mcfarlane A. 2001. Interim Storage of Spent Fuel in the United States. *Annual Review of Energy and the Environment* 26: 201-35

155. Janberg K. 2002. *History and Actual Status of Aircraft Impact and Anti-Tank Weaponry Consequences On Spent Fuel Storage Installations*. Presented at MIT Workshop on Spent Reactor Fuel Storage, Cambridge, MA

156. Thomauske B. 2003. *Realization of the German Concept for Interim Storage of Spent Nuclear Fuel - Current Situation and Prospects*. Presented at Waste Management 2003, Tuscon, AZ

157. Alvarez R, Beyea J, Janberg K, Kang J, Lyman E, et al. 2003. Reducing the Hazards from Stored Spent Power-Reactor Fuel in the United States. *Science and Global Security* 11: 1-51

158. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, White House, Washington, DC

159. Anonymous. 2003. Nuclear Regulatory Commission (NRC) Review of 'Reducing the Hazards from Stored Spent Power-Reactor Fuel in the United States.' *Science and Global Security* 11: 203-11

160. Alvarez R, Beyea J, Janberg K, Kang J, Lyman E, et al. 2003. Response by the Authors to the NRC Review of 'Reducing the Hazards from Stored Spent Power-Reactor Fuel in the United States.' *Science and Global Security* 11: 213-23

161. Maerli MB, Schaper A, Barnaby F. 2003. The Characteristics of Nuclear Terrorist Weapons. *American Behavioral Scientist* 46: 727-44

162. Makhijani A. 2001. *Plutonium End-Game: Managing Global Stocks of Seperated Weapons-Usable Commercial and Surplus Nuclear Weapons Plutonium*, Institute for Energy and Environmental Research, 2001

163. Dilger F, Halstead R. 2003. The Next Species of Trouble: Spent Nuclear Fuel Transportation in the United States, 2010-2048. *American Behavioral Scientist* 46: 796-811

164. Garwin RL, Charpak G. 2001. *Megawatts and Megatons*. Chicago: University of Chicago Press. 412 pp.

165. Tierney K. *Strength of a City: A Disaster Research Perspective on the World Trade Cdener Attack*, Social Science Research Center

166. Fischhoff B, Gonzalez RM, Small DA, Lerner JS. 2003. Evaluating the Success of Terror Risk Communication. *Biosecurity and Bioterrorism* forthcoming

167. Adibi MM, ed. 2000. *Power System Restoration: Methodologies and Implementation Strategies*. New York: IEEE Press. 690 pp.

168. Asmus P. 2001. The War Against Terrorism Helps Build the Case for Distributed Renewables. *The Electricity Journal* 14: 75-80

169. Dunn S. 2002. Micropower: New Variable in the Energy-Environment-Security Equation. *Bulletin of Science, Technology and Society* 22: 72-86

170. Jacobson MZ, Masters GM. 2001. Exploiting Wind Versus Coal. *Science* 293: 1438-

171. Staunton RH, Kueck JD, Kirby BJ, Eto J. 2001. Demand response: An overview of enabling technologies. *Public Utilities Fortnightly* 139: 32-9

172. Hirst E, Faruqui A. 2002. Demand response: How to reach the other side. In *Electric Perspectives*, pp. 16-33

173. DeCarolis JF, Keith DW. 2001. Letter: The Real Cost of Wind Energy. *Science* 294: 1000-3