

Cyberthreats: A Major Driver for Distributed Generation

Joel N. Gordes
Environmental Energy Solutions
P.O. Box 101
Riverton, CT 06065 USA
jgordes@earthlink.net
Revised November 2004

Abstract

While there have long been those very few (e.g. Lovins & Lovins) who have pointed out the vulnerability of the grid to physical attack, they had been largely ignored until the event of 9/11/01. That showed that the critical infrastructure of the nation was potentially at greater risk from terrorism than had been previously imagined.

Unfortunately, most of the response to the threat has been limited to the physical infrastructure considerations and while 9/11 was supposed to lead to “new ways of thinking,” it has been difficult to discern where this has evidenced itself in practice thus far. Few planners in business and industry have been made aware that damage to the grid can also be inflicted via various forms of cyber attacks that can take both physical and non-physical forms.

There are ways to fortify the electric infrastructure and build societal resiliency if new paradigms are adopted that would substitute distributed generation for transmission projects.

Introduction

With the introduction of new technology comes many advantages but what is frequently overlooked are the disadvantages that may make society more vulnerable to situations where threats were previously not a concern. Nowhere is this more evident than with the change to a digital economy that, while providing the ability to greatly increase productivity, may concurrently exposes society to unacceptable risks unless precautions are taken to decrease new vulnerabilities.

The most familiar risks include computer viruses, worms and hacking that have resulted in denial of service attacks that can force a company to curtail the electronic portion of its business; a sector that is

growing rapidly. In one case there is an unsubstantiated report that a Fortune 500 company was the victim of a more serious attack: “The computer network of a Fortune 100 company was obliterated last week by a new virus that one official called ‘the first legitimate incident of cyberterrorism’ he had ever seen. Although Hodges declined to name the attacked company, he said 10 sites and several thousand servers and workstations had been infected...’These guys were very smart,’ Hodges said. ‘They had a good enough idea of where to put it in order to make it spread very quickly.’” [1] However, use of information warfare (now popularly called cyberwar or cyberterrorism) in one of its many other forms can also have much broader implications if one or more aspects the critical infrastructure itself is the actual target; in this case, the electric grid.

This paper will attempt to capsulize and mainstream the work begun by some in the military as well as a few private sector individuals and then build upon it to provide solutions using new distributed resource technologies

Historic Reference

It has long been held in military circles that, “we always prepare for the last war”. Indeed, the major lesson of Pearl Harbor was not “be prepared” as most popularly assume but to understand the changes in the nature of war. Historically, even the attack at Pearl Harbor was no surprise.

As early as October 1924 General Billy Mitchell prophesized, “...I am convinced that the growing airpower of Japan will be the decisive element in the mastery of the Pacific... Air operations for the destruction of Pearl Harbor will be undertaken... The attack to be made on Ford Island at 7:30 a.m... The Philippines would be attacked in a similar

manner...The initial successes would probably be with the Japanese.” [2]

He re-enforced this in April 1926 when he said, ““A surprise aerial attack on Pearl Harbor will take place while Japanese negotiators talk peace with the U.S. officials, moreover the attack will come on a Sunday Morning.” [3]

The Nature Of The Threat

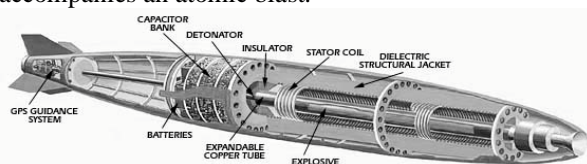
The 9/11 attack on the World Trade Center was no surprise either although it was a shock. That the same structure had been attacked once before with the plan to topple one tower into the other should have taken any "surprise" out of the equation but we failed to listen to the terrorists themselves. Still, we apparently have not learned the lesson of Pearl Harbor as we make elaborate and expensive preparations for past scenarios that may be the entirely wrong response as opposed to even newer forms of warfare that are just emerging. Unfortunately, some of our fellow countrymen will be accomplices to it; not out of evil but out of an inability to fathom the nature of change.

One example of the new threat is called cyberwar or cyberterrorism and outside of military circles and a few other corporate strategists, it has mostly been ignored by business, industry and the news media. While it may not seem as dramatic as flying an airliner into the World Trade Center, it has the potential to bring about far greater damage including massive loss of life.

Definitions of Cyberthreats

In one form it involves the use of computer hacking to take down portions of the critical infrastructure from anywhere in the world. This means the loss of electric service, natural gas, pipelines, communications and even certain aspects of transportation.

In another more physical form it could incapacitate any appliance, generator, auto or other device that has incorporated computer chips. This takes place when a relatively inexpensive device called a flux compression generator (see Fig. 1) [4] is used to induce an electromagnetic pulse similar to what accompanies an atomic blast.



An early warning of our vulnerability in a computer-dominated society actually took place in Hartford, Connecticut when a crow took out all electric service to the downtown business district. According to a 2/20/1983 Courant account, Travelers Insurance was forced to go into an emergency data recovery exercise that had not been used in recent memory. Peter Libassi, a Senior VP there, noted then that:

"Sometimes you have to wonder just how advanced technology is when something like this can cause these problems with this kind of equipment...Potentially this could have cost the company a lot of money." [5]

Since 1983 dependence on computers has proliferated to extraordinary proportions into all aspects of life from control of the electric grid to the operation of each and every automobile making Libassi a prophet on par with the aforementioned Gen. Billy Mitchell. Unfortunately few pondered his wisdom or other lonely voices who have sounded similar warnings. Among them:

Noted cyberwar expert Winn Schwartau has warned that, "Modern societies are composed of four critical highly interrelated, and symbiotic infrastructures upon which their national and personal survival depends: The power grid is the foundation of it all." [6] Richard Clarke, former White House advisor on cyberwar has commented: "The owners and operators of electric power grids, banks and railroads; they're the ones who have to defend our infrastructure. The government doesn't own it, the government doesn't operate it, the government can't defend it.the military can't save us." [7]

Admiral Herbert Brown, Deputy Commander of U.S. Space Command charged with response to cyberwar stated in a 4/9/00 "60 Minutes" interview that "virtually any country that has a computer has an opportunity to enter into cyberspace and be disruptive...[The ability to bring down a power grid] is absolutely real." [8]

The message is the same from Bush National Security Advisor Condoleeza Rice who said:

"It is a paradox of our times: the very technology that makes our economy so dynamic and our military forces so dominating--also make us more vulnerable...And everyday it is driven home to us that the threat is not just theoretical....Protecting our nation's critical infrastructure can only be done in concert with private industry." [9]

Fellow appointee Secretary of Defense Rumsfeld has also asked to shift priority to defending against cyberattack. Even more direct has been Assistant

Fig. 1: A \$400 flux compression generator bomb.

Secretary of Energy for Energy Efficiency and Renewable Energy David Garman who noted:

Aside from its obvious environmental benefits, solar and other distributed energy resources can enhance our energy security. Distributed generation at many locations around the grid increases power reliability and quality while reducing the strain on the electricity transmission system. It also makes our electricity infrastructure less vulnerable to terrorist attack, both by distributing the generation and diversifying the generation fuels. So if you're engaged in this effort, it is my view that you are also engaged in our national effort to fight terrorism. [10]

Lest there be any doubt that it can really happen, it has actually been attempted with a confirmed attack on the California Independent System Operator (CAL ISO) in late April 2001 in the midst of their energy problems that highlighted the potential problems that will be addressed. It was reported....

For at least 17 days at the height of the energy crisis, hackers mounted an attack on a computer system that is integral to the movement of electricity throughout California, a confidential report obtained by the Los Angeles Times shows....The hackers' success, although apparently limited, brought to light lapses in computer security at the target of the cyber-attack, the California Independent System Operator, which oversees most of the state's massive electricity transmission grid. [11]

While unsuccessful in that attempt, it would be unrealistic to believe that over time nation states, terrorist groups or empowered individuals will not succeed at some future point. They may have the ability to produce economic dislocation either on a broad geographic scale or concentrated in critical areas such as where major power lines and gas pipelines intersect. With most new generation employing natural gas this becomes particularly significant.

The Distributed Resources/Distributed Generation Solution(s)

As with so many terms, the words "distributed resources" and distributed generation (DG or DR) [12] have distinctive meanings to different groups depending upon their market position, familiarity with the technologies, biases and even fears. Unfortunately, in certain Northeast jurisdictions, some opponents of decentralized power systems have sought to purposely denigrate the potential contributions of DR/DG by defining it in terms that marginalize its value in front of regulators and legislators. This necessitates researching the many varied meanings and providing what may hopefully be a consensus definition that is accepted by the

broadest possible audience. Definitions found attributable to reputable groups include:

US DOE I

Distributed power is modular electric generation or storage located near the point of use. Distributed systems include biomass-based generators, combustion turbines, concentrating solar power and photovoltaic systems, fuel cells, wind turbines, microturbines, engines/generator sets, and storage and control technologies. Distributed resources can either be grid connected or operate independently of the grid. Those connected to the grid are typically interfaced at the distribution system. In contrast to large, central-station power plants, distributed power systems typically range from less than a kilowatt (kW) to tens of megawatts (MW) in size.

<http://www.eren.doe.gov/distributedpower/su/blvl.asp?item=definition>

US DOE II

"Distributed energy resources (DER) refers to a variety of small, modular power-generating technologies... DER systems range in size and capacity from a few kilowatts up to 50 MW. They comprise a portfolio of technologies, both supply-side and demand-side, that can be located at or near the location where the energy is used."

<http://www.eere.energy.gov/der/basics.html>

Electric Power Research Institute (EPRI) I

Integrating distributed energy resources. The new system would also be able to seamlessly integrate an array of locally installed, distributed power generation (such as fuel cells and renewables) as power system assets. Distributed power sources under 20 MW per unit could be deployed on both the supply and consumer side of the energy/information portal as essential assets dispatching reliability, capacity and efficiency. Today's distribution system, architecture, and mechanical control limitations, prohibit, in effect, this enhanced system functionality. (Electricity Sector Framework For The Future, Volume I. Achieving The 21st Century Transformation, Aug. 6, 2003. p. 29.) Full study at:

<http://www.epri.com/journal/details.asp?doctype=features&id=671>

EPRI II

"Distributed resources are small generation (1 kW to 50MW) and/or energy storage devices typically sited near customer loads or distribution and sub-transmission substations."
<http://www.epri.com/targetDesc.asp?program=262184&value=03T101.0&objid=287595>

American Gas Association

Distributed generation (DG) is the strategic placement of small power generating units (5 kW to 25 MW) at or near customer loads. Situated at a customer's site, distributed generation can be used to manage energy service needs or help meet increasingly rigorous requirements for power quality and reliability. Located at utility sites such as substations, distributed generation can provide transmission and distribution (T&D) grid support and expand the utility's ability to deliver power to customers in constrained areas. Distributed generation technologies include such resources as industrial gas turbines, reciprocating engines, fuel cells, microturbines, wind-power, and photovoltaics.
http://www.aga.org/Content/ContentGroups/Newsroom/Issue_Focus/Distributed_Generation.htm

California Energy Commission

"Distributed energy resources are small-scale power generation technologies (typically in the range of 3 to 10,000 kW) located close to where electricity is used (e.g., a home or business) to provide an alternative to or an enhancement of the traditional electric power system."
<http://www.energy.ca.gov/distgen/index.html>

Toward a Consensus Definition of DR/DG

Taking the common attributes of the preceding definitions, a consensus definition might be:

Distributed resources include conservation and load management with modular electric generation and/or storage located near the point of use either on the demand or supply side. DR includes fuel-diverse fossil and renewable energy generation and can either be grid-connected or operate independently. Distributed resources typically range from under a kilowatt up to 50 MW. In conjunction with traditional grid power, DR is capable of high reliability (99.9999%) and high power quality required by a digital society.

Point of Conflict

Wind energy presents a very special case in regard to distributed generation that makes it difficult to categorize. While individual turbines clearly fall within the generally agreed upon size parameters, a wind farm may lie outside the uppermost limit. For instance, is a 300 MW wind farm distributed generation? While it is a renewable source, exceeding the 50 MW upper limit may throw it out of the category. In addition, even if it is below 50 MW, if it is on a contiguous wind farm, it may not be adequately decentralized. Finally, because it may be located in a remote area far from the loads that it will serve, it requires vulnerable and costly transmission. On the other hand, a small wind installation whose loads have the ability to be used locally may satisfy all parameters to be considered DG.

How DG Makes the Grid More Resilient

There are at least three major ways in which DG can lead to reduced grid vulnerability.

1) By physically dispersing the location of small, modular generators mostly on the customer side of the meter provides physical resiliency. It also allows for some continued operation, perhaps within what is termed an "adaptive" or "micro-grid," if the overall transmission system has been disrupted either physically or by cyberattack. The Electric Power Research Institute (EPRI) concurs when they state:

Adaptive islanding. Following a terrorist attack or major grid disruption from natural causes, initial reaction will focus on creating self-sufficient islands in the power grid, adapted to make best use of the network resources still available. To achieve this aim, new methods of intelligent screening and pattern extraction will be needed, which could rapidly identify the consequences of various island reconnections. Adaptive load forecasting will also be used to dispatch distributed resources and other resources in anticipation of section reconnection and to help stabilize the overall transmission-distribution system. [13]

2) By locating the distributed sources closer to the place of use, it minimizes the importance of transmission which is the major point of vulnerability. This is confirmed by James Castle, manager of operations at ISO-NY who said:

"...the system was usually operated by running the cleanest and least expensive generating stations. But the system could be less vulnerable if plants close to the high demand cities were started up, to minimize the importance of transmission lines." [14]

Distributed generation takes it a another step further and adds significant generation that is not only redundant but dispersed; both required for survivability.

3)By diversifying the mix of fuels/technologies used by the distributed units there is safety from disruption of any one fuel source. Natural gas which is gaining in use has the potential to become a fuel “monoculture” in many locations. Merely incapacitating a pipeline compressor at a critical location could disrupt the flow of gas to large areas. Even without terrorist actions, during the past winter in the Northeast, there were warnings of rolling blackouts issued. These were followed by charges that gas was diverted from electricity production to heating uses since it may have been more profitable not to generate electricity. This brings up serious issues of public safety that a growing gas monoculture will only exacerbate.

Centralization Versus Decentralization

Distributed resources, alone, do not offer resiliency unless they are also within a decentralized framework. “Centralized” and “decentralized” are two additional terms that are too loosely used and lead to much confusion.

Lovins and Lovins define centralization in terms of its weaknesses (in terms of physical vulnerability but applicable to cyberthreats as well) [15]:

Today's predominantly centralized energy systems:

- consist of relatively few but large units of supply and distribution;
- are composed of large, monolithic components rather than of redundant smaller modules that can back each other up;
- cluster units geographically, for example near oilfields, coal mines, sources of cooling water, or demand centers;
- interconnect the units rather sparsely, with heavy dependence on a few critical links and nodes;
- knit the interconnected units into a synchronous system in such a way that it is difficult for a section to continue to operate if it becomes isolated, so failures tend to be system-wide;
- Provide relatively little storage to buffer successive stages of energy conversion and distribution from each other, so that failures tend to be abrupt rather than gradual;

- Locate supply units remotely from users so that the links must be long;
- Tend to lack the qualities of user-controllability, comprehensibility, and user independence. These qualities are important to social compatibility, rapid reproducibility, maintainability, and other social properties...important...to resilience.

A well-designed decentralized system addresses each of these weaknesses and builds an adaptive grid able to compensate for each of them.

An Additional Point of Conflict

Another point of conflict comes with the drive for large new transmission lines. Proponents claim they will lead to more robust energy delivery to avoid episodes like the August 14, 2003 Blackout as well as provide enhanced energy security. There are multiple flaws in this claim:

1)Adding redundancy [additional lines] if it is still within a centralized system will not improve resiliency. The National Academies report cautions:

A direct way to address vulnerable transmission bottlenecks and make the grid more robust is to build additional transmission capacity, but there are indications that redundancy has a dark side (in addition to increased costs). The likelihood of hidden failures in any large-scale system increases as the number of components increases. Modeling techniques are only now emerging for the analysis of such hidden failures. [16]

In addition, it can actually work to the detriment of DG which is best used on-site running with the grid as a backup for reliability and power quality attributes rather than transporting it over any large distances. As such, DG does not benefit from construction of such lines.

2) If significant amounts of funding are placed into transmission upgrades as currently planned, that funding is no longer available for competing technologies such as DG. DG could be implemented more economically by utilities who could provide some incentives for private sector facilities to use DG much as they do now with existing C&LM programs.

3)Because transmission lines are such a large investment into long-term infrastructure, it locks society into a future where newer, more resilient technologies may be disadvantaged. Continuing the payment for that infrastructure also provides

the justification to create arguments to keep new, competing technologies out. To put the large transmission line build-out first means there may not be discretionary funding for the other vital portions of a truly adaptive grid. A recent EPRI study appears to recognize what some utilities do not or articulate in any meaningful way:

A portfolio of innovative technologies, such as those described in this report, can comprehensively resolve the vulnerability of today's power supply system in terms of its capacity, reliability, security and consumer service value. These "smart technologies" will also open the door to fully integrating distributed resources and central station power into a single network, in a manner than can reduce system vulnerability rather than add to it—as is typically the case today—while also steadily improving the efficiency and environmental performance of the system. [17]

Figure 2. The Bionic Shoe



As a technological aside, it is instructive that within the last few months there has been an announcement of a running shoe (Figure 2) that has electronic sensory elements within it allowing it to make 20,000 readings per second. This allows it to correct the shoe's shape to the runners foot depending upon exact conditions at any given time. That our society has seen the use of this technology in a "bionic" running shoe before application to our vital electric infrastructure raises certain questions about which EPRI report cited above has said:

Lack of technical innovation strongly reflects the state of uncertainty in the electricity sector. Technology decisions are largely driven by the management of existing assets, with particular focus on reducing cost and reducing/hedging risk. Capital expenditures as a percent of revenue are at an all-time low, and operating and maintenance budgets remain extremely tight at most utilities. There is little incentive for introducing new technology when the recovery of investment is so uncertain. [18]

Unfortunately we are not seeing strategies actively put forward in transmission plans that systematically provide a blueprint for this "portfolio of innovative technologies" but, rather, only the single solution of large new lines that appears to pay no heed to energy security considerations.

Lessons Of The 2003 Blackout

Efforts that reconstructed the events of the days and minutes prior to and at the blackout by the U.S.-

Canada Joint Taskforce have determined the following four principle causes and one corollary conclusion in their final report:

- FirstEnergy (FE) and ECAR failed to assess and understand the inadequacies of FE's system. This was particularly the case with respect to voltage instability and the vulnerability of the Cleveland-Akron area, and FE did not operate its system with appropriate voltage criteria and remedial measures.
- Inadequate situational awareness at FirstEnergy. FE did not recognize or understand the deteriorating condition of its system.
- FE failed to adequately manage tree growth in its transmission rights-of-way.
- Failure of the interconnected grid's reliability organizations to provide effective real-time diagnostic support.
- Failures to act by FirstEnergy or others to solve the growing problem, due to the other causes. [19]

As detailed as the report is, in a certain technical sense, it has not adequately addressed certain specific conditions widely reported in the press at the time of the event. One involved the loss of "situational awareness" (Cause #2 by the Task Force) when an engineer at the Midwest grid organization asked engineers at FE to explain why they had not responded to a line outage reported sometime earlier. According to one account:

"We have no clue. Our computer is giving us fits, too," replied a FirstEnergy technician identified as Jerry Snickey. "We don't even know the status of some of the stuff (power fluctuations) around us."

A short time later, a technician at the Midwest Independent Transmission System Operators, the group that monitors the Midwest power grid, expressed frustration with FirstEnergy's failure to diagnose the problems erupting in their power system.

"I called you guys like 10 minutes ago, and I thought you were figuring out what was gong on there," the MISO technician, identified as Don Hunter, complained, according to the transcripts.

"Well, we're trying to," replied Snickey. "Our computer is not happy. It's not cooperating either." [20]

While the final US-Canada report did acknowledge that the Blaster worm had first appeared three days

prior to the event (a point not made in the draft report) they summarily concluded:

This NCS analysis supports the SWG's [Security Working Group] finding that viruses and worms prevalent across the Internet at the time of the outage did not have any significant impact on power generation and delivery systems. [21]

It appears strange that a report on an outage of this magnitude for which an enumerated cause is "situational awareness" did not provide greater detail on this specific reference to the nature of the computer problems. However, there has been reassurance that the Blaster worm was not a causative factor or related. [22] Still, this does not preclude future actions by cyberterrorists learning from such an event to employ such methods. If all remedies suggested in the report are applied but massive failures continue due to such attacks, the perceived risk to the centralized electric system as structured may lead to a loss of faith in the utility sector as well as lack of confidence in the government to protect the nation's ability to protect critical infrastructure.

Regardless of the causes of this particular incident, some experts believe additional underlying endemic conditions must be solved before any resiliency is ensured.

Show Me the Money

When Willie Sutton, the notorious bank robber, was caught, the authorities questioned him and one of the questions was, "Willie, why do you rob banks?" The not too bright but quite literal Sutton is said to have replied, "That's where they keep the money." [23] The same advice should be taken from the National Academies report when they say:

Today there is a growing interest in distributed generation—generators of more modest size in close proximity to load centers. This trend may lead to a more flexible grid in which islanding to maintain key loads is easier to achieve. Improved security from distributed generation should be credited when planning the future of the grid....Recovery of the invested funds through rate mechanisms or in some part through homeland security funding must be examined. [24]

Energy security is a homeland security issue as energy is one of the two primary critical infrastructures upon which all others are dependent (telecom being the other)--and they have the money. While it is unclear whether EPRI is literal in its meaning of "incentive" as used below, they generally seem to share this opinion with the National Academies:

Protecting the nation's power infrastructure has a strong public-good dimension, and a robust federal "homeland security" incentive will be needed from the outset. Investments made for such essential infrastructure security must be immediately and fully recoverable. [25]

But this funding is far from adequate as an even more recent study by the Council on Foreign Relations on lack of funding for emergency responders makes clear. Former Senator and security expert Warren Rudman is Chair and cybersecurity expert Richard Clarke, cited earlier, is Senior Advisor. That report states:

Estimated combined federal, state, and local expenditures therefore would need to be as much as tripled over the next five years to address this unmet need. Covering this funding shortfall using federal funds alone would require a five-fold increase from the current level of \$5.4 billion per year to an annual federal expenditure of \$25.1 billion. [26]

Any forward looking homeland security strategy (and renewable energy deployment strategy) would seek to use some of these funds for distributed resources, for these first responders and to maintain power to other critical services such as hospitals, communications and transportation. If co-located in areas of high electric congestion, they would concurrently serve two important yet unrelated purposes.

Conclusions

- Terms such as "distributed resources" and "centralization" are poorly understood by proponents and adversaries of distributed resources as well as utility and ISO personnel and regulators. A common definition must be agreed upon.
- Mere redundancy, such as new transmission lines, if still within a centralized system, offers little resiliency and may merely offer additional points of failure.
- Building resiliency into the grid must encompass multiple actions taking place on a coordinated basis and include conservation and load management, distributed resources, adaptive grid deployment and transmission upgrades. There is no one silver bullet, only silver buckshot. [27]
- The trend toward purely grid-tied renewable energy systems (such as PV) without storage capacity, while moving the industry closer to price targets, sacrifices the "value proposition" that some storage provides. It also violates one of Lovins & Lovins' cautions to buffer against abrupt failures with storage. State and utility program designers should consider allowing

systems with battery storage and providing a partial incentive to consumers who choose this option.

- DG success stories prove the worth of these technologies when even small amounts of power become critical and provide viable models that can be replicated.
- The Department of Homeland Security, in conjunction with state programs, should provide partial funding for DR systems that add to energy security and enhance the ability of first responders to operate when the grid is down.

A Plan

There are ways in which the infrastructure can be fortified to provide resiliency to the electric grid but this can only occur if all involved begin to think in new paradigms. The energy sector is at a crossroads in this respect and the following plan is suggested:

Large new, expensive transmission tower plans by utilities across the nation to alleviate power congestion further centralize energy and may make the country vulnerable to cyber and physical attacks when there are alternatives that can mitigate much of this problem. Transmission upgrade plans should be re-examined from a national security perspective before they are cast in stone since they can set the standard for a generation and lock in older technologies as some utility monopolies have in the past. This may mean bringing in new players who are not constrained by traditional regulatory and/or utility thought patterns or profit motivations.

Use of load management and small, fuel diverse generators that are more widely distributed have the potential to provide a more robust system that is less vulnerable to physical and cyber attacks and should be considered as alternatives.

Since these distributed generators are most often paid for, at least in part, and placed on customer premises to insure power reliability and quality, the societal cost may be less since facility owners will pay for a large share rather than ratepayers footing the entire bill.

Because most distributed generation units are extremely clean and small, this option for congestion alleviation may be quicker to implement due to less need for environmental and other regulatory oversight being required. In the case of certain fuel cells, both Massachusetts and California have blanket environmental emissions approval.

Utilities should be allowed to ratebase any incentives payments to drive the private sector toward distributed technologies up to 25 megawatts in size. There should even be consideration of allowing them to build and own such facilities in a step backwards from deregulation to provide them incentive not to oppose alternatives that are in the best interest of the nation. This would take a page from the Netherlands that allows utilities to build combined heat and power facilities in that nation and has resulted in 40% of the nation's power being supplied in that manner.

Unfortunately many high level utility executives are rushing to promote these vulnerable large new transmission lines and federal, regional and state agencies appear anxious to endorse this as the approved solution. They, like the "best and brightest" military minds on December 7, 1941 are guilty of cultural lag. They are still thinking in terms of a world prior to 9/11/01 rather than a world in which we must reduce our vulnerabilities or continue to suffer the consequences of still not having learned the real lessons of Pearl Harbor.

References

- (1) Personal correspondence via Nancy Pitblado on 12/23/98 from Network Associates.
- (2) American Airpower Heritage Museum. <http://www.avdigest.com/aahm/trquotes.html>
- (3) Op. Cit.
- (4) Stertz, B. "Crow Short-Circuits Phone, Power," *The Hartford Courant*. 2/20/1983.
- (5) Wilson, J. "E- Bomb," *Popular Mechanics*. 9/2001. pp. 50-53.
- (6) Schwartau, W. Information Warfare, "Electronic Civil Defense," Thunder's Mouth Press, New York, 1996. p. 43.
- (7) Steve Croft. "60 Minutes," segment on "Cyber War." 4/9/2000.
- (8) Op. Cit. "60 Minutes," 4/9/2000.
- (9) "Understanding Risk and U.S. Economic Security" Remarks by Condoleezza Rice at Partnership For Critical Infrastructure Annual Meeting . 3/22/2001.

[10] Garman, D. Speech at UPEX'01 Conference. Sacramento, CA. 10/02/2001.

(11) Morain, D. "Hackers Mounted Attack on Power System, Report Says," *San Jose Mercury News*. 6/10/2001.

[12] The term distributed resources includes distributed generation and demand side management. With that understanding, the terms will be used interchangeably in this paper.

[13] Electricity Sector Framework For The Future, Volume I, Achieving A 21st Century Transformation. Electric Power Research Institute. August 6, 2003. p. 31.

[14] Matthew L. Wald, "Electric Power System is Called Vulnerable, and Vigilance is Sought," *New York Times*. 2/28/02.

[15] Lovins, Amory B. and Lovins, L. Hunter, *Brittle Power, Energy Strategy for National Security*, Brick House Publishing Co. (Andover, MA) 1982. p. 218.

[16] *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academy Press. Committee on Science and Technology for Countering Terrorism, National Research Council. p.302.

[17] *Electricity Sector Framework for The Future*, Volume I, Achieving A 21st Century Transformation. Electric Power Research Institute. August 6, 2003. p 4.

[18] *Electricity Sector Framework for The Future*, Volume I, Achieving A 21st Century Transformation. Electric Power Research Institute. August 6, 2003. p 18.

[19] "U.S.-Canada Power System Outage Task Force: August 14th Blackout Causes and Recommendations," Final report, (April 2004). pp. 18-20.

[20] H. Josef Hebert, Associated Press. *Calls Show Pre-Blackout Utility Confusion*. September 3, 2003.

[21] U.S.-Canada Power System Outage Task Force: August 14th Blackout Causes and Recommendations," Final report p. 133

[22] Discussion with Alison Silverstein, former member of the FERC staff and staff to the Blackout Commission on 10/7/04.

[23]) Related by Dr. William Flynt at the ICATHS Conference at UCONN on September 25, 2003.

[24] *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academy Press, Committee on Science and Technology for Countering Terrorism, National Research Council. p.192. 2002.

[25] *Electricity Sector Framework for The Future*, Volume I, Achieving A 21st Century Transformation. Electric Power Research Institute. August 6, 2003. p. 7.

[26] *Emergency Responders: Drastically Underfunded, Dangerously Unprepared*. Report of an Independent Task Force Sponsored by the Council on Foreign Relations. July 2003.

[27] Attributable to Dr. Carl Weinberg, former Manager of R&D at PG&E.