RATING THE STATES FOR ENERGY SECURITY

Joel N. Gordes
Environmental Energy Solutions
PO Box 101
Riverton, CT 06065
Jgordes@earthlink.net

Susan M. Gouchoe
Policy Program Manager
NC Solar Center at NCSU
Campus Box 7401
Raleigh, NC 27695-7401
susan_gouchoe@ncsu.edu

Stephen S. Kalland
Associate Director
NC Solar Center at NCSU
Campus Box 7401
Raleigh, NC 27695-7401
steve_kalland@ncsu.edu

ABSTRACT

Since the attack on Sept. 11th, 2001 there has been a heightened awareness of the need to protect critical infrastructure previously thought to be secure from attack.

While 9/11 was "supposed to change the way we all think," in the energy realm there is little evidence of this. In fact, the "business as usual" scenario toward greater centralization through FERC-endorsed Independent Transmission Providers (ITPs, formerly known as Regional Transmission Organizations or RTOs) moves forward with many built-in vulnerabilities going virtually unnoticed.

This paper will address some of the vulnerabilities that are built into centralized energy systems with poor fuel diversity and discuss how utilization of renewable and distributed energy technologies can help rectify these problems.

A key aspect of this research will be to construct a checklist or profile that will provide a snapshot of both how vulnerable each state might be to both physical and cyberattacks against their critical energy infrastructure and what policies are in place to promote the use of renewable and distributed energy resources. . The study will make use of information that, for large part, is readily available but never before aggregated to arrive at an index for such a comparison and, hopefully, as a guide for corrective action. The paper will conclude by providing an actual ratings/profile for one state.

1. THE NATURE OF VULNERABILITY

Partly due to a false sense of security it has never been ingrained in the design or operation of our energy systems that energy security must become a primary consideration.

Indeed, in current literature numerous high level officials and strategists repeatedly cite energy systems as the target of choice to incapacitate the economic viability of the nation by rendering all other infrastructure dependent upon energy unusable. In the words of Winn Schwartau, a noted expert on information warfare:

> 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. We run it all on electricity, no matter how it is generated, and distribute it over a huge web of overhead wires and underground cables...[1]

The vast majority of Americans still believe that the task of defense is purely a military function rather than one that could involve each and every one of them. Unfortunately, military responsibility alone is no longer the case.

> 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. This is the first time where we have a potential foreign threat to the United States where the military can't save us. [2]

1.1 Physical Infrastructure Vulnerabilities

In presenting to power officials at a February 2002 symposium, Lt. Col. Bill Flynt, director of the Threats to Critical Infrastructures program at the Foreign Military Studies office of the US Army cautioned:

> In a single-superpower world, there's a single best target…You're the best face of that best target…Your corporations [power companies] are the best target set.[3]

The targets can be both physical in nature, i.e., generating plants as well as their ancillary and support structures such as fuel storage, as well as cyber, wherein computers and information systems become both the weapons and the target.

A particularly inviting set of targets is the spent fuel pools used for the storage of used fuel rods from nuclear plants. While never meant to be stored indefinitely on-site, they have become virtually permanent fixtures and are usually not hardened sites capable of withstanding bombs or other forms of ordinance.

Another tempting target is the web of transmission facilities that links the limited number of generators together in a delicate synchronous network used to transport the power over longer distances. Because there are a growing number of areas that are transmission constrained, there is the tendency to construct additional lines that traditional utility planners also believe bring greater resilience. A recent National Academies study takes issue with this in saying:

> 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.[4]

Redundancy, alone, within a centralized system may provide little solution and may, in fact, lead to more frequent and wide-spread losses. This can occur by increasing the complexity of the grid wherein the failure of a single component could lead to a cascading failure of the system.

Substations that feature a number of transformers are also vulnerable due to the difficulties in defending them from physical or electronic attack. Many of these transformers are custom made and, according to the National Academies report, might take a number of months for replacements to become available. Unless power could be re-routed during that period, certain areas would not enjoy full service.

As the electric grid has become more centralized, computerized and sophisticated, it has become standard for Independent Systems Operators (ISOs) to centrally control large regions of the country in dispatching electricity from the plants within their territory. This is most often done on economic grounds where the least expensive plants are brought on line first. These ISOs' command, control, communications and computer control (C^4) functions provide many advantages including: reduced need for personnel; greater speed in dispatching or throttling back plants; increased information on grid operations. What is sacrificed is survivability that is only partially offset by redundancy of satellite centers capable of assuming control if the primary is disabled. It might not be difficult for a small group of determined terrorists to disrupt all of these facilities concurrently either via physical or electronic means.

In recent years the Federal Energy Regulatory Commission (FERC) has encouraged the formation of Independent Transmission Provider (ITP, formerly called a Regional Transmission Organization or RTO) that would be responsible for the transmission assets of several ISOs. One reason for instituting ITPs is to prevent market abuse that has taken place; notably in California. What has not been generally perceived is that the formation of ITPs can further centralize the system by shifting greater command and control from local entities (ISOs) to those located farther from the actual generation sources. This has the potential to further the distance the physical assets from the decision making powers who may or may not have adequate information available on which to make timely decisions on grid conditions and required actions. In response to a question on this, FERC Commissioner Nora Meade Brownell did not connect the creation of ITPs with greater vulnerability.[5] From limited preliminary work, this appears consistent with opinions from others in traditional utility and regulatory roles.

1.2 Cyber Vulnerabilities

Less known but potentially as costly in terms of lost economic activity would be acts of cyberterror, cyberwar or information warfare (IW) carried out by use of computers or attacking embedded semiconductors. In the words of cyberwar expert Winn Schwartau:

> IW can attack individuals, organizations, or nation states (or spheres of influence) through a wide variety of techniques:
>
> - Confidentiality compromise
> - Integrity attacks
> - Denial of service
> - Psyops
> - Dis/Misinformation, media, etc.
>
> Most clearly, though, the distinctive feature of pure IW is that it can be so easily waged against a civilian infrastructure in contrast to a military one. This is a new facet of war, where the target may well be the economic national security of an adversary.[6]

1.2.1 SCADA as a Target

Specifically, in one form, cyberwar involves the use of computer hacking (codes, viruses, Trojan Horses, dis/misinformation) to incapacitate portions of the critical infrastructure from anywhere in the world. This means the potential loss of electric service, natural gas and other pipelines, communications as well as transportation systems. One method by which to accomplish this is to use the Supervisory Control and Data Acquisition System (SCADA) or Distributed Control Systems (DCS) as an entry point into the utility control system. Many of these systems use standard commercially available software with known weaknesses that are connected to the internet. This leaves them open to intrusion and, in cases where the intruder may have been a former employee, particularly prone to tampering. In one well-reported incident, a former employee was able to release raw sewage into drinking water supplies after multiple attempts before being apprehended.[7] Had this been a power-connected attack, there would have been the potential for even greater harm.

In another instance, an April 2001 attack against the California ISO went undetected for 17 days and while it did not cause harm to the grid it was an indicator of weaknesses in the system.[8]

1.2.2 Flux Compression Generators: The “E-Bomb”

Another more physical form of IW is the so-called E-bomb that can incapacitate any appliance, generator, auto or other device that has incorporated solid state semiconductors. This takes place when a relatively inexpensive device (~$400) called a flux compression generator is used to induce an electromagnetic pulse (EMP) similar to that which accompanies a nuclear blast.[9] This is a not a hi-tech device to build nor does it require a sophisticated aerial delivery system since the device could take on various shapes and be delivered via any vehicle from a light aircraft to a UPS truck. Its effective area is limited by such variables as size, altitude of detonation, distance from critical electronics and nature of shielding materials if any. An ideal target for such a weapon would be the control center(s) for an ISO or an ITP/RTO inasmuch as destroying their command, control, communications and computers would render it difficult to impossible to carry out dispatch of generation units in an orderly manner and/or maintain synchronicity of the grid.

Unless the electronics in question are protected against such a weapon by being placed in what is termed a “Faraday cage,”[10] they become useless and you are effectively “back to the stone age” in terms of the operability of electronic equipment. Cost makes this defensive option highly unlikely.

2. DEVELOPING A DEFENSIVE STRATEGY

2.1 Centralization Vs. Decentralization

Key to developing a defensive strategy is discerning the difference between centralized and decentralized systems. Centralized systems, by their very nature, are more susceptible to interruption and failure than are decentralized systems. This is because a single point of failure in a centralized system has an increased potential to take down the entire grid.

All too often discussion of these systems employ fuzzy, undefined terms that mean very different things to different people. Without basic definitions, it become difficult if not impossible for strategic planners to communicate with each other as well as policy makers, utilities and others involved in grid design and operation. To that end, the following definitions are provided to articulate a beginning common ground. Lovins and Lovins define the weaknesses of centralized systems as being characterized by:

- relatively few but large units of supply and distribution;
- units made of large, monolithic components rather than redundant smaller modules;
- geographically clustered units, for example near oilfields, coal mines, sources of cooling water, or demand centers;
- sparsely interconnected units , with heavy dependence on a few critical links and notes;
- interconnected units knitted into a synchronous system in such a way that it is difficult for a section to continue to operate if it becomes isolated -- that is, since each units operation depends significantly on the synchronous operation of other units, failures tend to be system-wide;
- relatively little storage to buffer successive stages of energy conversion and distribution from each other, so that failures tend to be a abrupt rather than gradual;
- supply units located remotely from users so that the links must be long;
- a lack of user-control ability, comprehensibility, and user independence. These qualities are important to social compatibility, rapid reproducibility, maintainability, and other social properties...important...to resilience.[11]

In contrast to these characteristics, distributed generation is characterized by numerous, small, modular, fuel diverse generators capable of independent operation when the grid is disrupted. This provides the resilience and flexibility required to form a more robust electric grid required by a modern digital society.

2.2 Diversity of the Generation Mix

Energy resource diversity is an issue at both the national and state level but particularly at the latter since many states that have little or no indigenous energy resources and require import of primary fuels via pipeline or rail to produce their electricity. These lines of supply, themselves, are vulnerable and particularly overdependence on any one increases the vulnerability of the entire state.

With the advent of the highly efficient and environmentally desirable combined cycle gas turbine, there is already a trend for states to provide approval for these new centralized facilities without considering effects on energy security. Interruption of natural gas to a state without a local supply could carry severe consequences, particularly if it occurred in winter when the fuel would also be required for space heating needs.

Diversity must be examined not only within a framework of fossil and nuclear sources but also by looking at renewable forms and whether policies are in place to shift from the energy sources that are more vulnerable/interruptible to the those that are less vulnerable. This is a very state-specific determination since, for example, West Virginia might rate relatively well with a high percentage of local/secure coal in its mix but would still need to provide balance in order to obtain a high score in this category.

3. THE METRICS, DATA SUPPORT & APPLICATION

The metrics chosen to rank state energy security need to reflect efforts to: (1) decentralize the grid by removing financial and regulatory barriers to installing grid-connected distributed and renewable energy systems; and (2) diversify the energy mix (including actions toward renewables, such as requiring green power procurement by the state or electricity generation using renewable resources). Many experts agree that these two steps can lead to a more robust system. Thus, factors selected for this project include:

Regulatory Environment & Oversight
1) Streamlined environmental permitting for clean distributed generation (DG);
2) Favorable Standardized Interconnection Rules (SIRs);

3) Grid downtime as an indicator over fifteen years; and
4) Non-onerous standby/back-up rates, exit fees and insurance requirements for DG and renewables.

Diversification of the fuel mix including % renewables
5) Current and projected energy mix;
6) State Government Green Power Procurement Policies; and
7) Availability of a Renewable Portfolio Standard or Green Power Option to Commercial and Industrial (C&I) and residential consumers.

Financial Incentives
8) Clean Energy and Conservation & Load Management Funds to serve C&I/residential sectors;
9) Net metering favorable to consumers; and
10) Tax Incentives for Renewables, energy efficiency & DG

3.1 Data Sources for Metric Application

3.1.1 DSIRE Database

The Database of State Incentives for Renewable Energy (DSIRE), available online at www.dsireusa.org, is the nation's most comprehensive, up-to-date source of information on government and utility incentives, policies, and programs that promote the deployment of renewable energy technologies. DSIRE can be used to identify the types and details of such policies implemented in each state. For example, users can quickly identify whether and to what extent a state offers financial assistance for renewable projects or requires the use of renewable resources in the utilities' resource portfolio. Along with a summary of each program and identification of key state contacts, DSIRE provides links to legislation, regulatory orders, and other authorizing documents.

DSIRE includes information on the following programs:

Financial incentives*:* income, sales and property tax incentives; grants, rebates and loans; production incentives; and industrial recruitment programs;

Regulatory policies: renewables portfolio standards; public benefits funds; fuel mix and emissions disclosure; net metering & interconnection rules; line extension analysis requirements; contractor licensing; equipment certification; construction & design policies; green power procurement policies; requirements for utility green power options; and solar and wind access laws; and

Outreach and voluntary programs*:* Million Solar Roofs Initiative programs, state-wide renewable energy education campaigns and technical assistance programs; utility green pricing programs and voluntary PV installer certification programs.

3.1.2 Energy Information Administration (EIA)

The Energy Information Administration of the US DOE is an invaluable resource for determining a number of factors on state energy use. For the purposes of this study, its most important piece is the fuel mix. This can be found by accessing http://www.eia.doe.gov/emeu/states/_states.html and then clicking on the desired state two-letter identifier.

Under the "Electric" heading, click on "Summary" to see a listing for a number of tables and charts that can supply the fuel mix for the state. Table 5. Electric Power Industry Generation by Energy Source 1990, 1994, 1999 provides the appropriate mix by MWh and some retrospective trending information. Because there is some lag time between EIA receiving information, it may be that some state agencies can supply more current information for this parameter.

3.1.3 State Regulatory Agencies

Sometimes less accessible but highly useful are regulatory materials by State Public Service, Public Utility, Siting and Environmental agencies that oversee different aspects of the electric industry.

Public Service/Public Utility Commissions are useful in obtaining rating information unavailable through DSIRE and EIA that may include: Grid Outage times Standby/Back-up Rates and Green Power Offerings. Environmental regulators are the most likely source for information concerning permitting for distributed generation and any special treatment for clean sources.

4. CONNECTICUT AS A SAMPLE RATING

See below for a sample rating using Connecticut as an example. Each of the ten questions falls within the more general categories of: 1) Regulatory Environment & Oversight; 2) Diversification of the fuel mix including % renewables; and 3) Financial Incentives. Each factor is rated on a scale from one to ten but at this point in the development of the rating, no attempt has yet been made to assign a relative importance to either the general categories or individual questions. That may be considered in follow-on work.

Energy Security Rating Profile Connecticut

Regulatory Environment & Oversight

1) Streamlined environmental permitting for clean DG
[10 Points]

Energy sources that are less than 2 ppm NOx such as solar, wind, fuel cells and some microturbines will require no environmental permitting. Diesels above 37 kW diesel must have a permit and there are limitations on how many hours they can run. New rules will conform to the Regulatory Assistance Project (RAP) model which can be viewed at: http://www.raponline.org/ProjDocs/DREmsRul/Collfile/ReviewDraftModelEmissionsRule.pdf[12]

2) Favorable Standardized Interconnection Rules (SIRs)
[3 Points]

Connecticut has no formalized interconnection rules either for distributed generation or renewable energy systems but a Department of Public Utility Control docket is forthcoming. At this point, there have been few interconnections of any significance on which to base utility behavior in this regard but projects greater than 10 kW must still pay the Competitive Transition Assessment. Ease of interconnection may possibly become a metric in performance-based ratemaking for determining utility rate of return.

3) Grid downtime as an indicator over fifteen years.
[5 Points]

With major storms excluded (except as noted) the following figures are available from a local utility (represents approximately 80% of Connecticut customers):

	1990	2002
Average number of times a customer is interrupted per year (SAIFI)	1.75 Times	.88 Times (prelim)
Average interruption duration for those who lost power (CAIDI)	101 minutes	131 minutes (prelim)
Total Outages Excluding Major Storms	11,644	12,289 (prelim)
Total Outages Including Major Storms	11,992	16,780 (prelim)

While certain parameters, such as number of interruptions per customer, show marked improvement, the length of the interruption for those actually affected have increased. Excluding major storms number of outages shows a modest 5.5% increase while total outages that do include major storms have increased 39.9%. The latter may indicate a long term climate shift to more intense precipitation events, a point made by Dr. Thomas Karl and other researchers at the National Oceanographic and Atmospheric Administration.[13]

4) Non-onerous standby/back-up rates, exit fees and insurance requirements for DG and renewables
[5 Points]

Currently, the State has no policy on back-up or standby rates for distributed generation or renewable energy sources but the State's major utility has made overtures calling for one. Exit fee bills have been twice introduced into the legislature but have not passed.

Diversification of the Fuel Mix Including % Renewables

5) Current and projected energy mix.
[2 Points]

	2002	2011
Coal	8%	8%
Gas	24%	47%
Oil	*35%*	*11%*
Nuclear	28%	29%
MSW	3%	3%
Hydro	2%	2%

Renewables make up no significant portion of the mix in the foreseeable future.

It is evident the trend will make the state overly dependent upon natural gas, none of which is produced within the state and is subject to interruption and price fluctuation. Lack of internal renewable resources and the will to develop what does exist results in projections of no significant renewables in the mix by 2011.

6) State Government Green Power Procurement
[0 Points]

There is currently no plan for green power procurement by the State nor has any plan been articulated for implementation in the immediate future.

7) Availability of a Renewable Portfolio Standard or Green Power Option for C&I and residential consumers
[3 Points]

There is a renewable portfolio standard established under PA 98-28 but the DPUC has ruled that the standard offer and default service are exempt from this requirement. Failure of a competitive market to develop has resulted in no additional renewable energy attributable to the RPS. The Connecticut Electric Coop which did have the EcoWatt green power offering ceased operation in late 2002 and Green Mountain has withdrawn from activities in the state.[14]

Financial Incentives

8) Clean Energy and Conservation & Load Management Funds to serve C&I/residential sectors. Per capita or kWh metric. **[5 Points]**

Public Act 98-28 established both a Conservation and Load Management Fund as well as a Renewable Energy Investment Fund. The Conservation Fund receives 3 mils/kWh for a total of ~$86 million per year. The Renewable Fund began at .5 mils/kWh (~$14 million per year) and rises to 1 mil/kWh over a four year period.

Large deficits for fiscal years 2003 and 2004 have placed both of these funds in jeopardy wherein their assets have already been and may continue [100% reduction] to be raided for one-shot deficit reductions.

9) Net metering favorable to consumers
[8 Points]

PA 98-28, the restructuring act, also had provisions for net metering for consumers allowing for resale to the grid at retail price equal to the amount used and then any excess is bought at avoided cost.

10) Tax Incentives for Renewables, EE & DG
[4 Points]

The only tax incentive for distributed generation or renewables in Connecticut comes in the form of a 15 year property tax exemption for all renewable energy systems approved on a local option basis. Sales taxes on systems are still in force as are corporation taxes for those involved in production, sales and installation of renewable energy systems.

Total Points 45

5. CONCLUSIONS

In the past, judging from the heavily centralized nature of our energy infrastructure and lack of diversity within most state energy mixes, it appears that energy security has not been seriously considered as a planning factor in its design. This has left energy systems vulnerable to natural disasters, terrorism and other hazards that threaten not only economic well-being but also the lives and welfare of individuals.

In order to determine future actions that can be taken to design and obtain a more resilient energy infrastructure that is more decentralized, fuel diverse and when it fails does so more gracefully, it is important to obtain a measure of how the current system measures to an idealized model. The method described in this paper provides one example of such a model which can be built upon and refined to provide what could become a valuable planning tool to that end.

END NOTES

[1] Winn Schwartau, Information Warfare, "Electronic Civil Defense," Thunder's Mouth Press, New York, 1996. p. 43

[2] Richard Clarke Director Office of Cyber Security, Homeland Defense Council interviews by Steve Croft on "60 Minutes" segment on "Cyber War." 4/9/00.

[3] Matthew L. Wald, *Electric Power System Is Called Vulnerable, and Vigilance Is Sought*, New York Times. Feb 28. 2002.

[4] *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academy Press. p.302. 2002.

[5] Response to question by Joel N. Gordes on RTOs to Commissioner Nora Meade Brownell. *What the Deal II: CPES Conference*. September 13, 2001.

[6] Winn Schwartau, *Information Warfare, Electronic Civil Defense*, Thunders Mouth Press, New York, 1996. p. 584. Wilson, J. "E- Bomb," Popular Mechanics. 9/01 pp. 50-53.

[7] Barton Gellman, *U.S. Fears Al Qaeda Cyber Attacks,* Washington Post, July 26, 2002

[8] Dan Morain, "Hackers Mount Attack on Power System, Report Says," San Jose Mercury News, June 10, 2001.

[9] Wilson, J. "E- Bomb," Popular Mechanics. 9/2001. pp. 50-53.

[10] A Faraday Cage may be described as a web of tightly spaced copper used as an enclosure of sensitive equipment containing semiconductors and is used to protect them from EMP.

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

[12] Interview with Christopher A. James, Director of Planning & Standards, Bureau of Air Management, Connecticut Department of Environmental Protection on 3/24/03.

[13] U.S. Climate Tilts Toward the Greenhouse, Science, Vol. 268, Apr. 21, 1995. P. 363.

[14] Interview with Mark J. Quinlan, Connecticut Department of Public Utility Control on 3/24/03.