

**Distributed Power Generation for Homeland Security:**

**Proposal for a New Federal and State  
Partnership**



**Lewis Milford  
President,  
Clean Energy Group (CEG)**

Assisted by Ruth O'Meara-  
Costello, CEG Intern

*Disruption of electricity has been a weapon of war in Iraq. Throughout the past summer, following the cessation of active combat operations by the United States, looters or saboteurs in Baghdad destroyed long distance power lines, stole valuable parts of the electrical system, and destroyed dozens of 100-foot electric towers.*

*Residents suffered in heat up to 120 degrees, huge backups of sewage resulted because of the failure of electric pumps, and damage to local electrical lines made it impossible for farmers to irrigate their fields, with tensions at a fever pitch.<sup>1</sup> During the recent blackouts in the U.S. and Canada, many Iraqis gloated, making statements like: "Let them feel our suffering" after their months of life without electricity.<sup>2</sup>*

Unlike the August 14<sup>th</sup> blackout in U.S. and Canada, though, the attacks on the Iraqi power grid had an obvious political purpose – to undermine reconstruction efforts, killing hope and increasing the odds against a quick return to normalcy. They were not accidental, but an element of an organized war plan.

In fact, documents prepared by the Iraqi Intelligence Service as early as January of 2003 contain a plan that "outlines 11 steps, including...sabotaging power plants" to disrupt U.S. occupation of Iraq. According to administrators and military officials, "a substantial amount of the damage to Iraq's essential services is not the result of impoverished looters, but of more organized elements out to undermine allied administration of Iraq."<sup>3</sup>

While US officials said the situation was improving, they seemed genuinely surprised that the electrical power grid would be a target of war.

But for anyone who follows issues of war and energy the only surprising thing about the Iraq situation is that the tactic was considered surprising. Destruction of power systems is a combat strategy as old as modern warfare.

Targeting power systems was an Allied strategy used in World War II. Indeed, before the incidents of sabotage in Iraq, our own government warned continuously of terrorist attacks to our US power system. Long before the terrorist attacks in the U.S., reams of government studies showed how terrorists could wreak havoc on our power systems.

With all this attention to links between security and electricity, we have not seen significant official support for smarter, more resilient power systems at home. Instead, various congressional subcommittees actually slashed funding for a Defense Department fuel cell

<sup>1</sup>Andrews, Edmund L., "After the War: Energy; Thieves and Saboteurs Disrupt Electrical Services in Iraq." NYT, June 21, 2003.

<sup>2</sup>Price, Niko. "Iraqis Gloat Over U.S. Blackout; Offer Tips on How to Beat the Heat." AP Friday, August 15, 2003.

<sup>3</sup>Gordon, Michael R. "After the War: Intelligence; Iraqi Saboteurs' Goal: Disrupt the Occupation." NYT, June 28, 2003.

program this past summer. The program is designed to enhance our national security through these smarter energy technologies.<sup>4</sup>

Such actions reduce our national security when we should do all we can to increase it. The fragility of power systems makes them top terrorist targets. Given that sad truth, it is time for our government at all levels to act vigorously to create new power systems that are more resistant to terrorist threat. A partnership between federal and state government, utilizing the resources and expertise of state clean energy funds, is necessary. Such a partnership could install new technologies in key facilities, protecting America by ensuring reliable power in emergency facilities such as hospitals and emergency bunkers, the continued functioning of telecommunications, and reliable, independent power in areas such as street lighting and railway crossings.

The August 14<sup>th</sup> blackouts showed us just how much chaos can result when the lights go out. The day after the blackouts, the New York Times reported that “the city mobilized 10,000 police officers during the night, responded to 80,000 calls to 911—more than double the average number for a day—and fought 60 fires, many of them attributed to the use of candles. The city’s Emergency Medical Services responded to 5,000 calls—600 more than their previous record—and police and fire personnel made more than 800 elevator rescues.”<sup>5</sup> Interfering with these essential services were glitches in backup power; when generators failed at a Verizon office, for example, “power shortages caused communications gaps for dispatchers trying to relay 911 calls to ambulances.”<sup>6</sup> Similarly, in some hospitals and nursing homes generators broke or ran out of fuel, putting patients at risk.<sup>7</sup> And that’s not to mention the lingering effects of the outage, including six billion dollars in economic losses, affecting businesses like grocery stores, restaurants, and airlines.<sup>8</sup> Losses were great, and could have been much worse, had the blackouts been terrorist-related rather than accidental.

The environmental possibilities of distributed generation technologies such as fuel cells and PV are well known, but today’s security needs make it imperative that we consider them in the light of security investments.

Recent events have shown us the potential for damage to our current system, and therefore created an opening for change. In the course of developing new distributed systems, we also could create new jobs and new economic and investment opportunities for the nation. It would not be the first time that war boosted America’s technological prowess.

### History of War and Energy

It is now common to say that electricity is the lifeblood of modern society. Without it, life as we know it cannot go on. Electric power usually comes from central generation plants miles away from homes, offices and factories, with electrons surging over long transmission lines. It is an elaborate system where any failure can transform a city or region into chaos, as happened August 14<sup>th</sup>. The causes of that massive power outage are still unclear, but early evidence indicates that it began with nothing more than one company’s failed power lines.<sup>9</sup>

That has been the case in Baghdad, Boston or Berlin, and it’s been that way ever since Thomas Edison invented the central power plant.

Central energy systems have been targeted very effectively during times of war, most notably in Germany during World War II. “Electric power was the vital part of the German energy system... [By 1944] with the destruction of the main electric power plants, the German war economy was essentially incapacitated....”<sup>10</sup> Albert Speer, Hitler’s strategist, wrote that, “The destruction of all industry can be achieved with less effort via power plants,” highlighting the danger of vulnerable power facilities.

In Japan, however, such destruction was far more difficult to achieve due to the relative decentralization of Japan’s power grid. According to the US Strategic Bombing Survey (Pacific), the electric power system in Japan “was never a primary target because most of the power facilities in Japan were “so numerous, small and inaccessible that their destruction would have been impractical if not impossible.”

<sup>4</sup>Department of Defense Appropriations Bill, 2004. Report of the Committee on Appropriations, Together with Additional Views. 108<sup>th</sup> Congress, 1<sup>st</sup> Session, Report 108-187. U.S. Government Printing Office, Washington, 2003.

<sup>5</sup>“Parts of Country May Enter Weekend Without Power,” by James Barron and Kirk Semple. New York Times, August 15, 2003.

<sup>6</sup>“911 System Glitched Out,” by Melissa Grace. Daily News (New York) August 17, 2003.

<sup>7</sup>“The Blackout: Hospitals; Lessons Learned on 9/11 Help Hospitals Respond.”

By Clifford J. Levy with Kate Zernike. The New York Times, August 16 2003

<sup>8</sup>“A 6B Battering: Wide range of industries feels effects of power outage.”

Newsday, August 19, 2003.

<sup>9</sup>“Splintered Midwest Grid Helped Outage to Spread,” by Rebecca Smith and Joseph T. Hallinan. The Wall Street Journal Online, August 19, 2003.

<sup>10</sup>Clark and Page, “Energy, Vulnerability and War at 50 (Norton 1981).

### *Security Management Institute*

Winter 2003

*Ruth Marie and Lauren Herald  
Editors, SMI News*

*Security Management Institute News* is published by the Security Management Institute of the Association of Energy Engineers. Articles of interest to SMI are welcomed by the Editor. Please send text and bio via e-mail or on computer disk in Microsoft Word. Photographs may also be sent via e-mail if they are in JPEG format and a high resolution of 300 dpi, or you may send photographic prints for us to scan.

info@aeecenter.org  
4025 Pleasantdale Road, Suite 420  
Atlanta, GA 30340-4264  
Phone: 770-447-5083 ext. 210  
Fax: 770-446-3969

The leading historians of this issue have written, "There is nothing new about targeting energy facilities during times of war...The examples of Germany and Japan in World War II offer a clear-cut demonstration of the disadvantages of a centralized system of energy production in time of war..."<sup>11</sup>

But despite the lessons learned from the WWII experience, or perhaps due to the U.S. sense that we were invulnerable to similar attacks, these lessons had no effect on energy and emergency planning in America during the ensuing decades. Nevertheless, the risk that power systems in the US could be the target of terrorist attacks, and that guarding them alone was not enough, was well known.

"There is little doubt that overhead transmission lines and the pipelines that carry electricity and fuel in this country are vulnerable to terrorist attack, particularly the switching centers and aboveground valves. They are essentially unguarded, vulnerable to a variety of weapons, and difficult to repair. Less vulnerable are the refineries and power plants. They are guarded – often by personnel trained in counterterrorist tactics – and are generally designed to withstand accidental, if not intentional, damage. Even so, they remain viable targets for internal attack."<sup>12</sup>

### Conventional Emergency Planning

This indifference to power related terror risks was a sign of the times. The notion of prevention against terrorism through active measures to reduce threats was not in keeping with the conventional view of emergency preparedness in America in the post-World War II era.

Emergency management in the U.S. has its roots in military "civil defense" planning, where the primary governmental function is to maintain social order. Emergency management practices in the US took the energy system as it developed – especially nuclear plant risks - - and focused on post-disaster planning and mass evacuation, not prevention.

According to experts, "this preoccupation with only responding to disaster ignored the importance of preparedness, mitigation and recovery."<sup>13</sup> It is in these areas particularly that energy technologies are of great importance and carry great potential.

According to disaster management theory, there are four elements of conventional emergency management thinking.

U.S. preparation for terrorist attacks must be evaluated in the light of the 4 elements of disaster planning:

- **Mitigation:** "policies and actions taken before an event which are intended to minimize damage when an event does occur." (E.g. Make buildings disaster resistant)
- **Preparedness:** "enhance the ability to respond" (E.g. Emergency plans, training)
- **Response:** "actions taken at time disaster strikes...to reduce threats." (E.g. Warning, evacuation)
- **Recovery:** "longer term efforts to reconstruct and restore."<sup>14</sup>

Response – after the fact – was (and it could be argued still remains) the principal mission of emergency management officials.

### Unsuccessful Challenges to Conventional Thinking

It cannot be said that emergency management officials were unaware of alternative views that took account of more aggressive use of localized energy systems. Such warnings and recommendations have been made for years. Emergency management agencies often have been made aware of the risks posed by centralized power systems.

The Federal Emergency Management Agency (FEMA) in the late 1970s commissioned a report to explore alternative strategies – to focus on dispersed and decentralized energy generation as a means of reducing risk and damage from power related disasters, particularly "major nuclear crisis or war." The FEMA "Energy and Defense Project" "evaluated a number of dispersed, decentralized and renewable energy sources (solar, wind, fuel cells) which offer potential for reducing national vulnerability, increasing the self-sufficiency of local communities and strengthening national security."

That report explained the importance of addressing energy system vulnerability: "Because the energy sector is vital to the industrial, agricultural, communications, and other sectors of a society, a failure in the ability to produce and distribute energy throughout the United States would leave the country unable to support or defend itself." In particular, "American society depends on large-scale power plants for the operation of food production and distribution, transportation, communication, and for the ability to defend itself."<sup>15</sup>

- "Current US energy systems are highly vulnerable, due to requirements for imported resources and due to the centralized nature of

<sup>11</sup>Clark and Page, "Energy, Vulnerability and War at 50 (Norton 1981).

<sup>12</sup>Clark and Page at 56.

<sup>13</sup>Dynes, Governmental Systems for Disaster Management (U. Delaware Disaster Research Center) (undated manuscript).

<sup>14</sup>Tierney, "Disaster Preparedness and Response" (U. Del Disaster Research Center)(1993).

<sup>15</sup>"Dispersed, Decentralized and Renewable Energy Sources: Alternatives to National Vulnerability and War," California Academy of Sciences Dec. 1980 (FEMA), page 1.

These plants are “increasingly centralized,” and “depend on other centralized systems of fuel production, transportation, refining, and storage”, a dependence that increases the vulnerability of vital electrical systems.<sup>16</sup> The petroleum industry, the report explains, is also “very vulnerable”—not just because of centralized facilities, but because of political chaos in the Middle East (a concern which has not lessened today).<sup>17</sup>

The final conclusions of the report, now more than twenty years old, leave one with an eerie sense that they could have been written yesterday.

- “Current US energy systems are highly vulnerable, due to requirements for imported resources and due to the centralized nature of the systems themselves.”
- “Dispersed, decentralized and renewable energy resources can reduce national vulnerability and likelihood of war by substituting for vulnerable centralized resources.”
- “National policies and goals need to be developed to strengthen current inadequate energy emergency contingency planning and incorporate decentralized and renewable energy sources in planning.”<sup>18</sup>

This 1980 FEMA report quickly made its way into the dustbin of history, in the waning days of the Carter Administration. In the next administration, its policy recommendations were evidently ignored.

Ironically, the report, as timely as it is, is now out of print and no longer available from even FEMA itself. Only the National Archives has copies for the public to read.<sup>19</sup>

### **Neglect in 1980s and 1990s**

During the 1980s various outside advocates and government agencies continued to press for a decentralized energy approach to terrorism and disaster mitigation. But almost a sense of despair accompanied efforts in the 1980s to look at these unconventional approaches. A typical comment from the emergency management literature tells the story of neglect in that period.

“There is little doubt that overhead transmission lines and the pipelines that carry electricity and fuel in this country are vulnerable to terrorist attack, particularly the switching centers and aboveground valves. They are essentially unguarded, vulnerable to a variety of weapons, and difficult to repair. Less vulnerable are the refineries and power plants. They are guarded – often by personnel trained in

counterterrorist tactics – and are generally designed to withstand accidental, if not intentional, damage. Even so, they remain viable targets for internal attack.”

This inattention to energy security at the national level was confirmed when a Department of Energy (DOE) working group on “Energy Vulnerability” was disbanded in 1988. This occurred despite almost contemporaneous claims that terrorists could easily disrupt power systems.”<sup>20</sup>

During the ensuing years, in keeping with this pattern, utilities made little investment in power risk prevention. According to Congressional investigators in 1990,

“Utilities historically have expended great efforts to ensure reliability, but only over the last few years have they started to take seriously the possibility of massive, simultaneous damage to multiple facilities. Awareness of the threat, however, has not led to the implementation of many measures to counter it. Few if any utilities plan their system and its operation to accommodate multiple, major failures, and key facilities are still left unprotected.”<sup>21</sup>

The Congressional report did note the possibilities offered by dispersed energy systems, writing that a “system that emphasizes numerous small generators close to loads is, overall, less vulnerable to sabotage.” But without any terrorism, it was hard to justify the costs. It said that “the total system costs of moving toward dispersed systems are not clear, and substantial governmental incentive might be necessary to expedite the trend toward smaller units.”

But the investigators issued a warning: “With the level of terrorism in this country as low as it is, many people will be skeptical of the need for any action, especially major investments... However, terrorism could increase much faster than the measures to counter it could be implemented... *If a rapid increase in terrorism seems at all likely, then even expensive measures are reasonable insurance.*”<sup>22</sup>

In the absence of terror incidents, more reports were commissioned that further confirmed the risk. In 1997, President Clinton’s Commission on Critical Infrastructure Protection said that the entire nation’s infrastructure would profoundly suffer from “prolonged disruption in the flow of energy.” In dire language, the commission reported that, “Our fundamental conclusion is this:

<sup>16</sup>Ibid, page 59.

<sup>17</sup>Ibid, page 10.

<sup>18</sup>“Dispersed, Decentralized and Renewable Energy Sources: Alternatives to National Vulnerability and War,” California Academy of Sciences Dec. 1980) (FEMA)

<sup>19</sup>The report was later issued as a book by one of its authors, Amory Lovins, under the title **Brittle Power: Energy Strategy for National Security**. Lovins argues that: “a strategy of resilience could seek to ensure that if complete grid failure did occur its consequences to energy users would be trivial.” Over 20 years later, such a strategy has yet to be implemented.

<sup>20</sup>Clark and Page at 56 (1981).

<sup>21</sup>Clark and Page at 56 (1981).

<sup>22</sup>Congressional Office of Technology Assessment, “Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage,” (June 1990) at 4.

Waiting for disaster is a dangerous strategy. Now is the time to act to protect our future.”

In 1998 President Clinton issued a Presidential Order on Critical Infrastructure Protection known as Presidential Decision Directive 63.

The Directive addressed “critical infrastructures” – those physical and cyber-based systems essential to the minimum operations of the economy and of the government. They include systems such as energy, finance and telecommunications.

The Directive concluded that these systems “have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and natural causes, and physical and cyber attacks.”<sup>23</sup>

However, Presidential Directive 63 on critical infrastructure protection went the way of many well-intentioned government programs.

A President’s Commission was formed. A lead federal agency, DOE and the Sandia National Laboratory, was designated to lead the energy sector review.

The Partnership for Critical Infrastructure Security was launched at the World Trade Center in 1998. In keeping with the conventional thinking of the time, the principal infrastructure threats identified were from high-tech cyber hackers, not low-tech terrorists. As a result, the energy work – like that in other industry sectors – focused almost exclusively on information technology threats to the grid operation. The recommended solutions tell the tale: “Information Sharing, Cyber Intrusion Database, Training and Awareness, Information Assurance Tools and Physical and Cyber Security Best Practices and Standards.”<sup>24</sup>

### **September 11 and Energy**

Despite the repeated cautionary reports and studies, neither the federal government nor any state incorporated new forms of energy protection into disaster planning prior to 2001. Warnings never led to action.

And even more warnings were forthcoming, after the attacks of September 11. Most concerned the vulnerability of the central grid. U.S. Homeland Security Director Tom Ridge stated,  
“We need to talk to our energy companies... We need to ramp up our security and deal with what may occur.”

Ridge warned that companies need to be on high alert for possible attacks.

Immediately after the September attacks, the North American Electric Reliability Council (NERC) issued its first-ever warning instructing grid security operators at 21 locations across the U.S. and Canada to assume heightened levels of readiness. The head of NERC conceded, “Any technologically complex system is at risk if someone wants to disrupt it.”<sup>25</sup> The most vulnerable components include the system’s long haul transmission lines, regional control centers, nuclear plants and electric substations. Knocking out a substation could interrupt power “for a number of weeks,” according to experts.

The warnings were familiar, as were the conventional solutions proposed: to “harden” the central grid, through police posting at critical junctures, remote monitoring and reinforcing computer systems. These were understandable as initial reactions.

But experts know that sole reliance on grid-based solutions is insufficient and impractical. “You can’t build a Great Wall of China around all the lines,” said Brantley Eldridge, executive director of the East Coast Central Area Reliability Council. “If someone is willing to die for the cause, you can’t stop it.”<sup>26</sup>

The nature of the attacks should have suggested a more nuanced discussion about ways to achieve greater building security with energy solutions. Three related stories following the September 11<sup>th</sup> attacks suggest how the new kind of threat demands new solutions.

Engineering analysis of the WTC 7 building collapse, a tower that was not struck but that fell soon after the other two buildings, suggests that the giant diesel tanks stored on site for the backup generators – some in the basement and others at the 23d floor -- might have been the cause of the fire that destroyed the building. Large diesel tanks with about 30,000 gallons of diesel fuel were stored at the building to power generators for the mayor’s emergency command bunker. That bunker and the building were destroyed, some believe, because the protection systems around the tanks were breached, leading to a disastrous fire that brought the building down. The New York Times commented, “Across the country, diesel powered generators are used in buildings like hospitals and trading houses,

<sup>23</sup>Directive 63 at [www.clinton2.nara.gov/WH/EOP/NSC](http://www.clinton2.nara.gov/WH/EOP/NSC).

<sup>24</sup>President’s Commission on Critical Infrastructure Protection, Energy Sector (David Jones Commissioner). Apparently with little sense of irony about the efforts to deal with threats with reports, three weeks after the World Trade Center attack, the head of the Commission told Congress that one of the group’s top goals was for a “cross-sector and public-private information-sharing architecture.” No other progress was reported on actually reducing risk from terrorist attack in any sector (Kenneth Watson, “Critical Infrastructure Protection: Who’s in Charge?” Testimony before US Senate Committee on Government Affairs, Oct. 4, 2001. See also, Rana and Sagalow, “Partnership Interim Results, (July 25-27, 2000) Slide presentation).

<sup>25</sup>Wagman, “Energy Insight Today”, Sept. 14, 2001.

<sup>26</sup>Ibid.

where avoiding power outages is critical. Partly for that reason, an understanding of what happened in 7 World Trade Center is vital to investigators....”<sup>27</sup>

In a related story, following the anthrax attacks in Florida, the main federal Centers for Disease Control laboratory in Atlanta was closed during a power failure, delaying for fifteen hours critical analysis of the bioterrorism samples.<sup>28</sup> Like that lab, most critical public health and research facilities depend on insufficient backup systems in case of power failures, often relying on old systems or even single diesel backup generators.

In another case, shortly after September 11, a network news report looked at how well conventional diesel backup power supplies protect the country's children from the risk of a terrorist attack on chemical weapons storage supplies.

The report outlined the astonishing fact that 12 percent of the country's chemical arsenal – seven million pounds of deadly nerve gas, mustard gas and other substances – is kept in 89 bunkers in Umatilla, Oregon. A military worst-case scenario plan concluded that a fully loaded plane with fuel crashing into one of the bunkers could release enough poison to kill 10,000 people.

The facility's main line of defense is a \$50 million emergency disaster plan that relies on sirens and a system of emergency radios to warn the 30,000 people within an 8-mile radius of the plant. Schools are equipped with shelters for the children, with pressured rooms and air purifiers.

But when a school demonstrated the equipment for NBC news, an emergency generator failed--something the critics say is typical of faulty disaster planning.<sup>29</sup>

These three cases highlight the links between our energy supplies and advanced technology, and how our dependence upon it poses new risks. One expert writes that “changes in technology lead to new threats and new disaster-related problems. For example, the increasing dependence of business on computers to maintain operations means that power outages will be increasingly disruptive.”<sup>30</sup> And as we've become more dependent on our technology, technology itself has become more vulnerable: “Growing complexity and interdependence, especially in the energy and communications infrastructure, create an increased possibility that a rather minor and routine disturbance can cascade into a regional outage.”<sup>31</sup>

The disruption of essential facilities from terrorist related power outages can entail significant loss of life and property.

### **New Unconventional Solutions Needed**

Terrorism and energy issues should effect new thinking and new solutions. Planning for power outages has usually assumed the cause of an outage to be either equipment or weather related, and responses to outages related to these causes are necessarily different from responses to terrorism. “Length of outages, coordination of attack, and scope of damage make conflict conditions very different from blackouts caused by hurricanes or heightened electricity demand.”<sup>32</sup>

Faced with these risks, many experts dealing with the problem of energy system vulnerability have returned to solutions first advocated decades earlier. In an unusual statement of support for renewable and distributed energy, former top government security chiefs endorsed clean energy options in a letter to Congress. On September 19, 2001, a week after the attacks, the former head of the CIA Woolsey, former National Security Advisor to President Reagan MacFarland, and former Chairman of the Joint Chiefs of Staff Moorer wrote, “Our refineries, pipelines and electrical grid are highly vulnerable to conventional military, nuclear and terror attacks. Disbursed, renewable and domestic supplies of fuels and electricity...address those challenges. Fortunately, technologies to deliver these supplies have been advancing steadily since the Middle East fired its first warning shot over our bow in 1973. They are now ready to be brought, full force, into service.”

After 9/11, many in the media also recognize distributed renewable energy as a means of increasing our national security. The Christian Science Monitor wrote, “The events of September 11 sealed the national security argument for a massive national investment in renewable energy.”<sup>33</sup> A chorus of public commentators has called for more action:

- “A shift toward renewable energy and conservation can also help reduce our vulnerability to terrorist attacks.”<sup>34</sup>
- “Distributed renewable energy systems, such as rooftop solar photovoltaic (PV) systems, small wind turbines and fuel cells...suddenly begin to look like an enlightened approach to generating electricity that bolsters national security while addressing global climate change

<sup>27</sup>New York Times, “Engineers Suspect Diesel Fuel in Collapse of 7 World Trade Center,” November 29, 2001.

<sup>28</sup>Atlanta-Journal Constitution, “Lawmakers Push for more CDC Funding,” Oct. 23, 2001.

<sup>29</sup>NBC Nightly News, Transcript, October 29, 2001.

<sup>30</sup>Dynes, “Governmental Systems for Disaster Management,” (U. Del. Disaster Research Center) (undated manuscript).

<sup>31</sup>President's Commission on Critical Infrastructure Protection, “Critical Foundations,” (1997).

<sup>32</sup>Zerriffi et. al., “Electricity and Conflict: Advantages of a Distributed System.” *El-sevier Science Inc.*, January/February 2002 p. 55-65.

<sup>33</sup>Mazarr, “Terrorism, the Energy Trap and the Way Out,” Christian Science Monitor, October 10, 2001.

<sup>34</sup>Hochschild and Hochschild, “Hooray for the Red, White Blue and Green,” Los Angeles Times, Nov. 11, 2001.

<sup>35</sup>Asmus, “The War Against Terrorism Helps Build Case for Distributed Renewables,” Power to the People web site.

- and other environmental concerns.”<sup>35</sup>
- “The political turmoil in the Middle East could provide the strongest incentive yet for the United States to increase research into renewable energy...”<sup>36</sup>

### **Market Strategies and Emerging Technologies**

The introduction of distributed generation technologies into the marketplace, demanded by current security concerns, nonetheless faces certain barriers and therefore requires a well-defined strategy. New innovative technologies typically cannot compete in the marketplace on the basis of price and performance against mainstream, dominant technologies. The same is true of renewable and clean power technologies, including technologies relevant to national security.

Renewables have had years of government research and development support, leading to a proliferation of various technologies. However, these technologies continue to face significant competitive challenges, most significantly in the area of unit cost. The truth is that most power generated by clean power technologies is more expensive than conventional grid power, a typical “price-performance” barrier that has kept renewable and clean technologies from achieving mass-market appeal.

These barriers to moving clean power technology into mainstream markets are nothing new. Ironically, many of the same difficulties faced the entry of electricity into new markets at the end of the 19<sup>th</sup> century. Which begs the question: what should be done to adapt market rules that have worked before to replace other technologies, in order to achieve success for clean energy today? This question takes on great relevance in the new context of national security energy needs.

Professor Clayton Christensen of Harvard Business School is the author of groundbreaking work on the road that “disruptive technologies” typically take to market success. His framework, which is directly relevant to any clean energy replacement strategy, can be summarized as follows:

- Potentially “disruptive technologies” bring to a market different values than had been available before. These products may be cheaper, simpler, smaller and/or sometimes more convenient to use than a conventional “sustaining” technology (such as the model of central, vulnerable power plants). Or they may provide an entirely new service (on-site reliable power).
- Nonetheless, at the outset these disruptive technologies are usually only valued by a few fringe customers who have different needs and

values than mainstream customers.

New technologies are often first commercialized in emerging or insignificant markets.

- Although traditional firms do not often commercialize these technologies, the values of disruptive technologies rejected by mass markets are actually in demand in smaller, emerging, “niche” markets.
- The key strategy for innovation over time has been to “develop new markets that valued the attributes of the disruptive products, rather than search for a technological breakthrough so that the disruptive product could compete as a sustaining technology in mainstream markets.”<sup>37</sup>

Emerging clean energy technologies like fuel cells and PV appear to be disruptive technologies. They share values that generally are not now demanded in traditional, mainstream markets—higher unit costs, environmental benefits and more reliable, more secure on-site power quality.

Even as these attributes block their entry into *mainstream* markets, however, they could have enormous value in new *niche* markets, perhaps in security settings. Higher costs are already a fact of life; companies now spend billions on power applications with multiple redundant back up systems. Moreover, “premium power” reliability in our computer economy will be increasingly important to more and more customers of all classes, as microprocessors make their way into every facet of our national economic life.

Security’s increased importance is obvious, as we must now face the possibility of deliberate terrorist disruption of our increasingly important electrical systems.

The security potential of distributed generation technologies should make their integration into U.S. markets an immediate priority.

### **State and Federal Partnership Needed**

But so far, there is no coherent federal or state strategy in this area. Over the years, we have seen a proliferation of reports warning of terrorist related harm to our power systems. But without any harm, no action was taken. Now, we have seen the tremendous harm that can be done to buildings and life, but our government’s focus has largely been on conventional power strategies that have changed little since World War II. Little action has been taken on basic power-related security measures on-site.

What is needed is a new partnership between the states and the federal government to create an energy security initiative for our critical public and private facili-

<sup>36</sup>Associated Press, “New Momentum for Alternative Fuels,” Oct. 26, 2001.

<sup>37</sup>Christensen, Clayton M. The Innovator’s Dilemma: When New Technologies Cause Great Firms to Fail. Boston, MA: Harvard Business School Press, 1997.

<sup>38</sup> “States Emerge as Clean Energy Investors: A Review of State Support for Renewable Energy” by Mark Bolinger, Ryan Wiser, Lew Milford, Michael Stoddard and Kevin Porter. *The Electricity Journal*, November 2001. Available on the web-site of the Clean Energy States Alliance, at [http://www.cleanenergystates.org/CaseStudies/bolWiserSbcEj\\_2001.pdf](http://www.cleanenergystates.org/CaseStudies/bolWiserSbcEj_2001.pdf).

ties.

We propose the outlines of such an initiative here.

Many states, as part of their electricity deregulation actions, have established clean energy funds to support the use of newer and cleaner energy technologies. These funds will invest nearly \$4 billion over the next several years to create jobs, develop indigenous energy resources and protect the environment.

Many of these new technologies benefit the homeland security mission as articulated by the President. Utilization of distributed energy such as solar and fuel cells can harden telecommunications, secure pipelines and enable emergency preparedness operations such as police and fire to operate when power lines are down or pipelines are inoperative.

Many critical public facilities have existing limited power protection; often a single diesel generator is all that stands between operation and blackouts. In some cases, no added protection is available at all.

These clean energy funds are exploring ways to cooperate regionally and jointly deploy their resources to lower technology costs and increase the quality and quantity of clean energy installations.<sup>39</sup> These state funds could be deployed to leverage federal investments in security. A new partnership between states and the federal Office of Homeland Security could lead to greater energy security at critical facilities.

In particular, there are many instances where use of these technologies could create more protective energy systems in "critical" public and private facilities that serve homeland security missions. These applications include:

**a) Utility/Telecom Security:**

- hardening and back-up power for repeater stations
- pipeline cameras and sensing equipment (molecular sniffers)

**b) Public Space and Transportation Security**

- remote power for sensing and camera units in parks, bridges and reservoirs
- independently powered street and area security lighting, including parks, bridges, key roadways, and tunnels
- independently powered railroad crossings, lights, marine and river-way lighting

**c) Emergency Preparedness**

- reliable power for data centers, telecommunications, 911, emergency bunkers, hospitals and other critical public emergency facilities
- drop and plop electric generation units, which are very movable
- drop and plop water pumping units
- quick-fasten solar-powered traffic signal lights

Other security applications need to be explored, but to date neither the federal government nor the states have systematically identified where these critical security power needs could be met with more resilient, distributed power sources.

A partnership of state and federal officials, with federal and state fund support, could do the following:

- 1) Identify Critical Facilities.** States would identify critical federal, state and local facilities where further investigation of the economic and engineering issues could lead to installation of clean energy technologies such as solar and fuel cells to enhance security.
- 2) Evaluate Feasibility of Installations.** The states would conduct feasibility studies to determine the practical costs and benefits of clean energy installations to reduce power related security risks, and make available financial support to help defray capital costs of installations.
- 3) Joint Purchasing and Deployment.** If a multi-state deployment program is developed, the states could aggregate purchasing of technologies (solar panels or fuel cell systems) to reduce overall costs and otherwise obtain favorable terms and conditions.
- 4) State and Federal Partnership.** States and the federal government could share financial, technical and other resources in a partnership arrangement to raise the needed capital make these facilities more energy secure with these technologies.

<sup>39</sup> "Clean Energy Initiative: A Report on How Foundations, State Funds, and Social Investors Could Pursue Joint Investments." Prepared by Lewis Milford, Philip LaRocco, and Robert Sanders, July 2003.

### Conclusion

If the U.S. is to meet the challenge posed by the vulnerability of our energy systems, a new appeal to energy security is needed. Fuel Cells and PV are potential aids in seeking security, but other useful technologies include micro-turbines, diesels, and UPS systems. Which technologies are most practical will depend upon competitive factors such as public funding and support, reliability, environmental constraints and benefits, operating and capital costs, availability and other factors.

Such technologies would address two related issues: energy independence and increased security. The energy independence of the United States could be greatly increased through many domestic measures to lead us away from our dangerous dependence on oil and therefore on the Middle East, such as domestic uses of technologies like fuel cells that could lead to reduced oil use in transportation and power projects. Increased building security, on the other hand, can be achieved through onsite distributed generation technologies and the use of reliable backup systems. The decentralization and dispersion of U.S. energy production could address both goals, providing for greater long-term security of the United States.

An organized national strategy, arising from a partnership between state and national governments, for the increased use of clean energy technologies in U.S. markets would create jobs, slow environmental degradation, and help to secure the U.S. economy from terrorist disruption. A partnership could begin to create a more sustainable and secure energy future for the US, while enhancing the safety of all Americans. It is time to start a dialogue that brings about these benefits now.

### **About the Author**

*Lewis Milford is a lawyer and President of Clean Energy Group (CEG), a non-profit organization he founded in 1998. CEG's mission is to increase the use of cleaner energy technologies in the U.S. and abroad through creative financing, business partnerships, public policy and advocacy.*

*CEG works with public officials from around the U.S. that are responsible for over \$3.5 billion in new clean energy funds in a project originally called the Clean Energy Funds Network, and now called the Clean Energy States Alliance ([www.cleanenergystates.org](http://www.cleanenergystates.org)), which was developed to help fund officials create and coordinate efforts to expand clean energy markets. CEG manages the Clean Energy States Alliance, a new nonprofit organization, assisting these funds in multi-state strategies. CEG is also managing the Public Fuel Cell Alliance (PFCA), which will develop an information clearinghouse, create joint state and federal funding initiatives and pursue related activities that will improve the quality of joint state and federal efforts to promote fuel cells. CEG also works with public officials in Europe interested in trans-Atlantic efforts to build clean energy markets.*

*Mr. Milford has a Juris Doctor from Georgetown University Law Center and is a Phi Beta Kappa graduate of Rutgers College. He is married with two children. His family lives in Middlesex, Vermont.*

*Ruth O'Meara-Costello assisted Mr. Milford on this article. Ms. O'Meara-Costello is a student at Harvard Law School, class of 2006, and an honors graduate of Harvard College (2002). She was a summer intern with Clean Energy Group in 2002 and 2003.*

### **Related Courses**

#### **New Realtime Distance Learning Courses**

##### **3D Load Profiling Using Interval Meter Data**

*Date(s): March 15, 2004*

[www.aeecenter.org/realtime/LoadProfiling/](http://www.aeecenter.org/realtime/LoadProfiling/)

##### **Performance Contracting 2003**

*Date(s): January 7 and April 20, 2004*

[www.aeecenter.org/realtime/PConline/](http://www.aeecenter.org/realtime/PConline/)

##### **Realtime Energy System Integration**

*Date(s): February 9, 2004*

[www.aeecenter.org/realtime/RTsystems/](http://www.aeecenter.org/realtime/RTsystems/)

Or visit [www.aeecenter.org/relatime](http://www.aeecenter.org/relatime) for information on all realtime courses