LIGHTS OUT by Ted Koppel
A Book Report and Comments by David G. Schwartz, M.D.

So why discuss electric power outage as a health issue? Wearing seat belts, not driving drunk or distracted, wearing hard hats and helmets, keeping poisons out of reach of children, training in swimming and water safety, firearm safety, hazardous materials and fire safety, preventing falls, etc., all are vital health issues. "Safety First," and "Be Prepared" are well known clichés that demand our respect. Preparing for a possible (and probable) extended electricity outage is a part of that. Discussing broccoli vs. cookies has no relevance when food is all gone. Getting annual flu shots fades in relevance when confronted with typhoid or cholera.

I intend for Ted Koppel's warning not to be a "voice crying in the wilderness." This issue demands our careful attention, because our health, safety, and physical survival could be put at stake suddenly without warning.

A cyber attack on the electrical power grid could leave large segments of the country without electricity for several months, and depending on how the disaster is handled, a majority of the population could perish.

Ted Koppel is not a "prepper," or a doomsday forecaster. A forty-two year veteran of ABC News, noted by New York University to be one of the top 100 journalists of the past hundred years, recipient of 8 Peabody awards, 42 Emmys, and numerous other awards, he points to a crisis that has not been given due attention. He felt it his responsibility to bring it to the fore. This book deserves to be a best seller. It is immensely readable, it has an engaging narrative, and it calls us to action.

Why sound such an alarm bell? Is this paranoid hysteria? Unfortunately it is not. We can only solve problems like this if we confront them directly and stare the facts "in the face," without sugar coating.

An electrical power outage of this magnitude would have consequences far beyond any hurricane, flood, blizzard, volcano, or earthquake. Current disaster preparedness plans show no resemblance to what would be needed in this type of cyber-attack. This would be an act of war, likely perpetrated by an anonymous enemy with a poorly traceable origin.

This calls us to do what can be done to prevent terrorism and terrorist attacks in general, to repair the vulnerable power grid, and to have national, state, local community, family, and individual disaster plans in place.

Our whole modern society's functioning is almost totally dependent on electricity, without which it could be suddenly thrust into the 19th Century. Without a 19th Century infrastructure to support it, that could be catastrophic.

Why is the grid so vulnerable? Its functioning is entirely dependent on --- THE INTERNET? (You've got to be kidding!). Yes, really, the Internet. Whose crazy idea was this? The Internet was originally designed for ease in communication, and security was not included in the equation. It has never had good security since then. In using the Internet to control the electrical grid, efficiency was chosen as the main purpose. This complex network of electrical power companies sharing electricity with each other to make smooth flow of current to consumers and industry (and the military!) was not designed with security or resiliency in mind. That would have been too expensive, would cut into profits and would result in much higher rates paid by consumers. Granted, many of the large power companies have spent billions to provide security against cyber attacks, but the smaller providers cannot afford that expense, and the system is only as strong as the weakest link. Taking down a small supplier would have a domino effect on the whole system, because of the extreme interdependence of every facet of the grid. From our experience so far, we know by now that there is no computer system so secure that a hacker cannot eventually break into it. Multiple suppliers and fluctuating demand require constant coordination by computerized systems to keep a balance between demand and supply. An irregular power surge could cause lines to melt and could destroy transformers. Automatic shut-offs are built in to prevent damage in case of dangerous irregularities in current flow. Hackers could shut down these automatic shut-offs and could prevent information to reach the monitors so that no one would know that the meltdown was occurring, leading to further damage. This was what happened in the Stuxnet cyber attack on Iran's centrifuges by the U.S. and Isreal. The damage went undetected until it was not repairable.

Mr. Koppel explains in detail the vulnerability of the Large Power Transformers (LPT's) needed for transmitting electricity over long distances in huge power lines. Many of the LPT's are antiquated. All of them are vulnerable to destruction by electricity overload; they are out it the open, vulnerable to damage by semiautomatic rifles, and they could not be quickly replaced. Why not? They are not uniform, and each is custom made and could take months to build. They cannot be transported on railroads because they are too large and heavy. Shipped on highways, one would take 2 lanes of traffic, a trailer 70 feet long with 190 wheels. This is one of the major reasons why significant damage to the grid could take months to repair.

Now, granted, a cyber attack of this magnitude would require a highly sophisticated knowledge of the electrical grid with painstaking preparation, time, and expense, and would need expert hackers. Several countries already have that capability, and terrorist organizations are in the process of acquiring it. ISIS probably has the financial means to purchase the expertise needed. It is not like cyber attacks are anything new or unexpected. Cyber attacks of various types go on every day across national boundaries, costing billions of dollars to commerce and industry. The U.S. ability to wage war against countries with this ability is essentially held hostage. Any attack by the U.S. would be subject to retaliation. This country, which has not had war on its own soil since the Civil War, could now experience that. North Korea is not subject to counter cyber attack because it has little electricity. Also terrorist groups have little vulnerability because, like North Korea, they have nothing to lose. Cyber attacks could level the

battlefield between large and small countries. If Saddam Hussein had had that capability to do cyber attacks in 2003, the Iraq invasion could indeed have become "the mother of all battles." Live in a glass house and throw stones? It makes sense not to make any more enemies, given this vulnerability. We have to recognize that the Internet can be used as a WMD (Weapon of Mass Destruction). In my opinion, to give the control of the power grid over to the Internet is like giving one's personal life support system to a random rotating group of strangers, some of whom could be criminal gang members.

Mr. Koppel says it is difficult to alert the public about an impending crisis, especially when the topic is complicated and defies brief explanation. People think there are experts we can defer to. In my opinion, if there are any experts, they are "asleep at the switch." In a democracy, before the experts can act, they need to be goaded by the people, or at least be given permission. In order to make the grid secure, much taxpayer expense and a lot of individual and industry privacy and autonomy would have to be given up to have such an extensive overhaul or rebuilding of the grid, requiring months of work. A lot of efficiency would have to be sacrificed. Constant surveillance of every corner of the grid would be necessary.

In 2010 the House of Representatives passed legislation to work on repairing the vulnerabilities of the electrical system. It has been stuck in the Senate, where it has been bogged down ever since, over issues of cost and privacy. Conflict between government regulators and industry has impeded coordinated action. Local companies are not covered by federal regulation. Only if the public is aware of the enormity of the threat and is committed to fixing the problem, will government act, and industry will need to cooperate, and small companies will have to be subsidized.

Well, what is the probability that such an attack will occur? The author quotes Janet Napolitano, former chief of Homeland Security, when asked what are the chances that a nation-state or an independent actor could knock out one of our power grids, she replied, "Very high, 80-90%." No insurance company or re-insurer is willing to cover the consequences of such an attack, mainly because it is nearly impossible to assess the risk and its costs. If such insurance were available, the premiums would be prohibitively high.

As with repairing the vulnerability of the grid, a similar deficiency is in responding to such a disaster after it occurs. FEMA is ill prepared to deal with a crisis on such a massive scale, as we have witnessed its deficiencies in smaller crises. Industry and business are not prepared to do their part Millions of gallons of fuel in underground storage tanks could not be pumped out because gas stations cannot afford to have back up diesel generators. Stockpiles of "meals ready to eat" in warehouses lose value over time, and manufacturers don't want to store up a massive backlog that would expire if not used. Other major relief organizations like the Red Cross would be incapable of responding adequately to such a prolonged disaster.

Some groups like "preppers" constantly prepare for emergencies by having extra food, water, first aid supplies, tools, etc., and some have farms, gardens, and ponds for fish, and

guns for hunting wild game. They would not have enough to share with large numbers of people.

The author's visit to the Church of Jesus Christ of the Latter-Day Saints (Mormons) in Salt Lake City revealed a model of disaster preparedness unparalleled by any other group or government. Having a history of being subject to persecution and attack, and having had to move as refugees from one state to another, it is a strong tenet of the church to be well prepared for disasters.

The church encourages families to keep several months supply of food and water stored. It has a huge distribution center that makes Wal-mart's look like a 7-11, and smaller centers are positioned throughout the country. Its trucking system can move supplies almost anywhere, and has the best safety record of any trucking system. Its response to Hurricane Katrina put the federal government to shame. While FEMA was floundering, the church had evacuated almost all of its 2500 members before the storm hit, and it distributed supplies in an orderly fashion to people who needed them. The church has 52 farms, ranches, and orchards, 12 canneries and processing plants, and dairies with 5000 cows. They give away approx. $145 million worth of food annually, and they sell about 60% of what is grown. In the event of a massive crisis, instead of the food being sold, it would be distributed to the members in need. The church is relatively independent of any out side supplier. Although the church provides for its own, it also encourages its members to share with other neighbors in need who may not be members.

In regard to the question of defending itself with weapons against looters and lawless armed gangs, the church's position is that it leaves that area to the law enforcement of the state. Individuals are instructed to make their own decisions based on their particular guidance from their Heavenly Father regarding that issue.

So the Mormons have probably the best model for disaster preparedness, but it may be a long shot to emulate their system, since it depends in a hierarchical power structure unparalleled by most any other organization except the military.

In the event of such a major crisis, the military would have responsibility to maintain order and probable would be the organization most able to deliver massive amounts of food to tens of millions of people. Then the question is whether the military itself would have sufficient numbers of personnel.

The author does not propose details of how the nation could adequately respond to such a crisis, but he makes a case for industry and government to find common ground to work out a plan for distribution of supplies and for citizens and industry to give up some degree of privacy for security, both for surveillance of the grid to prevent a cyber attack, but also to respond to the aftermath of an attack. He says public awareness is the key to repairing the vulnerabilities proactively, instead of waiting until a crisis happens, as is too often the way it goes.

I would make some recommendations of my own, some of which are proposed in the book, others not.

1. Stop making enemies. This is the proverbial "elephant in the living room" that few choose to look at. Terrorism is the cost of empire. I'll save the elaborating on this for near the end of this article, as it is rather lengthy.
2. Failing that, the fallback position is defense. The most logical step would be to repair the electrical grid. Privacy concerns and rights would have to be subservient to survival, and there would have to be sharing of information between industry and government to get the job done. The NSA would have to be granted powers of surveillance of the entire grid, since an attack on it would be an act of war. Public pressure needs to be brought to bear on the Congress to work on repairing the system. The electrical grid needs to be broken up into smaller, disconnected systems, a more decentralized system. This would be more costly and would be less efficient, but much safer.
3. Rehearsals need to be run regarding plans for providing food, water, sewage disposal, shelter, evacuations, policing, etc. This needs to be coordinated with the Dept. of Homeland Security, the NSA, the military, state agencies, local community organizations, families, and individuals, with as much or more intensity than the Civil Defense rehearsals during the cold war regarding preparing for a nuclear attack, or the air raid drills in London during the German bombing in WWII.
4. All hospitals, nursing homes, educational institutions (which could be converted to shelters) fuel repositories, and vital government buildings, fire departments, rescue squads, etc. need to be equipped with photo-voltaics with battery backup as well as diesel generators with abundant storage of diesel fuel.
5. All new buildings need to be required to be equipped with photovoltaics with batter backup for partial coverage of electrictiy needs for basic survival.
6. For individuals, in weighing the advantages of urban vs. rural life, this may tip the balance toward rural, where wood stoves and solar ovens can cook food and heat water, in addition to warming the house. Rural life may allow more solar access for photovoltaics and may provide more opportunity for gardening, raising animals, hunting, sewage disposal, shallow wells or springs or creeks or ponds (with water purifiers), etc. Urban dwellers may want to pursue community urban gardens, rooftop gardens. Choosing where to live may include avoiding desert areas (such as Las Vegas) where water supply is scarce and depends on large municipal supplies. Choose to make friends with Mormons, the Amish, Native Americans, preppers, and other groups that have experience with self-sufficiency, food storage, and non-electric lifestyles. Encourage children to join the Scouts. Connect with your neighbors. Discuss assisting each other in times of need. Stock up on supplies of freeze-dried food and encourage them to do the same, with more than enough supplies for yourself to share with others.
7. If considering whether to join the Peace Corps or similar organization or working for an NGO like Oxfam that works with people in developing countries for sustainable development and food production, this may tip the scales toward doing that, at least until the threat level goes down in this country.

Now, to elaborate on #1:

The U.S. has many times facilitated the overthrow of democratically elected governments, helped establish oppressive regimes, has invaded many countries, and has kept military bases all over the world, sometimes trying to act as "policeman of the world," all in the name of protecting our "interests" which means the financial, economic, political empire, for the purpose of importing cheap goods. Read Andrew Bacevich's book, The End of Empire. Terrorism is most often the result of a people being occupied by a foreign country. ISIS is not fundamentally about religion. A vast majority of Muslims oppose it and all that is stands for. Religious fanaticism can be a convenient organized channel to funnel the frustration of people who are exploited economically and feel dominated and invaded by a foreign culture of materialism and moral and ethical depravity, with global corporations exploiting them, grabbing their farmlands, having no compassion and disregarding basic human rights. People do not want to kill us to get what we have. They want us to stop ramming our materialistic culture down their throats. Many young people in this country are repulsed by the shallow materialism, greed, glamour, the lack of moral compass, in our culture, and they are drawn to a radical religion that gives them structure and goal to strive for that goes beyond self. If we had a culture that inspired young people to be committed to goals and aspirations that go beyond self, for the good of all people and the planet, they would be attracted to positive idealism instead of to violent religious sects.

These are some of the things we need to address if we want to stop making enemies and stop breeding terrorism. Culture change can take a long time, but we are seeing positive developments in that direction, away from the ideology of materialism, selfishness, and addictions, toward compassion, justice, and cooperation. When the positive change takes over, it may still be a long time until terrorism fizzles out for lack of a huge enemy to react to. Meanwhile, the fallback position is, "Be Prepared."

Ted Koppel's book is a "must read" for anyone who puts "Safety First," regardless of whether you agree with my assessment of the situation.