THE STORMRIDER ISSUE 21

Freedom and Country Living and Power Grids

THE STORMRIDER ISSUE 21

How come it’s so dark in this picture. Alright who is the wise guy who took out the power grid?! But seriously, my prepper friends, are you ready for power grid sabotage? I have some helpfull information for you to consider. God bless you!

Shawn Stevens

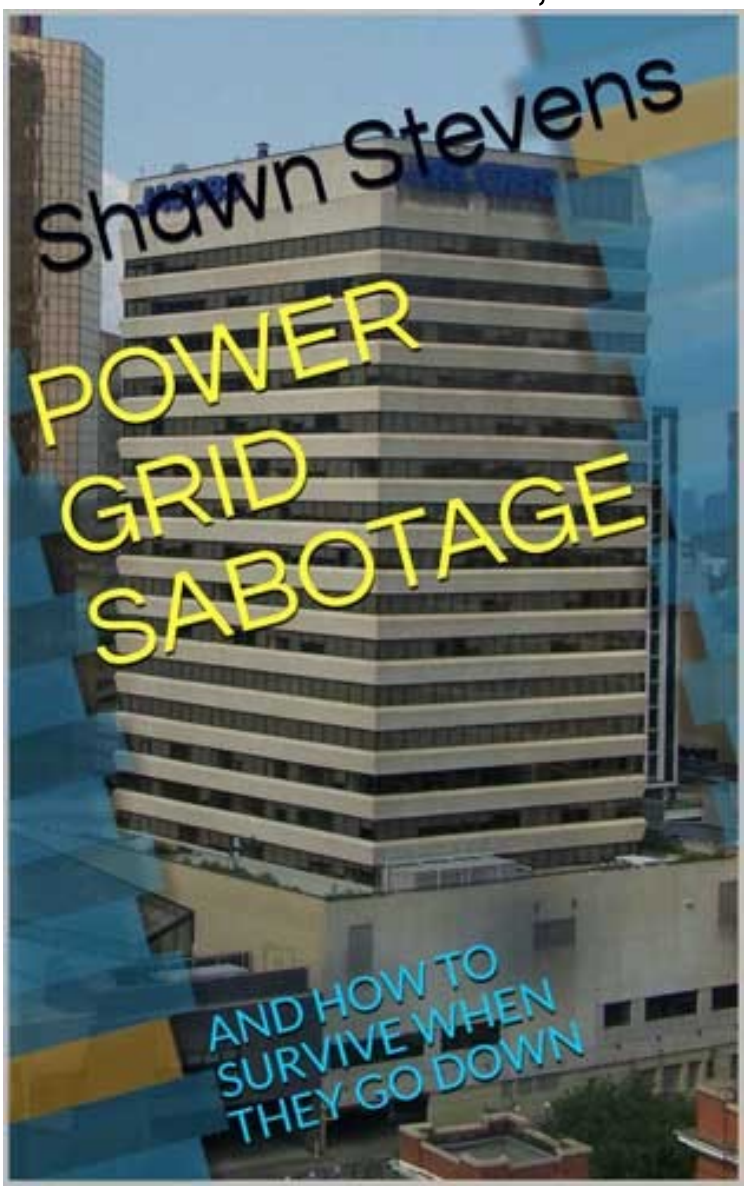
Visit our website: https://hobbyhomesteadingprepper.ca/

PREPARING FOR POWER GRIDS BEING TAKEN DOWN

Most of us have experienced a blackout. We understand and accept the temporary inconveniences when a power station is experiencing a short circuit. However, what is our response to having a catastrophic failure of an entire electrical system of a city or of multiple cities? What if the cause for such a failure is found to be fowl play, foreign interference or even a terrorist strike? I invite you to purchase my e-book "POWER GRID SABOTAGE AND HOW TO SURVIVE WHEN THEY GO DOWN."

Our power grids are susceptible to four kinds of attack, a cyber attack, logic bombs, a kinetic attack and an EMP. Cyber attacks are the most common type of attack to a grid system. This is where a hacker is trying to hack into our grid system and in some way reprogram the system so that it will fail. A second kind of attack is a "logic bomb." This is where a component of a computer system has been made by a foreign country and the government of that country has had that component altered so that hidden malicious software will activate at their command. Power grids can also shut down by kinetic attacks which are actual physical attacks on a power station. Lastly, and most ominously, a entire grid system can theoretically be taken out and rendered inoperable by an EMP attack. Nuclear weapons let out

electromagnetic pulses when they detonate. Such pulses destroy electronics. It is believed that if a high yield nuclear weapon was detonated 40 to 400 kms above the earth's surface it could emit an EMP capable of destroying the electronics of an entire Continent. Russia has conducted low yield EMP experiments, or at least one that we know of, over its own territory.



In my book "**POWER GRID SABOTAGE AND HOW TO SURVIVE WHEN THEY GO DOWN**" you will learn more about these types of attacks and more importantly, what you can do to protect your family if we ever loose our grids.

In this book you will learn:

- Has Canada ever experienced a serious crash of it's power grid system?
- Is the Canadian power grid system independent of the American power grid system?
- How are power grids susceptible to being hacked?
- What is a Logic Bomb? What is an EMP attack?
- Have the power grids of other nations been taken down by cyber attacks?
- How do we prepare for loosing powergrid electrical power?
- Things that you can buy to prepare yourself and your family for a crashing of the power grid system
- Things that you and your family can do during an electrical blackout.
- And more!

WHEN THE POWER GRID GOES DOWN

Electrical power, we use it to run appliances, run computers and just about every type of machinery. Some even use it to power their cars. What happens when it is gone and not just gone for a little while? What if our power supply is gone, knocked out, by some unexpected cause and is not coming back anytime soon?

Most of us have experienced a blackout. We understand and accept the temporary inconveniences when a power station is experiencing a short circuit or a power line is torn down in a storm. However what is our response to having a catastrophic failure of an entire power station or of a cascading failure of more than one plant but of an entire electrical system of a city or of multiple cities? What if the cause for such a failure is found to be fowl play, foreign interference or even a terrorist strike?

Some would say “Oh that would never happen here” or “Our government will take care of us should something like that ever happen.” Friend, we live in a fragile world. There are many forces at work in our world that would like to see our society be held hostage or even collapse. The power grids that our cities depend on are vulnerable to many threats. Natural disasters like

earthquakes and solar flares also have potential for rendering a power grid inoperable.

Cities are dependant on electrical power. The problem with this kind of dependency is that computers, satellites and even power grids contain vulnerable electric components which can be tampered with by hackers on the other side of the world. Transportation, communication, fuel supply, energy supply and even food and water supply are all vulnerable to disruption when they are targeted by hackers. Many preppers have seen the need to prepare for cyber attack.
So how do we handle loosing all power? The key to mitigate the impact of such a loss is to prepare for it in advance. My short list of things to buy is this:

•An electric generator. A generator is simply a device that converts motion power into electricity for use. You can purchase gas or diesel powered ones from many hardware sources. Some places will rent them.

•Propane powered stoves and other equipment. Many camp stoves, barbeques, RV stoves, etc use propane, a cheap alternative fuel.

•Solar Panel Systems. These are the ultimate in alternative energy. Solar panel systems can be installed

on homes, rvs and other places providing power from the sun.

•Wind turbines. These work like solar panels just they get power from the wind and not the sun.

This is my shortlist. For a longer list consider purchasing my e-book "**POWER GRID SABATOGE AND HOW TO SURVIVE WHEN THEY GO DOWN**."

SAVE THE POWER GRIDS

Are our power grids safe? Is anything being done to protect them? Most people are either unaware that power grids can be made more secure or they have never thought about it. When a power grid is beefed up with security and infrastructure upgrades it is called the "hardening" of a grid. Have Canada's grids been hardened?

In trying to find out whether our grid system has been hardened I went to the Canadian government website and surfed through their search box for articles on Canadian power grids. Here, I found information stressing the importance of grid security and grid hardening. In the summary of a report by Mourad Debbabi, who chairs the NSERC/ Hydro-Quebec/Thales Industrial Research in Smart Grid Security, we are told

“Recent cyber security incidents demonstrate that smart grids could be subject to debilitating and disrupting attacks that might have severe security and economic consequences, and even endanger human lives.” 1 What can be done to defend human lives and mitigate the security and economic consequences of power grid attack? First, we need to understand that there are a couple of components to power grid systems that are especially important. These components are Large Power Transformers (LPT) and Supervisory Control and Data Acquisition Systems (SCADAS). These are especially important because they are absolutely critical to the operation of power plants.

LPT's are gigantic in size and have to be disassembled and reassembled for transport. They are typically transported by rail but regular rail cars are not sufficient to handle their weight. Railways typically can handle loads of 100 tons. However, LPT's can be two or three times that weight. Special rail cars called Schnabel railcars are brought in for these kinds of loads. These transformers cost millions of dollars. They are not mass produced but, rather, are custom assembled and this process can take between five months to five years. Supervisory Control and Data Acquisition Systems (SCADAS) are critical to the operation of power plants. This component is a control system made up of computers, networked data communications and graphical user interfaces (GUI). They are used in almost

any computerized infrastructure, not only in power grids. Grid systems use thousands of them. Not all SCADAS are connected to the internet but those that are are a point of vulnerability even if they are supposedly protected by firewall or VPN solutions.

How do you harden your power grids? One way is to protect these two components, LPT's and SCADAS. The electronics of SCADAS and LPTs, along with any electrical components, can be protected from electromagnetic pulses by encasing them in metal. This is known as a faraday shield. Can these components be encased while they are still in use? Not necessarily. What this means is that we need to have a large supply of SCADAS on hand stored in faraday shielded structures. We also need to have backup LPTs that are not in use but stored and shielded so that they can be utilized in event of an electromagnetic pulse.
SCADAS and LPTs are not the only components that should be shielded. We should have back-up fuel generators and backup vehicles and machinery that can move components around in time of a shut-down.
As well as shielding components, there are surge arrestors and blocking devices that can be added to grid systems. All of these measures can be used to effectively harden our grids and make them truly “smart grids.”
Shawn Stevens

Endnotes
1)https://www.nserc-crsng.gc.ca/Chairholders-TitulairesDeChaire/Chairholder-Titulaire_eng.asp?
References
https://www.nserc-crsng.gc.ca/Chairholders-TitulairesDeChaire/Chairholder-Titulaire_eng.asp?pid=981
https://www.energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf
https://en.wikipedia.org/wiki/SCADA#Security_issues
https://en.wikipedia.org/wiki/Faraday_cage
Dr. Peter Vincent Pry. Blackout Wars.State Initiatives To Achieve Preparedness Against An Electromagnetic Pulse Catastrophe. icgtesting.com. Printed in the USA.LVOW03s0009090816 499513LV00037B/626/P

LOOKOUT POWER GRIDS! EMP AND A REVOLUTION IN MILITARY AFFAIRS

An Electromagnetic Pulse, EMP, is what occurs every time a nuclear weapon is detonated. An EMP destroys electronics of every kind. It is now known and understood that the effects of EMP are increased if they are emitted from a high altitude. It is theory that a large nuclear weapon detonated 40 to 400 kms above the earth's surface could emit an EMP capable of destroying the electronics of an entire Continent. The Russians have been studying EMPs for a very long time. In the years of 1961 and 1962, the USSR conducted what is know as the K project, nuclear tests in which they detonated a 300 kiloton nuclear weapon over their own people at an altitude of 290 klms. This created a massive EMP and did much damage. A great deal of study has been done on EMPs since that time.

It is understood that with every generation there are technological advances to military weaponry. Modern weapons can sometimes make older weapon systems ineffective. One example of this was in Germany in World War II. Hitler utilized a rapid strike, multi-pronged system of attack that involved airpower, mobile infantry, armoured divisions and artillery in a highly coordinated way. It was called Blitzkrieg. Most of Europe was not ready for Blitzkrieg and fell quickly. It was a long hard battle to win it all back.

Ever since the time of WWII, military leaders have been devising their own types of Blitzkrieg plans. Nikolai Vasilyevich Ogarkov, former Marshal of the Soviet Union, began theorizing about what he called the Military Technological Revolution. This drew much attention from the United States Defence Department who spinned off of Ogarkov's ideas and coined the phrase “A Revolution In Military Affairs” to describe their own system of highly coordinated, multifaceted attack strategy. The concept was also applied to the plans and tactics of other nations, not just the United States.
For a long time now it has been suspected that Russia has EMP as part of its own strategy for a revolution in military affairs. The decisiveness of a first strike, an EMP strike, is something that a victim nation would not likely be able to recover from. A rapid first strike that disabled all electronics in North America followed by a

land, sea, and air invasion would truly be a revolution in military affairs.

Iran has expressed much interest in EMP technology and the international community is concerned that this technology does not fall into the hands of North Korea either. The United States was very concerned when on April 16, 2013, North Korea orbited its KSM-3 satellite on a trajectory over Washington and New York at the ideal altitude for an EMP mega-disaster. If such a satellite had been housing a nuclear weapon it is theorized that it could have wiped out North America's Eastern power grid. North America's Eastern grid also supplies much of our energy supply in Canada.

Shawn Stevens

References

https://en.wikipedia.org/wiki/Revolution_in_Military_Affairs
https://en.wikipedia.org/wiki/Soviet_Project_K_nuclear_tests
Dr. Peter Vincent Pry. Blackout Wars.State Initiatives To Achieve Preparedness Against An Electromagnetic Pulse Catastrophe. icgtesting.com. Printed in the USA.LVOW03s0009090816 499513LV00037B/626/P

DON'T LET YOUR NATIONAL POWER GRIDS SUFFER A KINETIC ATTACK

There are many ways that a power grid can be attacked. It can be hacked into and suffer cyber attack. It can be logic bombed. It can be walloped by an Electromagnetic pulse. It can suffer a kinetic attack. A kinetic attack, simply put, is an actual physical attack on a power grid. Does this happen?

Yes this happens.On June 9, 2014, The entire country of Yemen, a country of twenty-four million, lost power to all of its sixteen cities when terrorists destroyed key transmission towers. This is the first time that a nation has had its entire electrical system taken out.
On January 25, 2015, eighty percent of Pakistan lost power due to terrorists destroying key transmission towers. Then there is the Metcalf Incident.

The Metcalf incident happened on April 16, 2013. A mysterious sabotage attempt was conducted on a transformer substation in San Joes, California. The North American Electric Reliability Corporation and the Utility Pacific Gas and Electric later referred to it as merely an act of vandalism and it, initially, did not get much attention by the press. However, when the Federal Energy Regulatory Commission conducted an investigation they discovered that a very sophisticated attack had been conducted. The attackers used an

underground communications tunnel that they accessed through a manhole and they disabled communication cables and the 911 cable. They shot up the substation with AK-47 rifle fire in key places where the system is most vulnerable. Then they escaped without being detected. What is the significance to Metcalf? This power station is crucially important, sending power to Silicon Valley.

Kinetic attacks are very bold. They are active warfare and may involve lethal force. They may be conducted by terrorist organizations, organized crime or foreign governments. While we hear a lot about cyber security and cyber protection, let this not be the only protection that our government uses to defend power grids. It would be ironic to have all of the cyber firewall and VPN protections in place only to have a hooded man cut through the light-duty chain fencing around our power grids and shoot up our power stations.
Kinetic attacks are actual physical attacks and they should be defended against by actual physical security measures. Armed guards, physical barriers, alarm systems and other measures may be employed to defend our power grids.

Shawn Stevens

References
Dr. Peter Vincent Pry. Blackout Wars.State Initiatives To Achieve Preparedness Against An Electromagnetic Pulse Catastrophe. icgtesting.com. Printed in the USA.LVOW03s0009090816 499513LV00037B/626/P
https://en.wikipedia.org/wiki/Kinetic_military_action

JUST WHEN YOU THOUGHT YOUR POWER GRIDS WERE SAFE – RADIO FREQUENCY WEAPONS

What are Radio Frequency Weapons (also called direct energy weapons)? Electromagnetic radio frequency emitters are components of many products that we use today such as wireless computers, Global Positional Systems, cell phones, etc. However, radio frequency emitters can be weaponized to interfere with or even damage electronics.
Power grids are not immune to radio frequency weapons. Disruptive radio emitions can cause systems to fail. The consequences of this depends on what system is targeted and how critical that system is to operation. The trend today is to make power grid systems more and more automated and for them to require fewer and fewer operators to run them. The danger of this is that the more automated the system, the greater the chance of the entire system crashing rather than just a component.

There are different types of radio frequency weapons. One type will emit a constant emition that causes ongoing disruption while the device is on. Another kind of radio frequency weapon will emit a strong signal in one great burst designed to do permanent damage. Radio frequency weapons can be disguised as a package, a briefcase even a pop can. Larger ones can be inside a utility truck as the operator poses as a utility repair technician. These weapons are so attractive to terrorists and governments because they can be so covert. Also, they can be remotely activated. Also, they can work through walls and other obstacles.
Radio frequency weapons could do havoc to Canadian power grid systems. By creating a large open monitored areas between power plant equipment and parking lots, and other public areas it may be possible to diminish their effectiveness. The closer they are to the power plant itself, the more effective these weapons are.

Shawn Stevens

References
https://en.wikipedia.org/wiki/Directed-energy_weapon
Pry, Peter, Phd. Blackout Wars: State Initiatives To Achieve Preparedness Against An Electromagnetic Pulse (EMP) Catastrophe icgtesting.com. Printed in the USA.LVOW03s0009090816 499513LV00037B/626/P
The Threat of Radio Frequency Weapons To Critical Infrastructure Facilities. TSWG & DETRO PUBLICATIONS. 2005. https://apps.dtic.mil/dtic/tr/fulltext/u2/a593293.pdf