

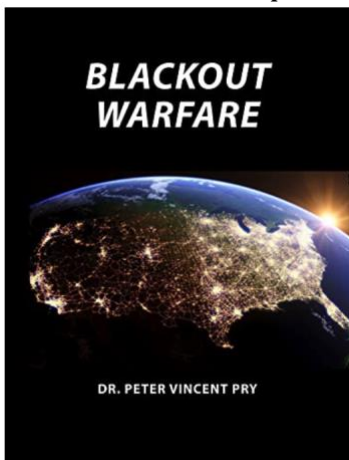
Posse+Plus, Wood County Texas

Blackout Warfare and EMP Preparation

Blackout Warfare: Attacking The U.S. Electric Power Grid A Revolution In Military Affairs
How to Prepare for an EMP Event (pages 19-26)

Introduction

“Blackout Warfare” is the term used in this report to describe a revolutionary new way of warfare planned by Russia, China, North Korea, and Iran that is still little understood in the United States, but poses an imminent and existential threat to Western Civilization. These



potential adversaries describe their new way of warfare as “Non-Contact Wars,” “Total Information War,” “Cyber Warfare” or “Electronic Warfare” but the focus is all the same—using cyber-attacks, sabotage, and electromagnetic pulse (EMP) weapons in combination to blackout national electric grids to achieve quick and decisive victory.

The Congressional EMP Commission describes this unprecedented new threat well: “Combined-arms cyber warfare, as described in the military doctrines of Russia, China, North Korea, and Iran, may use combinations of cyber-, sabotage-, and ultimately nuclear EMP-attack to impair the United States quickly and decisively by blacking-out large portions of its electric grid and other critical infrastructures. Foreign adversaries may aptly consider nuclear EMP attack a weapon that can gravely damage the U.S. by striking at its technological Achilles Heel, without having to confront the U.S. military.”

BLACKOUT WARFARE
Attacking The U.S. Electric Power Grid
A Revolution In Military Affairs



Dr. Peter Vincent Pry

With An Introduction By

Dr. William R. Graham and Ambassador R. James Woolsey

CONTRIBUTORS

Admiral William O. Studeman (Retired)

Ambassador Henry Cooper

Congressman Curt Weldon

Dr. William A. Radasky

Colonel Robert P.J. Lindseth (Retired)

Colonel Kevin Riedler (Retired)

Dr. Edward M. Roche

Michael Mabee, CSM USA (Retired)

Professor Zhanna Malekos Smith, Esq.

Professor Cynthia Ayers

David T. Pyne

Jeffrey R. Yago

Dr. John M. Poindexter

EMP Task Force on National and Homeland Security

“The synergism of such combined arms is described in the military doctrines of all these potential adversaries as the greatest revolution in military affairs in history—one which projects rendering obsolete many, if not all, traditional instruments of military power,” warns the EMP Commission.

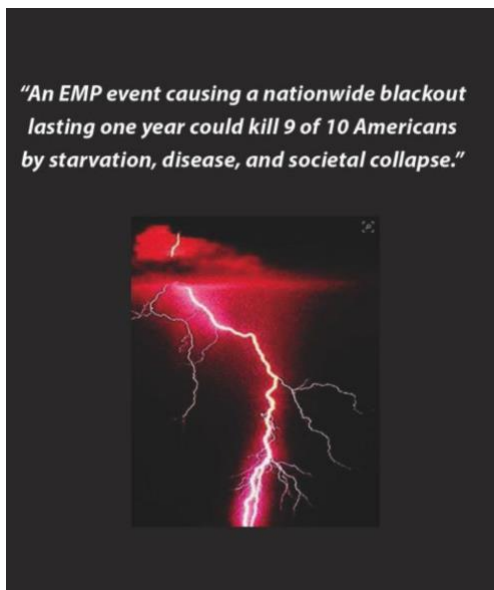
Blackout Warfare that paralyzes the U.S. electric grid and other life-sustaining critical infrastructures—communications, transportation, natural gas and petroleum, business and finance, food and water infrastructures, and the military—could kill most Americans.

“A long-term outage owing to EMP could disable most critical supply chains, leaving the U.S. population living in conditions similar to centuries past, prior to the advent of electric power. In the 1800s, the U.S. population was less than 60 million, and

those people had many skills and assets necessary for survival without today's infrastructure. An extended blackout today could result in the death of a large fraction of the American people through the effects of societal collapse, disease, and starvation." The EMP Commission estimates up to 90% of the U.S. population could die from a nationwide blackout lasting one year.

The military would be paralyzed by a nationwide blackout, as CONUS military bases depend for 99% of their electricity upon the civilian electric grid.

U.S. strategic thinking and planning for Cyber Warfare in 2021 is analogous to thinking and planning about future warfare by the Allies in 1939, before nearly losing World War II to Nazi Germany's revolutionary Blitzkrieg and Imperial Japan's revolutionary use of carrier aviation.



Today, the Pentagon thinks World War III will be fought much like World War II, a clash between air, naval, and land power; takes cybersecurity seriously, but not seriously enough; and is totally blind to the larger threat, the real threat, from combined-arms Blackout Warfare.

Today, U.S. experts on cybersecurity, sabotage, and EMP do not cooperate, do not talk to each other, see each other as irrelevant, or worse as undeserving competitors for resources.

Almost no one "connects the dots" that adversary cyber aggressions are the tip of the spear, often coordinated with missile or satellite launches and strategic forces exercises, practicing combined-arms Blackout Warfare.

The stage is set for the U.S. and its allies to be surprised in a way far worse than 1939-1941, surprised technologically, tactically, operationally, and strategically, in a war that might be won and lost at the speed of light.

Washington might not even know who launched the Blackout War, since cyber, sabotage, and EMP attacks can all be made anonymously.

For the first time, subject matter experts in all relevant disciplines will think about attacks against the U.S. electric power grid, first individually, and then collectively, learning from each other and pooling their talents to outline against the U.S. a coordinated combined-arms Blackout War:

Chapter I "Weaponizing the Weather": Potential adversaries would likely exploit severe weather in making an attack on the national electric grid, circumstances permitting.

Chapter II "Cyber-Attacking Electric Power Grids": Hacking, worms, logic bombs, and other cyber-weapons are deployed to attack the national electric grid.

Chapter III “Physical Security”: Small teams of highly trained commandoes can attack a surprisingly small number of electric power substations to achieve a national blackout.

Chapter IV “Non-Nuclear EMP (NNEMP) Attack”: NNEMP warheads delivered by sophisticated stealthy cruise missiles, unsophisticated drones, or man-carried can blackout the grid.

Chapter V “Nuclear High-Altitude EMP (HEMP) Attack”: The ultimate “cyber-weapon” attacks not only the national electric grid, but all the other critical infrastructures at the speed of light.

Chapter VI “Advancing National Preparedness Against Blackout Warfare”: Makes recommendations to protect electric grids and other critical national infrastructures from EMP/ Cyber/ Sabotage.

Chapter VII “Conclusions And Commentary”: What have the experts learned from thinking about Blackout Warfare?

Key Judgments

Potential adversaries including Russia, China, North Korea, Iran and international terrorists have the capability to inflict a protracted nationwide electric power blackout on the United States—causing the collapse of such life-sustaining critical infrastructures as electric grids, communications, transportation, business and finance, food and water—and severely crippling U.S. capabilities to project military power. Blackout Warfare can be waged with cyber-attacks, physical sabotage, Non-Nuclear Electromagnetic Pulse (NNEMP) weapons, and/or nuclear High-altitude Electromagnetic Pulse (HEMP) attack. Any one of these means could inflict a protracted nationwide blackout. But a conservative military planner is likely to use all his capabilities in combinations calculated to achieve the greatest damage and the most decisive results. Weather may be exploited in Blackout Warfare, as electric grids are most vulnerable in severe weather, including extremes of hot and cold weather.

Russia and/or China is likely to make a massive cyber-attack against the entire U.S. electric grid prior to the outbreak of conventional or nuclear war, or during an extreme international crisis, to deter or defeat the U.S. with “gray-zone aggression” instead of or prior to outbreak of a “real shooting war”: consistent with their military doctrine that Cyber Warfare is an unprecedented and decisive Revolution in Military Affairs. For U.S. relations with both Russia and China, the emergence of viable paths to cyber-attacks against critical infrastructure as a new strategic weapon has lowered the barriers to conflict, and presents a heightened danger with the potential to disrupt the long-standing balancing calculus dependent upon nuclear deterrence.

North Korea, Iran, and non-state actors probably cannot inflict a protracted nationwide blackout on the U.S. by cyber-attack, but could do so with small numbers of special forces using small arms, explosives and/or NNEMP weapons to attack electric grid substations and control centers. Russia, China, and North Korea presently have the capability to make a HEMP attack that would blackout the U.S. electric power grid and other life-sustaining critical infrastructures. Iran may have clandestinely developed capabilities to make a HEMP attack against the U.S. or may soon be able to do so. Russia, China, and North Korea have developed

“Super-EMP” nuclear weapons that can generate extraordinarily powerful HEMP, exceeding hardening standards for U.S. military forces.

The HEMP threat is not merely theoretical, but well-established empirically, including by real world blackouts: “With few exceptions, the U.S. national electric grid is unhardened and untested against nuclear EMP attack. In the event of a nuclear EMP attack on the United States, a widespread protracted blackout is inevitable.” (EMP Commission Chairman, Dr. William R. Graham)

Chapter I: Weaponizing The Weather

WEAPONIZING THE WEATHER by Dr. Peter Vincent Pry An attack on the U.S. electric power grid, with the objective of causing a regional or nationwide protracted blackout, is likely to exploit severe weather as a weapon. Hurricanes, heat waves, ice storms, tornadoes, summer temperature highs and winter lows, and other weather extremes, can stress electric grids and tax emergency resources, facilitating attacks by cyber, sabotage, and EMP to orchestrate a protracted blackout.

Chapter II: Cyber-Attacking Electric Power Grids

CYBER-ATTACKING ELECTRIC POWER GRIDS: A NEW STRATEGIC WEAPON by Dr. Edward M. Roche The United States faces imminent danger from a devastating cyber-attack against its electrical grid. This attack is more probable because a Revolution in Military Affairs has weakened the deterrence traditionally associated with conventional and nuclear weapons, changed the escalation ladder, and consequently lowered the barrier to intensive conflict between the superpowers. In April 2021, Russia massed troops on Ukraine’s border apparently threatening an invasion, raising alarms in the U.S. and NATO. Ventriloquizing for the Kremlin, Putin intimate and director of Russia’s state-run international media giants, RT and Sputnik, Margarita Simonyan, in a TV interview declared: “Russia will invade Ukraine, sparking a conflict with the U.S. that will force entire cities into blackouts... All-out cyber warfare, nation-wide forced blackouts.” “War is inevitable,” according to Russia’s Simonyan, “I do not believe that this will be a large-scale hot war, like World War II, and I do not believe there will be a long Cold War. It will be a war of the third type: the cyber war.”

Russian TV described cyber-attack options ranging from small-scale to existential threats, including: blacking-out part of New York City (Harlem was mentioned), or blacking-out the state of Florida, or blacking-out the entire continental United States. To defeat the U.S., according to Russia’s Simonyan: “We don’t even need the nukes.”

Moscow’s Cyber War knockout blow—blacking-out U.S. electric grids and other critical infrastructures, has been planned for years:

Of course there are different levels of attack, ranging from small irritating skirmishing actions to a major attack aimed at taking out electrical power for a region of America or a single large metropolitan area. At the top extreme is an all-out attempt to disable the nation’s entire electrical grid aiming to plunge the country into a chaotic and horrifying darkness. For a small Nation State, it is doubtful they could assemble enough capability successfully to launch a

cyber-attack nationwide against such a giant electrical grid in its entirety. One of America's rival superpowers could.

Cyber-attacks by tradition are broken down into two classes. One type is the "supplementary" variety, the other is "stand-alone". In the supplementary form, cyber-attacks are used to assist projection of military force. Cyber becomes one of many tools in a military confrontation. The highest priority targets usually are the command and control systems of the enemy's military. Only if the conflict reaches a higher level of intensity does it become a possibility to engage civil society targets.

If there were cyber-attacks on both military and civilian targets, and these were being deployed as a supplement to national military force, then this would mean the parties were engaged in a "Total War." This is the highest and most unfortunate level of conflict, but if we follow the traditional and accepted concepts regarding nuclear deterrence this scenario is unlikely between the superpowers. Under traditional strategic defense theory, all-out cyber conflict would take place only as an adjunct to either conventional or nuclear war.

A new form of cyber-attack against the electrical grid has emerged in the form of a "non-shooting" war between Nation States. This type of attack might take place between superpowers as something that is short of use of conventional or nuclear force. Some argue that "non-kinetic" cyber-attacks are not an "armed attack" under international law and thus there is no right given to a Nation State for self-defense under Article 51 of the United Nations Charter. Consequently, they argue, this lowers the chance of kinetic retaliation.

In Cyber, China Is A Mortal Threat To The United States

The People's Republic of China appears to be the world's leader in cyber-espionage, at least if measured by volume of pilfered information. In addition, it is the world's largest manufacturer and consumer of electrical power and electrical equipment. It is reasonable to assume that in the course of China's R&D on electrical grid systems, it has conducted extensive technical research (patent analysis; tear-downs of foreign-manufactured equipment; evaluation of operational procedures; industrial espionage of newer technologies).

In addition, after the Gulf Wars, China's military establishment adopted a "crash" program to develop cyber capabilities. China also has sent to the United States many scientists who have penetrated the control chambers of America's electrical grid operators. This access has given China's agents numerous opportunities to collect extensive intelligence on the U.S. grid, including both operating and recovery procedures as well as characteristics (specific machine and hardware identities) of its supporting ICT (Integrated Control Technologies) control systems.

We can expect that a cyber-attack by China against electricity in the United States would have the following characteristics:

a) China has the capability to disable all or at least very large parts of the electrical grid (Eastern, Western, Texas Grid Interconnects) as well as target specific areas, such as power in a single metropolitan area;

b) A massive cyber-attack against the entire electrical grid would take place within the context of a general war between the United States and China, but a large-scale conventional or nuclear war is highly unlikely;

c) More likely is a massive cyber-attack against the entire U.S. electric grid prior to the outbreak of conventional or nuclear war, or during an extreme international crisis, to deter or defeat the U.S. with “gray-zone aggression” instead of or prior to outbreak of a “real shooting war” consistent with China’s military doctrine that Cyber Warfare is an unprecedented and decisive Revolution in Military Affairs;

d) China is prepared to use targeted attacks against America’s electrical grid as a stand-alone method of fighting what it calls “U.S. Hegemony”;

e) There is a moderate chance of some irritating event such as an accidental boat collision on the high sea leading to a repeat of the Hainan Island incident, leading to another fabricated “patriotic” cyber-attack against the United States, perhaps against a small portion of the electrical grid (but not against the entire system, and only if there was significant loss of Chinese life in the incident);

f) China might engage in a cyber-attack against electrical grid systems of low-criticality as a symbolic warning if it feared an attack from the United States;

g) China may engage in brokering of vulnerability information about the electrical grid in the United States as an unscrupulous profit-making activity, with exploits being sold to Non-State Actors or nations such as Russia.

Russia Is The Best Prepared To Defend Against Cyber-Attack And Use Cyber As A Strategic Weapon

Russia does not have the amount of money or human resources of China but it does have superior strategy-making capabilities. In addition, Russia has a long-proven track record of being able to develop world-class offensive capabilities in any field using a fraction of the resources of the United States.

Russia does not brag and publicize its cyber warfare capabilities as does the United States, but from examination of publicly available documents, we know that if needed, it can closely integrate its military with all resources in civil society, including all of its hackers.

Russian cybersecurity companies routinely monitor the world’s Internet, and are sensitive to any threats. Unlike the United States, Russian law passively encourages development of robust hacking skills because it is not illegal for its citizens to hack computing resources outside in other countries.

Finally, Russia has a reliable habit of always launching a counter-strike if it has been attacked, and this includes in the cyber domain. We can expect that a cyber-attack by Russia against the electrical grid of the United States would have the following characteristics:

- a) Russia is capable of launching a massive attack that would shut down in one coordinated attack at least 80% of America's electrical grid;
- b) Russia has developed the capabilities of attacking high-criticality SCADA systems in the electrical grid, as well as all other systems;
- c) Russia likely knows more about EMP than the United States given its extensive testing and development of EMP weapons;
- d) A massive Russian attack against the entire electrical grid would occur within the context of a major strategic conflict between Russia and the United States
- e) During an extreme international crisis, a massive Russian cyber-attack against the entire U.S. electric grid prior to the outbreak of conventional or nuclear war is likely, to deter or defeat the U.S. with "gray-zone aggression" instead of or prior to outbreak of a "real shooting war" consistent with Russia's military doctrine that Cyber Warfare is an unprecedented and decisive Revolution in Military Affairs;
- f) Russia's response to a major cyber-attack made by the United States is likely to be at least proportional but more likely disproportional and massive, possibly even resulting in Russian nuclear retaliation as threatened in their military doctrine;
- g) Like China, Russia possibly would use a targeted cyber-attack against a low-criticality electrical grid system as a show of force and warning to deter escalation in a conflict by the United States;
- h) Russia likely has experimented with placement of cyber logic-bombs in portions of America's electrical grid;
- i) Russia is more capable than other countries in placement of assets (human agents) into critical parts of the management structure of the American electrical grid.

Chapter III: Physical Security: The Electric Grid's Dirty Little Secret

PHYSICAL SECURITY: THE ELECTRIC GRID'S DIRTY LITTLE SECRET by Michael Mabee One of the easiest ways for a terrorist organization, a state actor or a homegrown radicalized group to really hurt the United States and kill thousands, tens of thousands or even millions of people would be a coordinated physical attack against the U.S. electric grid. What is perhaps most disturbing is that the government has known for over 4 decades about the vulnerability of the electric grid to physical attacks, yet very little has been done to protect it.

The North American electric grid is an amazing human accomplishment. It is the largest machine in the history of the world, built piece by piece over many generations. This machine is literally the life support system for the United States. The "electric grid" is actually thousands of entities, both public and private sector, that operate in an interconnected system to facilitate the generation, transmission and distribution of electrical power.

The grid is made up of power generation—such as nuclear, coal and gas-fired power plants, hydroelectric facilities, wind turbines and solar farms, high voltage transmission lines that span long distances across the country and local distribution lines which bring the power to our homes and businesses. This interconnected—and vulnerable—patchwork is what allows the United States to support her human population.

Everything that enables 330 million people in the country to survive is wholly reliant on the electric grid. All of our critical infrastructures, including food, water, fuel, transportation, financial, communications, medical systems and our national defense infrastructure, are all completely dependent on the electric grid. This cannot be overemphasized: Our national security is dependent on the electric grid.

Believe it or not, there are no physical security requirements for most of the electric grid. It is just a big, fat, juicy, soft target.

We have known for four decades about the grave danger posed by physical attacks on the electric grid, and yet today there is no physical security standard for the vast majority of the grid. A coordinated physical attack on multiple grid facilities can be achieved by an unsophisticated domestic group or a sophisticated terrorist organization or in a covert operation by a state actor. A coordinated physical attack could cause wide area and long-term blackouts, impacting critical infrastructures and endangering the public.

Chapter IV: Non-Nuclear EMP Attack

NON-NUCLEAR EMP ATTACK by Dr. Peter Vincent Pry Non-Nuclear Electromagnetic Pulse (NNEMP) weapons, more commonly known as Radio-Frequency Weapons, are non-nuclear weapons that use a variety of means, including explosively driven generators or high-power microwaves, to emit an electromagnetic pulse similar to the E1 HEMP from a nuclear weapon, except less energetic and of much shorter radius.

The range of NNEMP weapons is rarely more than ten kilometers. International scientific and electronic engineering organizations describe the NNEMP threat as “Electro-Magnetic (EM) Terrorism” and, less dramatically, as “Intentional Electro-Magnetic Interference” (IEMI). Non-Nuclear Electromagnetic Pulse (NNEMP) weapons is the term used here to emphasize that the NNEMP threat has significant similarities to nuclear HEMP, similar technical solutions, and poses a much greater threat than implied by the word “Interference” in IEMI.

“There is enormous diversity in possible electromagnetic weapon designs, for both large scale and highly focused attacks, both against civil and military targets,” according to Dr. Carlo Kopp, one of the world’s leading experts on NNEMP weapons, “There are many possible taxonomical divisions for electromagnetic weapons”:—“Directed Energy Weapons vs. ‘one shot’ E-Bombs;”—“Nuclear (HEMP) E-Bombs vs. Non-nuclear E-Bombs;”—“Narrow Band Weapons vs. Wideband or UWB [Ultra-Wide Band] weapons;”—“High Power Microwave vs. ‘Low Band’ weapons;”—“Persistent Area Denial (AD) weapons vs. Non-Persistent weapons;”—“Explosively pumped vs. Electrically pumped weapons.”

Unlike the nuclear HEMP threat, NNEMP weapons are much more readily available to and easily exploitable by terrorists and the least sophisticated state actors. NNEMP weapons can

be built relatively inexpensively using commercially available parts and design information available on the internet. In 2000, the Terrorism Panel of the House Armed Services Committee conducted an experiment, hiring an electrical engineer and some students to try building an NNEMP weapon on a modest budget, using design information available on the internet, made from parts purchased commercially, available to anyone.

They built two NNEMP weapons in one year, both successfully tested at the U.S. Army proving grounds at Aberdeen. One was built into a Volkswagen bus, designed to be driven down Wall Street to disrupt stock market computers and information systems and bring on a financial crisis. The other was designed to fit in the crate for a Xerox machine so it could be shipped to the Pentagon, sit in the mailroom, and burn-out Defense Department computers.

But a terrorist or criminal armed with the “EMP Suitcase” could potentially destroy electric grid SCADAs, possibly shutdown transformers, and blackout a city. Thanks to NNEMP weapons, we have arrived at a place where the technological pillars of civilization for a major metropolitan area could be toppled by a single madman.

The “EMP Suitcase” can be purchased without a license by anyone.

According to the Wall Street Journal, a classified study by the U.S. Federal Energy Regulatory Commission found that damaging as few as 9 out of 2,000 EHV transformers could trigger cascading failures, causing a protracted nationwide blackout of the United States.

Special mention must be made of the ongoing technological revolution in Non-Nuclear EMP weapons, which are becoming more powerful, more miniaturized and lighter-weight, and deliverable by cruise missiles or drones. The marriage of NNEMP warheads to drones or cruise missiles, preprogrammed or equipped with sensors to follow high-power electric lines and to target control centers and transformers, introduces a major new threat to national power grids.

A non-explosive High-Power Microwave warhead, for example, can emit repeated bursts of electromagnetic energy to upset and damage electronic targets. Such a warhead, attached to a programmable drone or cruise missile, could follow the powerlines to attack numerous transformer and control substations, until its energy is exhausted. Relatively small numbers of NNEMP cruise missiles or drones—perhaps only one capable of protracted flight—could inflict a long nationwide blackout.

Thus, NNEMP might be able to achieve results similar to a nuclear HEMP attack in blacking-out power grids, though the NNEMP attack would probably take hours instead of seconds.

Russia may still be the world leader in NNEMP weapons, as was the USSR during the Cold War. Russia’s nuclear-powered cruise missile, the Burevestnik (Storm Petrel, NATO designation SSC-X-9 Skyfall), now under development, makes little sense as yet another missile to deliver nuclear warheads, as advertised by Moscow. The Storm Petrel’s engines, powered by a nuclear reactor, theoretically will give it unlimited range and limitless flying time for crossing oceans and cruising over the U.S. The Storm Petrel could be a nuclear-powered version of CHAMP, able to fly much farther and longer and armed with a more potent NNEMP warhead, electrically supercharged by the nuclear-reactor.

“EMP weapons could also be used clandestinely to take out important targets during peace time, when the use of conventional weapons would be considered outrageous, as it will be difficult to prove who exactly was responsible. Such incapacitating applications of EMP could also prove to be an effective deterrent against enemies contemplating military action.”

Dozens of nations reportedly have NNEMP weapons or are developing them. Some of these are Russia, China, North Korea, Iran, Pakistan, India, Israel, Germany, the United Kingdom, France, Australia, and Switzerland. Ukraine’s Yuri Tkasch, Director of the Kharkov Institute of Electromagnetic Research, which was the leading design bureau for the USSR’s NNEMP weapons, is a one-man worldwide proliferator of NNEMP technology to any buyer.

The technological revolution in NNEMP weapons threatens to become an electromagnetic “Pearl Harbor” for nations, like the United States, that fail to fully comprehend the threat and have not protected civilian critical infrastructures and military systems.

NNEMP Attack On The U.S. Electric Grid

Described here are two possible technical scenarios for Non-Nuclear EMP attacks on the U.S. electric grid, out of many possible scenarios. The political-military scenarios are also many.

Political-Military Scenarios

Political-military scenarios for NNEMP attack on the U.S. national power grid include:

Surprise attack “bolt from the blue” in peacetime, based on adversary calculation that war is eventually inevitable; NNEMP attack during a crisis but prior to outbreak of a “shooting war” as a warning and/or preemptive strike designed to cripple U.S. power projection capabilities; NNEMP attack coordinated with the outbreak of a traditional “shooting war”; NNEMP attack as a last-ditch effort to reverse the tide of a losing war; NNEMP attack in the aftermath of a lost war, for revenge.

The scale of an NNEMP attack on the U.S. electric grid could include: Temporary blackout of a city to send a warning (as China did to Mumbai, India in October 2020 by cyber-attack). Protracted blackout of a state or region to send a bigger warning and/ or to cripple particular U.S. military capabilities; Protracted nationwide blackout of the U.S. electric grid to defeat the U.S. without a traditional “shooting war” and possibly to eliminate the U.S. as an actor on the world stage (as described in the military doctrines of Russia, China, North Korea, and Iran).

Scenario #1: Lower-Tech NNEMP Attack Scenario #1 is the kind of threat that is well within the technological and operational capabilities of Iran, North Korea, virtually any nation state, and major terrorist or criminal organizations. Scenario #1 entails a lower-tech NNEMP threat employing weapons which must be man-delivered by automobile or panel truck. The postulated NNEMP weapons are lower-tech also in power, requiring about 10 minutes to maximize damage against the electronics in unmanned electric grid control substations associated with EHV transformers.

Scenario #1 postulates that every panel truck armed with an NNEMP weapon has a two-man crew, one to drive and one to operate the weapon. The NNEMP weapon illuminates the

target—an EHV transformer control substation—for 10 minutes. Then the panel truck moves to the next target, the nearest next substation, located on average 40 road miles away, traveling on average 50 mph.

Scenario #2: Higher-Tech NNEMP Attack Scenario #2 is the kind of threat that is well within the technological and operational capabilities of Russia and China, plausibly within the capabilities of North Korea and Iran, and even possibly within the capabilities of major terrorist or criminal organizations.

Scenario #2 entails a higher-tech NNEMP threat employing CHAMP-like drones or Unmanned Aerial Vehicles (UAVs) that can be preprogrammed or guided to attack EHV transformer control substations. The postulated NNEMP weapons are higher-tech also in power, requiring about 1-5 minutes to maximize damage against the electronics in unmanned electric grid control substations associated with EHV transformers.

Scenario #2 postulates an NNEMP drone or UAV that can fly 100 mph, locate the target, pause to make an NNEMP attack, and sustain these operations continuously for 24 hours. China's Pterodactyl UAV is exactly the kind of drone/ UAV capable of such operations, if armed with an NNEMP warhead. Russia has similar UAVs, including the Skyfall cruise missile, powered by a nuclear reactor, that could conceivably energize a super-charged NNEMP warhead. Iran has demonstrated drones, UAVs, and cruise missiles capable of precision attacks on Saudi Arabian oil facilities, that could be modified to make an NNEMP attack.

Scenario #2 postulates, after illuminating the target for 1-5 minutes, the drone or UAV moves to the next target, the nearest next substation, located on average 20 flight miles away, traveling on average 100 mph.

NNEMP drones/ UAVs could be shipped into the United States undetected, stored in warehouses located nearest targets in the electric grid, launched and operated from secure warehouses. This scenario would require three secure warehouses, one located in the Eastern grid, one in the Western grid, and one in the Texas grid.

Acquiring replacement equipment and installation will require many weeks or months, if even possible when all critical infrastructures—communications, transportation, petroleum and natural gas, business and finance, food and water infrastructures—are inoperable or severely crippled due to protracted nationwide blackout.

Chapter V: High-altitude Electromagnetic Pulse (HEMP) Attack

HIGH-ALTITUDE ELECTROMAGNETIC PULSE (HEMP) ATTACK by Dr. Peter Vincent Pry A Revolution In Military Affairs Nuclear HEMP attack is part of the military doctrines, plans and exercises of Russia, China, North Korea, and Iran for a revolutionary new way of warfare against military forces and civilian critical infrastructures by cyber, sabotage, and HEMP. This new way of warfare is called many things by many nations.

In Russia, China, and Iran it is called Sixth Generation Warfare, Non-Contact Warfare, Electronic Warfare, Total Information Warfare, and Cyber Warfare. Some U.S. analysts, the

very small number paying attention, call it Cybergeddon, Blackout War, or Combined-Arms Cyber Warfare.

Significantly, because HEMP attack entails detonating a nuclear weapon at such high altitude that no blast or other prompt effects injurious to humans are delivered, only the HEMP that immediately damages only electronics, potential adversaries do not appear to regard nuclear HEMP attack as an act of nuclear warfare. Potential adversaries understand that millions could die from the long-term collateral effects of HEMP and cyber-attacks that cause protracted black-out of national electric grids and other life-sustaining critical infrastructures.

At least some regard this relatively easy, potentially anonymous, method of inflicting mass destruction as an attractive feature of what they describe as a “Revolution in Military Affairs”. Ignorance of the military doctrines of potential adversaries and a failure of U.S. strategic imagination, as noted in military writings of potentially hostile powers, is setting America up for an HEMP Pearl Harbor.

Russia, China, North Korea and Iran appear to regard nuclear HEMP attack as the ultimate weapon in an all-out “Cyber War” aimed at defeating U.S. and allied military forces on the battlefield and in a theater of operations. They also see HEMP and Combined-Arms Cyber Warfare as a means of defeating entire nations by blacking-out their electric grids and other critical infrastructures for longer periods of time than technologically developed societies, including the U.S., can tolerate without major disruption and loss of life.

Russia for example, Russian General Vladimir Slipchenko in his military textbook Non-Contact Wars describes the combined use of cyber viruses and hacking, physical attacks, non-nuclear EMP weapons, and ultimately nuclear HEMP attack against electric grids and critical infrastructures as a new way of warfare that is the greatest Revolution in Military Affairs (RMA) in history.

“In practically all preceding generations of wars... weapons were employed that acted against targets primarily by kinetic, chemical and thermal energy. In addition to these arms... new ones will also appear in... wars of the future.... Weapons based on new physical principles having an electromagnetic effect will see considerable development.

They will represent a form of casualty and damage producing effect on targets through the energy of electromagnetic emissions of various wavelengths and levels of power generated by radio frequency and laser weapons and by means of electronic countermeasures using a conventional or high-altitude nuclear burst.... Depending on the power of emission, such weapons will be capable of... suppressing practically all classic electronic equipment... causing the melting or evaporation of metal in the printed circuit boards... or causing structural changes of electronic elements...”

Like Nazi Germany’s Blitzkrieg (“Lightning War”) Strategy that coordinated airpower, armor, and mobile infantry to achieve strategic and technological surprise that nearly defeated the Allies in World War II, the New Blitzkrieg is, literally and figuratively, an electronic “Lightning War” so potentially decisive in its effects that an entire civilization could be overthrown in hours.

According to General Slipchenko, HEMP and the new RMA renders obsolete modern armies, navies and air forces. For the first time in history, small nations or even non-state actors can humble the most advanced nations on Earth.

Super-EMP Is A... First-Strike Weapon

“The further direction of the work on the development of Super-EMP was associated with the increase of its kill effect by focusing Y-radiation, which should have resulted in an increase of the pulse’s amplitude. These properties of Super-EMP make it a first strike weapon, which is designed to disable the state and military command and control system, the economy, ICBMs, especially mobile based ICBMs, missiles on the flight trajectory, radar sites, spacecraft, energy supply systems, and so forth.

Super-EMP is obviously offensive in nature and is a destabilizing first-strike weapon. The Russian nuclear component relies on the Super-EMP factor, which is the Russian response to U.S. nuclear blackmail.

China’s military doctrine sounds an identical theme about the revolutionary implications of HEMP and Information Warfare. According to People’s Liberation Army textbook World War, the Third World War—Total Information Warfare, written by Shen Weiguang (allegedly, according to the PRC, the inventor of Information Warfare).

“Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse... and quickly achieve breakthroughs in those technologies...”: “With their massive destructiveness, long-range nuclear weapons have combined with highly sophisticated information technology and information warfare under nuclear deterrence.... Information war and traditional war have one thing in common, namely that the country which possesses the critical weapons such as atomic bombs will have “first strike” and “second strike retaliation” capabilities.... As soon as its computer networks come under attack and are destroyed, the country will slip into a state of paralysis and the lives of its people will grind to a halt. Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse... and quickly achieve breakthroughs in those technologies in order to equip China without delay with equivalent deterrence that will enable it to stand up to the military powers in the information age and neutralize and check the deterrence of Western powers, including the United States.”

“In future high-tech warfare under informatized conditions, information warfare will span multiple dimensions, including ground, sea, air, and the EM spectrum. Information superiority has already become central and crucial to achieving victory in warfare... If the communications equipment used for the transmission of battlefield information were attacked and damaged by an opponent’s EMP weapons, then the one attacked would face the danger of disruption in battlefield information transmission. EMP severely restricts the tactical performance and battlefield survivability of informatized equipment.”

An article in the newspaper of the People’s Liberation Army notes that “The United States is more vulnerable than any other country in the world” to attacks by HEMP and Combined-Arms Cyber Warfare:”

Some people might think that things similar to the 'Pearl Harbor Incident' are unlikely to take place during the information age. Yet it could be regarded as the 'Pearl Harbor Incident' of the 21st century if a surprise attack is conducted against the enemy's crucial information systems of command, control, and communications by such means as electronic warfare, electromagnetic pulse weapons, telecommunications interference and suppression, computer viruses, and if the enemy is deprived of the information it needs as a result.

Even a super military power like the United States, which possesses nuclear missiles and powerful armed forces, cannot guarantee its immunity... In their own words, a highly computerized open society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems and from power plants to iron and steel works, relies entirely on computer networks.... When a country grows increasingly powerful economically and technologically... it will become increasingly dependent on modern information systems.... The United States is more vulnerable to attacks than any other country in the world..."

We as a nation are not "connecting the dots" through a profound failure of strategic imagination. Like the Allies before the Blitzkrieg of World War II, we are blind to the unprecedented existential threat from HEMP attack that could befall our civilization—figuratively and literally, from the sky, like lightning. High-altitude electromagnetic pulse (HEMP) attack is technically and operationally the easiest, least risky, and most effective use of a nuclear weapon available to a nuclear-armed state or non-state actor.

Any nuclear weapon, even a primitive first-generation weapon like the A-bombs that destroyed Hiroshima and Nagasaki, will produce gamma rays and fireballs that generate the high-frequency (E1 HEMP), medium-frequency (E2 HEMP), and low-frequency (E3 HEMP) electromagnetic pulses. HEMP attack delivers a three-fold punch to electronics small and large, ranging from personal computers to national electric grids and everything in-between,

Nuclear HEMP attack entails detonating the weapon at such high altitude that no blast, thermal, fallout or effects other than HEMP are experienced on the ground. HEMP is like "super-lightning" in that it delivers a shock much more powerful than lightning against, not a point, but against electronics over a vast area.

A single nuclear weapon can potentially make a HEMP attack against a target the size of North America.

E1 HEMP is much faster (lasting nanoseconds) and much more powerful than lightning, cannot be stopped by devices designed for lightning protection, can damage and destroy small electronics and control systems necessary for the operation of everything from automobiles to airplanes, including electric grids, communications, and all other critical infrastructures.

E2 HEMP is as fast (lasting milliseconds) and as powerful as lightning and can be stopped by lightning protection, but many commercial enterprises and homes lack lightning protection.

E3 HEMP is much slower (lasting seconds) but has much more net energy than lightning, is potentially more powerful than the electromagnetic fields that could be generated by a solar super-storm that can melt transformers designed to carry hundreds of thousands of volts.

Because HEMP propagates in three “waves” their damaging effects will be dynamic and mutually reinforcing, the E1 HEMP damaging and destroying systems (including possibly lightning protection) that opens the door for wider and deeper damage by E2 and E3 HEMP.

Any nuclear weapon detonated at an altitude of 30 kilometers (18 miles) or higher will generate a potentially catastrophic HEMP. A nuclear detonation at 30 kilometers altitude will generate a HEMP field with a radius on the ground of about 600 kilometers (360 miles). Detonated at 400 kilometers (240 miles) altitude, the radius of the HEMP field will be about 2,200 kilometers (1,320 miles).

HEMP Attack Is Easy

Accuracy is not necessary for an HEMP attack because the target altitude (30-400 kilometers) is so wide, and the radius and the coverage of the HEMP field is so vast. HEMP attack does not require a re-entry vehicle, heat shield, shock absorbers and other paraphernalia associated with a nuclear missile warhead designed for blasting a city. These are unnecessary for an HEMP attack, which detonates the warhead above the atmosphere, in outer space.

HEMP attack can be executed by a wide variety of delivery vehicles, anything that can loft a nuclear weapon to 30 kilometers or higher. Possible delivery vehicles against the United States include a satellite, a long-range missile, a medium-or short-range missile launched off a freighter, some kinds of cruise missiles and anti-ship missiles (like Russia’s Club-K exported to Iran), a jet fighter or some kinds of jet airliner doing a zoom climb, even a meteorological balloon.



EMP AREA BY BURSTS AT 30, 120 and 300 MILES

Gary Smith, "Electromagnetic Pulse Threats", testimony to House National Security Committee on July 16, 1997

HEMP Fields and Effectiveness The size of the HEMP field on the ground is determined by the altitude of detonation, HEMP propagating from the point of detonation to the horizon. The higher the altitude of detonation, the bigger the HEMP field on the ground. In general, HEMP field strengths on the ground are stronger when the weapon is detonated at lower altitudes, where the effects are more concentrated within a smaller radius, and weaker when the weapon is detonated at higher altitudes, where the effects are within a larger radius and cover a bigger area. HEMP effects are dangerous at all altitudes.

Varying the altitude of the HEMP attack can be used to adjust the size of the HEMP field to better fit the target. Since the radius of the HEMP field is not highly sensitive to altitude, relative to any delivery system (even the Houthis or Taliban could use commercial off-the-shelf technology to rig a fusing system that will detonate within less than one kilometer of the desired altitude) again accurate delivery is not an issue.

HEMP fields are strongest at the center, where the peak field is located, and reduce in strength toward the margins. As a general rule, HEMP field strength at the outer edge of the field will

be about one-half of the peak field strength. Even for a primitive first-generation nuclear weapon, the entire field is dangerous, not just the peak field. Damage to electric grids and other critical infrastructures will not be limited to the HEMP field.

Cascading failures will propagate far beyond the HEMP field through an unprotected electric grid, assuming the HEMP field is smaller than the electric grid being attacked. For example, a 10 kiloton weapon detonated at 30 kilometers over the U.S. Eastern Grid would generate an HEMP field about 600 kilometers in radius, much smaller than the Eastern Grid. But the national electric grid being aged, over-taxed with demand, always operating on the verge of failure, capable of blackouts that put 50 million people into the dark because of cascading failures from a tree branch (like the Great Northeast Blackout of 2003), the entire Eastern Grid would certainly be plunged into a protracted blackout from such an EMP attack. The U.S. cannot survive without the Eastern Grid which generates 75 percent of the nation's electricity and supports most of the national population.

For nuclear weapons of normal design, a high-yield weapon will generate a more powerful HEMP field than a low-yield weapon, but the difference in field strength is not nearly as great as the difference in yield. For example, a 1,000 kiloton nuclear weapon will not generate an HEMP field 100 times greater than a 10 kiloton nuclear weapon. Indeed, a 10 kiloton weapon will generate an E3 HEMP field nearly as powerful as the 1,000 kiloton weapon, but over a smaller area.

Even a primitive first-generation nuclear weapon such as terrorists might build, like the first nuclear weapon ever built, the 10 kiloton bomb that destroyed Hiroshima, detonated at 30 kilometers altitude, will generate an HEMP field that at the weakest, on the margins, will be several thousand volts per meter. This is enough to put at risk all unprotected civilian and military systems within the field.

Super-EMP Weapons

"Super-EMP" weapons, as they are termed by Russia and China, are nuclear weapons specially designed to generate an extraordinarily powerful E1 HEMP field. Super-EMP warheads are designed to produce gamma rays, which generate the E1 HEMP effect, not a big explosion, and typically have very low explosive yields, only 1-10 kilotons. According to Russian open sources, a Super-EMP weapon can generate a peak E1 HEMP field of 100-200,000 volts per meter, which would be 50-100 kilovolts/ meter at the margins. Even HEMP hardened U.S. strategic forces and C3I (Command, Control, Communications, Intelligence) are potentially vulnerable to such a threat.

Why won't the threat of U.S. nuclear retaliation assuredly deter a nuclear HEMP attack, just as the USSR was deterred from nuclear aggression throughout the Cold War? Deterrence depends on knowing who launched the HEMP attack so they can be punished by retaliation. But a HEMP attack can be delivered anonymously. Launched off a freighter, a submarine, by jet, or by satellite (hundreds of satellites are in low Earth orbit), the perpetrator of HEMP attack might never be identified. HEMP attack can destroy radars, satellites and their downlinks and other national technical means necessary to identify the attacker. Bomb debris from a weapon detonated at high-altitude for HEMP attack is not collectible, unlike debris

from a nuclear weapon detonated in a city, so forensic analysis cannot identify the perpetrator. HEMP attack leaves no fingerprints.

The Congressional EMP Commission estimates that a HEMP attack causing a protracted nationwide blackout lasting one year could kill up to 90 percent of the American people through starvation and societal collapse.

One of the biggest and most dangerous myths about HEMP attack is that the consequences would be confined to a relatively small region comprising a few states, similar in extent and severity to the electric blackouts experienced during hurricanes. In fact, HEMP attack by a single nuclear weapon, such as those now possessed by North Korea, would almost certainly result in a protracted nationwide blackout.

Chapter VI: Advancing National Preparedness Against Blackout Warfare

Dr. Peter Vincent Pry

The Congressional EMP Commission in 2017 recommended a White House “EMP Czar” to lead the functional equivalent of a Manhattan Project to quickly protect the nation from existential threats posed by solar and manmade electromagnetic pulse (EMP). The new White House “Cybersecurity Czar” should also serve as an “EMP Czar” since EMP attack is part of adversary planning for Cyber Warfare: “Combined-arms cyber warfare, as described in the military doctrines of Russia, China, North Korea, and Iran, may use combinations of cyber-, sabotage-, and ultimately nuclear EMP-attack to impair the United States quickly and decisively by blacking-out large portions of its electric grid and other critical infrastructures...

The synergism of such combined arms is described in the military doctrines of all these potential adversaries as the greatest revolution in military affairs in history—one which projects rendering obsolete many, if not all, traditional instruments of military power.”

Protecting from EMP/ Cyber/ Sabotage the national electric power grid—the keystone critical infrastructure that energizes operations of all other life-sustaining critical infrastructures—must have highest White House priority as these threats are more imminent than climate change, imperil the existence of modern electronic civilization, and could kill millions: “A long-term outage owing to EMP could disable most critical supply chains, leaving the U.S. population living in conditions similar to centuries past, prior to the advent of electric power. In the 1800s, the U.S. population was less than 60 million, and those people had many skills and assets necessary for survival without today’s infrastructure. An extended blackout today could result in the death of a large fraction of the American people through the effects of societal collapse, disease, and starvation.”—EMP Commission

Chapter VII: Conclusions and Commentary

“Someday science shall have the existence of Mankind in its power, and the human race commit suicide by blowing up the world.”—Henry Adams (1862) DR. PETER VINCENT PRY (Executive Director, EMP Task Force)

The A-bomb that destroyed Hiroshima killed 135,000. An H-bomb detonated over New York City could kill 10 million. A HEMP attack over North America could kill 300 million. So too could a cyber-attack, special forces sabotage, and/ or Non-Nuclear EMP (NNEMP) attack that blacks-out electric grids and other life-sustaining critical infrastructures for a year, causing 90% of the population to perish from starvation eventually.

Immediately, few or no fatalities may result from HEMP, cyber, sabotage and NNEMP attacks on electric grids, an attractive feature of this revolutionary new mode of warfare. Adversaries can, in effect, hold hostage the lives of the North American population (330 million), whose salvation will depend upon the U.S. government focusing all resources on their rescue, instead of fighting World War III.

Blackout Warfare, the term of art used here to describe a military strategy focused on attacking national electric grids and electronics that sustain military and civilian critical infrastructures, is called many things by many nations. In the United States, the Congressional EMP Commission calls it Combined-Arms Cyber Warfare. Russian military doctrine writes of No Contact Warfare, Electronic Warfare, and Network Centric Warfare. China calls it Total Information Warfare. Russia, China, North Korea, and Iran all call it Cyber Warfare. But their version of Cyber Warfare, and all these other labels for the same concept, include special forces sabotage, NNEMP, and nuclear HEMP attack.

Blackout Warfare seems the best name for a military strategy that attacks electric grids in order to blackout all national critical infrastructures. The EMP Commission warns that this new way of warfare is regarded by adversaries as the greatest Revolution in Military Affairs in history: “Combined-arms cyber warfare, as described in the military doctrines of Russia, China, North Korea, and Iran, may use combinations of cyber-, sabotage, and ultimately nuclear EMP attack to impair the United States quickly and decisively by blacking-out large portions of its electric grid and other critical infrastructures

Foreign adversaries may aptly consider nuclear EMP attack a weapon that can gravely damage the U.S. by striking at its technological Achilles Heel, without having to confront the U.S. military. The synergism of such combined arms is described in the military doctrines of all these potential adversaries as the greatest revolution in military affairs in history—one which projects rendering many, if not all, traditional instruments of military power obsolete.”

Russia, China, North Korea, and Iran are right—that Blackout Warfare is the greatest Revolution in Military Affairs in history. The U.S. electric grid is a technological Achilles heel, vulnerable to attack by many different means. **Blackout Warfare could quickly and relatively easily paralyze all U.S. critical infrastructures, including those analyzed for vulnerability by the EMP Commission: Government, Military, Electric Power, Telecommunications, Transportation, Petroleum and Natural Gas, Banking and Finance, Food and Water, and Emergency Services.** Imagine the consequences of the collapse of all these critical infrastructures, as would happen by blacking-out the electric grid—electric power being the keystone critical infrastructure that sustains all the others—some failing immediately, others within hours, virtually all within 72 hours (after exhaustion of emergency power).

It would be the end of civilization.

Is it just a temporary blackout or is it an electromagnetic pulse?

Suppose you are at work and the lights go out. How do you know if it is a common temporary blackout or the result of an electromagnetic pulse?

Temporary Blackout	Electromagnetic Pulse (EMP)
Cell phones still work	Cell phones probably do not work
Two-way radios work	Two-way radios do not work
Automobiles still work	Automobiles stall on the road causing accidents
Traffic lights may not work	Traffic lights will not work
Backup generators work	Backup generators will not come on
Flashlights work	LED flashlights may not work
Pacemakers work	Pacemakers may not work
Battery powered computers work	Computers and tablets will not work
Battery powered radios work	Even battery powered radios will not work
Air traffic would be normal	Airplanes will fall out of the sky
Information is still available	Little or no information is available
The affected area is limited in size	The affected area is large in size
Power will be restored relatively soon	Power may not be restored for months or years

The effects of an electromagnetic pulse depends on the size of the weapon used, the height at which it detonates, and how far you are from the detonation.

Now that you have determined that an EMP is the most likely explanation for the current situation your first thought should be to go home. Try to start your car. If it was running and then stopped when the EMP hit, turn it off and wait a minute then try to start it again.

If that does not work, and you have the tools to do so, remove the negative battery connection from your car, turn on your headlights and depress the brake pedal and then reconnect the battery. Some electronic components will go into "latch" mode when exposed to an EMP and will reboot when the battery is disconnected and then reconnected. If the car still does not work, strongly consider walking home. Older vehicles are more likely to start using this procedure than newer vehicles. Make sure you have a proper sized wrench for the negative battery connection stored in your car.

Civil society will likely start to disintegrate in two to three days when people realize help is not on the way or when food and water rapidly become scarce.

When you get home fill every container you can with drinking water. Pots, pans, and even the bathtub. Water from the public utility will likely only last a few hours or at most a couple of days.

A Super-EMP weapon that can generate a field of 100-200 kilovolts/meter, and 50-100 kilovolts/meter at the margins or a severe mass coronal ejection will melt transmission lines and fuse together parts of electronic devices. Even if the electronic devices are not plugged in when the event occurs the power cord on each device will act as an antenna delivering thousands of volts to the device.

Electromagnetic Pulse (EMP) Shielding

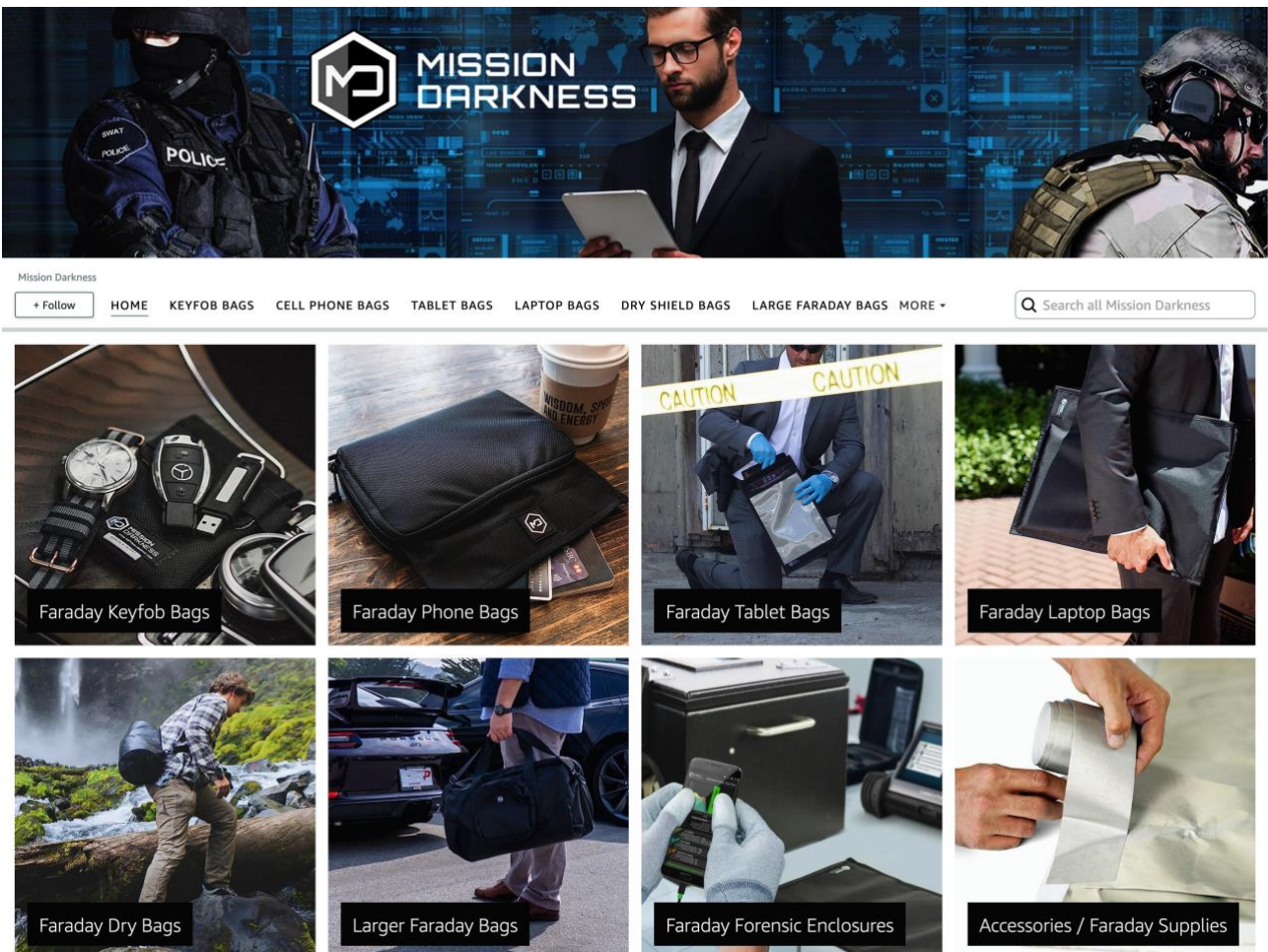
It is reasonable to assume that every unprotected electronic or electrical device will be made inoperable by an electromagnetic pulse attack. This includes appliances, automobiles, cell phones, computers, tablets, LED lights, airplanes, radios, electronic dependent rifle and pistol scopes, battery operated portable tools, generators, medical devices, etc..

Properly shielded electronic devices would be usable after an electromagnetic pulse attack. These devices can be divided into those that need to be used occasionally before and then after an electromagnetic pulse attack and those set aside to be used only after an electromagnetic pulse attack. These designations will help determine the proper type of shielding for those devices.

EMP Shielding bags are convenient for devices that are occasionally needed before and after an EMP attack and must be returned to their shielding bags after use. Shielded boxes and cans are more suited for devices that are set aside for used only after an EMP attack.

(Note: All batteries must be removed from devices before placing them in long term shielding.)

EMP Shielded Bags



The image displays the Mission Darkness website interface. At the top is a banner with the company logo and the text "MISSION DARKNESS" set against a background of a SWAT officer, a man in a suit, and a soldier. Below the banner is a navigation menu with links for "HOME", "KEYFOB BAGS", "CELL PHONE BAGS", "TABLET BAGS", "LAPTOP BAGS", "DRY SHIELD BAGS", "LARGE FARADAY BAGS", and "MORE". A search bar is located on the right side of the menu. The main content area features a grid of eight product images, each with a caption:

- Faraday Keyfob Bags
- Faraday Phone Bags
- Faraday Tablet Bags
- Faraday Laptop Bags
- Faraday Dry Bags
- Larger Faraday Bags
- Faraday Forensic Enclosures
- Accessories / Faraday Supplies

DRY FARADAY SHIELD TOTE 15L

MISSION DARKNESS

SHIELDS LARGE VULNERABLE ELECTRONICS

50 LITER CAPACITY ACCOMMODATES BULKY ELECTRONICS PLUS ACCESSORIES

CAN FLEX TO FIT WIDE OR TALL ITEMS

Interior usable dimensions: **15"** (38cm) L X **11"** (28cm) W X **18.5"** (47cm) H

Mission Darkness Dry Shield Faraday Tote 15L // Waterproof Dry Bag for Electronic Device Security & Transport // Signal Blocking, Anti-Tracking, EMP Shield, Data Privacy for Phones, Tablets, Laptops

Visit the Mission Darkness Store
4.7 ★★★★★ 415 ratings | 18 answered questions
Amazon's Choice in Marine Dry Bags by Mission Darkness

Mission Darkness T10 Faraday Bag for Computer Towers & XL Electronics (Gen 2) Device Shielding for Digital Forensics, EMP Protection, Data Security, Anti-Hacking & Anti-Tracking Assurance

Visit the Mission Darkness Store
4.8 ★★★★★ 139 ratings | 17 answered questions
Amazon's Choice in Computer Hard Drive Bags & Cases by Mission Darkness

\$239⁰⁰

prime One-Day
FREE Returns

Refer friends and earn up to \$500 each year. Get a \$50 Gift Card for each friend who is approved for Amazon Visa.

Purchase options and add-ons

Payment plans

From \$39.83/mo (6 mo) with 0% APR

Brand Mission Darkness
Color Black
Compatible Devices Cameras, Laptops, Radio, GPS

Mission Darkness also provides a faraday bag tester phone application called “Faraday Test.” It uses cell phone signals and WiFi signals to test shielding in Faraday bags.

Shielded Boxes and Cans

Devices can be stored in properly shielded cardboard boxes, metal trash cans, and ammo cans. Extra heavy duty aluminum foil and conductive aluminum tape can be used to provide the shielding. Thicker aluminum foil provides more shielding and tear resistance than thinner foil. The aluminum tape must be conductive to provide proper shielding.

The shielded electronic device cannot come in contact with the inner side of the outer metal surface.

A cardboard box separates the shielded electronic device from the outer layer of aluminum foil.

Metal trashcans and metal ammo boxes must be lined on the inside with cardboard to prevent the shielded electronic device from coming in contact with the inside of the outer metal surface. All external seams on trash cans and ammo boxes must be sealed with conductive aluminum foil tape.

Reynolds 632 Extra Heavy Duty foil and 3M's 3340 aluminum foil tape with foil backing provide excellent shielding.



Reynolds 632 Extra Heavy Duty Aluminum Foil Roll 18"x500'

Visit the Reynolds Store

4.4 ★★★★★ 144 ratings | 9 answered questions

\$198⁹⁵ (\$198.95 / Count)

Refer friends and earn up to \$500 each year. Get a \$50 Gift Card for each friend who is approved for Amazon Visa.

Purchase options and add-ons

Payment plans

From \$33.16/mo (6 mo) with 0% APR



3M TALC Aluminum Foil Tape 3340, 2.5' x 50 yd, 4.0 mil, Silver, HVAC, Sealing and Patching Hot and Cold Air Ducts, Fiberglass Duct Board, Insulation, Metal Repair

Brand: 3M TALC

4.7 ★★★★★ 1,654 ratings | 60 answered questions

Price: \$20.98 (\$0.14 / Foot)

With Amazon Business, you would have saved \$100.80 in the last year. Create a free account and save up to 8% today.

May be available at a lower price from other sellers, potentially without free Prime shipping.

Pattern Name: Tape

Tape \$20.98 (\$0.14 / Foot)	Tape+ Coil Cleaner \$35.74 ✓prime	Tape+ Evap Foam \$36.07 ✓prime
---	--	---

Brand	3M TALC
Color	Silver
Material	high-strength aluminum foil



An electronic device packaged in a cardboard box then wrapped with Reynolds 632 Extra Heavy Duty foil. It is wrapped in the same fashion as a gift in a box.

All seams are carefully sealed with 3M's 3340 aluminum foil tape by thoroughly rubbing the complete surface of the tape.

This process is repeated to give the box two layers of shielding. As an alternative several smaller boxes can be wrapped once, then place in a larger box that is then also properly wrapped once, giving two layers overall.

Rebuilding a Personal Infrastructure for Survival

After an EMP attack or a severe coronal mass ejection it is reasonable to assume that every unshielded electrical/electronic device in your home will be inoperable. It can also be assumed that these unshielded electrical/electronic devices and the infrastructure to support them will not be repaired or replaced for many years if ever.

Think of what it would take to go camping for an extended period of time but hopefully in your own home. When you go camping you leave your normal electrical/electronic devices at home and take the infrastructure you need with you to the campsite. Your level of survivability and comfort depends on what you brought with you.

In thinking about an EMP attack you have the comfort and convenience of the electrical/electronic devices in your home before the attack and after the attack your everyday electric/electronic devices are rendered inoperable, and now you have to break out your camping gear in your own home to survive. Your level of survivability and comfort depends on what you shielded and stored. Fortunately, your home will provide you with a lot of what you will need.

You should also be aware that EMP attacks could come in waves over several weeks. After an initial attack you should not remove all your electrical/electronic devices from shielding. Select a few devices like flashlights and leave the rest shielded for later when further attacks are less likely.

Your new personal infrastructure should consist of mechanical devices that are not affected by EMP, wood burning appliances, devices that use limited amounts of gasoline, diesel, and propane, and shielded devices such as solar powered devices, rechargeable battery devices, and devices that can be supported with 12 volt DC automotive batteries.

While most cars and trucks will not operate after an EMP attack it is believed that in most cases automotive style lead acid batteries would survive and be usable after an attack. Your new personal infrastructure could include devices to take advantage of these 12 volt DC automotive batteries.

When camping you have to consider storing and cooking food, having enough water for drinking, cooking, and maintaining good hygiene, staying warm in winter, navigating in darkness, maintaining a toilet, nursing wounds and dealing with sickness, and perhaps a few extra items for comfort.

When rebuilding a personal infrastructure in your own home after an EMP attack the same necessities are required; storing and cooking food, having enough water for drinking, cooking, and maintaining good hygiene, staying warm in winter, navigating in darkness, maintaining a toilet, nursing wounds and dealing with sickness, and perhaps a few extra items for comfort.

Following are items to consider for rebuilding a personal infrastructure for survival after an EMP attack or a severe coronal mass ejection.

Mechanical Devices

The great thing about mechanical devices is that they do not need to be shielded. They are neither electrical nor electronic so they rely on human labor not electrical power. They can be helpful before an EMP attack and life saving after an EMP attack.

- Mechanical can opener
- Hand cranked grain mill
- Wind up clock
- Treadle sewing machine
- Wind up wrist watch

Wood Burning Devices and Associated Tools

We are blessed in East Texas with an abundance of trees and wood for fuel. Wood can be used for cooking, heating water, and heating homes. Wood burning devices also do not need to be protected from an EMP attack.

- Rocket stove
- Hibachi
- Cowboy grill
- Wood heating stove
- Hand saw for cutting limbs and trees
- Manual log splitter or maul
- Axe
- Wheel barrel
- Matches and lighters
- Chainsaw without electronics

Devices That Use Limited Amounts of Gasoline, Diesel, Propane and Other Fuels

Devices that use limited amounts of gasoline, diesel, and propane can be very helpful but are dependent on the storage of fuel. In some case a small amount of stored fuel can last for months. *Note: Do not use gasoline/diesel stoves and heaters, or any generators indoors.*

- Candles
- Kerosene lamp (include replacement wicks)
- Camp stove, unleaded gas, sterno, or propane
- Space heater, propane
- Small dual fuel camping generator, gasoline/propane (shielding required)

Solar Stand-Alone Devices

- Solar oven
- Solar powered flashlights or lamps (shielding required)
- Solar generator (shielding required)
- Solar watch (shielding required)
- Solar calculator (shielding required)

Solar radio (shielding required)

Many solar electronic stand-alone devices include a storage battery and can charge USB connected devices such as cell phones, tablets and flashlights. Cell phone networks are not likely to be available but cell phones and tablets could still contain useful information and be used as a camera or calculator.

AA and AAA Battery Powered Devices and Associated Equipment

AA and AAA rechargeable batteries (shielding required)

Solar AA and AAA battery charger (shielding required)

AA or AAA Transistor radio with VHF, UHF, and shortwave (shielding required)

AA or AAA 2 way radios (shielding required)

AA or AAA LED flashlights or lamps (shielding required)

AA or AAA holographic rifle sights (shielding required)

The 120 volt AC AA and AAA battery charger is dependent on using 12 volt DC automotive type lead acid batteries, with a 12 volt DC to 120 volt AC automotive style inverter. Either a solar 12 volt DC automotive battery charger, or a small camping generator with a battery charger is needed to recharge the 12 DC volt automotive batteries.

12 volt DC Automotive Type Lead Acid Battery Devices

12 volt DC automotive batteries from stalled cars and trucks

Solar 12 volt DC automotive battery charger (shielding required)

Small 120 volt AC dual fuel gasoline/propane camping generator (shielding required)

120 volt AC to 12 volt DC automotive battery charger (shielding required)

12 volt DC to 120 volt AC automotive style inverter (shielding required)

12 volt DC fan (shielding required)

12 volt DC light (shielding required)

120 volt AC AA and AAA battery charger (shielding required)

Small 120 volt AC appliances that have been shielded could be occasionally operated with the 12 volt DC automotive type lead acid batteries and the 12 volt DC to 120 volt AC automotive style inverter. Small 12 volt DC appliances that have been shielded could also be occasionally operated directly from the 12 volt DC automotive type batteries.

Other Things to Consider

Old cell phones (shielding required)

Old tablets (shielding required)

Old computers (shielding required)

USB drives with important information (shielding required)

Duplicate chipped car keys and fobs (shielding required)

Satellite phone (shielding required)

Colloidal silver generator (shielding required)

Digital ohm meter (shielding required)

Multi battery tester (shielding required)

Cordless power tools (shielding required)
Stove top coffee pot
Compass

Automobiles, Trucks, Tractors

The most EMP vulnerable components in vehicles are the solid-state devices. This includes computers and sensors. Newer vehicles have more solid-state devices than older vehicles. Newer solid-state devices are also miniaturized making them more vulnerable.

The first vehicles started being produced with ECU's (electronic control units) in the 1970's making them more susceptible to an EMP attack than earlier models. While vehicles manufactured before this time are less vulnerable to damage from an EMP attack they can still be affected if they are located near enough to the EMP weapon detonation. If they are close enough starters, alternators, and coils can be severely damaged.

EMP Whole-House Shielding

There are devices sold to the public that are installed on a building's circuit breaker panel that claim to provide EMP protection to the electric/electronic devices within the building. The sellers of these products claim that they work much like circuit breaker lighting protection but designed specifically for EMP attacks and severe mass coronal ejections.

When lightning strikes a power line a surge of electricity flows along the line and enters the building possibly damaging sensitive electronic devices. A surge protector installed on a circuit breaker box can dampen this effect.

The surges created by an EMP attack or a severe mass coronal ejection are induced through the air into every length of wire exposed to the EMP pulse. This includes wires on the supply side of the circuit breaker panel and the wires within the building. Even the cord attached to an appliance used to plug it into the wall acts as an antenna creating a high voltage surge within the appliance damaging sensitive electronics.

When the military shields electronic equipment it is first enclosed in an EMP shielded enclosure then every penetration of that enclosure must be fitted with isolation and dampening protection. These penetrations allow connection of the electronic equipment to power sources and other devices.

EMP whole-house shielding will not adequately protect electric/electronic devices from an EMP attack.

Unshielded Solar Systems

Unshielded solar panels are more resistant to EMP attack and severe mass coronal ejections than the unshielded inverters and other electronics used in solar systems. Shielding and storing inverters and other electronics for use after an EMP attack or severe coronal mass ejection should be considered. When paired with surviving solar panels these shielded and stored inverters/electronics could provide a considerable amount of electrical power.