RESILIENCE (HTTPS://WWW.DOMESTICPREPAREDNESS.COM/RESILIENCE/)

Cascading Consequences: Electrical Grid Critical Infrastructure Vulnerability

by GEORGE H. BAKER & STEPHEN VOLANDT
Wed, May 09, 2018

If there were a prolonged nationwide, multi-week or multi-month power failure, neither the federal government nor any state, local, tribal, or territorial government – acting alone or in concert – would be able to execute an effective response. This bleak outlook results from understanding that so many critical infrastructures depend on electricity. As such, effective recovery cannot be expected through top-down assistance alone. Without electric power, the goods and services essential to protect life and property would be at risk by day three or perhaps longer depending on preparedness levels. Consequently, it is vital that citizens, households, communities, businesses, and governments be as informed and prepared as possible.

Citizens of the United States are dependent on secure and reliable electric power for their current way of life. If electric power were not available for weeks, months, or even a year, then cascading impacts would degrade multiple critical infrastructures, for example:

- Water supply and wastewater treatments;
- Telecommunications and the internet;
- Food production and delivery;
- Fuel extraction, refining, and distribution;
- Financial systems;
- Transportation and traffic controls;
- Government, including public works, law enforcement, and emergency services;
- Hospitals and healthcare;
- Supply chains; and
- Other critical societal processes.

Loss of life could be catastrophic. Life itself would change.

The recently published InfraGard community preparedness guide, *Powering Through: From Fragile Infrastructures to Community Resilience (*hereafter *Powering Through),* states that no post-industrial society has yet experienced a widespread and prolonged electric blackout. Thus, nations that develop resilience and recovery plans for long-term, wide-area electric power blackouts are in uncharted territory. Although there may be unforeseeable points of failure, cascading effects, and barriers to recovery, plans can still be made for prevention, mitigation, adaptation, and recovery. Imperfect plans, thoughtfully developed, are far better than no plan at all.

This article examines the national power grid and the most significant threats to it. Of particular note, Dr. George Baker developed and others helped refine an important matrix of impacts from five threats to the grid and other key infrastructures. Threats evaluated include:

- Coordinated physical attacks;
- Cyberattacks against industrial control systems and/or other cyber-enabled technology;
- An electromagnetic pulse (EMP) generated by detonation of one or more nuclear warheads in the upper atmosphere over the United States;
- An EMP caused by a coordinated attack using radio frequency weapons; and

- A severe solar storm caused by an Earth-directed coronal mass ejection (CME).

Some human-caused threats might utilize a natural disaster to mask and extend infrastructure damage.

High-Impact Risks to the Electric Grid & Other Critical Infrastructures

There are two types of hazards: *naturally occurring events*, such as a solar geomagnetic storm, a pandemic, or other random events; and *acts of human volition*, such as a human-caused electromagnetic pulse (EMP) attack, a coordinated cyberattack, or a coordinated set of physical attacks on critical grid equipment or related critical infrastructures. This article, drawn from *Powering Through*, presents a summary of the risks associated with dependencies on technologies that are increasingly vulnerable to the "triple threat" of cyber, solar geomagnetic storms (GMD), and electromagnetic pulse (EMP) weapons (see Table 1).

Table 1. Potential Impacts on Critical Infrastructure Affecting the Electric Grid

Equipment at risk	EMP (nuclear)	Solar storm	Cyber	Physical attack	Radio frequency weapons
Transformers	R	R	R-Y	R	R
Generator Stations	R	G	R	R	R
SCADA/Industrial Controls	R	R	R	R	R
Utility Control Centers	R	R	R	R	R
Telecommunications including cellphones	R	R	R	Y	Y
Radio Emergency Communications	R	P	Y	Y	Y
Emergency SATCOM Communications	R	P	Y	Y	Y
Internet	R	R	R	Y	Y
GPS	R	P	Y	Y	Y
Transportation	R	Y	Y	Y	Y
Water	R	Y	R-Y	Y	Y

Legend: Red = direct permanent effects. Yellow = Cascading effects if no backup power. Pink = temporary effect (0.5-36 hours) assuming backup power. Gray = direct effects uncertain. Red-Yellow = potential permanent effects plus cascading effects.

Comments From *Powering Through* on Equipment at Risk

Transformers – Transformers are vulnerable to EMP, solar GMD, or physical attacks. Because unprotected relays (http://www.gurevich-publications.com/articles_pdf/problems_dpr_testing_engl.pdf) supporting transformers can be rapidly opened and closed, transformers may be damaged or destroyed via remote manipulation. Radio frequency weapons can be used to disable substation controls, but are unlikely to affect the transformers themselves directly unless targeted substation supervisory control and data acquisition (SCADA) systems cause secondary damage. If these are attacked and disabled, then the time to replace high-voltage and ultra-high-voltage transformers is likely to be lengthy, and often dependent on overseas manufacturers. There are smaller transformers, designed to serve the residential and small business consumer, that are generally less vulnerable, more easily transportable, and manufactured in the United States. Hence, these transformers might be replaced relatively quickly.

Generator Stations – Unless protected, grid generators at electrical power stations may be disabled by an EMP. Generator control electronics are highly susceptible to EMP. If there is a severe solar storm, there is evidence that the generators themselves could be harmed (https://ieeexplore.ieee.org/document/6672072/). Cyber, physical, or radio frequency weapon attackers may target grid generator stations.

SCADA/Industrial Control Systems (ICS) – These industrial control devices regulate the operation of machinery, breakers, and transformers. SCADA systems are vulnerable to EMP and radio frequency weapons (RFWs). Solar GMD could debilitate SCADA operations if SCADA electronics are connected to long landlines. Since they are accessible from the internet, they may be targeted in cyberattacks. They also may be targets of physical and RFW attacks.

Grid Control Centers – Control facilities vary in size and are the hubs for grid communication and SCADA networks. They provide important situational awareness for directing both normal grid operation and grid reconstitution following a blackout. Because of their long-line interfaces, they are highly susceptible to EMP and GMD effects. If communications lines going into or out of the center were disabled, SCADA functions would be disabled. A cyberattack could target the SCADA devices used in the control center. The facilities could be targets for physical and RFW attacks.

Cellphones – Although many individual cellphones may be unharmed, the phones depend on cell towers interconnected with the local and long-haul telecommunications networks, which are vulnerable to EMP, GMD, RFW, cyberattacks, and physical attack.

Radio Emergency Communications – Some of the emergency radio systems – such as the Federal Emergency Management Agency, National Radio System – continue to work if they are hardened. However, in an EMP, public radio stations and their power sources may not be hardened and may fail. In a solar storm, this communication may be temporarily disabled by atmospheric conditions, but could return in hours to days. The other threats would not affect radio systems if the attack were focused on the grid.

SATCOM – The military's Military Strategic and Tactical Relay, MILSTAR system is EMP protected and will continue to operate. Some additional military portable UHF SATCOM radios that link through high-orbit geo-stationary satellites may also continue to function. Unhardened ground stations may fail in an EMP environment. Commercial satellite phones rely on satellite and ground stations that are likely to fail under EMP stress.

Internet – An EMP would disable key elements of the internet and users' IT equipment. A cyberattack on the grid taking out the generators, SCADA devices, and control centers would also have a cascading effect on internet data centers depending on the capacity and longevity of their back-up power resources. A solar storm can damage long-haul internet interconnects including both metallic and fiber optic links (the latter due to the vulnerability of optical fiber regeneration equipment). Physical or RFW attacks targeting grid assets would disable local internet equipment within Endpoint Group data centers and substation control facilities, but leave the larger internet intact.

Transportation – Railroad signals and highway traffic signals could be directly damaged by an EMP and cause significant delays. Controls and communications elements that use rails for transmitting communications signals are in great jeopardy if not protected and tested. A solar storm should not disable these transportation items if backup power is available for the duration of the grid failure. Likewise, a cyberattack or RFW attack on the grid would not disable transportation systems if backup power is available. In a widespread grid blackout, standard operating procedures to close ports safely could result in delays in prioritized reopening of U.S. ports that are essential for throughput of disaster relief supplies. Chemicals or liquefied natural gas facilities within ports could benefit from backup power capabilities that prevent hazardous chemical releases due to loss of external power. In turn, preventing these chemical releases could avert extended port shutdowns after regional grid blackouts and help to re-establish priority supply chains and accelerate lifesaving and recovery operations.

Water – Because water purification and wastewater purification plants are controlled by SCADA devices, these could be disabled by EMP. Backup emergency diesel generators and solar panels are also vulnerable to E1 pulses (the first of three electromagnetic pulses created by an EMP) unless the generators and the solar panel inverters and controllers are EMP-protected. A cyberattack or RFW attack on the grid would not directly disable the water/wastewater systems if protected backup power were available. Nevertheless, if electric substations continue to be exempt from cyberprotection standards for "high-impact" grid assets, adversary takeover of substation controls could disable aqueduct pumps and locks, as well as other water and wastewater pumps and motors that provide essential water pressure and that process and manage wastewater products.

Probability

Powering Through states:

> *The likelihood of natural event hazards is generally independent of efforts to prevent, mitigate, or recover from such events. Solar storms cannot be deterred, though the consequences can be mitigated. In contrast, the likelihood of volitional acts may be affected by both preventive measures and by the deterrent effects of initiatives to mitigate and recover.*

Powering Through continues:

> *Severe solar geomagnetic storms have been recorded over recent millennia, but their impact on electrical systems has been measured with increasing accuracy only since the August-September 1859 Carrington event. Various models in the past decade estimate the probability of severe solar geomagnetic storms – of the magnitude of the Carrington event or the May 1921 New York Central Railroad storm – as approximately 8% to 12% per decade (http://blog.givewell.org/2015/07/13/geomagnetic-storms-using-extreme-value-theory-to-gauge-the-risk/).*

It is very important to examine the consequences of a long-term power outage and not to concentrate on the probability.

In more than seven decades since nuclear weapons were employed in World War II, a high-altitude electromagnetic pulse (HEMP) attack has not occurred. EMP-optimized atmospheric testing occurred before a Limited Test Ban Treaty, a ban on testing in outer space, the atmosphere, or underwater, took effect in 1963. Deterrence of nuclear weapon use has been successful to date. However, the past may also be a prologue.

Even if most nation states are deterred, not *all* nation states (including failed states) and all subnational groups will be deterred if EMP vulnerabilities are not addressed and diminished. There is no credible way to assign a probability to HEMP attack or to ground-based or cruise missile radiofrequency weapons employment that may not violate the Environmental Modification Convention. However, it is reason for concern that approval for asymmetrical warfare, including a HEMP attack, is found in foreign military literature.

With these diverse hazards in mind, it is essential to recognize that government entities at the federal and state levels cannot protect critical infrastructures by themselves. Public-private partnerships will be necessary, and planning concepts and suggestions for broader audiences must extend beyond government.

Readiness Gap

The authors have considered various scenarios that range from two to three weeks without power on a regional basis, to continent-wide loss of power for over one year. It is certainly possible for an adversary or solar weather to disrupt electrical power for longer than a year. Accepting this possibility is the first major step in readiness planning. Aiming for readiness that can address a one-year outage is daunting; however, that effort will do much to provide for limited-term outages of up to two-three months. Recent events in Puerto Rico caused by Hurricane Maria make it obvious how challenging it can be to restore electrical power even with the remainder of the nation providing assistance.

As of 26 September 2017 (https://en.wikipedia.org/wiki/Hurricane_Maria), 95% of the island was without power and, due to the cascading effects of power loss, less than half the population had tap water and 95% had no cellphone service. Two weeks after the hurricane, 89% of the population was still without power, 44% without water service, and 58% without cell service. One month after the hurricane, there was only slight improvement as 88% of the population lacked power, 29% lacked tap water, and 40% lacked cell service. Three months after the hurricane, 45% of the population still had no power (1.5 million people) and 14% had no tap water; cell service was returning, with over 90% of service restored and 86% of cell towers functioning.

Powering Through observed:

> *On its Ready.gov website (https://www.ready.gov/build-a-kit), the U.S. Department of Homeland Security advises the American public to store food and water for at least three days. As useful as that is for a starting point, high-impact events must also be considered. Many who assume that the government will provide support as soon as day four may think that they do not need to plan for extended emergencies at all.*

In the West now, they are encouraging their citizens to be prepared for two weeks. This is significantly better than three days.

Powering Through continues to illustrate that:

> *In the event that a widespread failure of electrical power, which takes down critical infrastructures for a much longer duration, sufficient relief, whether from government and/or other sources, probably will not be available. Depending on the duration of the infrastructure failure, consequences for unprepared citizens could go well beyond economic loss to include sickness and death from dehydration, disease, pollution, exposure, starvation, fire, and civil unrest. Consequences for the nation could include a breakdown of coherent central government (local, state, and federal), leading to possible loss, at least temporarily, of effective sovereignty: the full right and power of governing bodies to govern themselves without outside interference. There could also be unacceptable delays in recovery, resulting in extensive loss of life and property. All of these are unacceptable risks.*

The U.S. House of Representatives has passed several bills that address U.S. electric power grid vulnerabilities. The Federal Energy Regulatory Commission sponsored research at Oak Ridge National Laboratories to characterize EMP effects on the national power grid. There are several indications that these threats are being taken seriously by federal officials. For example, the White House National Science and Technology Council's National Space Weather Strategy (https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/final_nationalspaceweatherstrategy_20151028.pdf) and National Space Weather Action Plan (https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/final_nationalspaceweatheractionplan_20151028.pdf) are strong indicators. In addition, the Defense Threat Reduction Agency (http://highfrontier.org/wp-content/uploads/2016/07/DTRA-IAN-Press-Release-June-24-2016.pdf) has recognized the EMP effects on the national electric power grid in a request to strengthen the critical civil infrastructure on which military facilities in the United States depend for at least 98% of their electricity. The Department of Energy and Electric Power Research Institute issued a Joint Electromagnetic Pulse Resilience Strategy (https://www.energy.gov/sites/prod/files/2016/07/f33/DOE_EMPStrategy_July2016_0.pdf) in July 2016. The Department of Homeland Security Office of Infrastructure Protection explicitly noted the EMP threat to the cyber industry in the public and more detailed "For Official Use Only" reports issued in 2016 (https://www.nanog.org/sites/default/files/Thompson - Key Findings.pdf) by the Regional Resiliency Assessment Program. All of the foregoing initiatives validate the threat.

However, no plan or preparation exists at the national level that addresses long-term electrical power outages that span large regions or the continent. In such a case, there would be no neighboring state or region that could provide the depth of assistance required to promptly assist the general public, businesses, and local or state governments. Each region would be grappling with its own problems (see Figure 1).

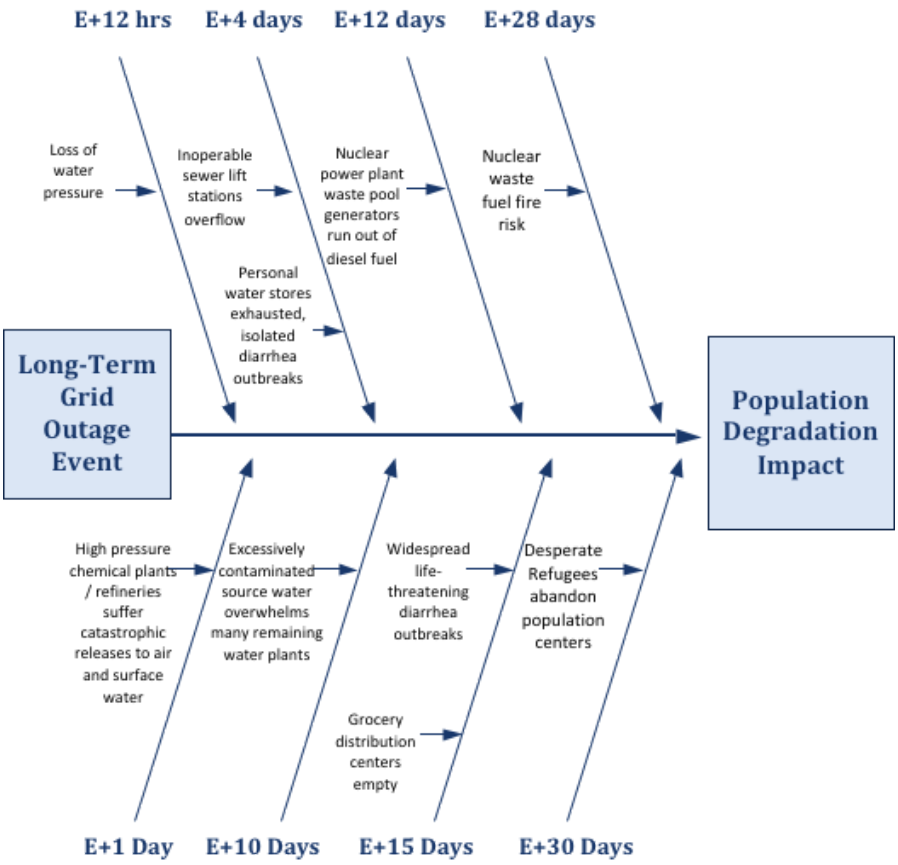

Fig. 1. Long-Term Power Outage Worst Case Timeline, as shown in *Powering Through*, p. 166 (*Source:* Stephen Volandt, Auroros Incorporated).

Recommendations

Acceptance of the threats presented in this article as being credible is the first step in any recommendation. For example, Section 1913 of The 2018 National Defense Authorization Act (https://www.congress.gov/bill/115th-congress/house-bill/2810/text/pap) addresses EMP specifically. Additionally, The Congressional EMP Commission has been granted permission to publicly release two reports regarding EMP:

- EMP Commission, Volume I, Assessing the Threat from EMP Attack – Executive Report, July 2017, publicly released April 2018 and available at: http://www.dtic.mil/dtic/tr/fulltext/u2/1051492.pdf (http://www.dtic.mil/dtic/tr/fulltext/u2/1051492.pdf%20/t%20_blank); and
- EMP Commission, Volume II, Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures, July 2017, publicly released April 2018 and available at: http://www.dtic.mil/dtic/tr/fulltext/u2/1051494.pdf (http://www.dtic.mil/dtic/tr/fulltext/u2/1051494.pdf)

Overall, a strategy to protect and rapidly restore lifeline sectors – including water, electricity, food, medical and emergency services, and telecommunications – offers the potential to maximize "shelter in place" capabilities and minimize uncoordinated evacuations. Uncoordinated evacuations have the potential to escalate threats to public safety, protection of supply chains, and equitable distribution of life-essential goods and services.

As stated in the *Powering Through* preparedness guide:

> *The United States needs to augment the planning and investments that are essential to cope with extended duration catastrophes. Whole community participation in both planning and recovery must be the new norm, and this vital process needs to start now and continue. The fundamental criterion for success should be prepared individuals and communities capable of surviving long-term infrastructure failure, while at the same preserving families, assisting others in their communities, and defending the nation.*

The White House National Science and Technology Council in October 2015 issued the National Space Weather Strategy and the National Space Weather Action Plan, calling for the "whole of community (https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/final_nationalspaceweatherstrategy_20151028.pdf)" to plan for a severe solar storm and noting that other threats could cause similar effects. In 2016, the Department of Energy and the Electric Power Research Institute issued a Joint Electromagnetic Pulse Resilience Strategy (https://www.energy.gov/sites/prod/files/2016/07/f33/DOE_EMPStrategy_July2016_0.pdf) for the national electric power grid. Also in 2016, the Defense Threat Reduction Agency recognized the operational importance of grid survivability (http://www.stop-emp.com/Final-DTRA-IAN-Press-Release -w-logos-centered.pdf) in the event of an EMP, and requested proposals to strengthen the private sector and military critical infrastructure upon which defense missions depend. The Department of Homeland Security Office of Infrastructure Protection specifically noted the EMP threat to the telecommunications industry in a 2016 report prepared for the Regional Resiliency Assessment Program (https://coar.risc.anl.gov/ashburn-va-regional-resiliency-assessment/). Finally, the 2018 National Defense Authorization Act calls out the vulnerability of military bases caused by their dependence on the electrical power grid instead of relying on locally produced electricity. The foregoing documentary findings validate the threat and underscore the urgent need for infrastructure planning and protection. Assessments are still needed for households, communities, and organizational readiness to manage the risks described in this article.

InfraGard, more formally the InfraGard National Members Alliance is a nonprofit consisting of more than 50,000 volunteers committed to assessment and protection of critical infrastructures throughout the United States. InfraGard sponsored the December 2016 publication of Powering Through: From Fragile Infrastructures to Community Resilience, an Action Guide Powering Through, Version 1.0, which was researched and prepared by InfraGard's Electromagnetic Pulse Special Interest Group (EMP-SIG) volunteers. Powering Through examines actions that could be taken now to be more resilient, protect life and property during grid outages, and prepare for expedited recovery. Most of the content of this article is taken from this action guide, which is available at: https://www.amazon.com/Powering-Through-Infrastructures-Community-Resilience/dp/0998384402 (https://www.amazon.com/Powering-Through-Infrastructures-Community-Resilience/dp/0998384402)

Dr. George H. Baker (pictured above), is a professor emeritus at James Madison University, where he directed the JMU Institute for Infrastructure and Information Assurance. Previously, he led the Defense Nuclear Agency's Electromagnetic Pulse (EMP) program, directed the Defense Threat Reduction Agency's assessment arm, and served as a senior scientist for the Congressional EMP Commission. He is a member of the Foundation for Resilient Societies' board of directors. He holds an M.S. in Physics from University of Virginia, and a Ph.D. in Engineering Physics from the U.S. Air Force Institute of Technology. Currently, he is CEO of BAYCOR, LLC – a consulting company primarily devoted to preparedness for and protection against major electromagnetic threats to critical infrastructures including nuclear EMP, solar storms, and radio frequency weapons.

Stephen Volandt, vice president of Auroros Inc., currently serves as a vice-chair of the FBI's InfraGard Electromagnetic Special Interest Group (EMP-SIG). He has over 30 years of experience leading projects that assess and transform critical operations with focus on capability portfolio management and cascading consequence management. He has led teams for the FBI, Headquarters

Army, and Headquarters Marine Corps to address enterprise-wide operations and systems improvement. His experience spans operations in austere locations, weapons of mass destruction neutralization, nuclear terrorism, cybersecurity, and infrastructure readiness and protection. His current passion is the establishment of vibrant, resilient, and self-sustaining communities.

Significant contribution to this article was provided by:
William R. Harris is an international lawyer specializing in arms control, nuclear nonproliferation, energy policy, and continuity of government. He is a member of the board, secretary, and a principal investigator involved in reliability standard development for critical infrastructures for the Foundation or Resilient Societies. He formerly served as a space operations lawyer for reconnaissance and communication systems of the United States government. He served as a senior (legal) advisor to the Commission on Electromagnetic Pulse (EMP) in January-December 2017. Since September 2017, he has been a vice chair of the EMP Special Interest Group of InfraGard, a nonprofit committed to protection of critical infrastructures. He holds a B.A. from Harvard College and a J.D. from Harvard Law School.

Mary D. Lasky is the chairman of the InfraGard Electromagnet Pulse Special Interest Group (EMP SIG). She is the lead editor and author of "Powering Through: From Fragile Infrastructure to Community Resilience" an action guide on being prepared if there is grid failure. She is a Certified Business Continuity Professional (CBCP). She has been the program manager for business continuity planning for the Johns Hopkins University Applied Physics Laboratory (JHU/APL). She is a past president of the Community Emergency Response Network Inc. (CERN) in Howard County, Maryland. She is a past president of the Central Maryland Chapter of the Association of Contingency Planners (ACP). At APL, she has held a variety of supervisory positions in Information Technology and in business services.

MORE IN RESILIENCE...

CBRNE Weapons & Islamic State – A Bad Combination
(https://www.domesticpreparedness.com/resilience/cbrne-weapons-islamic-state-a-bad-combination/)
by RICHARD SCHOEBERL - WED, APRIL 25, 2018

In Search of Infrastructure-Proof Emergency Alerts
(https://www.domesticpreparedness.com/resilience/in-search-of-infrastructure-proof-emergency-alerts/)
by RODRIGO (RODDY) MOSCOSO - WED, APRIL 18, 2018

Five Steps Toward Enhancing Climate Resilience
(https://www.domesticpreparedness.com/resilience/five-steps-toward-enhancing-climate-resilience/)
by EMILY WASLEY - WED, APRIL 04, 2018

Evolving Needs: Interoperable Communications
(https://www.domesticpreparedness.com/resilience/evolving-needs-interoperable-communications/)
by THE METROPOLITAN WASHINGTON COUNCIL OF GOVERNMENTS' INTEROPERABLE COMMUNICATIONS REGIONAL PROGRAMMATIC WORKING GROUP - WED, FEBRUARY 21, 2018

View all articles in Resilience. (https://www.domesticpreparedness.com/resilience/)

DOMESTIC PREPAREDNESS (http://www.domesticpreparedness.com/)
P.O. Box 810
Severna Park, MD (Maryland) 21146
(410) 518-6900 (tel:+14105186900)