PATH TO SURVIVAL

FIELD BRIEF

Cyber-attack Brief

A short, practical field guide to the grid-down scenario most credible assessments rank as the most probable. What a grid cyberattack does, and why the boring preparation is what saves you.

THREAT CLASS: **Most probable / variable**

WARNING TIME: **None to minimal**

EXPECTED DURATION: **Hours to extended**

This brief is one of three in the grid-down series: EMP, Cyberattack, and Solar Storm. Each covers a distinct threat with a distinct response. Read all three, because the failure modes differ but the foundation they share is what actually keeps you alive.

01 · THREAT PROFILE

What a grid cyberattack actually is

> A cyberattack on the power grid does not need a nuclear weapon or a solar cycle. It needs code and access. That low barrier is exactly why most credible assessments rank it as the most probable of the three grid-down threats, and the one nation-state doctrine actively plans around.

This is the scenario that gets the least dramatic coverage and deserves the most attention. It lacks the cinematic quality of a nuclear pulse or a solar flare, which is precisely why people underprepare for it while overpreparing for the threats that make better stories.

4+

Nation-states with known grid-attack doctrine (Russia, China, North Korea, Iran)

Code

All it requires, no weapon or natural event needed

Combined

Increasingly conceived as combined-arms attacks, cyber paired with sabotage

THE KEY DISTINCTION

A cyberattack corrupts software, control systems, and the operational technology that runs the grid. It does not necessarily destroy the physical transformers the way a solar storm does. That can mean a shorter, more recoverable outage, or a targeted, repeatable one that returns the moment you think it is over.

02 · IMMEDIATE REALITY

The widest range of outcomes

> A cyberattack has the least predictable duration of the three threats. It could be hours if contained, or far longer if sophisticated and sustained. That uncertainty is the defining feature you must plan around.

WHY THE DURATION IS UNPREDICTABLE

- **If the systems can be cleaned and restored,** the physical grid is intact and power may return relatively quickly.
- **If the attack is sophisticated,** it can be designed to persist, to re-trigger after apparent recovery, or to resist restoration.
- **If it is timed to coincide with another crisis,** a storm, a heatwave, a physical attack, the combined effect is far worse than the cyberattack alone.

THE COMBINED-ARMS CONCERN

Security analysts increasingly describe grid cyberattacks not as standalone events but as one element of a combined operation, cyber paired with physical sabotage, potentially paired with other vectors, designed to black out large regions quickly and keep them down. This is why a cyberattack should not be imagined as a clean, brief inconvenience. Plan for the possibility that it is the opening move of something larger.

WHAT THIS MEANS FOR YOU

Because the duration is genuinely unknowable in advance, the only safe assumption is the pessimistic one. Prepare as if the outage could be extended, because a plan built for a long outage covers a short one automatically, while the reverse is fatal.

03 · PRIORITY ACTIONS

Why the boring preparation wins

> A cyberattack has almost no threat-specific gear. Faraday bags do nothing here, your electronics are fine, they just have nothing to connect to. This is why it is the most dangerous one to ignore: the only preparation that helps is the unglamorous foundation.

FIRST **Build the extended grid-down foundation.** This is essentially your entire cyberattack defense. Water, food, heat, sanitation, medical continuity, and power that works without the grid.

FIRST **Reduce dependence on digital systems.** Keep cash on hand, paper copies of critical documents, and offline versions of anything you would need if apps and banking are down.

NEXT **Secure a renewable power source,** because if the outage runs long, regeneration beats a battery you will drain.

NEXT **Keep a non-digital communication and information plan,** a battery or hand-crank radio to receive emergency broadcasts when networks are down.

THE DIGITAL-DEPENDENCE TRAP

Modern life routes almost everything through systems that fail in a cyberattack: card payments, banking, mobile networks, even digital medical records and prescriptions. A grid cyberattack can take these down even where your local power flickers back. The person who kept cash, paper records, and offline essentials keeps functioning. The person who digitized everything does not.

04 · RESILIENCE STEPS

Building for the unknown duration

> Since you cannot know how long a cyberattack outage lasts, resilience means being able to function across the full range, from a few hours to an extended period, without assuming which one you got.

LAYER	WHAT IT PROTECTS AGAINST
Cash reserve	Card and banking systems down. Keep enough physical cash for essentials over several days to weeks.
Paper records	Loss of digital access. Copies of ID, insurance, prescriptions, key contacts, account info, stored offline.
Offline essentials	App and network failure. Downloaded maps, reference material, medical info, not dependent on a live connection.
Stored supplies	Supply-chain disruption. Food, water, and necessities to ride out an outage of uncertain length.
Independent power	Extended grid failure. A renewable source, not just a battery bank.

THE MINDSET THAT MATTERS

A cyberattack is a reminder that modern convenience is a dependency. Every service you rely on that needs the grid, the internet, or a live network is a single point of failure in a cyberattack. Resilience is having a non-digital fallback for each critical function: payment, information, communication, records, and power. You do not have to abandon modern systems. You have to not be helpless without them.

SANITATION AND THE LONG TAIL

If a cyberattack outage extends into weeks, the same long-duration risks as any grid-down event apply. Water and sewage systems can fail, and disease becomes the primary threat. A sanitation plan is part of cyberattack preparedness precisely because you cannot rule out the long version in advance.

05 · THE FOUNDATION

What a cyberattack shares with every grid-down event

> A cyberattack is almost entirely the shared foundation, with a digital-independence layer on top. That foundation is what carries you through all three scenarios in this series.

Whether the control systems are corrupted by a cyberattack, the transformers destroyed by a solar storm, or the electronics fried by an EMP, the shared consequence is identical: no grid power for an extended, unknown period.

- [ ] **Water:** stored supply plus a way to filter and purify more. One gallon per person per day, minimum.
- [ ] **Food:** shelf-stable staples that need no refrigeration, enough for weeks to months, not days.
- [ ] **Heat and cooling:** a grid-independent way to stay warm in winter and manage heat in summer, that produces no dangerous indoor exhaust.
- [ ] **Sanitation:** a plan for when the toilets and water stop, disease is a leading disaster killer.
- [ ] **Medical:** backup for anyone dependent on refrigerated medication or powered devices.
- [ ] **Power:** a renewable source you can regenerate, not just a battery bank you will drain.
- [ ] **Digital independence:** cash, paper records, and offline essentials for when networks fail.

THE SINGLE MOST IMPORTANT SHIFT

Think past the two-week mark, and assume the pessimistic duration. A cyberattack could be brief, but a plan built only for brief is a plan that fails if it is not. What matters is whether any part of your setup renews itself without the grid, and whether you can function when the digital systems you depend on go dark.

06 · SUMMARY

Cyberattack brief, one page

FACTOR	CYBERATTACK
Probability	Highest of the three. Requires only code and access, and is actively planned by nation-states.
Warning time	None to minimal.
Failure mode	Corrupts control systems and software. Usually spares physical hardware and electronics.
Duration	Widest range: hours if contained, extended if sophisticated or combined.
Unique defense	Digital independence: cash, paper records, offline essentials. No useful gear-specific defense.
Shared defense	Extended grid-down foundation: water, food, heat, sanitation, medical, renewable power.

THE THREE ACTIONS THAT MATTER MOST

1. **Build the extended grid-down foundation,** which is nearly the entire cyberattack defense, and assume the pessimistic duration.
2. **Reduce digital dependence** with cash, paper records, and offline essentials, so a network failure does not leave you helpless.
3. **Secure a renewable power source,** because you cannot rule out the long version of this outage in advance.

READ THE OTHER TWO BRIEFS

A cyberattack is the most probable scenario and the least dramatic, which is exactly why it is underprepared for. The Solar Storm brief covers the certain-over-time threat, and the EMP brief covers the least likely but harshest one. The same foundation serves all three, which is the real lesson of the entire series.