DOI:10.1145/3325287

Peter J. Denning

The Profession of IT
An Interview with David Brin on Resiliency

Many risks of catastrophic failures of critical infrastructures can be significantly reduced by relatively simple measures to increase resiliency.

PHOTO BY CHERYL BRIGHAM

Many people today are concerned about critical infrastructures such as the electrical network, water supplies, telephones, transportation, and the Internet. These nerve and bloodlines for society depend on reliable computing, communications, and electrical supply. What would happen if a massive cyber attack or an electromagnetic pulse, or other failure mode took down the electric grid in a way that requires many months or even years for repair? What about a natural disaster such as hurricane, wildfire, or earthquake that disabled all cellphone communications for an extended period?

David Brin, physicist and author, has been worrying about these issues for a long time and consults regularly with companies and federal agencies. He says there are many relatively straightforward measures that might greatly increase our resiliency—our ability to bounce back from disaster. I spoke with him about this.

Q: What is the difference between resilience and anticipation?

BRIN: Our prefrontal lobes help us envision possible futures, anticipating threats and opportunities. Planners and responders augment these organs with predictive models, intel-gathering, and big data, all in search of dangers to anticipate and counter in advance. Citizens know little about how many bad things these protectors have averted. But this specialization in anticipation makes it hard for protectors to appreciate how we cope when our best-laid plans fail, which they do, sooner or later.

Resilience is how we cope with unexpected contingencies. It enables us to roll with any blow and come up fighting, keeping a surprise from being lethal. It's what worked on 9/11, when all anticipatory protective measures failed.

Q: Let's see what anticipation and resilience look like for a common threat, disruptive electrical outages. They can be caused by storms, birds, squirrels, power grid overload, or even preventive reduction of wildfire risk. Without power, we cannot use our computers or access our files stored in the Internet. Even our best disaster planning cannot fix the disruption if infrastructure damage is severe. Yet, communication is essential

for recovery. What can we do to preserve our ability to communicate?

On 9/11, passengers aboard flight UA93 demonstrated remarkable resilience when they self-organized to stop the terrorist plot to use that plane as a weapon against their country. If we want that kind of resilience to work on a large scale, we need resilient communications. Alas, our comm systems are fragile to failure in any natural or unnatural calamity. One step toward resilience would be a backup peer-to-peer (P2P) text-passing capability for when phones can't link to a cellular tower. Texts would get passed from phone to phone via well-understood methods of packet switching until they encounter a working node and get dropped into the network. Qualcomm already has this capability built into their chips! But cellular providers refuse to turn it on. That's shortsighted, since it would be good business too, expanding text coverage zones and opening new revenue streams. Even in the worst national disaster, we'd have a 1940s-level telegraphy system all across the nation, and pretty much around the world.

All it would take to fix this is a small change of regulation. Five sentences requiring the cell-cos to turn this on whenever a phone doesn't sense a tower. (And charge a small fee for P2P texts.) Doing so might let us restore communications within an hour rather than months.

Many efforts have been made to empower folks with ad hoc mesh networks, via Bluetooth, Wi-Fi webs, and so on. None of these enticed more than a tiny user base—nothing like what's needed for national resilience.

Q: It appears that solar power for homes and offices is at a tipping point as more people find it cheaper than the power grid. Localized solar power should also bring new benefits such as ability to maintain minimum electrical function at home during a blackout. Is independence from the electrical grid good for resilience?

It would be. One can envision a million solar-roofed homes and businesses serving as islands of light for their neighborhoods, in any emergency. But there's a catch. Under current regulations, almost all U.S. solar roofs have a switch that *shuts down* the home or business solar system when the electrical utility has blacked out. The purpose is to prevent spurious home-generated voltages from endangering repair linemen. This is a lame excuse for an insane situation. Simply replace that cutoff switch with one that would still block backflow into the grid, but that feeds from the solar inverter to just two or three outlets inside the home, running the fridge, some rechargers, and possibly satellite coms. Just changing over to that switch would generate archipelagos of autonomous, resilient civilization spread across every neighborhood in America, even in the very worst case. A new rule requiring such switches, and fostering retrofitting, would fit on less than a page.

Alas, our comm systems are fragile to failure in any natural or unnatural calamity.

Across the next decade, more solar systems will come with battery storage. But this reform would help us bridge the next 10 years.

Q: What about protection against electromagnetic pulse disruption?

Much has been written about danger from EMP—either attacks by hostile powers or else the sort of natural disaster we might experience if the Sun ever struck us head-on with a coronal mass ejection, commonly called a solar flare. These CMEs happen often, peaking every 11 years. We've been lucky as the worst ones have missed Earth. But some space probes have been taken out by direct hits and a bulls-eye is inevitable.

The EMP threat was recognized over 30 years ago. We could have incentivized gradual development of shielded and breakered chipsets, including those in civilian electronics. Adoption could have been stimulated with a tax of a penny per non-compliant device, with foreseen ramp-up. By now we'd be EMP resilient, instead of fragile hostages either to enemies or to fate.

Q: What about solar on the southward walls of buildings to power the buildings? Some cities are already doing this.

Sure, south-facing walls are another place for photovoltaics. But there's competition for that valuable real estate—*urban agriculture*. Technologies are cresting toward where future cities may require new buildings to recycle their organic waste through vertical farms that purify water while generating either industrial algae or else much of the food needed by a metropolis. With so much of the world's population going urban, no technology could make a bigger difference. The pieces are coming together. What's lacking is a sense of urgency. Pilot programs and tax incentives should encourage new tall buildings to utilize their southward faces, nurturing this stabilizing trend during the coming decade.

Q: You've also spoken about apps systems that turn your smartphone into an intelligent sensor. Can you say how this supports resiliency?

Cellphones already have powerful cameras, many with infrared capability. Soon will come spectrum-analysis apps, letting citizens do local spot checks on chemical spills or environmental problems, and feeding the results to governments or NGOs for modeling in real time. The Tricorder X Prize showed how just a few add-on devices can turn a phone into a medical appraisal device, like Dr. McCoy had in "Star Trek." Almost anyone could use such apparatus in the field with little training. Take a few measurements, and a distant system advises you on corrective actions.

Infrared sensors, accelerometers, and chemical sensors could provide a full array of environmental awareness systems by turning citizen cellphones into nodes of an instant awareness network. (I describe this in my novel *Existence*.)

Such a mesh is already of interest to national authorities. But the emphasis has been hierarchical—authorities send public reports down to citizens after gathering and interpreting data flowing upward. The hierarchical mind-set comes naturally when you are an authority with protective duties. But this can blind even sincere public servants to one of our great strengths—

the ability of average citizens to self-organize laterally.

Use your imagination. The greatest long-term advantage of our kind of society is that lateral citizen networks, while occasionally inconvenient to public servants, aren't any kind of macro-threat, but will make civilization perform better. This is in contrast to despotic regimes, for whom such citizen empowerment would be lethal.

Q: Some of your proposals are less familiar. You have spoken of "all sky awareness." What is that and how does it improve resiliency?

Defense and intelligence folks know we need better 24/7 omni-awareness of land, sea, and air. Major efforts involve protective services and space assets. When the Large Synoptic Telescope comes online in Chile, we'll find 100 times as many asteroids that could threaten our planet, or like the one that broke 10,000 windows in Chelyabinsk. Closer to home, dangerous space debris should be tracked round the globe.

Similar technology could improve air safety and impede smugglers by tracking both legal and illicit air traffic. For example, the cell networks I mentioned earlier could detect and triangulate aircraft engine sounds for comparison to an ongoing database, especially at low altitudes where drug smugglers and human traffickers operate, or where terrorists might attempt an attack, or detecting the path of airliners that stray, like Malaysian Air flight 370. Imagine those in peripheries like Canada, Alaska, or nearby waters automatically reporting sonic booms. Among myriad more mundane uses, these might perhaps localize incoming hypersonic weapons, of the kind announced recently by Russian President Vladimir Putin.

Sound implausible? In December 2018, a loose network of amateur 'plane-spotters' managed to track Air Force One visually, during President Trump's top-secret Christmas dash to a U.S. air base in Iraq. A U.K. photographer used these clues to snap the unmistakable, blue-and-white 747 jetting far overhead.

Another method: revive the SETI League's Project Argus, aiming to establish radio and optical detectors in 5,000 amateurs' backyards, spread around the world. As Earth rotates, these backyard stations would sweep the sky in overlapping swathes, sifting for anomalous signals, but also detecting almost anything interesting that happens up there. Argus failed earlier because of the complexity and expense of racks of equipment. Today—with a small up-front investment by some mere-millionaire—we could offer a small box for a couple of hundred bucks that could be latched to an old TV dish-antenna, then Wi-Fi linked via the owner's home. The dish—plus a small optical detector—could report detections in real time and any pair or trio that correlate would then trigger a look by higher-level, aimable devices.

Sure, most of the participants would think of their backyard SETI stations as helping sift the sky for aliens. So? As a side benefit, we'd become hundreds of times better at detecting almost any transient phenomenon overhead, improving both anticipation and resilience.

I can go on with a much longer list of unconventional and generally very inexpensive ways that very simple regulatory or incentive actions might transform national resilience, making society more robust to withstand shocks across the decades ahead.

Q: What about civil unrest or lawlessness if the disaster takes out or overwhelms local law enforcement? Easy to see gangs roaming affluent neighborhoods in SUVs stealing stuff and especially food, with no police to stop them.

I well-understand this worry! I've written collapse-of-civilization tales. (One of them, *The Postman*, was filmed by Kevin Costner.) Hollywood presents so many apocalyptic scenarios, we tend to assume we live on a fragile edge of collapse. But Rebecca Solnit's book, *A Paradise Built In Hell*, shows decisively that average citizens—whether liberal or conservative—are actually pretty tough and dynamic. They quickly self-organize to help their neighbors. A quarter or more of citizens will almost always run **toward** whatever the problem is. Take citizen response on 9/11, or when disasters hit their neighborhoods.

If "affluent neighborhoods" want to be safe, there's one method that works over the long run ... don't alienate the poor and middle class and ensure that the vast majority identify as members of the same overall tribe. As neighbors, we'll come to your defense.

Sincere people across the spectrum are right to worry about companies and governments collecting massive amounts of personal data on citizens.

Q: Anything to mitigate cyber attacks, including phishing and massive identity theft?

Sincere people across the spectrum are right to worry about companies and governments collecting massive amounts of personal data on citizens: from the ways they use their smartphones, to always-on mics at home and office (for example, Alexa). Phishing is another example where crooks use already open knowledge about you to lure you into fatal online mistakes. We all fret about disparities of power that may lead to the "telescreen" in George Orwell's *Nineteen Eighty-Four*. From facial recognition to video fakery to brainwave interpretation and lie detectors, if these techs are monopolized by one elite or another, we may get Big Brother forever. There are forces in the world who are eager for this. China's "social credit" system aims to the masses to enforce conformity on one another.

In the West, most people are right to find this prospect terrifying. The reflex in response is to say: "let's ban or restrict this new kind of light." And that is the worst possible prescription. The elites we fear will only gain great power if they can operate in secret, enhancing that disparity, because we won't be able to look back.

Consider. It matters much less what elites of all kinds *know* about you than what they can *do* to you. And the only thing that deters the latter is what *we* know about *them*. Denying elites the power to see has never happened (for long) anywhere in the history of the world. But denying them the ability to harm citizens is something we've (imperfectly) accomplished for 200 years. We've done it by insisting that *we* get to see, too. If not as individuals, then via the NGOs we hire to look for us.

As I appraise in *The Transparent Society*, the answer is *more* light, not less, for common citizens to be empowered by technology to take up much of the burden of supervising and arguing and applying accountability. The more we can see the less the bad groups can hide. If we do this, we'll not only be resilient, we'll *never* have Big Brother.

The answer to phishing, ID theft, etc., is the same as always—to catch and deter villains, by ending most shadows for roaches to hide in.

Q: We don't know how to do this because the Internet itself is baked in a cloak of anonymity. We are not going to redesign the Internet protocols anytime soon. We need more than light. Isn't the solution good locks on our databases?

Sorry, show me one time when "good locks" worked for very long. Every week, some previously "for sure" database is raided or leaks. All that needs happen is for any lock to fail once, at all, via code-breaking or hacking or phishing or human error, and the information is loose, infinitely copyable. If you base your sense of safety on secrecy, it will be impossible to verify what others *don't know*.

Look, I'm not saying that there should be no secrets or privacy! Our skilled protectors need tactical secrecy to do their jobs. But smaller volumes and perimeters are easier to defend and seal. It has always been U.S. policy that secrecy should bear some burden of justification and—eventually—a time limit.

This isn't the time or place to argue the point. Alas, the reflex to seek safety in shadows is so strong that folks forget how we got the very freedoms, wealth, and justice we worry about losing. Not by *hiding* but by assertively demanding to see. What I do ask is that you squint and look ahead 50 or 100, and ask *what is our baseline victory condition?*

In an era of high tech and lightning reaction times, we must rely on a highly professional cadre of protectors.

Every enemy of this enlightenment, individualist, open-society experiment—every lethal foe—is mortally allergic to light. They suffer when their plans, methods, agents, and resources are revealed. In contrast, we are at worst inconvenienced and—as shown by the Snowden and WikiLeaks affairs—even prodded to improve a bit. If, say in 50 years, there is worldwide transparency of ownership and power and action, then we win. We—a humanity that is inquisitive, confident, individualistic, and free—simply win.

Q: These resiliency proposals all sound so reasonable. Why have they not been implemented?

A cynic would answer that there's not much economic-constituency behind resilience. No big-ticket orders. How much money is to be made from a slightly costlier home-solar cutoff switch that would feed rooftop energy to three outlets in a million U.S. homes? I spoke about backup peer-to-peer texting at a defense industry conference where a Verizon vice-president in attendance went absolutely livid. Qualcomm tried subsequently to get them—and AT&T—to try some regional experiments; might P2P texting might actually turn a profit? Alas, no one wants to risk disruption, even though this one function could knit our entire continent together, in a crisis.

EMP resistance should have been slowly woven into civilian electronics for decades. And here's a thought—maybe it has been! After all, if we had truly savvy leaders, they would want to slide this protection into place as quietly as possible. Why? Because there is a critical vulnerability window, during which those who are thinking about hitting us might strike if they see the chance slipping away. History shows that such transitions can be dangerous, as revealed by John F. Kennedy in *While England Slept*.

Some bright folks are paying attention. Elon Musk told me he would fix the solar cutoff problem with his Power Wall storage system, and that *is* the answer ... in a decade. A $200 switch would still be worthwhile, till then. Another zillionaire expressed interest in the all-sky awareness project, but more for its contribution to SETI than national or world security. Membership in CERT—Community Emergency Response Teams—rises every year. And so it goes. Just way too slowly.

What truly matters is the very concept of resilience, which worked so well on 9/11 and at every turn of American history. The U.S. Army, till just one generation ago, always based its planning on vast pools of talented, healthy volunteers rushing in to fill the thin blue line. Sure, in an era of high tech and lightning reaction times, we must rely on a highly professional cadre of protectors. But the worst thing they could do is to declare "Count on us ... and *only* on us."

No. We love you and thank you for your service. But a time will come when you will fail. And when that happens, it will be our turn—*citizens*—to step up.

Help us to prepare, and we won't let you down.

David Brin (http://www.davidbrin.com) is an astrophysicist whose international best-selling novels include *The Postman*, *Earth*, and *Existence*. He serves on advisory boards (for example, NASA's Innovative and Advanced Concepts program or NIAC) and speaks or consults on a wide range of topics including AI, SETI, privacy, and national security. His nonfiction book about the information age—*The Transparent Society*—won the Freedom of Speech Award of the American Library Association.

Peter J. Denning (pjd@nps.edu) is Distinguished Professor of Computer Science and Director of the Cebrowski Institute for information innovation at the Naval Postgraduate School in Monterey, CA, is Editor of ACM *Ubiquity*, and is a past president of ACM. The author's views expressed here are not necessarily those of his employer or the U.S. federal government.