A New Paradigm for Internet Resilience to the Extremes of Climate Change

by David Theodore

Waking up to the internet disaster.

Welcome to the Information Age, where our livelihoods, healthcare and national security are tethered to the internet. We have apps to find parking, land a job and give ourselves an EKG, yet incredibly we find that in natural disasters, it's gone. All of it: internet, phones, text messaging; even 911.

It's no small irony that in storm ravaged communities, a Magic Marker and sheet of cardboard obviate all the electronic ingenuity of the past century. The problem is magnified for business and government where the growing dependence on data and the rise of extreme weather pose dire consequences for regional economies, public health and safety and even national security.

Widescale outages once statistically insignificant[1], now last days and weeks. Power outages have tripled, just in the past decade. The cost of business disruption is colossal, and the threat grows exponentially with the rise of cloud computing. Today, our most mission critical data lays in the tracks of climate change, and if your ear is close enough you can hear the whistle blowing.

The threat is *here*, and it's not just sea level rise.

Latest research on climate and the internet focuses on sea level rise, projected across decades. Yet, a more urgent threat is already here: extreme weather. Record breaking floods, precipitation and heat are the new norm, and all indications are that climate is in a worsening trend. If we don't adapt the internet to this reality, we'll be sunk long before sea levels get us.

The question is what to do, because left unchecked, losses will devastate every sector from health care to finance, hospitality, energy, water, transportation, even national security[4].

FCC Commissioner, Jessica Rosenworcel, speaks to a persistent problem:

Then: 2012

Now: 2020

Let's understand the problem.

The internet is a mystery to us. We don't know where it is or how we get to it. It's hard to address vulnerabilities we can't visualize. Therefore, to understand the fix, let's talk about how we access the internet.

The internet comes from internet data centers, thousands of them in the U.S. and worldwide. They're home to carriers, like Verizon and AT&T, as well as cloud providers like Amazon, Microsoft, Google and myriad others.

Internet data centers are hardened for a variety of threats, for which they're certified and rated along a tier structure. Except for data centers in floodplains or hazard zones, most are able to ride out the worst storms.

Yet a hardened data center isn't much help if you can't reach it, and so now we come to the crux of the problem. Our journey to the internet is wholly dependent on physical cable (fiber optics). While it seems that we live in a wireless world, smart phones and Wi-Fi operate only on the periphery of the internet, transmitting short distances before offloading their data to fiber. That conversion could be as close as your router, at your street corner or the nearest cell tower, and the reason for it, is that only fiber can support the volume of traffic in and out of data centers.

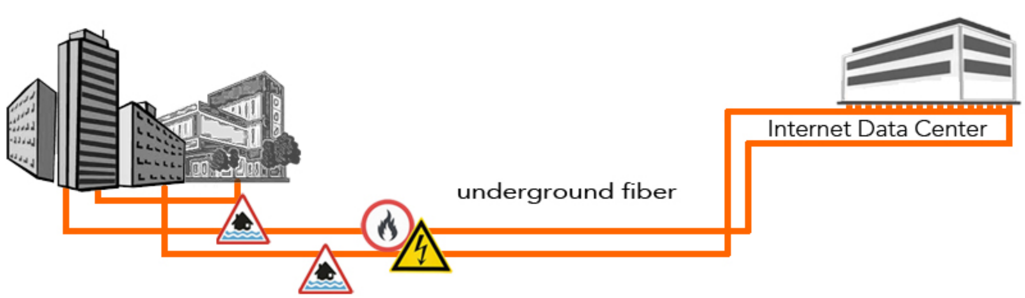
We need fiber for capacity, but it fails in extreme weather.

Fiber is strung on telephone poles ("40-foot high wooden sticks") and snakes through endless miles of underground, the whole of which is vulnerable to backhoes, vandalism and random casualties. Carriers know this, and so they build redundancies with diverse routes, manholes and building entrances, but widescale events, like flooding, trounce those measures.

Related: Blame Your Lousy Internet on Poles by Prof. Susan Crawford in Wired.

According to Paul Barford, professor of computer science at UW-Madison: "Much of the system was put into place in the '90s without much consideration of climate change. On top of that, much of the internet's physical infrastructure is aging. A lot of it was designed to last only a few decades and is now nearing the end of its lifespan."

Internet access in 2020



Power outages are no less concerning.

It's not only fiber that's vulnerable to climate, but also the electrical grid it relies on. According to Bloom Energy, there are more than 5.5 million miles of transmission lines in the U.S.—many atop 100-year old towers—and the primary causes of blackouts are high winds and storms.

Want a shocking statistic? Power outages cost $11 TRILLION in damages between 2005 and 2020. Alone it's a colossal stat, but it's even more daunting when you consider that the preceding 25-years saw *only* $600 billion in damages.

Related: "Roughly 4,000 miles of fiber-optic cables in US coastal cities could go underwater."

Meanwhile, in a crisis, carriers are more inundated than we are.

Internet resilience seems like a thing for big carriers with billions in infrastructure, so we don't think about it. And when we lose internet, we respond the same as to a power failure. We wait.

Yet carriers are scarcely equipped for the onslaught of climate disruption and needing them to save us is the worst place to be. In disasters they're inundated: dispatching contractors, bailing out cable vaults, going tree to tree, pole to pole, into manholes and deploying emergency rigs quaintly referred to as "COWs" and "COLTS" (cell on wheels and cell on light trucks).

It doesn't matter who you are or how vital your data, you're in the queue. As one responder put it after Hurricane Harvey, "We have the capability to bring back the network as quickly and safely as possible." Translation: You're out of luck, and it could be hours, days or weeks.

Meanwhile, states like California hold regular hearings with utility and telecom giants, but solutions are elusive. The fact is, monolithic providers have impossibly large footprints for fighting climate and despite the public ire, it's impractical to place all the burden on them.

Internet resilience takes a different approach.

Talk about internet resilience is always about protecting fiber. It recalls Maslow's Law: "If all you have is a hammer, everything looks like a nail."

Forget fiber.

For that matter, forget satellite and cellular as well. Satellite has its own weather challenges. As for cellular, towers are prone to wind damage, and most have only 8-hours of power backup. Many cell sites have none at all, such as off church steeples and city buildings.

> "A total internet failure is one thing that could stop any business in its tracks, yet few are preparing for this possibility, consultancy KPMG has warned."

The Solution

Let's say you're desperate to catch a flight. The airport is open and your flight is on time, but a storm scattered debris everywhere and all roads between you and the airport are impassible. You could throw up your hands, or if you had a helicopter with fuel, you could make the airport with time to spare.

Hence our solution for internet resilience. An all-aerial service for vital data, independent of public power and infrastructure, which overcomes hurricanes, flooding, heatwaves, blizzards, sea level rise; even terrorism.

Here's how it works.

The core of resilient internet is "millimeter wave" wireless[5]. Carriers have used it for years. We use it to connect client networks, rooftop to rooftop, to a secure internet data center out of harm's way. By that, we generally mean that it's not in hazard zone or a flood plain, as many are[6].

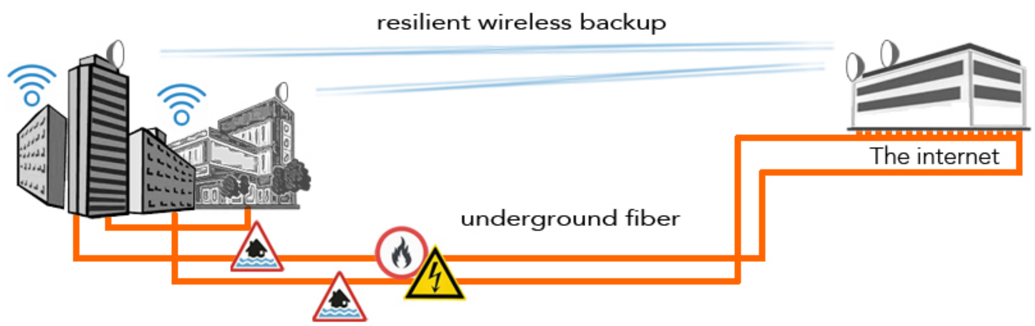
Millimeter wave is the closest wireless gets to fiber performance. It supports massive bandwidth—tens of gigabits per second—is encrypted and HIPAA approved. The downside is that it's limited to about 2-miles (typical), so for longer distances we also use microwave radio.

In the 1990s, microwave expedited internet access ahead of fiber deployment.

I adapted microwave for the early internet (1987), creating the first wireless broadband solution (a.k.a. fixed wireless), which met the full network data rate of 10 megabits per second. Fiber emerged in the mid-90's, and where availability could be months or years, microwave helped advance network deployment. Ultimately, fiber won the bandwidth war and subsequently, microwave served only fringe applications at data centers, if at all.

Today, climate resilience is a different application, well suited for wireless, because it's less about bandwidth and more about a critical lifeline.

In new Best Practices, millimeter wave acts as data lifeboats in extreme weather.



We leverage microwave and millimeter wave for their respective strengths. For instance, microwave wins for distance, but millimeter wave is best for urban environments, where it delivers the highest bandwidth, while also scaling the easiest, because it has the smallest RF (signal) footprint.

Related: "Boston is ranked eighth worldwide for expected economic losses due to coastal flooding."

So long as your building stands, you're getting internet.

As you might expect, stability of the wireless installation is paramount. For that matter, antennas are just 1-2 feet in diameter and with transmitters, weigh only about 20-pounds. The system is bolted to rooftops, through structural concrete, brick or angle iron. Attachment hardware—heavy-duty galvanized steel—outweighs the dishes they support. So long as the roof is standing, the client's getting internet.

Rooftops are best, but radio towers may be needed beyond city limits. Each such selection, however, must be scrupulously evaluated, and/or upgraded for accessibility, generator capacity and wind loading. Resilience could therefore be as solid as from rooftops, however I would rate tower installations as less than ideal.

Service in "the i of the storm."

What's the service like? You're looking at high-speed internet—building-wide—with options for outdoor Wi-Fi, for instance to cover a campus or plaza. Powering phones is the easy part.

Some will point out that, depending on threshold factors like distance, wireless performance may diminish in the heaviest storms. So then, while it's conceivable that a 5-gigabit connection could be throttled down by 50% in the eye of the storm, the impact is fleeting. Once the worst passes, service returns automatically to peak performance, and meanwhile terrestrial cable could be unavailable for days.

Resilient internet meets energy resilience.

Of course, resilient internet needs independent power, and not just for the wireless link, but for all else that wants access to it: in-building Wi-Fi, PCs, network and handheld devices, sensors, etc. For some, that will mean upgrading generator capacity.

Fortunately, we're dovetailing a booming industry of battery technology, generators and microgrids. Advances there can power internet access for days and weeks, depending on fuel service contracts and "islanding" capabilities for microgrids.

WHAT'S A MICROGRID? "A microgrid is a decentralized power system that can disconnect from the main grid and operate independently of it, reducing the frequency and severity of power outages and strengthening energy resilience for businesses and residents." Definition from Chris Ball.

As microgrids generate power apart from the grid, we generate internet apart from terrestrial infrastructure. The combination of sustainable power with uninterrupted internet is synergy at its best. Microgrids are the future and resilient internet will fuel their adoption like nothing else.

Related: Power Outages, Extreme Weather, & Microgrids Explained, by Chris Ball

Resilient internet keeps the "smart" in smart grids (and smart cities).

You've probably heard of "smart grids" and "smart cities," yet what makes them smart is data they pull from the internet. Generally speaking, no internet means no metrics, stats or data-driven anything, and that poses a bleak scenario.

According to Jonathan Strickland, "Smart grids could theoretically respond to customer needs more efficiently," … "But if the Internet were to collapse, a smart grid would be crippled. Massive power outages could become a problem across any country using such a system."

Likewise, without internet, smart cities lose data-driven decision making for traffic, public safety, citizen engagement and other services. Therefore, internet resilience must be a key consideration for smart city infrastructure.

Resilient internet enhances cyber security.

Intuitively, it would seem that data traveling over the air would be more vulnerable to interception than data contained in a wire, but not all wireless is the same. For instance, unlike omnidirectional antennas in cell phones, millimeter wave transmits in a tight, point-to-point beam, about 1-degree wide and high overhead. Excess signal that might be intercepted is so wispy it's absorbed by oxygen. To hack a transmission of this nature is like shooting a bullet with a bullet, and then encryption makes the impossible that much harder.

Resilience that scales like Legos.

As a rule, the greatest wireless bandwidth comes from point-to-point radios ("broadband wireless"), and those need line of sight between antennas. Some see that as a limitation, however creative path engineering goes a long way.

For instance, before fiber optics, AT&T's "Long Lines" microwave network spanned coast to coast with hundreds of interconnected radios. In my own experience, I once secured a continuous 700-mile wireless route between the Chicago MERC and the NYSE for high-frequency trading. It was one of the fastest data connections on earth, as described in the book, "Flash Boys."

What's key to wireless expansion is that every link in the chain is solid, installed to best practices and engineered for worst case weather. Reliability is then maximized by electronic redundancies and diverse path routing.

And for the best part, resilient internet is instant ROI.

Resilient internet pays for itself as ancillary bandwidth carrying everyday traffic, no different from fiber. It's billed monthly, and the cost of resilience may be offset by eliminating an equivalent expense for extra fiber circuits. Resilient internet isn't about adding bandwidth, but balancing risk. That said, cost savings from fiber may mean waiting for contracts to expire.

Final thoughts.

Climate readiness is an existential mandate for business and policy leaders, yet hardly anyone seems concerned about internet and data resilience. It's stunning when you consider that data is the "world's most valuable resource" and that hardly any industry can survive without it.

Still, I attended dozens of climate conferences and never once heard a speaker on internet vulnerability. I've scanned scores of vulnerability assessments for critical infrastructure and hardly find the word "internet." It doesn't appear once in a 56-page, blue-ribbon Bloomberg report, "The Economic Risks of Climate Change in the U.S.," nor in many similar publications.

The internet isn't so complicated, and neither is the vulnerability problem. The best practices I've detailed, work. We're not inventing new technology, but repurposing it according to new specifications, certified for extreme weather.

Climate resilient internet is a return to a more symbiotic relationship between wireless and fiber, only now with wireless acting as lifeboats for the internet. In this new paradigm, the synergy of resilient power and data represents the greatest climate adaptation opportunity on earth.

ABOUT THE AUTHOR

David Theodore graduated Boston College in 1983 and four years later, innovated wireless broadband for the emerging internet. Today, it's called "fixed wireless," the basis for home internet delivered by WISPs and major carriers.

David's startup, Microwave Bypass Systems, was one of the earliest tech firms at One Kendall Square. In 1987, it launched the "Etherwave Radio," the first wireless solution to meet Ethernet and IP specifications (802.3). The Etherwave provided full-speed, 10 Mbps access, connecting the first three dot com addresses on the internet: Symbolics, BB&N and Thinking Machines.

In its time, Microwave Bypass innovated teleradiology and distance learning, built Boston's early regional internet, connected world leaders in education, healthcare and technology, furnished Interop's first show access ('89), delivered the first wireless home internet service (for IT legend, Bill Joy), collaborated with Cisco Systems and licensed technologies to Motorola.

Microwave Bypass was widely covered in tech publications, little of which was digitized for the internet. Among its PR highlights, LAN Times named it one of the top 10 emerging tech firms, and Aberdeen Group wrote a glowing report, putting the company's market share at 75-80%.

After Microwave Bypass, David advanced low latency applications, designing one of the world's fastest data corridors for high frequency trading between the CME and the NYSE. Thereafter, he wrote about the emerging WISP industry and 5G, and advised fixed wireless providers, vendors and investors.

Today, as a climate activist and co-founder of Climate Resilient Internet, David is advancing new best practices to adapt the internet to climate change. Follow him on LinkedIn.

NOTES

[1] The irony of losing all means of electronic communication is compounded by the fact that radio is what gave us the Electronic Age. For some engrossing history, read, and/or watch the documentary, "Empire of the Air," by Ken Burns.

[2] Internet service providers quote wireless reliability into the "5-nines" (99.999%), however those calculations are based on historic weather data that no longer holds water.

[3] Fill is a euphemistic term for the sum of debris comprised mainly of wood products, household and industrial waste, animal carcasses, sludge and soil.

[4] Regarding national security implications, the Pentagon manages 704 coastal installations worldwide. At many bases, like Norfolk Naval Station, sea level rise is already interfering with early-warning radar and combat readiness of the Atlantic Fleet.

[5] Millimeter wave wireless is the bedrock of 5G technology. Interestingly, it's been out for at least two decades, starting with 60GHz and leading to 70/80GHz. At the lower 60GHz frequency, distance may be limited to a ¼ mile, whereas 80GHz frequencies may span several miles. Distance is relative to weather patterns characteristic to geographic regions. Unfortunately, today's weather frequently defies long established norms.

[6] Resilient internet changes nothing about your existing data centers. If your data center is 50-miles away, because of certain risk factors, those factors are no less valid. Stay where you are. Yet for climate resilience we aim for the nearest, most secure data center—outside of natural hazard zones—where your data may arrive safely.

In some ways, resilient internet is a throw-back. Before fiber, carrier and data center roofs were laden with microwave dishes. Dozens, sometimes hundreds of them. Some were mammoth in size, upwards of 12-feet in diameter, adding tons of weight to the roof. What happened to all those dishes is that most were torn down, because fiber proved a better investment. Now we're turning that clock back, except with dishes so small they're hardly visible from the ground.

REFERENCES

Andersen, Ted. "Cell and internet companies grilled over PG&E outage failures." *San Francisco Business Times*, Nov. 21, 2019

Ashford, Warwick. "Total internet failure: are you prepared?" *ComputerWeekly*, July 16, 2014.

Ball, Chris. "Power Outages, Extreme Weather & Microgrids Explained," *Bloom Energy*, Dec. 6, 2019.

Barford, Paul, Barford, Carol and Durairajan, Ramakrishnan. "Lights Out: Climate Change Risk to Internet Infrastructure." U. Oregon and U Wisconsin–Madison, July 16, 2018.

Beck, Margery A., Burns, Robert and Knickmeyer, Ellen. "Floods expose national security concerns over climate change." Christian Science Monitor, March 22, 2019.

Caperton, Mary Morton. "With nowhere to hide from rising seas, Boston prepares for a wetter future." *ScienceNews*, August 6, 2019.

Coffee, Joyce E. "Five Resilience Trends in 2019"

Crawford, Susan. "Blame Your Lousy Internet on Poles: THE WAR OVER HIGH-SPEED ACCESS IS FOUGHT ON 40-FOOT-HIGH WOODEN STICKS." *Wired*, Aug. 31, 2016.

C-Span. "The Communicators: The Impact of Hurricane Sandy on Telecommunications." Nov. 26, 2012

Dahlberg, Nancy. "Still no internet access or cell service? You're not alone." *Miami Herald*, Sept. 13, 2017.

Deloitte LLP. "The economic impact of disruptions to internet connectivity." Oct. 2016

Dodge, Blake. "Why the U.S. Can Expect More Power Outages like California's." *Newsweek*, Oct. 9, 2019

Fonseca, Felicia and Lieb, David. "Internet outages reveal gaps in US broadband infrastructure." *U.S. News and World Report*, March 27, 2015

Four Rivers Charter Public School. "Under Pressure: Exploring the Complex Truth of Natural Gas." 2019

Greenemeier, Larry. "How Can Cities Protect Themselves against Gas Explosions?" *Scientific American*, Apr. 7, 2014

Hartnack, Michael. "Rising Power Outage Cost and Frequency Is Driving Grid Modernization Investment." *Navigant Research*, Jun. 28, 2018

Hersher, Rebecca. "Rising Seas Could Cause Problems For Internet Infrastructure." *NPR, Science*, Jul. 16, 2018

Hughes, Trevor. "Attacks show fiber optic Internet cables vulnerable" *USA Today*, Sept. 16, 2015.

Hussain, Asim. "A Day Without Power: Outage Costs for Businesses." Oct. 8, 2019

Hussain, Asim and Pande, Preeti. "2020 predictions: The top energy trends we're anticipating this year." *Bloom Energy*, Jan. 24, 2020

Irwin, Neil. "Climate Change's Giant Impact on the Economy: 4 Key Issues." *New York Times*, Jan 17, 2019

Jochem, Greta. "Rising Seas Could Cause your Next Internet Outage." *Wired*, July 18, 2018.

Kelly, John. "Look out below: Danger lurks underground from aging gas pipes." *USA TODAY*, Sept. 23, 2014

Kohlstedt, Kurt. "AT&T's Abandoned "Long Lines" Microwave Tower Network." Oct. 20, 2017.

Knutson, Ryan. "Cell Networks Suffer Outages in Harvey's Wake." *Wall Street Journal*, Aug. 27, 2017

Kredo, Adam. "Vandalism in Arizona Shut Down Internet, Cellphone, Telephone Service Across State Incident raises concerns a domestic or international terrorist could tamper with U.S. infrastructure. *The Washington Free Beacon*, Feb. 27, 2015

Miller, Greg. "Undersea Internet Cables Are Surprisingly Vulnerable." *Wired*, Oct. 29, 2015

Seay, Bob. "Boston's Seaport Might Be Better Prepared For Climate Change Than We Think." *WGBH News*, Feb. 5, 2018

Soper, Taylor. "Comcast suffers outage in Seattle due to damaged fiber optic line." *GeekWire*, Apr. 9, 2015.

Strickland, Jonathan. "What would happen if the internet collapsed." Feb. 10, 2010.

Whittaker, Zack,"911 Emergency Services Go Down Across the US After CenturyLink Outage." *TechCrunch*, Dec. 28, 2018

World Bank, "Which Coastal Cities Are at Highest Risk of Damaging Floods?" Aug. 19, 2013

World Economic Forum, "The Global Risks Report 2020"