The Atlantic

What Happens If GPS Fails?

Despite massive reliance on the system's clocks, there's still no longterm backup.

(U.S. Air Force)

DAN GLASS

JUN 13, 2016 | TECHNOLOGY

In only took thirteen millionths of a second to cause a whole lot of problems.

Last January, as the U.S. Air Force was taking one satellite in the country's constellation of GPS satellites offline, an incorrect time was accidentally uploaded to several others, making them out of sync by less time than it takes for the sound of a gunshot to leave the chamber.

The minute error disrupted GPS-dependent timing equipment around the world for more than 12 hours. While the problem went unnoticed by many people thanks to short-term backup systems, panicked engineers in Europe called equipment

makers to help resolve things before global telecommunications networks began to fail. In parts of the U.S and Canada, police, fire, and EMS radio equipment stopped functioning. BBC digital radio was out for two days in many areas, and the anomaly was even detected in electrical power grids.

Despite its name, the Global Positioning System is not about maps; it's about time. Each satellite in the constellation (24 are needed, plus the U.S. has several spares) has multiple atomic clocks on board, synchronized with each other and to Coordinated Universal Time (UTC)—the time standard used across the world—down to the nanosecond. The satellites continually broadcast their time and position information down to Earth, where GPS receivers in equipment from iPhones to automated tractors acquire signals and use the minuscule differences in their arrival time to determine an exact position.

What if all these flying clock radios were wiped out, and everything on the ground started blinking 12:00?

While GPS was initially conceived to aid navigation, globally synchronized time is now a much more critical function of the system. Telecom networks rely on GPS clocks to keep cell towers synchronized so calls can be passed between them. Many electrical power grids use the clocks in equipment that fine-tunes current flow in overloaded networks. The finance sector uses GPS-derived timing systems to timestamp ATM, credit card, and high-speed market transactions. Computer network synchronization, digital television and radio, Doppler radar weather reporting, seismic monitoring, even multi-camera sequencing for film production—GPS clocks have a hand in all.

But last January's system failure brings up an often-ignored question: What if all these flying clock radios were wiped out, and everything on the ground started blinking 12:00? According to Mike Lombardi, a metrologist at the National Institute for Standards and Technology, "Nobody knows exactly what would happen." Since so many of these technologies were designed specifically with GPS

in mind, the unsettling truth, he says, is “there’s no backup.”

This isn’t a secret. Concern for the consequences of the country’s reliance on this invisible utility has been growing among industry and government workers for more than 15 years, after the Department of Transportation issued a report on the need for a backup navigation system, in 2001. But while the means to create one has existed since, a winding bureaucratic path has kept it from actually being implemented. And that leaves many of the everyday tools society depends on vulnerable until one is.

* * *

There are plenty of reasons GPS could fail.

Intentional attack is one, as emphasized by a declassified 2012 risk estimate by the Department of Homeland Security. One of the system’s most basic problems is its signals are weak enough to be easily obstructed. Truckers with cheap jamming devices designed to elude employer tracking have unintentionally interfered with airport systems; criminals thwarting GPS tags on stolen goods in shipping containers have accidentally shut down port operations. On a grander scale, North Korea has tormented South Korea with waves of jamming attacks. (Jamming devices are now illegal in the U.S., but not difficult to obtain illicitly.)

A few steps up from jamming devices in both complexity and damage are spoofers: systems that get GPS receivers to lock on to mimicked signal. Spoofers don’t trigger equipment alarms, and deliver altered time and position information to unaware users. It's been suggested that Iran used this tactic to lead astray two U.S. Navy patrol boats captured in the Gulf last January.

“It wouldn't take that large of an event to take out all GPS."

A plausible worst-case attack scenario would look something like this: Spoofers feed erroneous data to electrical substation equipment in a metro area, which could

overheat power lines and transformers, causing widespread outages. Meanwhile, multiple hidden jammers could cripple cellphone service, and also force fire, police, and emergency medicine departments to revert to old, single-frequency channels. Supplies in this scenario could only be bought in many places with cash, which would be limited without ATM service. According to the DHS report, it could take 30 days or more before the malicious devices are located and disabled. The longer it took, the more systems that would be compromised.

As for unintentional threats to GPS, the DHS risk estimate lists space debris, space weather, defective software, and good old-fashioned human mistakes, among other things. Of these threats, space weather is the most potentially catastrophic, according to Norwegian geophysicist Pal Brekke, whose country was hardest hit by the January outage. Eruptions of high energy radiation from the sun (known as solar flares) and ejections of electrically charged gases have disabled satellites in the past.

With satellites and the chips inside them getting smaller as technology progresses, "one particle from the sun that penetrates a satellite can ruin things," Brekke says. "It wouldn't take that large of an event to take out all GPS."

* * *

So far, mitigating the loss of GPS signals has involved two approaches. One is interoperability with other global navigation satellite systems like Russia's GLONASS (which also failed due to a ground control error in 2014) or the European and Chinese systems, both of which are expected to be up by 2020. The other is better clocks, says Lombardi, the NIST metrologist, who's published numerous articles on the topic. "The typical cell tower clock has an oscillator similar to that of a wristwatch," he says, "and can drift out of tolerance in minutes without a signal." How long a clock can maintain time on its own, called "holdover," also affects electrical grids, many of which rely on GPS-dependent devices called synchrophasors used to precisely regulate current flow, as well as help locate faults in the network. A lack of such timing technology was the reason it took some Canadian technicians three months to locate failures after the infamous

blackout of 2003.

Chip-scale atomic clocks the size of a penny are a promising new technology that can hold time for about a day, but are currently too expensive to deploy widely. Moreover, hedging and holdover still aren't backups for when space-based signals are simply unavailable.

The bulk of a more promising, comprehensive backup system already exists, right here on the ground. After the sextant but before GPS, navigators around the world used Long Range Aids to Navigation, or "LORAN," a terrestrial system of transmitters and receiving equipment first developed during WWII. By the mid-1990s, Loran "tower chains" provided coverage for North America, Europe, and other regions in the Northern Hemisphere. Its use declined in favor of the much finer accuracy of GPS after it became available for civil use in 1995, but the U.S. Coast Guard continued working on an improved system using the existing infrastructure. If adopted, "Enhanced" LORAN, or eLoran, could provide positioning accuracy comparable to GPS. Broadcast at hundreds of thousands of watts, the signal is virtually un-jammable, and unlike GPS, can even be received indoors, underwater, and in urban or natural canyons. It also turns out that eLoran can provide a UTC time signal with sub-microsecond time resolution across a large geographical area.

The technology is available—the Coast Guard demonstrated a working prototype last year—so why isn't America using it? John Garamendi, a California congressman, asked this question at a July 2015 congressional hearing on the Federal Radionavigation Plan, the nation's primary planning document for position, navigation, and timing (PNT). "There are two kinds of time," he opened, "real time ... and then federal time, which seems to be the forever time. The e-Loran system was identified as a backup 15 years ago, and here we are, federal time, not yet done."

Cost doesn't seem to be a problem. A complete alternate PNT system is estimated at $350 million to $400 million; it costs $1 billion yearly to maintain GPS. And science and industry appears to share a consensus that eLoran is the solution. Even

the Air Force Colonel and engineer who created GPS, Brad Parkinson, had been on record for years saying "eLoran is the only cost-effective backup for national needs."

In a 2004, a presidential directive tasked DHS and DOT with creating a backup to the GPS system. In 2008, the DHS issued a press release that it was committing to the system and transferred control from the Coast Guard to its National Protection and Programs Directorate. But push and pull between DHS and the Coast Guard appears to have slowed progress.

Space Katrina would be biblically catastrophic.

After this year's satellite error, many European officials who had previously followed America's reluctance to adopt eLoran stepped up development. Meanwhile, pressure from Garamendi, who argued in his address that "without an eLoran system in place ASAP, this country is in serious, serious jeopardy," prompted a letter to him from the Deputy Secretaries of Defense and Transportation informing that the PNT Executive Committee has agreed that an eLoran-based timing network "could provide a near term solution" (if private entities bore some of the cost) while they "continue [their] efforts to prescribe a complete set of requirements necessary to support a full complementary PNT capability for the nation." In other words, it seems: federal time.

* * *

Why is the sense of urgency among decision-makers so out of sync? Could some of it be similar to why people delay backing up our computers even though they've been telling themselves to for weeks? How do we decide, when presented a risk with unknown odds, when it's time to sacrifice time and resources to prevent it?

Now is a critically important time to answer that question, as the world actually been given odds on another, even more catastrophic risk than GPS failure: destruction of the electrical power infrastructure itself. On July 23, 2012, a billion-

ton cloud of electrified gases blasted off the far side of the sun at over six million miles per hour. According to professor Daniel Baker at University of Colorado, this coronal mass ejection (CME) "was in all respects at least as strong as the 1859 Carrington Event," referring to the strongest solar storm ever recorded, which set fire to telegraph stations and caused auroras down to Cuba. As was widely reported two years ago, if the 2012 CME had occurred one week later, it would have hit Earth.

Space Katrina would be biblically catastrophic. Power could be out for years while electrical transformers were repaired, if the resources are even available to do so. "Collateral effects of a longer-term outage would likely include disruption of the transportation, communication, banking, and finance systems, and government services; the breakdown of the distribution of potable water owing to pump failure; and the loss of perishable foods and medications because of lack of refrigeration," reads a 2008 National Academy of Sciences report.

In 2014, physicist from San Diego calculated the likelihood of a Carrington-level event in the next decade. The odds he came up with were 12 percent.

The predicament of events like this is not that they're occurring more frequently, but that the rapid development of technology is opening the tools on which humanity depends to an increasingly wide variety of rare but potentially destructive cosmic threats. In the span of a century, we've transferred much of the weight of modern society to global infrastructures with wobbly legs. If they collapse, time will very quickly appear to move backward.

ABOUT THE AUTHOR

DAN GLASS is a freelance writer living in New York. His work has appeared in *The New York Times*, *Wired.com*, and *Vice*, among other publications.

Twitter