
TUC 11

DEFENDING THE NATION'S CRITICAL INFRASTRUCTURE, FROM ROADS AND RAIL TO POWER AND WATER, ENABLED BY GEOINT.

security & RESILIENCE

BY MATT ALDERTON

The National September 11 Memorial & Museum is a solemn, sobering place. Located 70 feet below ground in Lower Manhattan, on the site of the former World Trade Center, it reverberates with memories of loss. Among the museum's most moving elements is the "In Memoriam" exhibit, which features portraits of the 2,996 men, women, and children who died in the 2001 terrorist attack. Also powerful are the enormous aluminum casts of the Twin Towers. Floating like ghosts in the buildings' original footprints, they're an overwhelming reminder of the attacks' strategic nature: Along with human lives, al-Qaeda targeted buildings and their associated structures, including several telephone switching hubs, a broadcast antenna, two electrical substations, a multimillion-dollar emergency command center, and two mass transit lines. When the towers fell, thousands of feet of roadway, water main, power lines, fiber optic cable, sewer pipes, and gas lines were among the rubble.

"The World Trade Center was such an integral part of the New York skyline that, of course, there was emotional value attached to it. But there was also server space there for processing financial transactions, and electric utility substations that switched power for Lower Manhattan," explained Talbot Brooks, director of the Center for Interdisciplinary Geospatial Technologies at Delta State University and co-author of *GIS for Critical Infrastructure Protection*.

Though a price cannot be placed on human life, terrorists know they can inflict economically crippling damage and wreak havoc by targeting infrastructure as well. Consider what would happen if a disaster damaged or destroyed the nation's power grid, as depicted by the National Geographic Channel in its 2013 film *American Blackout*. A fictional account of what would happen after a terrorist attack on U.S. power infrastructure, the film paints a dark picture. Traffic signals would go out, causing crashes and gridlock. ATMs, banks, and credit cards would cease to function, crippling the economy. Pumps supplying cities with running water and flushing toilets would stop working, causing a public health crisis from dehydration and disease. Gas stations would lack the power needed to pump gas, leaving trucks unable to deliver food and medical supplies. Hospitals would be unable to treat patients, and emergency responders unable to answer 911 calls. The panic and chaos that would ensue is why governments must protect not only people during disasters, but also critical infrastructure.

"It's not usually disasters themselves that are the big problem—manmade or natural, it's what they do to infrastructure," said Chris McIntosh, director of public safety industry solutions at Esri. "For example, a hurricane itself isn't necessarily a big problem. The big problem is the loss of services to people… The acute effects of the actual disaster impact a fairly localized group of people, but the loss of critical infrastructure impacts a much larger population."

Geospatial intelligence is the linchpin of incident planning, prevention, response, and recovery.

"Everything is somewhere—especially critical infrastructure," continued McIntosh. "If an incident occurs in a location and you're a decision-maker, the first thing you'll ask yourself is: 'How bad is it?' You're going to want to know: 'What is in the affected area? And what could be impacted by the loss of that area?'… With its fusion of location and location analytics, geospatial technology allows you to answer those questions in near real time to identify initial actions quickly."

THE CRITICALITY OF INFRASTRUCTURE

Infrastructure is to communities what the circulatory system is to the human body: a critical network supplying resources needed to function. In both cases, a lone clog in a single artery can cause a life-threatening heart attack.

"Critical infrastructure serves as the backbone of the nation's economy, security, and way of life," said Michael Donnelly, a geospatial data architect in the Department of Homeland Security (DHS) Geospatial Management Office (GMO). "It refers to basic, everyday needs and services—electricity, cell towers, or even bridges. By identifying such infrastructure as critical, we can prioritize its security and resilience."

The U.S. government has designated 16 sectors of infrastructure as "critical" (see sidebar on page 29), meaning if they were to be degraded or prevented from operating there would be significant, if not catastrophic, impact on the populous. The 16 sectors—each of which has a designated federal agency as its functional lead—were established in 2013 by Presidential Policy Directive-21: Critical Infrastructure Security and Resilience.

Individually, each sector is massive. Collectively, the scope is mind-boggling. The transportation sector, for example, includes approximately 450 commercial airports, 361 seaports, nearly 4 million miles of roadway, approximately 600,000 bridges, some 400 tunnels, 25,000 miles of waterways, about 2.2 million miles of natural gas distribution pipelines, and more than 140,000 miles of active railroad. The food and agriculture sector consists of approximately 2.2 million farms, 900,000 restaurants, and more than 400,000 registered food manufacturing, processing, and storage facilities.

Threats aren't just hypothetical. In April 2013, a team of unidentified gunmen assaulted Pacific Gas and Electric Company's Metcalf transmission substation near San Jose, Calif. Although a blackout was avoided by rerouting power, the 19-minute attack mangled 17 electrical transformers and resulted in more than $15 million worth of damage that took 27 days to repair.

A COMMON OPERATING PICTURE

Concerns about the vulnerability of critical infrastructure date back more than a century according to James Devine, senior advisor for science applications with the U.S. Geological Survey (USGS).

"When earthquake science began to develop around the turn of the 20th century, it was recognized almost immediately that when major events happen, infrastructure is a recipient of the damage. Not just an individual house or school, but a whole system," Devine explained. "During the 1906 earthquake in San Francisco, for example, the rupture of gas lines created fires, which did much more damage than the shaking."

It wasn't until after 9/11 that the federal government deployed GEOINT as a foundational solution. In February 2002, the Bush administration created the Homeland Infrastructure Foundation Level Data (HIFLD) Subcommittee to facilitate improvements across multiple levels of government in the collection, processing, sharing, and protection of geospatial domestic infrastructure data. The subcommittee includes representatives from the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, the DHS National Protection & Programs Directorate Office of Infrastructure Protection, the National Geospatial-Intelligence Agency (NGA), and the USGS National Geospatial Program Office.

"Key individuals [in these offices] … wanted to make sure everybody was working together to create foundation infrastructure information, instead of everybody recreating the same thing because

MULTIPLE CREWS from New Jersey's Public Service Enterprise Group fix poles and downed lines to restore power after Hurricane Sandy.

PHOTO COURTESY OF PSE&G

CYBER PROTECTION

As chaotic as an infrastructure failure could be, perhaps the scariest thing about them is they could be caused by just the click of a mouse, according to Michael Donnelly, a geospatial data architect with the Department of Homeland Security (DHS) Geospatial Management Office (GMO).

"The nation's infrastructure is more interdependent than ever before, and is at risk from a variety of hazards—including constant and sophisticated cyber threats," Donnelly said.

Those threats loom large, according to Robert Zitz, former deputy under secretary for preparedness with DHS and now a senior vice president with Leidos.

"The nexus between cyber and GEOINT in support of critical infrastructure protection is growing," Zitz said. "Protection is now both physical and cyber. They're woven together like a strand of DNA. Because if you look across all the sectors that make up critical infrastructure—water, power, food, transportation, and so on—the one thread that runs through all of them is the Internet. Every one of those sectors depends on the Internet, yet every one of them is also vulnerable because of it."

GEOINT helps DHS keep such risks at bay, according to Donnelly, referencing the DHS GMO's Geospatial Information Infrastructure (GII), a common geospatial enabling platform DHS uses to deploy data, tools, and apps that support critical infrastructure protection.

"One example of this GII capability is the Cyber Communications Common Operating Picture app," Donnelly said. "This app provides the National Cybersecurity and Communications Integration Center the ability to geospatially visualize, analyze, and report on threats and incidents to the nation's critical communications infrastructure ... The app can access hundreds of geospatial data layers, base maps, and imagery."

the infrastructure data DHS needs for homeland security is the same data needed for emergency preparedness and emergency response," said Booz Allen Hamilton Principal Justin Sherin, co-founder and program manager of the HIFLD Subcommittee, the goal of which was to create geospatial infrastructure data that could be shared not only among federal agencies, but also with state and local government as well as private sector partners.

Toward this effort, the HIFLD Subcommittee developed the Homeland Security Infrastructure Program (HSIP) data sets. Specifically, HSIP Gold, a unified geospatial data inventory assembled by NGA in partnership with DHS. First released in 2005 and updated with new data sets almost every year since, HSIP Gold contains more than 560 common geospatial data sets characterizing domestic infrastructure.

"The HSIP data sets are critical to the analysis and assessments conducted to support infrastructure security and resilience by providing a comprehensive common operating picture," Donnelly said.

HSIP is now leveraged for every natural and manmade disaster in which the federal government is involved, according to Sherin.

"There's nothing worse than going to a meeting and having two separate maps or reference points. That causes more confusion than coordination," Sherin said. "The HSIP product was monumental because it allows you to find [information] once and share it with everybody."

SEEING SUCCESS

The country has since seen the benefits of the common geospatial operating picture provided by HSIP and state and local equivalents. After Hurricane Sandy in 2012, GEOINT catalyzed efforts to protect critical infrastructure from future natural disasters—starting with facilities damaged by the storm, which have been eligible for mitigation grants to strengthen their resiliency.

In New Jersey, Public Service Enterprise Group (PSE&G), a gas and electric utility, has likewise used GEOINT to prepare for another event such as Hurricane Sandy.

"We had over 13 feet of storm surge at some substations," said Mike Weber, emergency preparedness manager at PSE&G, adding the utility lost 31 electrical substations to flooding during Sandy.

PSE&G leveraged GEOINT to identify approximately 100 mitigation actions it believes will keep electricity on in the event of another major storm.

"One of the bigger things we're doing is looking at critical infrastructure—which could include hospitals, police, fire, etc.—and seeing which circuits serve them, then developing a backup plan to ensure access to a second means of electricity for them so they don't end up going down," Weber said. "Because of resiliency and redundancy that we've built into our system, it's not going to be easy to take out power again."

Hurricane Sandy wasn't the only 2012 storm to illustrate GEOINT's role in infrastructure protection. In Fairfax County, Va., GEOINT helped local government respond to a historic derecho that left more than half the county without power during a June heat wave.

"It was critical for us to have visibility of our physical assets in Fairfax County so we could figure out where the impacts were to the community," said Fairfax County Chief Information Officer Wanda Gibson, who leads the county's GIS efforts. "We could determine where we needed to set up cooling centers, for example, and see where our senior centers were in case they needed assistance."

The county used geospatial data to visualize where the power was down, where roads were blocked, the locations of citizens with special needs, and which government buildings—including schools and courts—were operational.

When GEOINT is applied to critical infrastructure, livelihoods are saved just as often as lives, according to Dr. Joseph Fontanella, director of the U.S. Army Geospatial Center.

"In 2012, there was a record drought in the middle part of the country, so water levels along the Mississippi River were historically low. At the bottom of the river were exposed rock pinnacles that were impacting commerce throughout the Mississippi Valley," Fontanella said. "We developed some products and did some geospatial analysis that enabled

[the U.S. Army Corps of Engineers] to brief the White House and the Department of Defense on mitigation strategies, and they ended up demolishing some of these pinnacles to remove them as obstacles."

PREVENTABLE FAILURES

For every example of how GEOINT has helped governments protect and monitor critical infrastructure, there is an example of how it wasn't used to do so. During Virginia's derecho, for example, Verizon experienced equipment failure that left nearly 2.3 million Virginians without 911 emergency services, but the company didn't even know about the outage until Fairfax County called to report it.

Yet another example is the 2010 explosion of a broken PG&E natural gas pipeline in San Bruno, Calif., which killed eight people.

"You see critical infrastructure failing with sometimes pretty extreme consequences on a regular basis," Brooks said. "The gas explosion in San Bruno is an example of catastrophic critical infrastructure failure…It was a failure of intelligence to understand the gas pipeline system, its condition, and its relation to residential neighborhoods."

These and other failures are evidence of gaps GEOINT is well positioned to help fill. Before it can do so, however, systemic challenges must be addressed, according to Brooks.

"We in the critical infrastructure and emergency response sectors have the fundamental problem that we do not share data well at all," he said. "The electric utility company doesn't go to the gas company or the telephone company and say, 'Here, have all the GIS data for our entire gas distribution system.' Instead, they keep it and say it's proprietary."

From a business standpoint, this might make sense. But it's senseless when one considers the implications for critical infrastructure protection. Because power lines often share trenches with water, sewer, gas, and cable lines, a threat to one utility is often a threat to all. Even in the most vulnerable places like New York City, where infrastructure is packed tightly together, public and private data are widely segregated.

"We have a very good working relationship with our utility, but we do not ourselves have their data set in our possession," said NYC Office of Emergency Management Assistant Commissioner for Strategic Data James McConnell, who also serves as director of New York City's GIS Division. "The fact that we don't have it is not necessarily hindering our response, but having that level of detail would be very useful for looking at how various infrastructures interrelate and where there might be ways to increase resiliency or realize efficiencies."

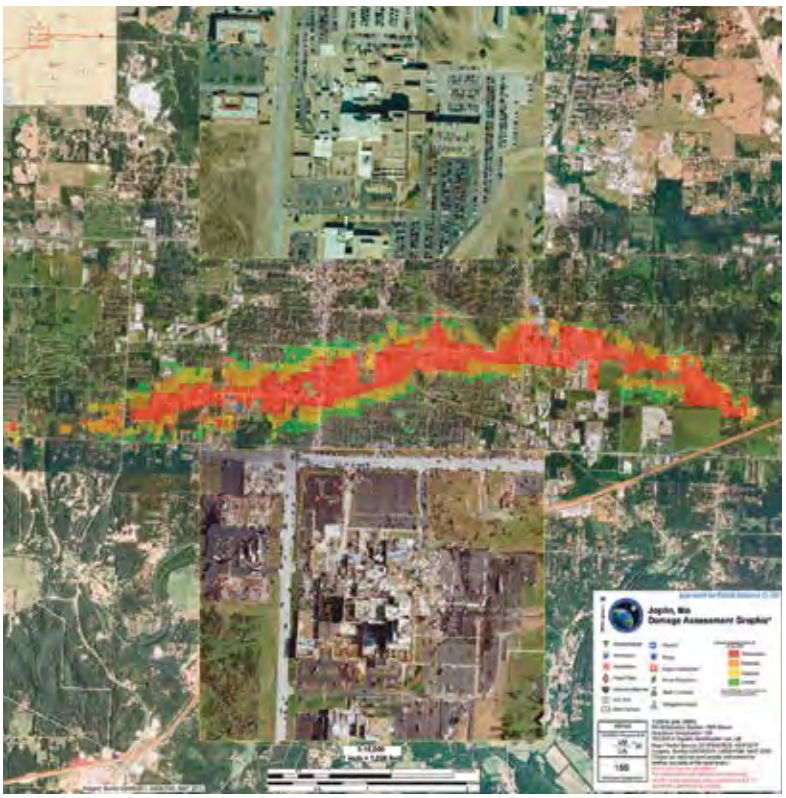
Although HSIP was designed to eliminate them, it likewise struggles with silos, according to NGA Branch Chief and Program Manager Todd Bolen, who said security concerns limit the federal government's ability to share geospatial information with state and local partners despite a strong desire to do so.

"In the post-9/11 timeframe, all levels of government are averse to sharing a significant amount of information about our critical infrastructure," Bolen said. "Where we have key water storage facilities, for instance, is a sensitive issue, so providing that information in an open forum on the [Internet] is a non-starter. In the digital age, however … those old policies seem anachronistic. There's no reason to have protections on some of the data we protected at the highest levels in the past, but those policies remain in place."

THE 16 SECTORS OF CRITICAL INFRASTRUCTURE

The Department of Homeland Security designates the following 16 sectors as critical infrastructure:

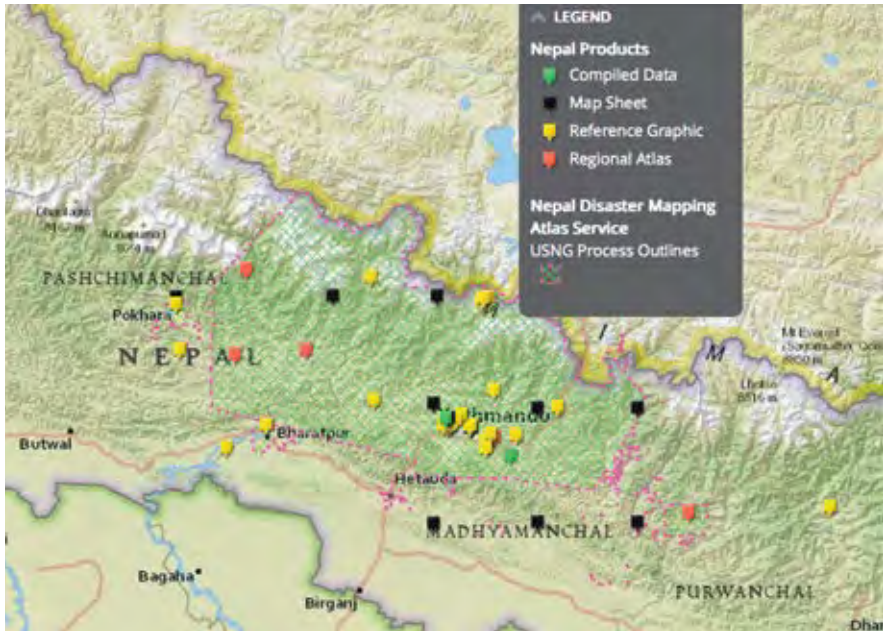
- Chemical
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government facilities
- Health care and public health
- Information technology
- Nuclear reactors, materials, and waste
- Transportation systems
- Water and wastewater systems



NGA DAMAGE ASSESSMENT graphics—such as this one of Joplin, Mo., following the May 22, 2011, tornado—are used for response and recovery efforts.

IMAGE COURTESY OF NGA

FOLLOWING the devastating earthquake that shook Nepal April 25, 2015, the National Geospatial-Intelligence Agency stood up a public website using Esri's ArcGIS platform to share valuable maps, imagery, and data overlays with first responders.



Another obstacle is education, according to McIntosh. On the one hand, he said, geospatial technology has advanced such that almost anyone in the critical infrastructure ecosystem could be a GEOINT user and consumer. On the other hand, only few are aware of the technology and how it can be applied.

"Right now, many people don't know what's possible," explained McIntosh, who believes geospatial technology should be a component of the Emergency Management Accreditation Program. "Technology is a fast-moving train, and it's outpacing the education policies and procedures of the emergency management community."

Utilities are a prime example, according to Weber. "I don't know if the utility industry knows the abilities geospatial technology can offer," he said.

Stakeholders at even the highest levels struggle to stay current.

"At DHS, our challenge is moving fast enough to keep pace with evolving threats to our critical infrastructure, and the development of new technology," Donnelly said.

TOWARD A HIGHER INFRASTRUCTURE IQ

In response to shortcomings, stakeholders are devising GEOINT solutions to strengthen critical infrastructure protection.

HIFLD is leading the way with the next generation of HSIP. In 2014, the working group became a subcommittee of the Federal Geographic Data Committee (FGDC), whose oversight has prompted a wave of improvements, according to Donnelly.

"HIFLD is now positioned to better coordinate across the federal government on improving HSIP's data holdings," he said. "[The HIFLD Subcommittee] is working to enable common operating data sets like HSIP to be more available to the entire homeland security enterprise."

HIFLD is working with data owners across the federal government to validate information and also looking at ways to improve the HSIP data set by enhancing metadata, building data tags to improve data discoverability, and building a dynamic online delivery mechanism to provide data updates to the user in real time. Simultaneously, the group is engaging commercial providers to license data to more users and conducting data layer reviews to determine which data can be made more widely available.

"States and locals see the value of HSIP data, but in many cases we can't share it with them because either it's licensed only to federal users or it's official use only, which limits its utility," Bolen said. "We've increased our licensing to now include state users as a step toward broadening access."

NGA is also transitioning administrative authority for HIFLD and HSIP to DHS, which is expected to further break down data silos.

"We're currently in a three-year transition plan with DHS, which will [be completed] by the end of FY18," Bolen said. "State and local support will be more effectively enabled once the majority of the program sits on the DHS side of the table."

State and local governments are doing their part, too, according to Brooks, who said cities such as Tampa, Minneapolis, and Charlotte, among others, are leveraging the Geospatial Information and Technology Association's (GITA) Geospatially Enabling Community Collaboration (GECCo) initiative to improve data sharing around critical infrastructure protection—particularly with the private sector, whose data is absent from HSIP even though it owns 80 percent of critical infrastructure in the U.S.

"Organizations like GITA and USGIF have a critical future role to play as neutral facilitators to the private sector," said Brooks, who is also president of GITA.

Both proactively and reactively, emergency managers and governments must make it a priority to leverage GEOINT for critical infrastructure protection, especially in the face of ISIS and other terrorist threats. As the Twin Towers' aluminum casts portend, a well-orchestrated attack on U.S. infrastructure could cause just as many tremors as a high-magnitude earthquake—tremors that could leave the nation without power, water, fuel, or food for an extended period of time and cause cascading catastrophe. Fortunately, ongoing efforts in GEOINT hold great promise for planners and first responders to both prevent and significantly mitigate future damage to critical infrastructure, be it from natural or manmade disasters.

WEB EXCLUSIVE
Read how UAVs are improving critical infrastructure evaluation at trajectorymagazine.com.

IMAGE COURTESY OF NGA