Understanding and Mitigating Catastrophic Disruption and Attack

Denise M.B. Masi, Eric E. Smith, and Martin J. Fischer

Analysts have amassed much data that points to vulnerabilities in telecommunications and cybersecurity. Examining past natural disasters and major attacks can provide valuable insight into mitigating new ones.

Communications is one of the critical infrastructure and key resources established by Homeland Security Presidential Directive 7 to protect the nation's resources from terrorist attacks. As part of that directive, the Department of Homeland Security established the National Cyber Security Center in 2008, primarily to protect classified networks. One of President Obama's first actions was to initiate a 60-day review of cyberspace policy, culminating in a report that stressed the need for the federal government and private sector to partner in solving cybersecurity issues—a thorny and technically demanding problem for telecommunications research.

Among those issues are the threats of events that can significantly disrupt the physical infrastructure or disable it from within by compromising data or services. Physically disruptive events can result in lost facilities or disrupt communications transport by destroying or damaging a vendor's point of presence, serving wire center, network operations center, or fiber-optic communications cables. Cyber attacks can involve widespread denial of service and malicious code, which compromise the security of classified facilities.

Although only some historic events are unusual enough in their source, severity, or mechanism to warrant the label "rare event," analysts can still glean valuable information. Even lesser events have the potential to do great harm, so it makes sense to examine both actual rare events and incidents that imply patterns building to a rare event. In either case, prediction, preparation, and mitigation are extreme challenges.

Inside Track

- The connection between electrical and telecommunications networks is a significant consideration in preventing and mitigating telecommunications disasters.
- As part of power source diversity planning, some carriers are connecting major telecommunications offices to two electrical substations.
- One expert has described the potential of a 15-minute cyber attack to catastrophically impact vital communication and utilities infrastructure in the United States.
- Modeling is integral to predicting and detecting the impacts of disruptions to telecommunications and the impacts of cyber attacks and other events that affect telecommunications networks.

Natural disasters

Natural disasters, such as hurricanes and earthquakes, can disable significant parts of the telecommunications infrastructure. The heaviest damage tends to be during and just after the disaster, which means that first responders' rescue and damage mitigation must target a local area, and residents must be able to learn about the event and the best response to it in a timely manner. Hurricane Katrina and the consequences of past severe earthquakes provide insight into how quickly and thoroughly a natural event can destroy a network's physical infrastructure.

Hurricane Katrina

On the Saffir-Simpson scale, Category 5 hurricanes are defined by tropical storms with maximum sustained winds greater than 155 mph and storm surges of over 18 feet. On August 29, 2005, Hurricane Katrina made landfall 54 miles southeast of New Orleans, delivering a Category 5 storm surge. Because New

Orleans is below sea level, the levee system broke and 80 percent of the city flooded.[1] As a result of these unique conditions, Katrina was by far the most damaging hurricane in U.S. history.

The U.S. Gulf Coast's telecommunications infrastructure, heavily concentrated in the New Orleans metropolitan area, suffered extensive damage during the storm. As Figure 1 shows, the storm destroyed nine BellSouth serving wire centers and affected 22 others. BellSouth lost service in 2.475 million lines. Long distance carriers were also affected. Sprint lost two facilities from flooding: a point of presence in Biloxi and a serving wire center in New Orleans. AT&T lost a fiber-optic regeneration hut near New Orleans, also from flooding. This outage reduced AT&T's transmission network capacity by five percent. Finally, Level3 suffered a power related outage at a fiber-optic regeneration hut south of Pearlington, Mississippi.[1]

As Figure 2 shows, facility downtime and outage severity were due either to physical damage or the electrical outage duration in the region. Because an extended electrical outage followed the storm, the telecommunications companies were forced to rely on stand-by diesel generators to power their facilities. These generators rely on fuel, which was in limited supply after the hurricane, so the facilities soon lost power and were offline. This connection between electrical and telecommunications networks is a significant consideration in preventing and mitigating telecommunications disasters.

Earthquakes

Less than .001 percent of earthquakes worldwide are a magnitude 7.0 or greater, with one such earthquake occurring in the United States about every two years.[2] Earthquakes of this magnitude can extensively damage the telecommunications infrastructure, and the consequences can last for days. The 1989 earthquake in Loma Prieta, California—the largest to occur since the 1906 quake in San Francisco—caused considerable traffic congestion in the Public Switched Telephone Network (PSTN) that continued for four days after the quake. Although no equipment or transport facilities were lost, experts speculated that more severe ground motions in this earthquake would have caused the loss of the telecommunications facility that housed AT&T and Pacific Bell equipment, which in turn would result in a communications loss in northern California for some time.[3]

Severe undersea earthquakes damage submarine fiber-optic cables, which can be extremely disruptive to communications. The 2006 Hengchun undersea earthquake near Taiwan, a magnitude 7.1, caused six submarine fiber-optic cables to break, which reduced capacities and interrupted communications for approximately five days within the Asia-Pacific region and between Asia and the United States and Europe.[4]

The threat of a 7.0+ earthquake is very real and possibly on the horizon. For example, geodetic data might be evidence that the San Andreas fault in California is nearing its seismic recur-

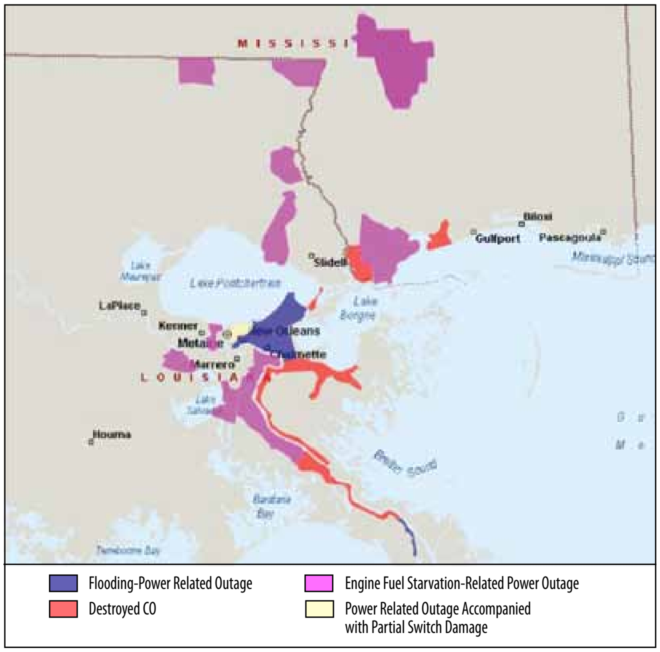


Figure 1. Causes of damage to BellSouth's physical infrastructure from Hurricane Katrina. The storm was responsible for destroying nine BellSouth serving wire centers and affected 22 others. Causes ranged from flooding to engine fuel starvation. Figure used with permission from IEEE (A. Kwasinki et al., "Telecommunications Power Plant Damage Assessment Caused by Hurricane Katrina—Site Survey and Follow-Up Results," *INTELEC*, 2006; https://netfiles.uiuc.edu/akwasins/www/Intelec06_Katrina.pdf).

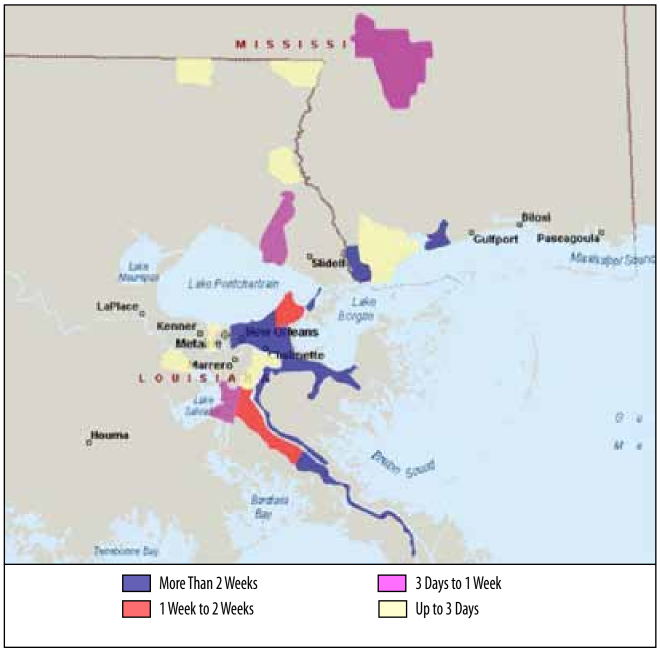


Figure 2. Severity of damage to BellSouth's physical infrastructure from Hurricane Katrina. Some of the 2.475 million lines that lost service were out for days. Figure used with permission from IEEE (A. Kwasinki et al., "Telecommunications Power Plant Damage Assessment Caused by Hurricane Katrina—Site Survey and Follow-Up Results," *INTELEC*, 2006; https://netfiles.uiuc.edu/akwasins/www/Intelec06_Katrina.pdf).

rence time, particularly in the southern part of the fault—a considerable threat to the Los Angeles area.[5] In a scenario posed by Pacific Tier Communications,[6] a strong earthquake could disable a well-known carrier hotel at One Wilshire in Los Angeles, disrupt submarine cable landing stations in Los Angeles and central California, and result in a tsunami that would hit Hawaii and several island nations in the South Pacific. This activity would severely degrade telecommunications services on the U.S. west coast and in the South Pacific. Only cable systems with automatic rerouting through the North Pacific would maintain connectivity.

Damage to only one carrier hotel is not likely to disrupt telecommunications nationwide, but an earthquake that takes out multiple carrier hotels could have more extensive consequences.

Planned disasters

As in natural disasters, the most significant damage is during and after a planned attack, and any first response must address a local area and its residents. The events of the September 11, 2001, attack on the World Trade Center in New York City are perhaps the most sobering example of how severely a terrorist attack can compromise the telecommunications infrastructure.

In addition to destroying or damaging the physical infrastructure in lower Manhattan, the attack caused congestion and blocking in cell calls, with volumes 50 percent higher than typical. As Figure 3 shows, increases were as much as 400 percent higher in the New York City area, with 75 percent of all cell phone calls blocked on the day of the attack. Verizon handled double the number of PSTN calls on that day, and high call volumes into and out of Washington, D.C. also caused call blocking.[7]

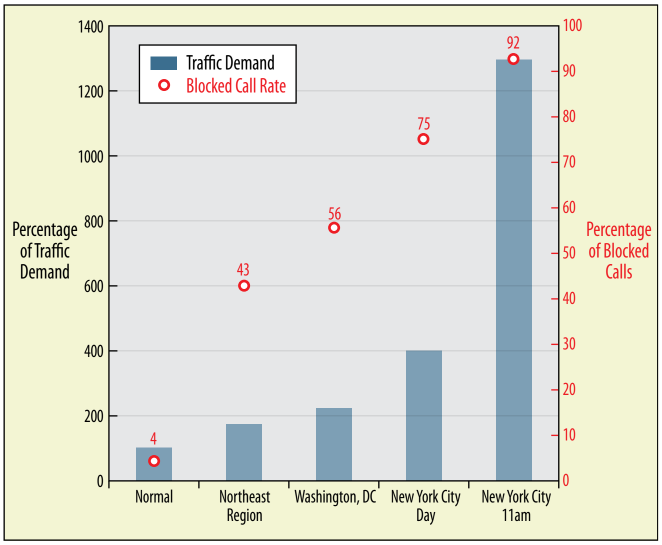


Figure 3. Blocked cellular call rate on September 11, 2001. Figure taken from *Report of Commission to Assess the Threat to the United States from EMP Attack* (p. 70). Image courtesy of the EMP Commission; www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf.

A Verizon central office building was damaged, which housed equipment belonging to customers of several competitive local exchange carriers and Internet service providers (ISPs). Approximately 14,000 business and 20,000 residential customers in New York City lost telephone and Internet service as a result, and data communications with a total capacity equivalent to about 90 OC 48 circuits (a processing capacity of about 224 gigabits per second).

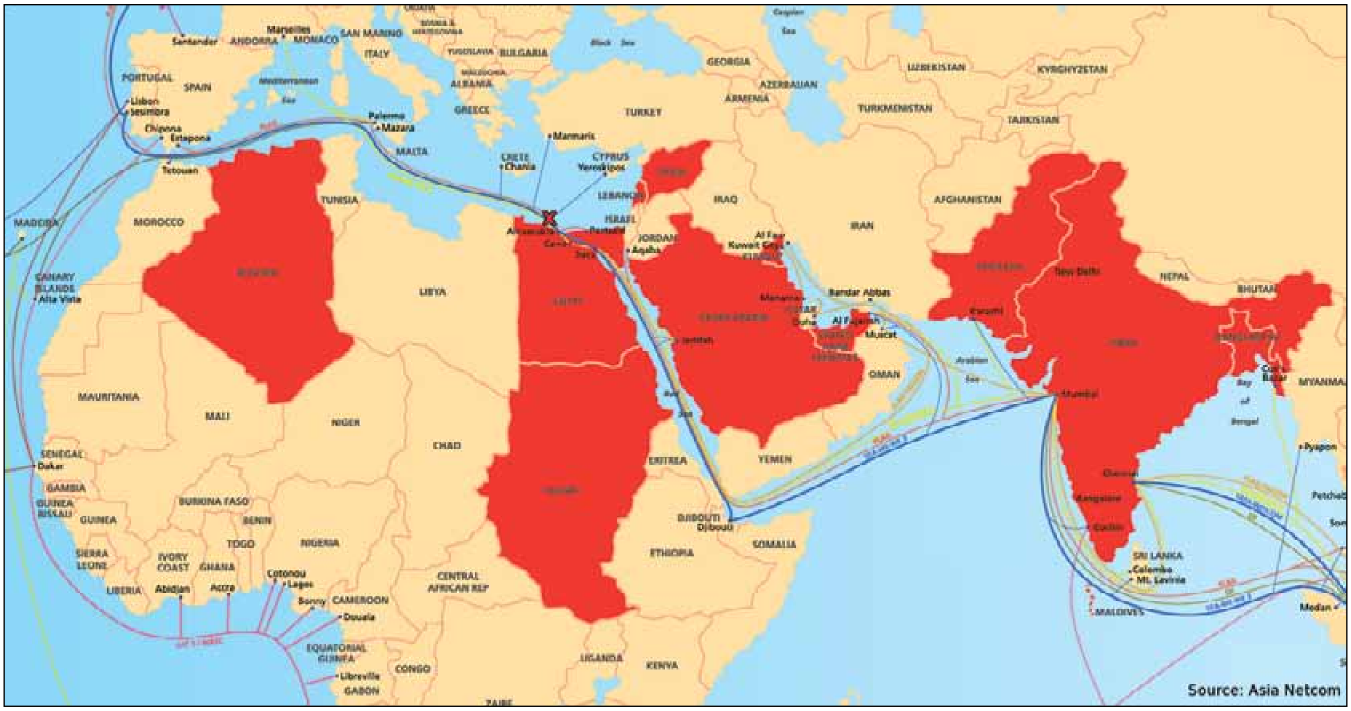
ISP points of presence within the World Trade Center were destroyed, including WorldCom, AT&T Local Service, and Verizon/Genuity. Sprint, PCS, Verizon, and AT&T Wireless customers lost service because the attack destroyed wireless repeaters in the World Trade Center. Finally, several ISPs had connectivity problems outside New York, including in Europe because their fiber-optic lines were being routed through Manhattan. The impact on the Internet overall was limited.

Cable cuts

Cuts to a fiber optic communications cable can be accidental or deliberate. A single or even a double cut to a fiber optic communications cable typically has little impact, since providers can reroute communications through alternative cables, but multiple simultaneous cuts can do significant damage because there is less chance that rerouting will be possible. Multiple simultaneous cuts in the same area can reduce the rerouting probability even more when the cuts are to undersea fiber optic cables, which typically connect continents.

In an incident on January 30, 2008, two underwater cables north of Alexandria, Egypt, were cut multiple times in the same area (the cause was never confirmed). Figure 4 shows the cables and affected countries. The two cables account for 76 percent of the transmission capacity among Europe, the Middle East, North Africa, and India. Both Internet services and call centers relying on the lines were affected. Other cables were cut in the same week, but with lesser impact. The Mediterranean areas affected have few alternative cables for rerouting, but providers were still able to restore Internet services after 24 hours at slower speeds. Full repair took weeks.[8]

Intercontinental undersea cable cuts are more likely than damaged underground cables to degrade telecommunications because rerouting is harder and more costly.[9] However, a series of underground cable cuts on April 9, 2009, in the San Francisco Bay area significantly impaired telecommunication services. Ten fiber-optic cables at four AT&T and Sprint locations were intentionally cut, resulting in loss of service to tens of thousands of customers in three counties. Wireless customers were impacted because some of the cut lines terminated at cellular base stations. Verizon customers were affected as well as AT&T and Sprint customers because Verizon was using some of AT&T's fiber. Some service was restored by traffic rerouting, although



Source: Asia Netcom

Figure 4. Multiple cuts in two undersea intercontinental cables. The countries in red were most affected by the cuts (red x above Egypt), which occurred on January 30, 2008. The two cables accounted for 76 percent of the transmission capacity among Europe, the Middle East, North Africa, and India. Image courtesy of Earl Zmijewski, Renesys; www.renesys.com/blog/2008/01/mediterranean_cable_break.shtml.

service was not completely restored until about 24 hours later.[10]

This extreme case of multiple cable cuts disabling telecommunication services in a region was likely due to sabotage, by someone who knew which network locations are most vulnerable and which manholes provided access to the network fibers.[9] The California cuts demonstrate how severely multiple underground fiber cuts can impact a smaller region.

Cybersecurity compromises

Although cyber attacks are increasingly common and thus not rare events in and of themselves, they do serve to highlight vulnerabilities, expose the use of unanticipated mechanisms, and sometimes result in a higher-than-expected disruption level. All these pointers are extremely valuable in planning prevention and mitigation.

In addition to potentially obtaining sensitive defense-related information, and harming civilian telecommunications, cyber attacks can damage Internet-linked control systems related to critical infrastructures such as the electrical grid, water-treatment facilities, refineries, pipelines, and dams. In 2008, a Central Intelligence Agency official disclosed that public utility networks outside the United States had been infiltrated and equipment had been disrupted, causing power outages in multiple cities.[11]

Some experts believe that a future attack is inevitable. Richard A. Clarke, the former counterterrorism czar, describes the potential of a 15-minute cyber attack to catastrophically impact vital communication and utilities infrastructure in the United States.[12] According to Clarke, a major cyber attack from another nation will indeed occur, despite best efforts to prevent it: "Our nation will still be devastated by a massive cyber attack on civilian infrastructure that smacks down power grids for weeks, halts trains, grounds aircraft, explodes pipelines, and sets fire to refineries." [12]

Several hostile incursions have already taken place, although the details are classified. The sidebar "Cyber Attack Intensity" describes attack details that are publicly available and that give a flavor of attack frequency, method, and intensity.

Prevention and preparation

Telecommunication companies are already taking preventive measures to harden their facilities against potential threats. Central offices or wireless base stations require protection techniques against lightning or electrostatic discharge such as grounding, shielding, and the use of surge-protection devices.

Packet and content filtering, intrusion detection and prevention systems, and authentication can help prevent or mitigate cyber attacks. The National Institute of Standards and Technology has a number of publications on standards and guidelines for the use of these measures. The government is in the process of instituting the Trusted Internet Connections Initiative to strengthen its cybersecurity preparation. The program will reduce the number of government access points and incorporate standardized security measures in those that remain. By the end of 2010, the government expects to have the implementation of this program about 80 percent complete.[13]

Analysts are also examining hypothetical events that could paralyze telecommunications. One of these is an electromagnetic pulse (EMP), which could disable essential switches and routers. The Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, established in 2001, has concluded that an EMP would damage a significant portion of the telecommunications circuits in the exposed area.

Mitigation

The impact of rare and catastrophic events on telecommunications can be mitigated by precautionary measures such as establishing a diversity plan for power sources, telecommunications fiber, data centers, and other equipment. Strategies to mitigate the impact of cyber attacks are also imperative.

Telecommunications

One strategy for planning power source diversity is to connect major telecommunications offices to two electrical substations, and some carriers are already doing this.[14] Mitigation also requires flexibility with margins, in addressing the failure—have planned limits but also a backup resource if those limits are exceeded. For example, backup generators generally have enough fuel only for up to 72 hours of electrical failure, and some catastrophic events have exceeded this planned life.[15] The National Resource Commission recommends that telecommunications facilities keep additional fuel stores on hand for backup generators and follow the Telecommunications Electric Service Priority program to improve the ability to withstand a sustained power loss.

Major telecommunications users should also avail themselves of the access diversity offered to government facilities under FTS2001 and Networx.[16] If service is lost, geographically diverse access services from a carrier point of presence all the way to the customer location through separate entrances will provide the greatest resilience to that loss. Carrier diversity (using two telecommunications carriers) might not guarantee diverse routing from the customer location to telecommunications facilities. Such access diversity is costly when special construction is required. Carrier backbone networks use diverse fiber to enable rerouting, which means that diversity in the access leg is more important. The use of services such as wireless, satellite, and radio can also increase diversity.

Cyber Attack Intensity

In 2003, the Department of Homeland Security created the U.S. Computer Emergency Response Team, and called on the Computer Emergency Response Team Coordination Center (CERT/CC; www.cert.org) at Carnegie Mellon University to help coordinate a defense against and response to cyber attacks.

The number of vulnerabilities reported to the CERT/CC has grown exponentially. In 2000, approximately 1,000 incidents were reported. In 2006, that number had ballooned to more than 8,000. CERT/CC has also noted more sophistication in the tools and techniques that intruders use and an increase in both the damage amount and the difficulty in detecting an attack and catching the attackers. Coincidentally, the knowledge required to initiate an attack had been decreasing.[1] These trends implied a vulnerability to a major attack.

Indeed, in February 2007, the Internet sustained a distributed denial of service (DDOS) attack to its Domain Name System root nameservers, which lasted 24 hours.[2] Of the 13 servers worldwide, two were badly affected. Because of the Anycast rerouting technology put in place after a similar attack in 2002, Internet users were hardly affected.

In 2008, the head of the Federal Bureau of Investigation's Cyber Division stated that as many as two dozen nations have taken an aggressive interest in penetrating U.S. networks,[3] and a high-ranking U.S. Air Force cyber official has ranked the United States as only fifth in the world in cyberspace capabilities.[4] In the same year, the Conficker code, thought to have infected more computers than any other worm, infected at least 12 million home, business, and government computers worldwide[5] and 10 months later still controlled 5 million.[6]

Another 2007 DDOS attack on Estonia (supposedly by Russia) resulted in denials of service that caused most of Estonia's government websites and some commercial sites to be unreachable for three weeks.[4] This event marked a new era in cyber attacks, in which adversaries routinely attempt to gain access to Department of Defense and other government networks.

References

1. J. Allen, *Information Security as an Institutional Priority*, Software Engineering Institute, Carnegie Mellon University; www.cert.org/archive/pdf/info-sec-ip.pdf.
2. *Factsheet—Root Server Attack on 6 February 2007*, ICANN, Mar. 1, 2007; www.icann.org/en/announcements/factsheet-dns-attack-08mar07_v1.1.pdf.
3. *The Cyber Threat Today: Major Attacks on the Rise*, Federal Bureau of Investigation, Oct. 17, 2008; www.fbi.gov/page2/oct08/cyberthreat101708.html.
4. W.T. Lord, Major General, USAF, "USAF Cyberspace Command: To Fly and Fight in Cyberspace," *Strategic Studies Quarterly*, fall 2008; www.au.af.mil/au/ssq/2008/fall/lord.pdf.
5. *Cybersecurity Collaboration Report*, The President's National Security Telecommunications Advisory Committee, May 21, 2009; www.ncs.gov/nstac/reports/2009/NSTAC%20CCTF%20Report.pdf.
6. J. Markoff, "Defying Experts, Rogue Computer Code Still Lurks," *The New York Times*, Aug. 26, 2009; www.nytimes.com/2009/08/27/technology/27compute.html.

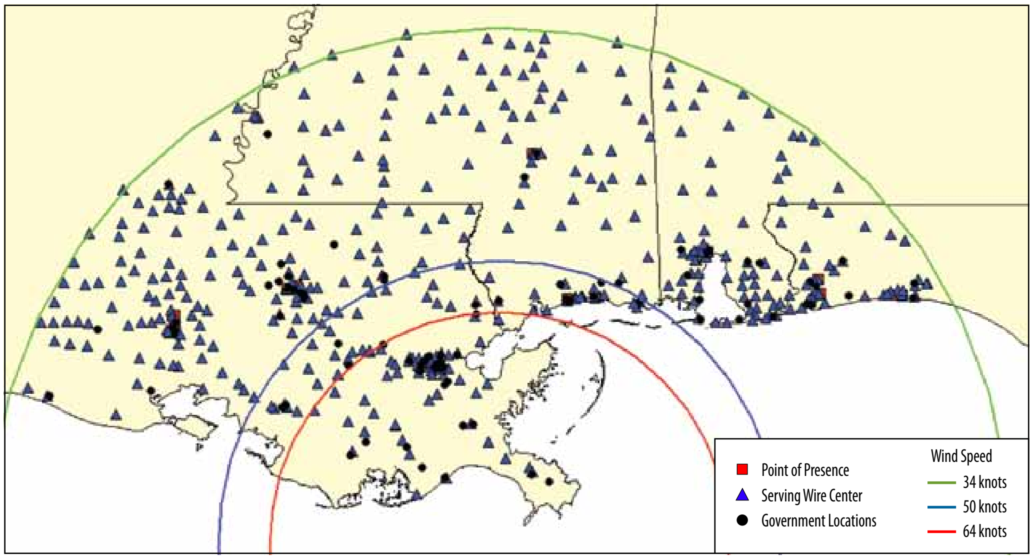


Figure 5. Sensitivity of the telecommunications infrastructure to Hurricane Katrina. Noblis used its Telecommunications Infrastructure and Sensitivity Tool to identify the points of presence, serving wire centers, and government locations in the area hit by Hurricane Katrina. The tool also identified the bandwidth used by each federal agency.

All these strategies to increase diversity will increase network design cost. Thus, it makes sense to identify the most important telecommunications facilities, fiber cables, and other equipment and give those elements priority in procuring access diversity. To aid in that prioritizing task, in 2004, Noblis developed the Telecommunications Infrastructure and Sensitivity Tool (TIST) to assist government agencies in analyzing their telecommunications traffic inventory on the FTS2001 contract. The team continued to refine TIST, which evolved to the Networx Pricer Inventory Module (NPIM) in 2009 with the addition of the traffic inventory on the Networx contract.

Immediately after Hurricane Katrina, a federal agency tasked Noblis to identify the points of presence, serving wire centers, and government locations in the affected area. Using TIST, Noblis was able to provide the graphic in Figure 5, listing the facilities, the bandwidth at each facility, and a breakdown of bandwidth by agency.

Cyber attack

According to a U.S. Department of Energy report evaluating the mathematical underpinnings of cybersecurity, work in five mathematical areas will aid in reducing the impact of attacks on Internet Protocol (IP) networks:[17]

- knowledge discovery and information science for massive real-time data;
- graph analysis of the Internet and its inherent structure;
- understanding the Internet as a dynamic, complex network;
- statistical assessments of cyber traffic and risk analysis; and
- structural study of the accessibility and vulnerability space.

The report also noted that a successful mathematical framework aids in understanding the distinguishing characteristics of flows and events and their distribution. Armed with these insights, analysts design protection points at critical junctures, such as having virtual security guards at transfer points and creating mechanisms that will detect a particular set of anomalies and intrusions. Collaborative efforts, such as the Conficker Working Group of experts from government, industry, and academia, can make progress in reducing the impact of cyber attacks. Some kind of knowledge framework will be critical in keeping pace with rapidly evolving cyber threats.

Prediction and detection

Modeling is integral to predicting and detecting the impacts of disruptions to telecommunications and the impacts of cyber attacks and other events that affect telecommunications networks.

Noblis' NPIM provides maps to enable the viewing of traffic inventory as well as software to conduct a sensitivity analysis. NPIM users use both the maps and software to examine the effect on traffic inventory if a point of presence or serving wire center is disabled during a hurricane, earthquake, or other rare event. Because the NPIM aids in conducting a sensitivity analysis of events, it is useful in planning, preparing, and designing damage mitigation strategies. For example, by examining use level, analysts can identify the points of presence and serving wire centers that are the most critical to the government's telecommunications networks in that particular area. After finding these critical locations, the tool can help identify facilities that could serve as alternatives in an access diversity plan.

Noblis has also developed IP-Surviv, a tool that aids in analyzing a network's ability to survive rare events such as terrorist attacks, natural disasters, and random electronics failures. The tool has already assisted analysts in quantitative studies of an IP network's resilience to the impact of a potential attack on the

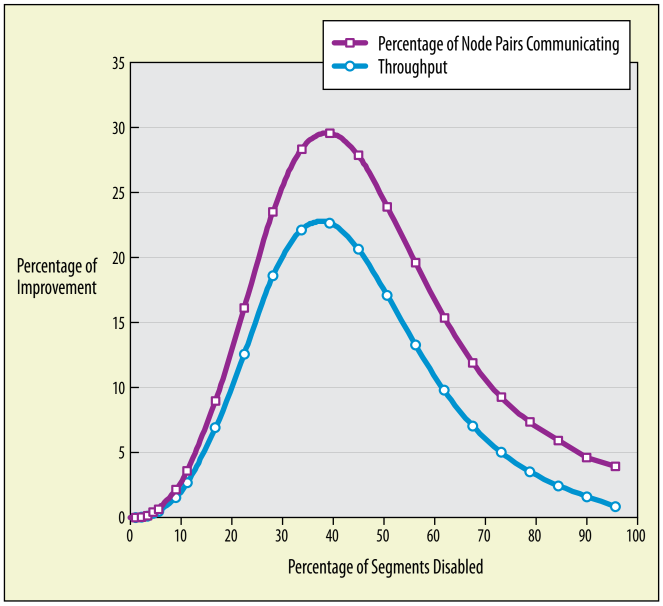


Figure 6. Mitigating attack consequences with Internetwork routing. Results from several failure scenarios show that modifying internetwork routing policies improves network survivability (communication and throughput) when the event causes major damage.

provider's IP network. Noblis has used the tool to analyze the rare event types just listed and has examined the resulting network throughput and connectivity. Results from several failure scenarios show that modifying internetwork routing policies improves network survivability when the event causes significant damage. In Figure 6, for example, the improvement is most dramatic when about 40 percent of the network is down. Worst case results were used to support the development of survivability objectives for telecommunications carriers that provide service for a federal agency's telecommunications priority service programs.

A set of national planning scenarios, intended for use in homeland security preparedness activities, can also aid prediction. Developed across agencies, the scenarios involve nuclear and chemical attack and natural disasters that could affect the telecommunications infrastructure. These scenarios are designed to assist with the development of national preparedness standards and measurement of capabilities, as well as being useful for modeling and simulation exercises.

The ability to use the communications and cyber infrastructure is critical to our nation's economy and security and is closely linked with other critical infrastructure sectors. Rapid, reliable communication is integral to any response in the immediate aftermath of a terrorist attack, natural disaster, or other event that could damage or incapacitate the U.S. communications and cyber infrastructure.

Modeling and simulation are proven ways to study previous events and are invaluable aids in developing contingency and mitigation of future events on a similar scale. ■

References

1. A. Kwasinski et al., *Telecommunications Power Plant Damage Assessment Caused by Hurricane Katrina—Site Survey and Follow-Up Results*, Telecommunications Energy Conference, 2006; https://netfiles.uiuc.edu/akwasins/www/Intelec06_Katrina.pdf.
2. *Earthquake Facts and Statistics*, U.S. Geological Survey National Earthquake Information Center; http://earthquake.usgs.gov/earthquakes/eqarchives/year/eqstats.php.
3. *The Loma Prieta, California, Earthquake of October 17, 1989—Lifelines*, U.S. Geological Survey Professional Paper 1552-A, Anshel J. Schiff, ed., 1998; http://pubs.usgs.gov/pp/pp1552/pp1552a/pp1552a.pdf.
4. *Asia Communications Hit by Quake*, BBC News; Dec. 27, 2006; http://news.bbc.co.uk/2/hi/asia-pacific/6211451.stm.
5. Y. Fialko, "Interseismic Strain Accumulation and the Earthquake Potential on the Southern San Andreas Fault System," *Nature*, vol. 441, 2006; http://sioviz.ucsd.edu/~fialko/papers/fialkoNature06.pdf.
6. *Risk and Security in the Telecommunications Industry Series—Part 1*, Pacific-Tier Communications; http://pacific-tier.com/blog/2009/10/risk_and_security_in_the_telec.html.
7. J.S. Foster et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures*, EMP Commission, 2008; www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf.
8. *Mediterranean Fibre Cable Cut—a RIPE NCC Analysis*, RIPE NCC; www.ripe.net/projects/reports/2008cable-cut/index.html.
9. M. Reardon, "How Secure Is the U.S. Communications Network?," *CNET News*, Apr. 13, 2009; http://news.cnet.com/8301-1035_3-10217550-94.html.
10. M. Reardon, "Service Restored in Silicon Valley after Fiber Cut," *CNET News*, Apr. 10, 2009; http://news.cnet.com/8301-1035_3-10216939-94.html.
11. G. Derene, "How Vulnerable Is U.S. Infrastructure to a Major Cyber Attack?" *Popular Mechanics*, Apr. 2009; www.popularmechanics.com/technology/military_law/4307521.html.
12. R. Clarke and R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, Ecco, HarperCollins Publishers, 2010; www.harpercollins.com/books/Cyber-War/?isbn=9780061962233.
13. E. Chabrow, "What's Happening with the Trusted Internet Connection?," *Government Information Security*, Mar. 1, 2010; www.govinfosecurity.com/podcasts.php?podcastID=451.
14. S.R. Bailey, *The Resilient Homeland—Broadening the Homeland Security Strategy*, Testimony to the House of Representatives Committee on Homeland Security, May 6, 2008.
15. National Research Council of the National Academies, *The Internet Under Crisis Conditions: Learning from September 11*, The National Academies Press, Washington, D.C., 2003.
16. J.R. Soltys, S. Chandra, and S.S. Rutherford, "Network Diversity as a Means to Reduce Catastrophic Failure Risks," *The Telecommunications Review*, Noblis, pp. 1–9, 2002; www.noblis.org/NewsPublications/Publications/TechnicalPublications/TelecommunicationsReview/Pages/2002TelecommunicationsReview.aspx.
17. *Mathematical Underpinnings for Science-Based Cyber Security*, U.S. Department of Energy White Paper; https://wiki.cac.washington.edu//download/attachments/7479040/doecybermath25feb08.doc.

Denise M.B. Masi is a fellow at Noblis, where her experience and research interests include queueing theory and simulation applied to telecommunications networks. Masi received a PhD in information technology and engineering from George Mason University. Contact her at dmasi@noblis.org.

Eric E. Smith is a lead engineer at Noblis, where his experience and research interests include mathematical programming as applied to telecommunications network design. Smith received a PhD in information technology from George Mason University. Contact him at eric.smith@noblis.org.

Martin J. Fischer is a guest editor of this issue. His biography appears on p. 10.