

The Internet Under Crisis Conditions: Learning from September 11

Jon Eisenberg¹ and Craig Partridge²

INTRODUCTION

Although secondary to the human tragedy resulting from the September 11, 2001, attacks on the World Trade Center and the Pentagon, telecommunications issues were significant that day both in terms of damage (physical as well as functional) and of mounting response and recovery efforts. The Internet has come to be a major component of the nation's (and the world's) communications and information infrastructure. People rely on it for business, social, and personal activities of many kinds, and government depends on it for communications and transactions with the media and the public. Thus there is interest in how the Internet performed and was used on September 11.

Unlike the situation with longer-standing telecommunications services (notably the public telephone network), there are few regulations, policies, or practices related to the Internet's functioning in emergency situations. Nor are there many publicly available data to help policy makers or the industry itself assess the Internet's performance—either on a continuing basis or in the aftermath of a crisis. No regular system exists for reporting failures and outages, nor is there agreement on metrics of performance. Some experiences are shared informally among network operators or in forums such as the North American Network Operators Group (NANOG), but that information is not readily accessible for national planning or research purposes. The decentralized architecture of the Internet—although widely characterized as one of the Internet's strengths—further confounds the difficulty of collecting comprehensive data about how the Internet is performing. It is therefore unsurprising that no definitive analyses exist on the impact of September 11 on the Internet, though a few conflicting anecdotal reports about its performance that day—such as several presentations at NANOG indicating relatively little effect and press accounts suggesting that the impact was severe—have appeared.

Responding to an initial request in early 2002 from the Association for Computing Machinery's Special Interest Group in Data Communication (ACM SIGCOMM), the Computer Science and Telecommunications Board (CSTB) established the Committee on the Internet Under Crisis Conditions: Learning from the Impact of September 11.³ The study's goals were twofold: to organize an exploratory workshop for gathering data and accounts of experiences pertinent to the impact of September 11 on the Internet, and to prepare a report that summarizes the Internet's performance that day and offers conclusions on better preparing for and responding to future emergencies.⁴

¹ Computer Science and Telecommunications Board, The National Academies, 500 5th St, NW, Washington, DC 20001, <jeisenbe at nas dot edu>.

² BBN Technologies, 10 Moulton St, Cambridge MA 02138, <craig at bbn dot com>.

³ Study committee members: Craig Partridge (chair), Paul Barford, David D. Clark, Sean Donelan, Vern Paxson, Jennifer Rexford, Mary K. Vernon.

⁴ This paper is based on Computer Science and Telecommunications Board, National Research Council, 2003, *The Internet Under Crisis Conditions*, National Academies Press, Washington, D.C., <<http://www.nap.edu>>. Used by permission. Support for this project was provided by the Association for Computing Machinery's Special Interest Group in Data Communication (ACM SIGCOMM); the IBM Corporation; and the Vadasz Family Foundation, a contributor to the Computer Science and

A diverse group of industry representatives and researchers participated in the workshop.⁵ They were invited to share information candidly, with the understanding that sensitive or proprietary information would not be published. Consequently, specific figures or names of organizations have been omitted in some instances. Following the workshop, additional information was gathered from a number of sources.

OVERVIEW OF TELECOMMUNICATIONS EVENTS ON SEPTEMBER 11

The overall human and economic costs of the September 11 attacks—which dwarf in significance the attacks' effects on the Internet—have been widely covered and are not examined here. Instead, this paper focuses on three issues related to the Internet: (1) the local, national, and global consequences of the destruction that occurred in New York City; (2) the impact of the crisis, including the actions of users as well as the effects of the physical damage; and (3) how people made use of the Internet in a time of crisis. The events of September 11, 2001, in addition to their other consequences, caused localized physical damage to the Internet in one of the network's most important hubs, New York City. Communications infrastructure located in the World Trade Center itself and nearby at the Verizon central office at 140 West Street, along with fiber-optic cables that ran under the Trade Center complex, was destroyed. Electrical power in Lower Manhattan was disrupted, and local telecommunications facilities there suffered a variety of problems with their backup power systems.

Serious effects on communications networks, however, were confined to New York City and a few other regions highly dependent on it for their connectivity. In some cases, automatic rerouting at the physical or network levels allowed Internet traffic to bypass many of the infrastructure's failed parts. Most local Internet-connectivity problems that could not be resolved by automatic rerouting were fixed within hours or days through the rapid deployment of new equipment or reconfiguration of the system.

Although users outside New York City were also affected by the events of September 11, most of the difficulties experienced were not due to serious problems in the Internet infrastructure itself but rather to disruptions stemming from subtle interdependencies between systems—it turned out that some services depended indirectly on connections made in New York City.

Even though their network connectivity had not been impaired, many users had difficulty reading some popular news Web sites. Unprecedented levels of user demand immediately following the attack severely stressed the server computers for these sites. Web service providers quickly took a number of steps—such as reducing the complexity of Web pages, using alternative mechanisms for distributing content, and reallocating computing resources—to respond

Telecommunications Board's program on information technology and society. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the organizations that provided support for the project.

⁵ Workshop participants: Fred Baker, Cisco; Aristotle Balogh, Verisign; Paul Barford, University of Wisconsin, Madison; K. Claffy, Cooperative Association for Internet Data Analysis; David D. Clark, Massachusetts Institute of Technology; Chase Cotton, Sprint Technology Services; Sean Donelan, SBC Communications; Stuart I. Feldman, IBM Research; Geoffrey S. French, Veridian; Deirdre Kostick, AT&T; Timothy Lance, NYSERNet; William LeFebvre, CNN Internet Technologies; Geraldine MacDonald, America Online; Bruce Maggs, Akamai/Carnegie Mellon; David Moore, Cooperative Association for Internet Data Analysis; Andrew T. Ogielski, Renesys; Craig Partridge, BBN Technologies; Vern Paxson, International Computer Science Institute's Center for Internet Research; John S. Quarterman, Matrix NetSystems; Lee Rainie, Pew Internet and American Life; Jennifer Rexford, AT&T Labs—Research; David Safford, IBM Research; Steve Schneider, State University of New York, Institute of Technology; Anthony Townsend, New York University; and Mary K. Vernon, University of Wisconsin, Madison.

successfully to demand.

Despite these problems, the fact is that the Internet, taken as a whole, was not significantly affected. For example, it did not suffer the kinds of overloads that are often associated with the telephone system in a time of crisis. The resilience of the network during the September 11 crisis was a credit to the ingenuity and perseverance of the people who worked to restore communication service near the attack sites; and fundamentally, it was testimony to the Internet's inherently flexible and robust design.

However, the Internet's performance on September 11 does not necessarily indicate how it might respond to being directly targeted. Furthermore, it is clear that the experience of individual Internet service providers (ISPs) and corporate networks on September 11 does not generalize: damage suffered, and ability to respond, varied widely from place to place. In particular, the modest effect on Internet communications overall does not indicate how well an individual ISP (and its customers) would fare in an attack targeted specifically to that ISP. Representatives of several ISPs reported that what made September 11 a relatively untroubled (albeit unnerving) day for them was simply the fact that their facilities were not concentrated at 140 West Street. In any case, the experience did establish the Internet's overall resilience in the face of significant infrastructural damage.

FINDINGS FROM THE STUDY

The study revealed a number of insights about what happened and did not happen to the Internet as a result of the attacks of September 11, 2001. It also provided a number of lessons learned that could reduce the impact of future crises, and it pointed to some ways in which the Internet itself could play a greater role in crisis response.

The events of September 11 had little effect on Internet services as a whole. The network displayed considerable flexibility that underscored its adaptability in the face of infrastructure damage and the demands imposed by a crisis.

In much of the data examined in this study, an observer would be hard-pressed to find any unusual impact from the events of September 11 outside the immediately affected areas. Connectivity indeed dropped on the morning of September 11 at some points throughout the Internet, and it dropped as well during several subsequent intervals when electrical-power disruptions affected telecommunications facilities in Lower Manhattan. But connectivity recovered quickly, and the magnitude of its loss was actually less than has been seen in other incidents affecting the Internet. For some users, however, the events of September 11 significantly affected their Internet experience, disrupting their connectivity altogether or limiting their ability to obtain information from certain news sites.

Measures of overall Internet traffic suggest that traffic volumes were somewhat lower on September 11 than on a normal business day, with many who normally would be using the Internet turning to television for news and to phone calls for reaching loved ones. Traffic did increase in two areas—the quest for news and the use of Internet communications as a substitute for telephone calls. News Web sites, straining under unprecedented levels of demand, took a number of steps to enhance their ability to handle the traffic (Box 3.1 in Chapter 3 describes CNN's experience in particular and the strategies it employed). Low-bandwidth e-mail and instant messaging were used as substitutes for telephone service, especially where conventional-telephone and cellular network congestion was high.

Overall, the Internet experience on September 11 was in no way comparable to the trials of some other communications media, such as the cellular phone services in greater New York, which suffered from local infrastructure damage and regional congestion. In part, this difference

reflects the Internet's unique design.

A number of examples of how the Internet was used in the hours and days immediately following the September 11 attacks highlight the flexibility afforded by that design. NYSERNet, a nonprofit networking consortium, was able to reroute connectivity to bypass physical damage in Lower Manhattan. It proved relatively easy to reconnect the New York Academy of Medicine to the Internet by means of a jury-rigged wireless link. When telephone service was impaired (through local damage to telephone circuits and disruption of some toll-free systems), some network operators were able to use instant messaging and voice-over-Internet Protocol (IP) to coordinate activities. CNN and other information providers adapted their content and modified the ways in which they delivered Web data to accommodate the extraordinary demand for news. A wireless instant-messaging service saw increased use on September 11 and in the following days. Various groups rapidly set up Web sites for exchanging information on the disaster and the possible whereabouts of missing people.

An important point about these responses is that they required no central coordination. Individuals and groups were able to spontaneously craft solutions to their problems and to deploy them quickly.

While one can conclude with confidence that the events of September 11 had little effect on the Internet as a whole, the precision with which analysts can measure the impact of such events is limited by a lack of relevant data.

The data available in this study to gauge the impact of September 11 included active measurements of packet delay and loss over a small fraction of the Internet's paths, selected passive monitoring of application-level behavior and global-routing activity, and data from a survey of Internet users. In some cases, this information was sufficient for drawing qualitative conclusions. But examination also revealed the paucity of Internet data available to the research community. Available data are limited for reasons that include the following:

- *Factors intrinsic to the Internet's design.* One cannot, for example, determine how many individual users are actually affected by the loss of routes to a particular set of addresses. It is also hard to know if users who have lost connectivity through one route have reestablished connectivity through another one—new connections might have been made at a higher level of aggregation, in which case data showing fewer routes available would not mean worse connectivity.
- *Modest size of the measurement universe.* The measurements of Internet activity that are made on a regular basis are rather limited. For example, connectivity is monitored to some extent by examining routing tables, but only from particular vantage points. Routes themselves are periodically traced to probe connectivity, but only with coarse time granularity. Data collected on traffic volumes (workload) are often considered proprietary, and much of the measurement of Internet activities is conducted by small research groups with modest resources. Moreover, the available analysis and modeling tools for probing Internet behavior could be much improved.
- *Tendency to simply discard data.* Even when information is collected, it is often retained only for a short time. In a number of cases, requests for workload data and other detailed logs of Internet activity during September 11 showed that the data had already been discarded by the time of the March 2002 workshop.
- *Nonavailability of good measures of the overall state of the Internet.* One of the consequences of the fragmented and often proprietary measurement infrastructure is that data are gathered piecemeal in diverse ways and stored in various formats; there is no commonly accepted way of standardizing what information is collected and integrating the data to enable

characterization of the Internet's overall health. Therefore, ready comparison of September 11 to a "typical" day was not possible. The information available in this study generally permitted only rough comparisons in the context of a particular set of data (e.g., data on the reachability of a particular set of Internet addresses suggest that the effects of September 11 were similar to those of a severed fiber-optic cable). One exception was that some conclusions could be drawn about the Internet as a whole when specific measurements could be correlated with data from surveys of Internet users (which are designed to be representative of all U.S. users).

The inability to measure in detail the effects of September 11 on the Internet does not by itself provide a clear mandate for building a new and widespread Internet measurement system, which would be both complex and costly. Gathering data across all Internet providers would probably require new regulations to compel their cooperation. There is, however, a relatively easy way to help improve understanding of the Internet's behavior during crises or other anomalous events: simply holding on to the relevant data. One lesson from September 11 with regard to Internet measurement is that important data from such circumstances are typically discarded soon after the fact. It may be useful to find ways to alert network managers to the importance of archiving data collected during significant events so that more detailed analysis can be performed later on.

The events of September 11 did have a major effect on the services offered by some information and service providers.

Although the Internet as a whole was largely unaffected by the events of September 11, those services and service providers that *were* affected were often hit hard. The surge in demand for news overwhelmed the Web-server capacity of at least two major news services, for example, and nearby infrastructure serving the New York Stock Exchange and its member firms was heavily damaged.

Also, while many of the effects of September 11 were highly localized (like the attacks themselves), some parties far from the physical disaster sites were affected—ISPs in parts of Europe lost connectivity because they interconnected with the rest of the Internet in New York City, and South Africa was cut off as a result of losing connectivity with the Domain Name System (DNS).

People's use of Internet services on and immediately following September 11 differed from what has been typical.

People used the Internet very differently in the aftermath of the September 11 attacks. For example, they sent less e-mail overall (although some substituted e-mail for phoning where the telephone networks were congested), and they used news sites more heavily. They made greater use of instant messaging. The overall picture that emerges is that individuals used the Internet to supplement the information received from television (which was the preferred source of news). Those unable to view television often substituted Internet news. The telephone, meanwhile, remained the preferred means of communicating with friends and loved ones, but chat rooms and e-mail were also used, especially where the telephone infrastructure was damaged or overloaded.

The levels of other activities on the Internet, such as e-commerce, declined. One consequence of this decrease was that in spite of larger numbers of person-to-person communications, total load on the Internet decreased rather than increased, so that the network was not at risk of congestion.

September 11 demonstrated the Internet's overall resilience to physical attacks. But it also revealed that in parts of the system, redundancy appears to have been inadequate.

The attacks of September 11 were not directed at the Internet. Nonetheless, because New York City is a major worldwide data-communications hub and a number of key communications links and facilities were concentrated in a handful of sites near the World Trade Center complex, the attack caused significant damage to Internet elements. On the basis of its analyses of the effects of the attack, of steps taken to restore connectivity, and of various "what if" scenarios, one can conclude the richness of the Internet's interconnectivity provides effective protection against a localized physical attack. Although workshop participants cautioned that a carefully designed, distributed attack against a number of physical locations, especially if carried out in a repeating pattern, could be highly disruptive, an attack at a single point or a small number of points is probably survivable.

Regarding the infrastructural damage that occurred on September 11, the level of Internet redundancy was adequate outside the immediately affected area. However, parts of the Internet were not as redundant as one might suppose. Links that were logically distinct turned out to run over the same fiber spans or to be connected to major systems through the same trenches or buildings. Co-location of capacity and equipment cuts expenses, but it obviously increases vulnerability to common outages. Improving the robustness of the communications infrastructure may require conscious trade-offs between reliability and cost. Finally, certain providers and certain regions of the world are heavily dependent on a few key connection points; diversifying those points would significantly improve robustness.

The connectivity problems outside New York City illustrate that end-to-end communication on the Internet depends on the functioning of several different (often geographically separate) systems such as local phone lines, modem banks, authentication servers, and DNS servers. In addition, some wireless applications (handheld devices at hospitals, for example) depend on Internet access to reach application services located in the same building. A hospital in New York City learned on September 11 that wireless personal digital assistants (PDAs), on which doctors rely to access medical information, were connected through an external ISP network. Thus when the hospital's sole link to the Internet was briefly broken by the collapse of the Twin Towers, doctors had trouble accessing hospital records. ISPs and users alike should be aware of these potential vulnerabilities and take appropriate steps to improve redundancy where connectivity is mission-critical.

The Internet experience on September 11 exposed a number of subtle operational issues that merit attention from users and operators.

Most disasters impart useful lessons on what might be done better in the future. The September 11 experiences of ISPs and users were no exception:

- *Internet operations depend on the public telephone network.* One specific vulnerability is the use of toll-free telephone numbers for communicating between different ISP operation centers. This practice makes Internet operations vulnerable to outages in the toll-free system (which involves an extra database lookup as compared with direct-dialing of a toll call). And the toll-free system indeed had a partial failure on September 11 as a result of call volume, complicating ISP coordination. More generally, although the public telephone network and the Internet are for the most part logically distinct, they are closely tied physically because both depend on the same fiber-optic infrastructure. This shared vulnerability suggests that in the future the two networks be analyzed together; for example, to what degree are they

dependent on the same physical facilities and to what degree can they actually substitute for one another?

- *Telecommunications-facility disaster planning should factor in support for operational personnel, and ensuring a capability for remote operation should be considered wherever possible.* One ISP reported difficulty in feeding its operations staff, as all the businesses around its center in Northern Virginia had closed. There was some difficulty getting diesel fuel delivered to backup power generators serving telecommunications facilities in Lower Manhattan. Key data centers were sometimes inaccessible as a result of areawide closures, even though they themselves had not suffered damage. Operators that could manage their sites remotely, however, reported that this capability was valuable for keeping services running.
- *Key businesses and services that must operate in a disaster should examine their dependence on Internet connections and plan accordingly.* Several examples of interdependencies arose in workshop discussions: (1) a New York City hospital relied on an external Internet link to connect wireless PDAs, (2) the NYC.gov Web site was disconnected from the Internet by the attack, and (3) major news sites had difficulty accommodating higher demand. Specific responses that may be appropriate for organizations and Web sites likely to be used in an emergency include these: (1) providing redundant network connectivity (from more than one network provider and by way of more than one physical link or conduit), (2) performing an end-to-end audit of Internet dependencies, and (3) establishing plans for dealing with greatly increased traffic loads.
- *Network operators and telecommunications interconnection facility operators should review their emergency power procedures.* Power problems caused transient disruptions to Internet connectivity as well as possible damage to the equipment because of overheating (when cooling systems failed). Most network operators and ISPs had already established procedures for dealing with power failures, and in New York City these procedures generally worked as planned. But not enough attention appears to have been paid to the possibility that some backup systems could fail. For example, a number of disruptions to the Internet occurred 8 to 12 hours after the power was shut off in Lower Manhattan because backup batteries and generators failed. Reports also suggest that ISPs, unlike some other utilities, were not granted access to the restricted zone in Lower Manhattan, which further complicated their recovery efforts. Specific problems included these:
 - Poor operating procedure resulted in a facility's backup generator being shut off to conserve fuel, which in turn led to service interruptions when grid electrical power was lost.
 - Fuel delivery problems, including delivery of the wrong type of fuel to one location, made it difficult to keep generators running.
 - Communications equipment was allowed to continue operating even when electrical power necessary for cooling systems had been lost.
 - Fiber termination circuits were not connected to generators and failed when their 8-hour batteries failed.
 - Backup generators shut down when their air intake filters became clogged with dust, a problem that could possibly have been averted if more rapid access for maintenance had been possible.

Several prudent steps could be taken to reduce future disruptions. Operators should evaluate their vulnerabilities to multiday electrical outages. In particular, the evaluation should determine the primary and backup power source for every major device (server, router, switch) and independently powered link (e.g., Synchronous Optical Network [SONET] or

point-to-point fiber). Operators should also identify how each device will respond to a power outage (after both primary and backup power fail) and how it will resume functioning when power is restored. Operators should develop contingency plans that allow them to provide services for the maximum period of time (in particular, all key devices should use the longest-lived backup power supplies available) and restore most services remotely after an outage. Operators should also identify special needs (e.g., fuel for generators and the space in which to place additional generators if required) that may require the consent of local authorities, and they should have plans for coordinating with authorities in the event of an emergency.

The experience gained from the events of September 11 points to ways in which the Internet could be better leveraged in future crises.

It is reasonable to anticipate—and thus to plan for—increased use of the Internet in future crises, and lessons learned from September 11 indicate some of the issues that deserve attention.

On the one hand, it is clear that in the immediate aftermath of a disaster, people will typically turn on television sets (to get news) and call family and friends on the telephone (to convey news, report on their status, or supplement television news with information of a more personal nature); they tend not to use the Internet. The data from September 11 show that this pattern held on that day; even heavy Internet users went first to the television and the telephone.

On the other hand, it is also clear that if the television or telephone were unavailable or failed to provide the information people needed, they turned to the Internet even if they normally were not heavy Internet users. For instance, it appears that much of the surge in demand at online news sites on the morning of September 11 came from people who did not have access to television sets at their workplace. People also appear to have used the Internet to supplement information available from other sources, as evidenced by marked shifts in topics searched on the Internet. These behaviors suggest that disaster planning should include examination of how the Internet might be used to disseminate information in a future crisis.

The experiences of September 11 also indicate the value of efficient Internet or Internet-style data communication in a disaster. These alternatives, such as text messaging and e-mail, make more efficient use of limited communications capacity than do other services. By midday on September 11, the cellular-phone networks in Manhattan were severely congested, yet there are reports that people who used their cell phones or wireless-equipped PDAs to send instant messages were able to communicate effectively. E-mail and instant messages were also used as a substitute for telephone calls.

Although better communication over the Internet could simply have been the result of the relative overprovisioning of the Internet-related communication infrastructure, there are several fundamental reasons why, for example, using a PDA to send a short text message such as “I’m OK and am walking home” is far more efficient and more likely to succeed than would a cell-phone call when the network is congested. First, the Internet degrades under load more gracefully than does the voice network. If sufficient capacity is not available, the cell-phone network will not permit new calls to be set up. In contrast, the Internet makes use of mechanisms that continue to accept new messages but reduce transmission rates when the network is congested. Also, by virtue of their flexible design, Internet-style communications lend themselves to human actions that reduce the load—whether by substituting a data-intensive voice call with a brief text message or by removing data-intensive graphics from a Web page (as CNN did in the face of high loads). A lesson here is that organizations responsible for disaster planning should encourage awareness of this more efficient way to communicate.