7

9/11: The *Cyber*-terrorist Attack

> *If it's a major cyber-event, it's going to have a physical tail. If it's a major physical event, it's going to have a cyber-tail. And as a result you can't separate physical from cyber.*[1]
>
> —*Brenton Greene*
> *Deputy manager, National Communications System*

> *The great uncertainty of all data in War is a peculiar difficulty, because all action must, to a certain extent, be planned in a mere twilight, which like the effect of a fog or moonshine, gives to things exaggerated dimensions and an unnatural appearance.*
>
> —*General Carl von Clausewitz*
> *On War, 1832*

It was 8 o'clock in the morning on what was shaping up to be a sun-drenched, breezy, and cheerful day in September when Brenton Greene sat down in a secure facility outside of Washington, D.C., for a classified briefing from the CIA. A 25-year veteran of the Navy's submarine force, the so-called "silent service," his career had taken him from the helm of the USS Skipjack and USS Hyman G. Rickover, both

[1] Author interview, October 29, 2002.

nuclear attack submarines, to service as a civilian member of the President's Commission on Critical Infrastructure Protection. The former sub commander was used to classified briefings and operating in the shadows, far behind the newspaper headlines and away from the television cameras. But this briefing promised to be different from any other he had taken part in. And Greene's relaxed, contemplative demeanor belied his true interest in what the CIA had to say.

He had been in his latest job for only six months. But as the deputy manager of the National Communications System (NCS), a relatively small agency established by President John F. Kennedy to ensure the uninterrupted availability of critical communications networks during times of national crisis, Greene's role in the meeting was crucial. But he wasn't alone. With him were representatives from seven other federal agencies and more than 40 technology and communications companies that own and operate many of the nation's most critical communications networks.

Once the briefing started, the CIA representatives began to outline what everybody in the room already knew in a general sense: that the international terrorist threat to the U.S. telecommunications infrastructure was real and growing more serious every day. But the CIA officers quickly captured the attention of their audience as they began to delve deeper into one of the first intelligence threat assessments to deal with the issues of cybersecurity and cyber-terrorism. Despite the obvious vulnerabilities to the nation's most critical systems and infrastructures from information warfare and cyber-terrorism, the CIA had only recently completed its estimate—five years after principle members of the National Security Telecommunications Advisory Council (NSTAC) forwarded a memorandum to President Bill Clinton that stated: "[the] integrity of the Nation's information systems, both government and public, are increasingly at risk to intrusion and attack. . .other national infrastructures. . .[such as] finance, air traffic control, power, etc., also depend on reliable and secure information systems, and could be at risk."[2] More importantly, the current sense of urgency, if there was one, was due in large part to Pennsylvania Republican

[2] "Information Sharing for Critical Infrastructure Protection," *Task Force Report of the President's National Security Telecommunications Advisory Council* (June 2001).

Curt Weldon, chairman of the Research and Development Subcommittee of the powerful House Armed Services Committee. During a hearing on March 8, 2000, Weldon harshly criticized the CIA for not yet having produced a National Intelligence Estimate (NIE) covering cyber-war and cyber-terrorism threats to the U.S. Much of Weldon's wrath also fell upon the shoulders of Clinton for failing to adequately address the issue of cybersecurity and critical infrastructure protection in his State of the Union address that year. "If this isn't the state of the union, I don't know what is," Weldon had said.[3]

The CIA and other participants at the NCS briefing agreed that although a strategic cyber-attack on U.S. critical infrastructures had not yet occurred, there was a growing body of evidence relating to the increased sophistication in information warfare (IW) capabilities of foreign nations. Many countries thought by the CIA to be developing IW programs considered cyber-attacks against public and private computer systems in the United States to be the kind of asymmetric warfare option they would need to level the playing field during a conventional military conflict with the U.S. In addition, the agency had previously warned that an attack would likely cut across the public and private sectors and civilian and military domains.

As the briefing continued, the conversation between the meeting participants began to take form. Such an attack would likely involve a major disruption of key telecommunications infrastructures serving other sectors of the economy, including banking and finance, electric power, and air traffic control.

"Everything runs on telecom," recalled Brenton Greene.[4] "If it's a major cyber-event, it's going to have a physical tail. If it's a major physical event, it's going to have a cyber-tail. And as a result you can't separate physical from cyber."

[3] Author present at Hearing of the House Armed Services Committee, Research and Development Subcommittee, Rayburn House Office Building, March 8, 2000. Weldon's remarks were in part driven by recent events, including the February 2000 denial of service attacks against some of the biggest e-commerce companies on the Internet that would later be attributed to a 14-year-old Canadian hacker nicknamed "Mafiaboy."

[4] Author interview.

As such, major disruptions could have a strategic economic impact on the U.S., including possible loss of public confidence in the delivery of services from those infrastructures. And the list of potential adversaries that could employ physical or electronic attacks against critical infrastructures was growing longer every day. Foreign governments, for example, continued to pose a serious and structured threat because of their access to sophisticated technology as well as intelligence support, funding, and organized cadres of professional technologists.

But terrorist organizations were also becoming more aware of the targeting potential offered by the telecommunications infrastructure, according to the CIA. And this was a lesson that had not been lost on the members of the NCS. Drawing on previous CIA testimony, the NCS had come into this meeting with the following analysis already having been conducted:

> *The global dependence on interconnected computers and the vulnerabilities thereof fostered the emergence of cyberterrorism. Furthermore, the manner in which terrorist groups have evolved renders them especially suited to using the Internet to achieve their goals. Many terrorist groups have undergone a transformation from strictly hierarchical organizations with designated leaders to affiliations of loosely interconnected, semi-independent cells that have no single commanding hierarchy, like Hamas and the bin Laden organization. Through the use of the Internet, loosely interconnected groups without clearly designated leaders are able to maintain contact and communication.*
>
> *Many terrorist groups are just becoming aware of the advantages that IT can deliver. As individuals within these groups become better at employing IT, they may become more aware of the potential damage that can be caused using this technology. Additionally, publicity is one of the primary requirements for a successful terrorist attack. Extensive coverage has been given to the vulnerability of the U.S. information infrastructure and to the potential harm that could be caused by a cyberterrorist attack. This may lead terrorists to feel that a cyber attack directed at the U.S. may garner considerable publicity. Terrorist groups may also feel that even an unsuccessful attack against the U.S. information infrastructure could gain tremendous publicity. It is possible*

> *that the publicity given to the potential of cyberterrorism could become a self-fulfilling prophecy. This will require an unprecedented degree of collaboration and cooperation between industry and government.*[5]

Despite years of foot-dragging by the Clinton administration to direct the intelligence community to develop a cybersecurity threat assessment, the composition of the NCS briefing audience was a testament to the commitment of career government employees to build and maintain that "unprecedented" partnership with the private sector. All of the representatives from the private sector were senior executives from their respective com panies, and all had government security clearances that granted them access to the most sensitive intelligence data pertaining to threats to the infrastructures that formed not only the lifelines of their businesses but the lifelines of the nation as well.

At approximately 8:46 A.M., Navy Captain J. Katherine Burton quietly entered the briefing room and walked calmly to where Greene was sitting. She leaned over his shoulder and whispered in his ear that an airplane had just crashed into the north tower of the World Trade Center in New York.

"We weren't sure yet if it was a Piper Cub, a 737, or what," recalled Greene.[6] With no other information to go on and no indications that this was anything more than a horrible accident, Greene calmly informed the other briefing participants in the room of the news and ordered the briefing to continue. For now, September 11 was simply another day and the accident in New York simply that—an accident.

In Washington, however, where Richard Clarke, Former National Coordinator for Infrastructure Protection and Counterterrorism at the National Security Council, had been giving a speech on the importance of cybersecurity, the world had already changed. Unable to get through his speech due to the incessant signaling of his pager, Clarke cut his presentation short and called back to his staff at the Old Executive Office Building adjacent to the White House to see what the emergency was. It was then that he was told a plane had crashed into the World Trade Center in New York.

[5] "The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications" (Office of the Manager, National Communications System, December 2000), pp. 28–31.

[6] Author interview.

Clarke rushed back to the White House. His first stop was to see Condoleezza Rice, the president's National Security Advisor, in her corner office of the West Wing. But Rice was already down the hall conferring with Vice President Dick Cheney. Clarke, knowing already that the plane crash was no accident, proceeded down the hall and interrupted the meeting between the vice president and Rice. "They asked me 'what do you think,' and I said immediately that it was a terrorist attack," recalled Clarke.[7] "Planes don't fly into the World Trade Center, I said."

There were few people in government at that time more qualified to make that call. A career government national security expert, Clarke had advised two former presidents on the threat of terrorism on U.S. soil. Educated at the Boston Latin School, the University of Pennsylvania, and the Massachusetts Institute of Technology, Clarke had spent his entire career focused on national security issues before becoming the nation's first counterterrorism chief under President Bill Clinton. He had even spent the better part of New Year's Eve 2000 locked away in a classified communications center watching for indications and warnings of pending terrorist attacks by Osama bin Laden's al-Qaeda terrorist organization. And while nothing happened that night to derail America's New Year celebration, Clarke had no doubt on the morning of September 11 who was behind the crashing of a jetliner into the World Trade Center.

Before a decision could be made on how to proceed, the Secret Service rushed in and told the vice president that he and Condoleezza Rice needed to be moved immediately to the East Wing bomb shelter, known as the Presidential Emergency Operations Center, or PEOC. Clarke then recommended that he remain behind in the West Wing and convene a secure video teleconference between all of the members of the president's cabinet and begin the process of coordinating the crisis response from the White House. He would maintain a direct secure telephone link with the vice president at all times.

Within minutes, the faces of the president's national security team, including Secretary of Defense Donald H. Rumsfeld, CIA director George J. Tenet, FBI director Robert Mueller, Attorney General John Ashcroft, and various

[7] Author interview.

others, appeared on the video screens of the secure teleconferencing system. The FAA informed Clarke that they thought there were multiple hijackings taking place. When asked how many, the FAA representative said as many as 10 or 11. It was then that the White House ordered the FAA to get every plane they could on the ground as fast as possible.

At the NCS briefing, the CIA managed to get through 17 more minutes of material when word reached the briefing room that a second aircraft had sliced through the south tower of the World Trade Center. It was exactly 9:03 A.M. Officials turned to the televisions, where CNN was showing live footage of the unfolding horror.

"It was clear then that there was some threat," recalled Greene. "When the second plane hit, I said, 'I'm leaving. I need to go look at the implications of this.'"

-.-. -.-- -... . .-. - . .-. .-. --- .-.

One of the first things that all U.S. military officers are taught is to accept the inevitability of the "fog of war," a phrase that refers to the uncertainty and confusion that often arises in the heat of battle as a result of a commander lacking adequate information about the enemy and terrain, or receiving faulty intelligence. More importantly, however, is the emphasis that U.S. military officer training courses place on being able to operate effectively and decisively under such circumstances. And on September 11, 2001, that training would be put to the test in America's own backyard.

On the fifth floor Strategic Information and Operations Center at the FBI's headquarters facility in Washington, D.C., Ron Dick, former director of the FBI's National Infrastructure Protection Center and a 24-year veteran of the FBI, began the process of setting up a 24-hour Cyber-Crisis Action Team (C-CAT) that would be responsible for not only helping Brenton Greene's physical recovery effort in New York but also monitoring the Internet infrastructure for signs of a follow-on cyber-attack that might target additional sectors of the economy. "There were a lot of unknowns," recalled Dick.[8]

[8] Author interview.

For the NIPC, September 11 and the days that followed would be a defining moment, more so than any other previous incident involving strictly Internet security. The NIPC had many enemies on Capitol Hill who believed that a law-enforcement agency such as the FBI was incapable of shifting its focus from prosecution to prevention. Prior to September 11, those critics had pointed repeatedly to studies by the General Accounting Office, the investigative arm of Congress, which routinely criticized the NIPC for failing to do its job—infrastructure threat detection, analysis, and warning—as if the NIPC were the only agency tasked to carry out such a mission.

The truth of the matter was that the NIPC was only one of many agencies and private-sector organizations that had a role to play in cybersecurity. And many of the shortcomings cited in the various GAO reports were shortcomings that could be fixed only by senior administration officials. Others were things the NIPC was never intended to do in the first place.

For example, a lack of timely warnings about viruses and other potentially dangerous security incidents was one of the main deficiencies routinely cited by the GAO. Some of the more than 80 warnings issued by the NIPC between 1998 and 2001 were issued in time to prevent widespread damage, but most, particularly those related to viruses, often came after the fact, said the GAO. In interviews, Dick often fought back in defense of his fledgling agency, stating vehemently, "You don't want the NIPC solely in the virus-warning business. There are plenty of other organizations that do that, including dozens of anti-virus companies."

The GAO also criticized the agency for its inability to conduct strategic analysis of threats to the critical infrastructure, a lack of staffing and expertise, and an inability to share information with the national security community that stemmed from its predisposition to treat everything as a law-enforcement investigation. But Dick would find an ally in Clarke, who repeatedly directed attention away from the NIPC's minor shortcomings and toward the true crux of the matter, which was the existence of multiple "stovepipes" in the federal government and the private sector. Although there is "a series of rich deposits" of data on vulnerabilities and threats, there is "very little capability to do data mining across the public/

private gap," Clarke had said publicly. "The expertise lies far more outside the government than in."

None of those issues, however, stopped the NIPC from responding to the catastrophic events of September 11 in a timely and aggressive manner. The NIPC's Cyber-Crisis Action Team began immediately to put together and activate contingency plans and information-sharing mechanisms with dozens of other federal, state, local, and private-sector organizations that could be put into action in the event of a major follow-on cyber-attack. And although that attack would not materialize during the immediate aftermath of the initial attacks in New York and at the Pentagon, the teams became a critical asset in the analytical effort to understand the infrastructure interdependencies and damages caused by the collapse of the World Trade Center towers. "We began to use the Cyber Crisis Action Team in coordination with the Special Technologies and Applications Unit to store and mine tremendous amounts of data to determine who may or may not have been in the buildings or on the flights that crashed, if there were other terrorists who were poised to strike, and a host of other normal investigative procedures," recalled Dick. Within two weeks of the attacks, the NIPC's C-CAT would be able to provide detailed briefings to the president and the vice president about how the terrorist cells used technology to carry out their murderous activities.

While Greene was rushing back to the NCS operations center to get a better understanding of what had happened in New York, civilian and military officials were boarding a militarized version of a Boeing 747, known as the E-4B National Airborne Operations Center (NAOC), at an airfield outside of the nation's capital. They were preparing to conduct a previously scheduled Defense Department exercise.

There are four E-4Bs, code-named "Night Watch," in the U.S. military arsenal. They exist to provide the president, vice president, and Joint Chiefs of Staff with an airborne command center that can be used to execute war plans and coordinate other emergency government operations in the event of a national emergency or destruction of ground command and control centers. As a result, they are often referred to unofficially as "the doomsday planes." One E-4B remains on alert at all times.

As the crew of the E-4B was preparing to begin the regularly scheduled training exercise, including the use and testing of the aircraft's various advanced technology and communications equipment, the Federal Aviation Administration was ordering all New York City area airports to cease flight operations. Minutes later, the Port Authority of New York and New Jersey ordered all bridges and tunnels in the New York area closed. The fog of war was thick and officials were left wondering if other airplanes were about to come careening out of the haze like jet-powered artillery shells.

President George W. Bush, who had been speaking to second graders at the Emma E. Booker Elementary School in Sarasota, Florida, was notified immediately of the unfolding crisis. At 9:30, Bush informed his audience and the nation that America had become a victim of "an apparent terrorist attack." Ten minutes later, the FAA ordered a historic nationwide grounding of all air traffic. It was clear to many officials, however, that the crisis was far from over. And that fact was driven home at 9:43, when American Airlines Flight 77 plowed through the thick concrete walls of the Pentagon.

There were thousands of airplanes still in the air and heading toward airports all over the country. And one of them, a 747 code-named "Night Watch," had only just taken off and was immediately ordered to cease the military exercise it was conducting and prepare to become the actual national airborne operations center. America was under attack.

-.-. -.-- -... . .-. - . .-. .-. --- .-.

As the president was being whisked off to a secure command and control facility at Offutt Air Force Base in Nebraska, the White House began an evacuation of all nonessential personnel. Specific concerns had been relayed by the intelligence community about the potential targeting of the White House and the Capitol building. It was an apparent effort to decapitate the government and sow mass confusion.

Clarke, acting on direct orders from the president and vice president, then initiated the emergency continuity of the government plan, which called for all federal departments to relocate to alternate sites and for the Speaker of the House of Representatives to be moved to a secure location outside of Washington. Although the secretary of defense remained at the

Pentagon, Paul Wolfowitz, the deputy secretary of defense, was moved to an alternate military command and control center. Shortly thereafter, all ports and border crossings were ordered closed, and all available military fighter aircraft were launched.

For Clarke, most of the morning was spent ensuring that all of the various orders relating to the emergency action plan were being carried out. Members of Clarke's staff would remain in close contact with the FBI's National Infrastructure Protection Center. Meanwhile, as the public watched the horrible human tragedy unfold live on television, Clarke, Dick, and their respective staffs were forced to deal with another possibility: that the morning's attacks could be one phase of a multipronged assault that could include attacks against the digital infrastructure of the U.S. economy. If that was the case, then they were staring at the one scenario that had often kept them awake at night.

Across town at the NIPC, Dick summoned his key advisors into an emergency meeting to analyze all available cyber-intelligence. Among those Dick relied on for expert advice were Bob Gerber, a career CIA officer who had been detailed to the NIPC to serve as the agency's chief of analysis and warning; Navy rear admiral James Plehal, who served as Dick's deputy and was a key link to the Defense Department establishment; and Les Wiser, the FBI agent responsible for tracking down CIA spy Aldrich Ames. A major cyber-attack now would prove absolutely devastating to the rescue and recovery effort and would almost certainly amplify the sense of fear and uncertainty far away from the epicenter of the main attack in New York. Such an assault had to be stopped at all costs.

But with the crash of hijacked American Airlines Flight 93 in Pennsylvania, the fog of war had settled firmly over official Washington. Despite the billions of dollars invested every year in advanced information technology designed to provide key government and military decision-makers with what is known in military parlance as "situation awareness," the fog of September 11 proved too thick to see through. America's national security community was thrown off-balance and had lost (in fact, may never have had) the initiative. What should have been an offensive war of maneuver had quickly turned into a reactive war fought from trenches and hardened bunkers.

-.-. -.-- -... . .-. - . .-. .-. --- .-.

September 11 was far from over when a small cadre of highly respected national security experts began warning of the potential for the physical attacks to be followed by cyber-attacks.

Marv Langston, the former deputy CIO at the Defense Department, characterized the events during an interview with *Computerworld* magazine as an act of war and said the country needed to be on alert for what he described as an "electronic Pearl Harbor."[9] Likewise, retired Air Force Lt. General Al Edmonds, who at one time headed the Defense Information Systems Agency, said he feared a cyber-attack could be next and added that such an event would be "absolutely paralyzing."[10]

Meanwhile, Atlanta-based Internet Security Systems, Inc. (ISS), which operates the IT industry's Information Sharing and Analysis Center (ISAC), placed its operations center on what it called AlertCon 3 (the highest is AlertCon 4), "in order to focus IT security efforts on the potential for (and defense against) an Internet component to these attacks." The IT-ISAC was one of several ISACs established in cooperation with the FBI and the NIPC to share information between the government and the private sector about cyber-threats.

In a threat assessment issued to the private sector members of the ISAC, ISS stated, "This is a time to partner all security assets on what is most important to your enterprise. While physical security concerns are paramount, it is essential to keep some eyes on the networks focused on malicious activity. We can expect a significant increase in disaster-recovery activity—plans being activated, dusted off, etc. No doubt the [disaster-recovery] industry will be sorely stressed at this point, and it would behoove staffs to consider security as a move to alternate sites is contemplated or enacted."[11]

At FBI headquarters, the NIPC began what Dick characterized as "harvesting" physical threat information pertaining to critical infrastructures

[9] See Dan Verton and Bob Brewin, "Companies Warned about Possible Cyberattacks," *Computerworld,* September 11, 2001.

[10] Ibid.

[11] Ibid.

and pushing that data out to thousands of private-sector companies that owned and operated those facilities, such as power plants, telecommunications facilities, water companies, and financial institutions. Dick relied on the FBI's InfraGard program and the various private-sector-run Information Sharing and Analysis Centers for much of that outreach effort. On September 11, ISACs had already been established in the Financial Services sector, the Electric Power sector, the Telecommunications sector, the Information Technology industry, and the computer software anti-virus industry. In addition, the NIPC would set in motion a daily threat briefing schedule for the Water sector, the Oil and Gas sector, and the Aviation and Railroad sectors.

Accurate and timely information was the only thing that could cut through the fog of war. And the government was doing everything it could to get that information flowing to the right people at the right time.

-.-. -.-- -... . .-. - . .-. .-. --- .-.

In the blink of an eye, the situation in New York went from horrible to unthinkable. Within 23 minutes of each other, the south and north towers of the World Trade Center collapsed, sending one million tons of concrete and steel crashing down on the city streets below, crushing the stuff of life into thin air. The scene was enough to take a person's breath away, like a punch to the stomach from a heavyweight boxer. But for Brenton Greene at the National Communications System operations center, it was immediately obvious that the series of murderous tragedies had now become a massive regional communications disaster extending from New York to the nation's capital.

When the last of the rubble fell to earth, the silence was deafening. Sound was muffled from the thick layer of dust and ash that blanketed the city like a snow. The face of lower Manhattan had changed. Through the grayness it appeared more like Stalingrad in 1943 or Berlin at the end of World War II. But the eerie silence, the gray of the fog of war, and the unnatural stillness of human life within the "red zone" concealed the massive digital disruption that had already begun to eat away at the nation's economic arteries and would only get worse as the day wore on. Lower Manhattan was not only the site of the worst terrorist attack in human history, it was also home to one of the most critical communications facilities in the nation. And that also made it the site of the worst cyber-terrorist attack in history.

The massive brick building located at 140 West Street, across the street from the World Trade Center and directly adjacent to #7 World Trade office complex, was built in the 1920s by the New York Telephone Company. It was known for its "exterior ornamental motifs, veined marble walls, travertine floors with bronze medallions, and a vaulted ceiling embellished with murals depicting the stages in the evolution of human communication."[12] On September 11, however, the building's more than 1,700 occupants knew it as the main regional switching station of Verizon Communications and the digital heartbeat of the nation's economy on Wall Street. The computers and switching equipment inside the facility were responsible for managing billions of bits of electronic data and tens of millions of telephone calls every day. And that was on a normal day.

With the disintegration of the two World Trade Center towers and the collapse of #7 World Trade later that afternoon, that digital heartbeat began to flat-line. Verizon's call volume reached twice the normal daily rate of 115 million calls in New York City and 35 million calls in the Washington, D.C., area. And although it remained operational, the wireless network experienced massive congestion that prevented most calls from getting through. During the peak of the chaos, Verizon experienced nearly 100 percent more traffic than normal on its nationwide wireless network. There were as many as ten wireless cell sites in New York City that were not operating, including those that were located at the top of the north tower of the World Trade Center. In addition, the infrastructure that connected the sites to the landline network went through the basement of the World Trade Center.

"We knew the damage was absolutely major," recalled Brenton Greene. "In the basement of No. 2 World Trade Center, there were two central office switches. You could characterize the World Trade Center buildings as being like two cities, and there was a major switch that controlled telecom-

[12] From New York City Landmarks Preservation Committee. Also known as the Barclay-Vessey Building, 140 West Street, it was designed by architect Ralph Walker and erected between 1923 and 1927.

munications for each of the buildings, and both of them were in the basement of No. 2 World Trade Center. And they just went away," he said. "We knew there would be a major impact, but the degree of the impact was not yet known."

In Washington, D.C., the impact was becoming clearer by the minute. Lack of interoperability between the communications equipment of the various agencies assisting in the search and rescue effort at the Pentagon forced officials to raid a local warehouse and commandeer radios for emergency workers. In addition, telephone and wireless cellular service in and around the nation's capitol remained unavailable to civilian users for most of the day. But there was one very important user who felt the impact of the massive communications loss several thousand miles away.

Secretary of State Colin Powell was in Lima, Peru, attending a meeting of the Organization of American States when he received word of the attacks. He immediately cut his trip short and boarded a government aircraft for the seven-hour flight back to Washington. The former chairman of the Joint Chiefs of Staff understood and appreciated the advantage the U.S. enjoyed over most nations when it came to the advanced electronics and communications capabilities. The former Army General had put his name on various Pentagon war-fighting manuals that outlined the Department's commitment to what the military called "network-centric warfare" and "information superiority." He had even written an article in *Byte Magazine* in 1992 titled "Personal Computer Technology May Determine the Outcome of Future Conflicts." But what really made Powell's experience on September 11 unique was his understanding and continued devotion to the military's decision cycle, known as the *OODA loop.* OODA is an acronym for the cycle of Observation, Orientation, Decision, and Action. For Powell, it was absolutely critical that he be inside of his counterpart's or enemy's loop. But on September 11, Powell got a taste of what communications must have been like for his early nineteenth-century counterparts.

"I never felt more useless in my life than on the morning of the 11th of September," Powell told members of the National Security Telecommunications Advisory Committee (NSTAC) during a meeting held at the State Department on March 13, 2002.[13] For most of the seven-hour return flight, Powell was unable to communicate with other senior government leaders in Washington. "Phones [were] gone because of what happened here and what happened to the [communications] system here in Washington," he said. "They couldn't get a phone line through. I was able to get some radio communications—two radio spots on the way back—but for most of that seven-hour period, I could not tell what was going on here in my capital, and I'm the Secretary of State."[14]

The implications of the communications failure on September 11 went beyond the seven-hour window during which Powell was unable to communicate with Washington. For Powell, this meant that there was the chance he and his Department could be severed from the world again in the future, removing the initiative from America's diplomatic and foreign policy efforts around the world. "Power to me now, as Secretary of State, is to be inside of everybody else's information loop or decision loop," he told the group of telecommunications experts. "I had called the President of Pakistan last Friday [March 8] to talk some business and just as I was concluding I said 'I'm sorry to hear about the deaths that occurred in Karachi today.' And he said, 'what deaths?' I'm inside his information loop."[15]

Powell was not alone in his distress. The National Airborne Operations Center that had converted literally on the fly from exercise status to real-world crisis management also had its share of trouble deciphering what was happening around the nation. Although the details are not known, a classified after-action report was produced that, according to one official who was on board the aircraft on September 11, does not paint a favorable picture of the government's overall crisis management capa-

[13] Steve Barrett, "Powell Asks NSTAC to Keep Nation Inside the Information Loop," *Telecom News*, Issue 1, 2002, p. 4.

[14] Ibid., p. 5.

[15] Ibid., p. 4.

bilities.[16] According to one government official, the nation was "deaf, dumb, and blind" for much of that horrible day in September.[17]

Back in Arlington, Virginia, Brenton Greene and the NCS staff began preparing for 24-hour operations—a state they remain in as of this writing. As afternoon turned to evening, officials began to piece together the true nature of the digital devastation in and around New York City and the Pentagon. In short, the destruction amounted to "the most significant challenge that the National Communications System had ever seen," recalled Greene.

In addition to the immediate wireless circuit overload, the collapse of the towers sent a massive steel beam slicing through a bundle of critical fiber-optic communications cables buried eight feet below the streets of Manhattan. The hulk of steel destroyed more than four million high-speed access lines and ruptured water lines that filled underground switching vaults with more than ten million gallons of water. As many as 300,000 voice telephone lines and 139 fiber rings in surrounding buildings and 26 building-specific fiber rings also failed as a result of the physical devastation. The damage also knocked out 1.5 million circuits that served the financial district, threatening the country's economic stability with each passing minute. The loss of connectivity to Wall Street was so severe that President Bush would soon establish three top priorities and communicate them personally to the NCS managers: rescue, recovery, and getting Wall Street back online.

The collapse of the towers had knocked out all primary power for much of lower Manhattan, and backup power, which was running on diesel fuel generators, began to fade quickly. Emergency responders and corporate disaster recovery specialists had failed to anticipate the physical impediments to getting fuel and spare parts onto Manhattan Island, which was now essentially surrounded by a blockade of bridge and tunnel police officers and military personnel at sea and in the air. Complicating matters was the fact that air transportation was no longer an option. Therefore, getting

[16] Author interview with sources either aboard the NAOC or familiar with the events of September 11.

[17] Ibid.

fuel delivered to keep the back-up power generators running was delayed due to the significant preplanning that was required to pass through security. In fact, security precautions and lack of planning denied Verizon officials timely access to their own facilities at the disaster site. Other telecommunications companies who had pledged support to the restoration effort had been completely denied entry into the disaster site and would only be able to get through using Verizon identification badges. Those delays had a direct impact on the time it took to restore services to the financial district.[18]

The electronic damage also extended to the transportation industry, cutting the electronic circuits that fed data to the tollbooths on the various bridges in the New York Area. When the first jetliner struck the north tower of the World Trade Center, it destroyed the Port Authority of New York and New Jersey headquarters facility, which housed 2,000 staffers and the central host servers for the E-ZPass electronic toll collection system. It would take a team of 15 engineers to recover the toll system, helping to ensure the flow of traffic, including emergency vehicles, into and out of Manhattan. When the towers collapsed, 75 Port Authority workers were among the more than 2,800 who perished.

Despite these difficulties, Greene was amazed at the sense of community and patriotism that had taken hold throughout the various private companies that only a day earlier considered each other ruthless competitors. Lucent Technologies, Inc., in Murray Hill, New Jersey, one of Verizon's main systems providers, rushed a 100,000-line switch to the scene to replace another massive switch that had been sent crashing through the window of the Verizon building at 140 West Street. The company also put all of its customer requirements on hold and made its entire inventory available to rescue services.

"Companies that were competitors with each other were all bending over backwards to help each other," recalled Greene. "There was a clear recognition of the urgent need to get our economic machine—Wall Street—back online."

[18] Steve Barrett, "NSTAC Chair Recaps Committee's Recent Accomplishments at March Meeting," *Telecom News,* Issue 1, 2002, p. 5.

Although the attacks had not caused any major disruptions in the military's command and control capabilities, the attack at the Pentagon also caused widespread damage to a host of highly sensitive computer networks and communications capabilities. Offices and facilities destroyed in the Pentagon attack included the U.S. Navy's Telecommunications Operations Center, sensitive chief of naval operations offices, and help desk operations within the U.S. Army's Information Management Support Center. Personnel, including telecommunications specialists and intelligence analysts assigned to those areas, were also among the casualties.

At the Pentagon, emergency orders were quickly put together for new secure communications equipment and computers. One such order involved more than 1,000 proprietary Secured Desktop Gateway communication enclosures to secure information stored on Pentagon workstations that had been set up temporarily in unclassified office locations away from the destruction. Pentagon officials were forced to establish a makeshift sensitive compartmented information facility (SCIF) to handle top-secret data securely. The delivery of the security equipment took two weeks to complete.

Although the Navy and the Defense Department refused to acknowledge any loss of communications capability as a result of the attack (it is traditional practice and prudent not to inform the enemy of your own losses or lack of capability), a former Navy intelligence officer who spoke on condition of anonymity said the location of the crash caused significant damage to many top-secret network operations within the Department of the Navy. The National Military Command Center was also filled with smoke. But the loss of the Navy offices and networks had little or no impact on the Navy's ability to communicate intelligence or orders to Navy warships at sea.

At the FAA and at airport control towers across the country, the situation was quite different. FAA officials around the country were reliant upon a basic voice teleconferencing link established on the morning of September 11 that the FAA called "an events network" to stay abreast of the situation. The teleconferencing line was and remains as of this writing nothing more than a 24-hour, always-open party line. It would be a year after the attacks before the FAA began providing the Pentagon's North American

Aerospace Defense Command (NORAD) with FAA control systems, specifically radar and voice, to improve military air defense operations in the event of another terrorist hijacking.

Despite the low-tech nature of the FAA's crisis coordination network on the morning of September 11, the agency managed in just three and a half hours to clear the skies over the entire U.S. of more than 4,500 commercial flights. During that time, there were at least 11 "suspect airplanes" that officials feared could have been hijacked; four of those aircraft did, in fact, take part in the attacks. Although the hijackings were not the classic hijackings FAA officials had been trained for and experienced over the years, "the calls to NORAD were timely," remarked an FAA official.[19] "We were all kind of coming to the same conclusion at the same time," the official said.

However, there were at least a few instances where critical information on flight restrictions did not reach its intended audience. While thousands of commercial jetliners were being ordered to land or diverted to airfields in Canada, several civilian general aviation flights took off from civilian airstrips. According to the FAA, either those pilots did not receive the order to cease flight operations or they ignored it.

-.-. -.-- -... . .-. - . .-. .-. --- .-.

As corporate requests for relocation and disaster recovery services began to climb, so did the death toll in the technology industry. The trauma caused by the unspeakable loss of life was compounded further during the restoration effort through the loss of critical expertise. Although no person is defined wholly by his or her profession, the economic attack perpetrated by al-Qaeda on that day extended beyond the digital arteries of corporate America and into the ranks of the personnel that watch over those arteries, which give life to the computers and databases that maintain client information to power the corporate decisions that determine a corporation's placement and direction in the

[19] See Dan Verton, "FAA Moving to Enhance Integration with NORAD," *Computerworld*, August 13, 2002.

market. For the first time, the saying "our people are our most important asset" was more than a slogan. Skilled people with corporate knowledge of systems and databases and business requirements were a critical infrastructure, too. And people had come under direct attack along with the structural symbols of America's economic and military strength.

Among those technology executives that lost their lives in the attacks were: a cofounder and chief technology officer of Akamai Technologies, Inc., in Cambridge, Massachusetts; the chief financial officer of Chatsworth, California-based optical networking company MRV Communications, Inc.; the vice president of market development and interim chief executive officer at ELogic Corporation; the director of business development at ELogic; the CFO of Netegrity, Inc., in Waltham, Massachusetts; the CEO and president as well as the director of development and the director of human resources of BCT Software AG, in Willstaat, Germany; the chief operating officer of Metrocall, Inc., in Alexandria, Virginia; an engineer with BEA Systems, Inc., in Liberty Corner, New Jersey; a director of horizontal scaling with Sun Microsystem's Software Systems Group; a senior mechanical engineer with Raytheon's Electronic Systems division; a senior quality control engineer at Raytheon; a vice president of operations for Raytheon's Electronic Systems; and hundreds from Cantor Fitzgerald financial services. There were many, many others.

By late afternoon on September 11, disaster declarations began pouring in to companies that specialize in helping other firms recover from major catastrophes. One of the largest such firms recorded 62 disaster declarations from 31 companies in the financial service industry. However, the panic and fear had quickly spread to other major cities around the country, such as Boston and Chicago, which have high concentrations of large office buildings. As a result, disaster recovery firms were forced to field multiple requests from companies that were dealing with voluntary building evacuations. Likewise, companies all over the country lost productivity as a result of the psychological impact that the human tragedy had on their workers, many of whom were too upset and distracted to continue working. In other cases, people who normally conducted business downtown in Manhattan's financial district were too afraid to venture into that part of the city for months.[20] It is nearly impossible to quantify the financial impact of such productivity losses. In the end, however, the first few hours after the initial attacks on September 11 surpassed all previous disasters that the business continuity industry had ever dealt with. Hurricane Floyd, for example, in 1999, produced 32 disaster declarations, and the World Trade Center bombing in 1993 led to only 8 disaster declarations.[21]

-.-. -.-- -... . .-. - . .-. .-. --- .-.

On September 12, the fog of war began to lift slowly and then the sun shined. That was also the first full day governed by an advisory issued by the FBI's National Infrastructure Protection Center. According to the advisory, all public- and private-sector members of the FBI's InfraGard program were to beef up physical and cybersecurity to protect against the potential for follow-on attacks, especially cyber-attacks. If a computer system was not absolutely mission-critical to the operation of the business, it should be shut down for the time being, advised the FBI.

"The FBI has no information of any additional specific threats directed against additional targets or critical infrastructures in the United States; however, infrastructure owners and operators should be at a heightened state of alert and should implement appropriate security measures—both physical and cyber," the advisory stated. An advisory is the second-highest alert condition that can be issued by the FBI to members of InfraGard, a joint program between the government and industry designed to share threat information about possible cyber-attacks and cyber-crime.

Lawmakers on Capitol Hill also wasted no time in focusing on the obvious vulnerability of the nation's critical cyber-infrastructure to terrorist attack. At a September 12 hearing of the Senate Governmental Affairs

[20] Several months after the attacks, I gave a speech at a technology user group association in upper Manhattan. The meeting organizer asked for a show of hands of how many people were still too afraid to hold their monthly meetings in their usual location downtown in the financial district. Standing in the front of the room, I looked out at the audience and watched dozens of hands being lifted into the air.

[21] See Carol Sliwa, "IT Disaster Declarations Flooding into Comdisco," *Computerworld*, September 11, 2001.

Committee, Senator Joseph Lieberman (D-Conn.) said, "Our enemies will increasingly strike this mighty nation at places where they believe we are not only dependent but unguarded. That is surely true of cyberspace infrastructure today."[22]

By September 14, officials began to get a glimpse of the financial toll on Wall Street stemming from the digital destruction. Preliminary estimates put the cost of rebuilding or replacing the information technology infrastructure for financial services companies whose offices were destroyed by the attack at anywhere from $3 billion to $5 billion.

The Bank of New York and Cantor Fitzgerald financial services were the stock brokerage companies that suffered the most damage on September 11. Cantor Fitzgerald lost nearly 700 people in the World Trade Center—a catastrophic loss by any estimation. The Bank of New York lost telecommunications connectivity to one of its primary data centers and several other facilities. The Bank of New York's communications failure, however, resulted in a cascading failure effect because that bank not only was responsible for clearing security transactions on behalf of its customers but also facilitated the flow of funds between the Federal Reserve and its member banks. "This telecommunications failure on the part of a single institution was large enough to damage critical components of our marketplace pending recovery," according to analysis by a senior member of NYFIX, Inc.[23]

For Richard Clarke, the digital destruction that severed Wall Street from the world was a nightmare come true. It had been only a month since he had toured the Verizon and stock market facilities and asked questions about the security precautions that were in place to protect such a large concentration of critical communications equipment. "What they told us was that after the 1993 attack against the World Trade Center they had diversified some of their routing capability," recalled Clarke. "We also talked to the stock market [officials] about the need for alternative sites and backup facilities." And while some of the work that was required to protect the heart of the nation's economy from life-threatening palpitations

[22] See Patrick Thibodeau, "Senate Committee Looks into IT Vulnerabilities," *Computerworld*, September 12, 2001.

[23] See Warren Pollock, "The Nation's Stock Brokerage System Must Fortify Itself Against Future Attacks," *The Journal of Homeland Security*, February 2002.

had been completed, it wasn't enough to withstand the devastation of September 11.

Within 18 hours of the attacks, however, Verizon had rerouted more than two million of the four million data lines that had been destroyed. Within two days, the wireless telecommunications industry deployed mobile "cellular on wheels" units that were capable of providing 125 percent of the wireless capacity that had been in the New York metropolitan area before the attacks.

Fortunately for the NCS, the Government Emergency Telecommunications Service, known as GETS, had reached full operational capability one week prior to the attacks. By September 11, 45,000 government officials and emergency workers had received GETS calling cards, granting them priority access to the nation's telecommunications networks. At the height of the chaos, more than 10,000 GETS calls were processed with a success rate greater than 95 percent, allowing key decision makers to communicate. As of this writing, the number of GETS cardholders has increased to more than 65,000. And in addition to government and emergency service personnel, senior officials from private-sector companies that own and operate various critical infrastructures are now among those carrying the cards.

However, the lack of wireless priority access was one of the most glaring shortfalls of the recovery and restoration effort. Although the GETS program had assisted officials who were trying to make emergency calls on the wired telecommunications network, those who were in remote locations and were trying to coordinate emergency and government response efforts using a cell phone were greeted with a busy signal. For Brenton Greene, it was a thorn in his side. Since arriving at the NCS in April 2001, he had been espousing the need for priority wireless services to anybody who would listen. Career NCS staffers had developed the idea for the program years earlier. "It was absolutely vital, but it wasn't funded," recalls Greene. "And it became crystal clear within minutes on 9/11 that we needed wireless priority capability for key decision makers and key first responders."

As of this writing, the NCS now has an initial operating capability for priority wireless access. The agency signed a contract in April 2002 with

VoiceStream Wireless Corporation to provide priority wireless access to the cellular telephone system serving the New York and Washington metropolitan areas. The goal, according to Greene, is to have a full, nationwide priority wireless capability in place by the end of 2003.

One of the most important factors in the recovery effort may have been a program formed by the Federal Communications Commission in 1998 known as the Telecommunications Service Priority Program, or TSP. The TSP program serves as a central database of the nation's most critical telecommunications circuits and infrastructure equipment, such as switches. Prior to the attacks of September 11, more than 40,000 switches were registered in the TSP database. And as it turned out, hundreds of those switches were key telecommunications circuits that supported Wall Street. In the days following the attacks, more than 598 TSP provisioning requests poured into the NCS from 46 different organizations. The ready availability of data on the switches and circuits that had been destroyed, coupled with the superhuman efforts of employees from the telecommunications industry and the government, was a critical factor in the reopening of the financial markets on September 17.

-.-. -.-- -... . .-. - . .-. .-. --- .-.

By September 18, the fog of war had thinned into a thin layer of silver haze that hovered above lower Manhattan. If there was a sense of clarity, however, it was in the extent of the devastation and the human loss, not in the predictions of what might happen next. The fear of the unknown took the form of crop dusters spraying deadly chemicals, biological agents being spread through the mail or through the ventilation system of a large building, or a crude nuclear weapon, known as a dirty bomb, making its way to the shores of the U.S. stowed away inside one of the six million cargo containers that arrive aboard foreign ships from faraway ports every year. Nobody thought that the next major crisis would occur on the Internet and come in the form of a devastating worm.

On the morning of September 18, the world woke up to the Nimda Internet worm, malicious code that can destroy data and has the ability to self-replicate and find its way through the Internet to other vulnerable computers. Nimda, which contained five different malicious payloads, infected all 32-bit Windows systems it encountered, including Windows 98, 2000, Millennium Edition, XP, and NT. It scanned systems for as many as 100 different vulnerabilities and automatically exploited them when found. Within 30 minutes of being discovered, Nimda had become a global problem.

At the White House, Clarke was immediately alarmed. Nobody could tell him who was responsible for the worm, which meant anybody could be responsible, including a nation-state sponsor of terrorism or some other surrogate of Osama bin Laden. Almost immediately, experts were warning that Nimda was spreading faster and more aggressively than any other worm they had ever seen and could easily begin to have an impact on overall Internet performance. Although there was no way to know for sure, this could have been part of the series of follow-up attacks that the national security community had been expecting.

"Nimda was a devastating attack," recalled Clarke, who remained on a 24-hour rotation in the White House Situation Room. "We had been expecting another wave of attacks. We were all still worrying about conventional terrorism. We didn't know if it would be more airplane attacks, truck bombs, chemical or biological or cyber attacks. And suddenly the cybersecurity team came to me and said there was a major worm going through the Internet and it was knocking off major companies."

Initially, the consensus among Clarke's staff of experts was that Nimda could have been related in some way to the September 11 attacks. "We still don't know for sure," he recalled during an interview in his office in December 2002. "But had Nimda happened on September 5, it would have been a big news story. A lot of companies, particularly in the financial world, shut down major pieces of their operations. It destroyed and corrupted databases. It was quite devastating, causing several billion dollars in damage."

It took some companies weeks to completely scrub their systems and networks of Nimda. One frustrated administrator told *Computerworld* that the worm infected "50,000 to 100,000" files in his company's data center. "We are smart people," he said. "This one just won't be stopped."[24]

Whether the Nimda worm was part of the September 11 effort to inflict even greater financial damage to the U.S. economy or simply the work of a crackpot, nuisance virus writer is a question that has yet to be answered as of this writing. Although Richard Clarke has his gut feelings about the worm, he acknowledges that it could have come from anywhere. "There are a lot of different people who can conduct cyber-warfare," he said. "There are countries that are creating cyber-warfare units. There are criminal groups engaging in cyber-crime. There are also some terrorist groups that we know are looking at using cyber-attack tools. But I don't spend a lot of time trying to figure out who's going to be the next attacker," said Clarke.[25]

"Let's assume for the sake of argument that the next cyber-attack is being planned by al-Qaeda. Well, we're trying to get al-Qaeda and we'll probably eventually either eliminate the group or reduce it to a small group that we don't have to worry about," he said. "But that won't end the threat to us from cyberspace. Someone else will come along who can use the vulnerabilities in our infrastructure to attack us. Don't worry about who is going to be the next attacker. You'll find out eventually, and you'll do what you can about them. Instead, worry about the vulnerabilities that are out there. Until we fix the vulnerabilities, we are at risk."[26]

-.-. -.-- -... . .-. - . .-. .-. --- .-.

Regardless of the mode of attack employed by terrorists in the future, September 11 showed how people, infrastructure, and technology are the three primary ingredients of a functioning U.S. economy in the twenty-first century. Remove any one ingredient from the equation, and you cause disruptions that have the ability to ripple across many sectors of the

[24] See Jaikumar Vijayan, "Nimda Needs Harsh Disinfectant," *Computerworld,* September 24, 2001.

[25] Author interview.

[26] Ibid.

economy, eventually having the potential to impact national security or public safety.

Despite these lessons, revealed as they were through the crucible of war on September 11, many in corporate America remain unconvinced. Two months after the attacks, the wounds still wet and raw, a survey of 459 chief information officers at major private companies found that just 53 percent of firms had business continuity plans, and less than half had information technology security awareness and training programs for employees.[27] The private sector remains drunk with denial.

But if the private sector has been operating under the influence, its bartender has been the federal government and its policy of allowing market forces to determine the level of investment in security. In an interview with former Virginia Governor James S. Gilmore III more than a year after the attacks, the former Republican Party chairman said the Bush policy of relying "on private sector willingness to take certain security measures and bear their costs" has had little impact to date on the state of security readiness in the private sector.

"Cyberterrorism is a threat to critical infrastructure," said Gilmore, who is the chairman of the congressionally appointed Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction.[28] "So far, pure public-private partnerships and market forces are not acting to protect the cyber-community," he said. "Our major concern is that there will be a major conventional attack and then they could launch simultaneously a cyber-attack in order to sow panic," said Gilmore. "The essence of guerilla warfare is that they choose the time, place, and method of attack. Cyberterrorism is a clear and present danger."

The terrorist attacks of September 11 clearly demonstrated the interdependencies that exist between physical and cyber-infrastructures and how the destruction or degradation of one can have catastrophic consequences for the other. And in the days and weeks that followed, Osama bin Laden praised the attacks not only for the human losses they inflicted, but also for

[27] See Dan Verton, "Disaster Recovery Planning Still Lags," *Computerworld*, April 1, 2002.

[28] Author interview.

the economic impact that the destruction had on American companies and the financial markets.

"They used to be interested in killing as many people as possible," said Clarke, referring to the changes taking place in the strategic focus of international terrorism. "They talked about creating a Hiroshima-like event. I think that was September 11," he said. "But then if you look at the messages from bin Laden after September 11, he starts talking about destroying the American economy. He refers to the glorious events of September 11 costing the Americans a trillion dollars. You could employ a lot of truck bombs and not really do much damage to the economic infrastructure of the U.S., because it is so diverse. But if you attack in cyberspace, you have a chance to hit the entire network, the entire financial services network, for example. Through physical attacks, that takes a lot of people and a major support network. And we would stand a pretty good chance of noticing. But with cyber-attacks you never even have to enter the United States."

Howard Schmidt, Clarke's deputy in the White House and the former chief security officer at Microsoft Corporation, agreed but added that in his mind the days are gone when cybersecurity and physical security could be approached separately. "There's a cyber-dimension to the physical, and there's a physical dimension to the cyber," said Schmidt.[29] "I don't think we can function in isolation in either one of these areas. At the same time a physical event occurs, if there's some disruption in the cyber-world, it could be a lot more problematic than just one or the other."

[29] Author interview.