Unclassified

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

AD-A208 668

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE *(and Subtitle)* Terrorism and the Communication Utilities		5. TYPE OF REPORT & PERIOD COVERED Final
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Linwood G. Greene, Jr.		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS U.S. Army War College Carlisle Barracks, PA 17013-5050		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS U.S. Army War College Carlisle Barracks, PA 17013-5050		12. REPORT DATE 23 February 1989
		13. NUMBER OF PAGES 25
14. MONITORING AGENCY NAME & ADDRESS*(if different from Controlling Office)*		15. SECURITY CLASS. *(of this report)* Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for public release; distribution is unlimited

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

Summary of three communications disasters and the current terrorist threat.

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

Communication disasters
Terrorist capabilities
Concern for domestic terrorist threat

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

Increasing international terrorist incidents, with Americans as the focal point, and the seemingly changing image of the Soviet Union could create an atmosphere conducive to domestic terrorism within the United States. This paper will explore the potential capabilities of terrorist groups. Then it will examine three past communication disasters in an attempt to determine if terrorism is a domestic threat, or specifically if the loss of a major communication facility is a threat to national security. Each disaster happened

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

Unclassified

independently of the others. This study takes the results of these accidents and postulates the effects of similar levels of damage caused by a concerted terrorist action. Analysis of pre- and post responses provides a foundation for recommendations for dealing with the terrorist threat.

USAWC MILITARY STUDIES PROGRAM PAPER

TERRORISM AND THE COMMUNICATION UTILITIES- A NATIONAL SECURITY CONCERN?

AN INDIVIDUAL STUDY PROJECT
INTENDED FOR PUBLICATION

by

Lieutenant Colonel Linwood G. Greene Jr.(Author)

Mr. James E. Trinnaman
Project Advisor

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013
23 February 1989

ABSTRACT

AUTHOR: Linwood G. Greene Jr., LTC, TC

TITLE: Terrorism and the Communication Utilities-A National Security Concern?

FORMAT: Individual Study Intended for Publication

DATE: 23 February 1989 PAGES: 22 CLASSIFICATION: Unclassified

Increasing international terrorist incidents, with Americans as the focal point, and the seemingly changing image of the Soviet Union could create an atmosphere conducive to domestic terrorism within the United States. This paper will explore the potential capabilities of terrorist groups. Then it will examine three past communication disasters in an attempt to determine if terrorism is a domestic threat, or specifically if the loss of a major communication facility is a threat to national security. Each disaster happened independently of the others. This study takes the results of these accidents and postulates the effects of similar levels of damage caused by a concerted terrorist action. Analysis of pre- and post responses provides a foundation for recommendations for dealing with the terrorist threat.

INTRODUCTION

As a Certified Protection Professional(CPP) and Security Supervisor with Bell Atlantic Corporation in Washington, D.C., I conducted physical security inspections of the utilities' Telephone Central Offices(TCOs). I inspected the TCOs with an eye for hardening the physical structure to prevent intrusion and possible harm to the plant equipment or employees.

Increasing international terrorist activity, with Americans as the focal point, caused me to ponder what would happen if a terrorist group would mount a coordinated attack on the public utilities in or around a major metropolitan area. My thoughts centered on several themes: (1) Could it be done? (2) How could it be done? (3) How easily could it be done? (4) What effect would an attack have on the utilities and national security? (5) Is such a threat a valid national concern? Finally, (6) How could a security supervisor better prepare an organization to prevent or respond to such an attack?

Initially, I was thoroughly convinced that an organization as large as Bell Atlantic, servicing the very heart of the U.S. Government, would have a carefully conceived Contingency Emergency Plan(CEP) with built-in redundancy to respond to a

terrorist attack. To my amazement I soon discovered that there is no published CEP for terrorism, nor is there redundancy built into the system. Further, my expressed concern over these deficiencies has so far met with only limited interest.

Upon reflection I feel this limited interest indicates lack of education as to the extent of the terrorist threat. We have experienced no major terrorist incidents involving public utilities on American soil. Therefore, no lessons have been learned. We continue operating with a false sense of security. Economics and a lack of understanding of the secondary effects that a coordinated terrorist attack would have on public utilities during the post response period also contribute to this false sense of security.

The purpose of this paper then is to explore the threat mentioned above by first looking at the potential capabilities of terrorist groups, analyzing the threat, and then postulating the possible damage terrorists could inflict. I will examine past communication disasters, seeking lessons learned from them.

THE THREAT

To most Americans the threat of large scale terrorist attacks on American soil is unbelievable. This perception is fostered, in part, by the increasing effectiveness of the anti-terrorist activities of the U.S. intelligence community, the Federal Bureau of Investigation, and state and local law enforcement agencies.(1)

But we must understand what a terrorist is and discover why he or she commits acts of violence in order to intelligently understand the threat. Surely there are no "typical" terrorists. But they do tend to display certain psycho-social profiles depending upon the group they represent. The July 1988 Protection of Assets Bulletin cited significant characteristics for current terrorists from a monograph that appeared in the April 1988 issue of the FBI Law Enforcement Bulletin.

A partial summary of the profile indicates that the terrorist leadership is politically active, literate, has high verbal skills, is well educated and well trained. I see the opposite in the followers. This leader-follower syndrome indicates the volatile nature of a terrorist organization.(2)

In, "Will Terrorists Go Nuclear?", B.M. Jenkins(CPP) indicates that a great deal of popular mythology about terrorists describes them as mindless, irrational killers -- persons like Bundy and Manson. But the violent actions of such persons do not describe most terrorists. Terrorists frequently do kill. And their killings, to a degree, are indiscriminate, but with a purpose. Further, their killings are are not irrational in the context of their political/religious purpose.(3) Americans must understand that terrorism is a threat or act of violence undertaken to create fear and focus attention on a particular political/religious movement.

Terrorist activities fall within a continuum -- ranging from

small autonomous groups fighting for political, religious or ethnic reasons to state-directed or sponsored terrorism. With nuclear parity, the INF treaty, and the continuing arms reduction negotiations, the likelihood of a nuclear confrontation is lessened. One of the negative results of this is the potential for an increase in terrorist activity by countries that are known to direct or sponsor terrorism such as Syria, Iran, Libya, North Korea, Cuba, and some Eastern Block states.(4) State direction or sponsorship of terrorist groups provides a safe, cheap, and sound course of action, compared with the risks of a nuclear or conventional confrontation. A recent example of state supported terrorist activity in the United States is the "Chicago Five" incident with the EL Rukns gang. Five members of the gang were convicted after an investigation found that their ringleader had made arrangements with Libya to blow up airplanes and government buildings for payments of up to $2.5 million. Fortunately, none of the terrorist acts ever took place.(5) The so called Libyan "hit teams" targeted against Libyan exiles and, allegedly at one time against President Reagan, provide another example of state directed terrorism.(6) Currently in the United States and Puerto Rico, remnants of at least seven terrorist groups operate autonomously. Their actions are ethnicly or politically motivated and basically right wing. None of these groups have perpetrated any incidents that can compare to international terrorist activity frequently covered in the news media.(7)

The bomb is the weapon of choice of most terrorist groups. The weekly news broadcasts of bombings in Lebanon or Ireland and the recent destruction by bomb of a passenger plane enroute from Europe to the United States illustrate the point. The bomb has been used during periods of political, racial, commercial and labor strife over the centuries. Thus the mere act of threatening to use or using the bomb has become a symbol of power.(8)

The FBI's 1986 bomb summary showed that the frequency and severity of bombings in the United States was down but still considerable. The report stated that in 1986 property damage amounted to $3.4 million, with 14 persons killed and 185 injured. Terrorists were implicated in 15 bombings.(9)

Technological advances in small but powerful weapons and munitions have also created an environment favorable to terrorist activity. These advances make the weapons cheaper and easier to transport and use.

Advanced weaponry and munitions in the hands of a terrorist group would be more devastating than any natural disaster that has occurred in the United States to date. This is particularly true if nuclear devices should become available to terrorist organizations.

Although I was unable to find any evidence of incidents of terrorists possessing or using "high tech" weapons, they are readily available. These weapons are designed for ease of use,

concealment, accuracy and destructive power. Some, such as the Light Anti-tank Weapon(LAW), are even disposable. "High tech" weapons and munitions offer distinct advantages : (1) They are light-weight. (2) They are simple to operate. (3) They have more destructive power. (4) They are more accurate. (5) They require no physical entry onto the targeted premises. (6) They increase probability of escape. (7) Finally, they decrease probability of detection. Examples of "high tech" weapons are the American-made Redeye, Stinger, Dragon and TOW precision-guided munitions(PGMs). The Soviet SA-7 and Sagger missile and the French-German Hot and Milan weapons systems are other examples. New shoulder-fired, multipurpose assault weapons include multi-shot rocket launchers. Silent grenade launchers, mini-grenades, and weapons firing duplex or triplex cartridges(that contain two or three bullets in tandem) are available. Also anti-tank rocket launchers can penetrate up to 2 meters of concrete or more than 1/2 meter of heavy armor. These rocket launchers have no backblast and can even be fired from inside a small room. Remote controlled mortars can be fired at a target using a timing device.(10) These weapons are mass produced by the United States and foreign governments for their armed forces. Some of these governments either sell to terrorists or sponsor terrorism to further their national aims.(11)

In sum, terrorists have the potential of becoming a major

force. Even more dangerous is a force that may have the state sponsorship to include weaponry, will and determination to pose a serious challenge.

The United States will become increasingly vulnerable to such challenges, in part because the entire infrastructure support system presents a wealth of lucrative high-tech targets.

LESSONS LEARNED

This section summarizes the catastrophic effect that fire and water had on communication facilities in three separate incidents. These incidents did not happen concurrently. Due to the courageous efforts, excellent emergency planning and cooperation of the Bell System, the effect in each case was limited to a matter of weeks. However, secondary effects are still being felt today. These communication disasters depict not only the immediate impact on the utility concerned but the impact on national security(military organizations) as well as the effects on police, fire emergency response capabilities and commercial enterprises.

NEW YORK- 1975(12)

The following summary was taken from a pamphlet released by AT&T in May of 1975.

On February 27, 1975 a short circuit in a sub-basement vault caused a five-alarm blaze that resulted in a major telephone service catastrophe. Within 17 hours, 170,000 telephones in Lower Manhattan were out of service. The fire damaged or

destroyed cable and switching equipment. Water damage rendered power equipment useless.

The fire knocked out service to 300 blocks in a three square mile area which housed offices, apartments, stores, 3 police stations,the Con Edison Power Company main office, New York University, 1 hospital, 1 clinic, 2 infirmaries and the Bernstein Institute. The initial emergency effort was to provide service to the hospital, the police and fire departments, and other vital agencies in the neighborhood.

Total response and restoration was beyond the capability of the New York company. Massive assistance from Western Electric, New Jersey Bell, Connecticut Bell, Pennsylvania Bell, the four Chesapeake and Potomac Telephone Companies and other sources was mobilized to aid in the restoration effort.

Mobile radio-telephone units from other Bell operating companies were brought in to provide emergency service. During the three-week outage, 400 coin telephones were also placed in storefront centers, mobile vans and special outdoor rack locations. Usage peaked at 105,000 calls a day- eight times the average usage of coin telephones in that area.

The Manhattan Chapter of the Telephone Pioneers of America organized volunteers to visit the blind and shut-ins in the affected area, to run errands, to take messages and place phone calls for them. A massive effort enabled the community to find locations of the coin telephones through distribution of

specially made maps written in four different languages.

The restoration effort impacted the transportation industry as well. Thirty trucking companies and 11 airlines were used to transport tons of equipment to the area.

An untold number of volunteers from New York and elsewhere along with more than 4,000 Bell System employees worked around the clock to restore the damaged TCO by 21 March 1975. Three weeks of fear, frustration, and teamwork proved fruitful. Monetary loss to the utility, stores and corporations within the affected area and loss to other areas of the country due to the deferral of equipment to the New York disaster has been estimated to be in excess of $100 million.

NEW ORLEANS- 1983(13)

The following summary was taken from the report on the New Orleans communication outage prepared for the Manager National Communications System by Booz, Allen, Hamilton, Inc.

On 7 April 1983, an unanticipated rainstorm caused unusually severe local flooding in the New Orleans area. The basement of AT&T/South Central Bell New Orleans Main Complex was flooded causing damage to the electrical system and the loss of both commercial and emergency power. Without power the TCOs system shut down when the plant's battery system was exhausted. The system shut down for 9 hours and 45 minutes. 50,132 local area lines were affected for 9 hours and 30 minutes. 566,272 long distance service lines were interrupted for 8 hours. Special

Service Lines -- a service that connects to or thru more than one TCO for 43,485 communications circuits -- were disrupted for 9 hours.

The impact of this disaster was minimized due to the time of the flood (night) and the effects of the flood on the morning of April 7 (most business & government offices shut down for the day). Therefore demand for service in the affected area was significantly reduced because of the circumstances.

Although access to long distance service was not available, New Orleans was not totally isolated from a telecommunications standpoint because other carriers maintained the capability to communicate through their systems throughout the shutdown period.

Some of the secondary effects of this national disaster follow. Of the approximately 1800 circuits routed thru the damaged TCO for use of the United States Transmission Systems (USTS), 35 percent remained in service; all special service circuits were out, including service provided GSA & MCI; an estimated 10 per cent of the 1000 Telex circuits and 700 TWX circuits provided Western Union were out of service; Satellite Business Systems (SBS) lost the use of its WATS extension to outlying cities for a short period.

The effects on federal, state, and local government offices varied. The severity was reduced by closings due to the flood. Military installations reported that the outage either disrupted or severely impaired their mission performance. The loss of

Automatic Voice Network (AUTOVON), Automatic Digital Network (AUTODIN), Federal Telephone System (FTS) and long distance service made it almost impossible for military activities to contact their headquarters. The Naval Air Station lost its weather service circuits needed to carry out its responsibility of hurricane prediction. The report also stated that representatives of the Air National Guard indicated they could not have launched their defensive/interceptor fighter aircraft that were on alert. If forces had been mobilized during the shutdown, the Navy Reserve would not have been able to perform its critical coordination functions. The Navy, Coast Guard and Army National Guard resorted to use of Military Affiliated Radio System (MARS) stations, HF and FM radio networks. The Government Services Administration's(GSA) experience was similiar to that of the military. Its FTS access lines were not restored until April 8 due to fusing problems in the New Orleans TCO.

The most severely handicapped government organization was the Federal Aviation Administration (FAA). Loss of service to the FAA's Houston center made normal air traffic control impossible. Special service circuits, providing data transmission capabilities, precluded the automatic hand-off of air traffic and caused the FAA to route traffic around the New Orleans area. They also had to impose flow control nationwide for air traffic destined for New Orleans. The cooperative actions taken by the FCC, AT&T, and the White House in response to this limited

shutdown were as follows. Total loss of communications between the Houston center and the New Orleans sector center was considered a major problem by FAA officials. FAA regional headquarters officials called the AT&T National Accounts Office in Washington and determined that AT&T could use military airlift capabilities to transport an emergency satellite terminal from Atlanta to New Orleans. FAA headquarters in Washington began coordinating with the Pentagon for suitable airlift. "FAA personnel reported that within a couple of hours the approval for the use of a C5A aircraft had been obtained from the Executive Office of the President".(14) The process moved rapidly to a point that instructions were being prepared to direct the tractor trailer driver to the correct loading area at the air force base in Georgia. Communications were restored prior to implementing the plan.

Response to this communications disaster was well within the capabilities of the local Bell System and AT&T personnel. Assistance from other telecommunications carriers was not necessary. Flooding at a different time of the day or of a longer duration may have caused greater problems.

CHICAGO- 1988(15)

This summary of the Hinsdale communication disaster was taken from an article which appeared in the September 1988 issue of the Protection of Assets Bulletin. Additional and more specific information on this incident will probably be available after

current litigation is complete.

On Mother's Day, Sunday, 8 May 1988, a fire at a Hinsdale, Illinois, TCO caused damages which approached the 1975 New York fire. The Illinois company is still reviewing and assessing the damages at this time. What is known are the facts reported to the press at that time. The TCO was unoccupied on weekends. The fire burned for approximately 30 minutes before a fire alarm was noticed by a console operator located in a telephone company facility 150 miles away in Springfield, Illinois. Reasons for the delay in noticing the alarm, reporting the alarm to the local fire department and the local fire department response are not quite clear. The results of the fire were catastrophic. The Telephone Company's direct equipment and repair loss was over $30 million. Service was lost to 35,000 local subscribers. 118,000 Long distance lines and 36,000 Special Services lines (data) were disabled. Subscribers included major corporations such as Eastman Kodak, Rockwell International, Hyatt, FTD, McDonalds, United Stationers and Ace Hardware. As in the previous communications disasters, the secondary effects were significant. FTD had processed almost all of its Mother's Day orders, so their losses were minimal. United Stationers relocated its operations but still lost an estimated $10 million in orders. Company officials estimated there would have been an additional $30 million loss if they had not had an alternative plan. Ace Hardware lost contact with 5 of its 15 distribution

centers and data had to be flown in. Order processing was delayed and rush orders were probably lost. In addition to the loss of local area access, there was a loss of contact with 50 other TCOs.

This paper does not offer an in depth study of the three communications disasters. But what my review of the disasters reveals is some sense of the magnitude of the impact of a communications disaster. Also, there are lessons to be learned from them -- lessons that can be used to better prepare the telecommunications industry for possible future incidents of an organized terrorist nature. The key to formulating the lessons learned is to visualize each incident as happening at the same time, but not due to a fire or flood. Visualize the effect a coordinated terrorist attack on multiple targets would have in a major metropolitan area such as Washington, D.C.

Three lessons stand out. First, any major incident involving either the electric or communications utilities in one or more metropolitan areas would have a devastating effect on not only the utility concerned but public health and welfare, public order and national security. Second, it is imperative that every public utility have a well thought out Contingency Emergency Plan(CEP). Third, a constant state of cooperation must exist between the private sector, federal, state and local governments.

THE CONCERN

In reviewing the literature on terrorism and reflecting upon the reaction of my peers when I inquired, it appears that a majority of the American public has a low concern for terrorism within the United States. Most feel terrorism is an international problem -- not a national problem.

On the other hand, corporate America's concern is rising as more and more terrorist acts are perpetrated against their overseas ventures and they become aware of the vulnerabilities here in the United States.

The Federal Government is highly concerned. An interview with a senior official of the National Communications System revealed that high level government and corporate executives of the communications industry have been studying the threat for the past seven years.(16) This group, the National Security Telecommunications Advisory Committee(NSTAC), meets with the President and his staff twice a year. One result of their work has been monies allocated by the government to reduce vulnerabilities.(17)

The U.S. Army and Air Force have expressed their concern with terrorism by placing the operational concept of terrorist activity in one of four major operational categories under Low-Intensity Conflict(LIC) doctrine. The other categories are insurgency and counterinsurgency, peacekeeping operations, and peacetime contingency operations.(18) This doctrine speaks to LIC as often localized, principally in the Third World, but as

containing regional and global security implications.(19)

The Federal Government also expressed its concern with the terrorist threat to the United States in a public document entitled the Public Report of the Vice President's Task Force on Combatting Terrorism. The report states that

> Our vulnerability lies, ironically, in the strength of our open society and highly sophisticated infrastructure. Transportation, energy, communications, finance, industry, medicine, defense, diplomacy and government itself rely on intricate interrelated networks. Given these inherent vulnerabilities, and the fact that Americans are increasingly the targets of terrorist attacks outside the United States. it is apparent that a potentially serious domestic threat exists.(20)

Without doubt, the potential domestic threat is real! Technology has actually "giftwrapped" sensitive high tech infrastructure support systems into small boxes. Increasing amounts of communications are located in single locations due to the introduction of "Fiber Optics" and the fully automated "Electronic Switching Systems", thereby increasing systemic vulnerability. The economics of centralizing communication and electronic equipment, while attractive to corporate executives, is potentially disasterous without redundancy. The establishment of the NSTAC and the response by government agencies in Washington, D.C. to the New Orleans communication disaster are indicative of the effects these disasters have on national security. Federal, state and local law enforcement agencies are doing an outstanding job identifying, tracking, and apprehending actual and potential terrorist groups. But they cannot do the

job alone! The communications, power, and transportation industries are so interrelated that they must join forces with governmental agencies to develop effective pre- and post-responses to potential domestic terrorism.

Providing advice to my corporation on ways to harden the physical plant, add redundancy, and establish a well planned and coordinated Contingency Emergency Plan would better prepare the organization to prevent or respond to a terrorist attack. Hardening of the physical plant offers only limited security. But efforts should continue to increase the difficulty of unnoticed physical entry and at least provide an early warning of any malfunction in equipment or attempted forced entry. Security guards and CCTV are the keys to hardening the physical plant. However, redundancy is not regarded as "economical" in light of the currently perceived threat. Government insistence(regulation) and assistance(money) and industry cooperation are key to establishing alternative means of communication and power availability. Limited CEP exists in every organization. However, a great majority of these plans address only natural and man-made disasters. Many that address terrorism cite only kidnapping as an act of terrorism under the heading of Executive Protection. Corporate security training is oriented towards verified threats(bomb,fire,work stoppage etc.). Other contemplated threats depend on the region the corporation is located -- for example the hurricane belt or the tornado

belt. The Federal Government has generally oriented its preparedness on natural disaster and conventional or nuclear warfare response.(21) The economic orientation of corporate America and, to some extent, of the Federal Government provides money only for securing against these known threats. In summary, CEPs are basically written in a vacuum with no apparent thought or understanding of effects on other entities within the metropolitan area. I feel that a coordinating document with national level emphasis and guidance should encompass all local, state, and federal interests.

A NATIONAL CEP (NCEP)

The three primary goals of a CEP are, in order of importance, (1) the protection of life, (2) protection of property, and (3) the restoration of normal activities.(22) The vital first step in development of the CEP is the establishment of an overall National Disaster Response Plan (NDRP). There is no need to re-invent the wheel. There is a wealth of expertise in formulating, exercising and implementing CEPs in America. All that is needed to address the potential terrorist threat is to integrate this expertise into a National CEP (NCEP) with the full backing of the Legislative and Executive branches of the Federal Government. The NCEP would replace mutual assistance agreements at times of national disasters. There are two sound reasons for a National Contingency Emergency Plan. First, it is imperative that active partnerships between the federal, state

and local governments and private organizations be formulated to lessen the initial effects of a major terrorist incident or concerted series of incidents. Second, without a NCEP, multiple disasters involving communications and electric power utilities and the transportation network could very well affect national security, public health and welfare and U.S. national and international stability.

Every utility corporation whose activities are predetermined to be of vital concern to U.S. national security interests should be represented, including AT&T, Regional Bell Operating Companies(RBOC's), and Con Edison Power.

The FBI is designated the Lead Agency of the Federal Government, with the responsibility for coordination of the federal response to terrorist incidents that take place within U.S.territory.(23) This agency would oversee the NCEP thru the Federal Emergency Management Agency(FEMA), which would be responsible for developing, testing, and implementing the plan with the assistance of the Department of Transportation(DOT), Department of Energy(DOE), Department of Defense(DOD), and the National Communication System(NCS). FEMA would design a NDRP concentrating on the areas shown below.:

National Disaster Response Plan Areas of Concentration for Development of the NCEP

	Area	Responsible Agency
I.	Education of the public.	Federal, state and local governments and private sector.
2.	Intelligence gathering.	Federal, state and local

		law enforcement.
3.	Containment of terrorist activity.	Federal, state and local law enforcement.
4.	Apprehension.	Federal, state and local law enforcement.
5.	Rapid response(restoration). a. Training b. Prelocation/identification of critical repair parts. c. Key needs of interrelated industries. d. National security restoration priorities.	Federal, state and local governments and private sector.

Federal, state and local funds along with corporate funds should be earmarked for the plan, with emphasis on the communications, transportation and electric power industries. Planning emphasis should be on restoration. Rapid restoration would encompass the first and second primary goals of CEP and dilute the secondary effects on other portions of the infrastructure not directly attacked.

In sum, a NCEP would place national resources up front alongside of corporate resources to better respond to a national concern.

This paper has explored the potential terrorist threat in the light of past communications disasters. It then postulates the possible damage terrorists could inflict through examining potentially comparable disasters. Finally, it extracts lessons learned that could lead to coordinated planning for such disasters. Even though each disaster happened in isolation, extrapolation of all the events happening in concert because of

coordinated terrorist activity is easy to visualize. Likewise, such terrorism is easy to execute and almost impossible to prevent.

The threat, technology and our infrastructure suggest that to linger longer with a false sense of security would be folly. A NCFP is a possible solution to a very real threat.

ENDNOTES

1. Timothy J. Walsh, CPP, ed. Protection of Assets Manual. Santa Monica: Merritt, 1988. Pp. 18-127 - 18-139: "Overview on World Terrorism," by Steven J. Van Cleave, CPP.

2. Timothy J. Walsh, CPP. "The Modern Terrorist Profile," Protection of Assets Bulletin, July 1988, p.2.

3. Timothy J. Walsh, CPP, ed. Protection of Assets Manual. Santa Monica: Merritt, 1988. Pp.18-61 - 18-80: "Will Terrorist go Nuclear," by Brian M. Jenkins, CPP.

4. Van Cleave, p.18-138

5. PDA Bulletin, February 1988, p.1.

6. U.S. Department of Army. Field Manual 100-20, Final Draft, Military Operations in Low-Intensity Conflict. Washington: 24 June 1988.

7. Van Cleave, p.18-129

8. Paul Fuqua, and Jerry V. Wilson. Terrorism: The Executives Guide to Survial. Houston: Gulf, 1978.

9. Timothy J. Walsh, CPP. "FBI Bomb Summary for 1986," Protection of Assets Bulletin, February 1988, p.1.

10. Timothy J. Walsh, CPP, ed. Protection of Assets Manual. Santa Monica: Merritt, 1988. Pp.18-105 - 18-119: "The Potential Arsenal of Tommorrow's Terrorist," by Brian M. Jenkins.

11. Ibid.

12. American Telephone and Telegraph, Miracle on Second Avenue: The Bell System's Response to a Major Service Disaster. USA: 1975.

13. Booz, Allen and Hamilton Inc. Telecommunications Emergencies: New Orleans Communication Outage April 7, 1983. Prepared for The Office of the Manager National Communications System. Bethesda: 1983.

14. Ibid .., p.4-6

15. Timothy J. Walsh, CPP. "A Risk Mismanagement Example," Protection of Assets Bulletin, September 1988, Pp.4-5

16. Bird, John P., Director for Analysis with the Office of Plans and Programs, National Communications System. Personal Interview. Washington: 15 December 1988.

17. John Tillinghast, and Bernard Stewart. White Paper: Security of Electric Power Supply. McLean: Science Applications International Corporation, 1986.

18. FM 100-20, p.1-10.

19. Ibid., p.1-1.

20. Vice President of The United States. Public Report of The Vice Presidents Task Force on Combatting Terrorism. Washington: Government Printing Office, 1986.

21. George C. Moore, and Judith A. Morgan. CPP Examination Study Guide. 3rd ed. Arlington: ASIS. 1987.

22. Ibid.

23. Public Report, p.8.