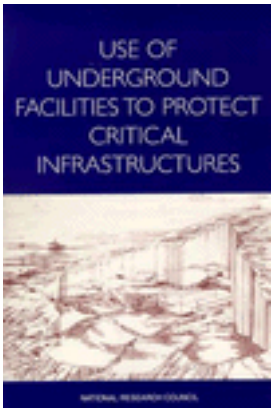

Use of Underground Facilities to Protect Critical Infrastructures: Summary of a Workshop

Richard G. Little, Paul B. Pattak, Wayne A. Schroeder, Editors; Board on Infrastructure and the Constructed Environment, National Research Council

ISBN: 0-309-59255-0, 70 pages, 6 x 9, (1998)

Use of Underground Facilities to Protect Critical Infrastructures

Summary of a Workshop

Board on Infrastructure and the Constructed Environment
Commission on Engineering and Technical Systems
National Research Council

Richard G. Little Paul B. Pattak Wayne A. Schroeder Editors

NATIONAL ACADEMY PRESS
WASHINGTON, D.C. 1998

NATIONAL ACADEMY PRESS 2101 Constitution Avenue, N.W. Washington, D.C. 20418

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

This study was supported by Contract No. S-FBOAD-94-C-0023 between the National Academy of Sciences and the Department of State on behalf of the Defense Special Weapons Agency. The views presented in this report are solely those of the workshop participants and do not represent the position or opinion of the Defense Special Weapons Agency, the Board on Infrastructure and the Constructed Environment, the National Research Council, or the National Academy of Sciences.

International Standard Book Number: 0-309-06288-8

Available in limited supply from: Board on Infrastructure and the Constructed Environment, HA 274, 2101 Constitution Avenue, N.W., Washington, D.C. 20418, (202) 334-3376

Additional copies of this report are available from National Academy Press ,2101 Constitution Avenue, N.W., Lockbox 285, Washington, D.C. 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu

Cover art: Schematic line drawing of underground facilities in Norway is reprinted by permission of the Norwegian Defence Construction Service

Printed in the United States of America.

Board On Infrastructure And The Constructed Environment

NRC Staff

*Deceased.

Acknowledgments

This report has been reviewed by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's (NRC's) Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the NRC in making the published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The contents of the review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their participation in the review of this report:

Dr. Brenda Meyers Bohlke, Parsons Brinckerhoff, Inc., Reston, Virginia

Mr. Reuben Samuels, NAE, Parsons Brinckerhoff, Inc., New York, New York

Dr. Eugene Sevin, NAE, Lyndhurst, Ohio

Mr. Peter Smeallie, Research Opportunities Management, Alexandria, Virginia

Although the individuals listed above have provided many constructive comments and suggestions, responsibility for the final content of this report rests solely with the NRC.

Contents

Introduction

BACKGROUND

Critical Foundations: Protecting America's Infrastructures, the report of the President's Commission on Critical Infrastructure Protection (PCCIP, 1997), concluded that the nation's physical security and economic security depend on our critical energy, communications, and computer infrastructures[1]. As our dependence on them increases, so too do the vulnerabilities of these infrastructures to a wide range of threats. During the Cold War, the federal government constructed a number of underground facilities (UGFs) to house critical personnel and functions associated with the national defense. Although this threat has warned, the threat of high-casualty terrorist incidents and the diffusion of technologies for weapons of mass destruction have increased. In light of these growing threats, the Defense Special Weapons Agency of the U.S. Department of Defense (DoD) requested the assistance of the National Research Council to investigate how these existing facilities, or new underground sites, may contribute to an emerging national focus on the security of our critical infrastructures.

The PCCIP noted that the potential threats to the nation's critical infrastructures range from natural disasters to criminal and terrorist activities to organized information warfare. Many of these threats are "cyber-threats" and are not readily addressed with traditional physical security techniques. However, some components of advanced information systems are vulnerable to physical damage, whether from terrorist bombings, earthquakes, or apparently ordinary traffic accidents. Other infrastructure systems, such as energy, transportation, and emergency services, also have critical elements that are physically vulnerable. Although the PCCIP did not directly address the role of UGFs for the protection of critical infrastructures, its report recommended a program of joint government and industry cooperation and information sharing to increase the security of our nation's critical infrastructures.

Secure UGFs offer one means of protecting these critical elements and systems. UGFs can be particularly attractive if the perceived threat level or the consequences of loss are high and the vulnerabilities cannot be addressed through system redundancy or other nonstructural means. Although buildings can be hardened (strengthened) against structural failure from earthquakes, explosions, or accidents, beyond a certain threat level or structural loading, providing protection for critical elements in hardened above-ground structures

[1] Critical infrastructures are systems whose incapacity or destruction would have a debilitating impact on the defense or economic security of the nation. They include telecommunications, electrical power systems, gas and oil, banking and finance, transportation, water supply systems, government services, and emergency services.

may cost more than building an underground facility. A cost-risk analysis can demonstrate the most cost-effective approach for obtaining the desired level of protection.

At the request of the Defense Special Weapons Agency, the Board on Infrastructure and the Constructed Environment of the National Research Council convened a workshop on April 6 and 7, 1998, on the use of underground facilities for the protection of critical infrastructure. The workshop, which was held at the National Academy of Sciences, in Washington, D.C., explored how existing UGFs constructed for defense purposes or new facilities might meet the nation's needs in protecting critical infrastructures. Workshop participants possessed expertise primarily in defense and security matters. Members of the commercial underground and tunneling communities also were in attendance.

The views presented in this summary of the workshop are solely those of the participants and do not represent the positions or opinions of the Defense Special Weapons Agency, the Board on Infrastructure and the Constructed Environment, the National Research Council, or the National Academy of Sciences.

ORGANIZATION OF THE WORKSHOP

Following a welcoming address by Maj. Gen. Gary Curtin, director of the Defense Special Weapons Agency, and a keynote address by Frederick Struble, former commissioner of the PCCIP, four technical panels were convened. Panel 1, "Infrastructure Protection Issues", provided an overview of the threats facing the nation's critical infrastructures. Panel 2, "Needs and Requirements of the Infrastructure Community", addressed issues and protective strategies from the viewpoints of selected infrastructure sectors. The third panel, "Experiences with Underground Facilities: Capabilities, Limitations, and Applications" gave an historical perspective on the use of UGFs and operating experiences with defense and commercial facilities. Panel 4, "Factors Influencing the Decision-Making Process" discussed the various technical, economic, and policy questions that must be addressed when considering an underground facility option. Donald Woodard discussed the key issues that commercial enterprises consider when contemplating an underground location and Arnfinn Jenssen provided a Norwegian perspective on infrastructure protection in the United States. Following the panel presentations and discussions, the workshop participants divided themselves between two breakout sessions to discuss technical and policy issues.

KEY ISSUES IDENTIFIED

Technical Issues

The following issues were identified in the technical breakout session:

- Threats to the infrastructure are both physical threats and cyber-threats; and an overriding concern is that most of the nation's critical infrastructures are owned by the private sector.
- The private sector's record on protecting infrastructures is mixed. A comprehensive solution involving UGFs will certainly require a partnership between the private sector and the federal government.
- Critical infrastructures must be defined.
- Tools and educational data should be developed to explore the long-term trade-offs between UGFs and other options to protect critical infrastructures.
- Going underground has some clear benefits, such as improved security and opportunities for dual uses of existing facilities.
- Cost is a major issue. In the United States (though not in Scandinavia) the initial construction cost of UGFs is considerably higher than the cost of above-ground facilities. Cost will be considered a "barrier" by some infrastructure owners and operators who are considering underground relocation. Over the entire life cycle of UGFs, there are operations and maintenance cost savings; in the long run, UGFs can be considered very cost competitive.
- Specific threats must be addressed, and UGFs must be well designed and difficult to attack. Technical concerns include external lifeline connections, fire, and protecting the facilities against chemical and biological weapons.

Policy Issues

The policy breakout session identified the following issues:

- Public perception is clearly a key issue. Corporate America needs to be made aware of the benefits of UGFs, and the public needs to be educated about their uses and benefits for protecting critical infrastructures.
- Cost is a major policy issue because of the substantial difference in cost between UGFs and above-ground structures. Before a more aggressive public effort can be mounted in support of an underground program, more definitive cost data must be available.
- The dual-use capabilities of facilities should be emphasized. A great deal can be learned from the Norwegian experience with dual-use UGFs. The

benefits of dual-use capabilities should be emphasized as a major advantage for future underground facility programs.

- The underground technical community should narrow its focus, identify specific infrastructure areas where UGFs could help, obtain good estimates of design and cost data for going underground for those particular infrastructure elements, and then reach out to the appropriate sectors (e.g., corporate executives and government) to adopt a longer-term program.

Reference

The President's Commission on Critical Infrastructure Protection (PCCIP). 1997. Critical Foundations: Protecting America's Infrastructures. Washington, D.C.: The President's Commission on Critical Infrastructure Protection.

Welcoming Address

Maj. Gen. Gary L. Curtin,
U.S. Air Force Director, Defense Special Weapons Agency

Gen. Curtin noted the timeliness of the workshop in light of the current national focus on ensuring the viability of critical infrastructures and interest in this topic worldwide as well as in the United States. He outlined the purpose of the workshop and provided some thoughts on why underground facilities (UGFs) can be part of a broader solution to the problem of protecting our nation's infrastructures. He cautioned, however, that, although using UGFs to protect vital infrastructures seems both obvious and direct for those familiar with them, the topic requires much more investigation before a national initiative to use UGFs to protect critical infrastructures can be recommended.

To some degree, the image of UGFs goes back to the Cold War when bomb shelters were to be used in the event of a nuclear attack on the United States. Sometimes UGFs were viewed as something from science fiction, places where clandestine alien forces might be hiding. The natural American reaction to UGFs is negative and this aversion has permeated consideration of the issue over the years. We now have an opportunity to reconsider UGFs because the environment has changed since the end of the Cold War. Significant and formidable new threats have arisen, including weapons of mass destruction, transnational and terrorist threats, and cyber-threats and information warfare. These new problems will require new solutions, especially as they relate to protecting critical infrastructures.

The report of the President's Commission on Critical Infrastructure Protection (PCCIP) emphasized that infrastructure be seen through the lens of national security. The commission's suggestions have interesting implications. The primary emphasis of the commission's report is on cyber-threats, but strong recommendations are also made concerning research and development (R&D), vulnerability assessments, and the need for backup facilities. Unfortunately, at the same time that the use of UGFs to house vital security and infrastructure functions is growing worldwide, the United States is closing UGFs associated with national security.

The Defense Special Weapons Agency (DSWA) has been involved in the survival of UGFs for many years, primarily based on work done by its Springfield Research Facility (SRF), and DSWA holds an annual conference for site managers of UGFs. This has turned out to be an effective networking and communications vehicle for people interested in these facilities. After the 1997 meeting, SRF was asked by the site managers to explore the use of UGFs to protect critical infrastructures.

DSWA convened a working group, chaired by George Baker, SRF director, that was substantially involved in planning the present workshop. Dr. Baker also briefed Gen. Marsh, chairman of the PCCIP, on SRF's capability to

perform vulnerability assessments and the potential role of UGFs in infrastructure protection.

Gen. Curtin described a trip to Norway with Arnfinn Jenssen, of the Norwegian Defence Construction Service, who showed him some of Norway's numerous UGFs. Both Norway and Sweden have built many world-class facilities and Gen. Curtin was particularly impressed with an air traffic control center near Oslo—one example of the key infrastructures that Norway has put underground. Although air traffic control centers are not normally placed underground, this is a very capable and secure facility.

Gen. Curtin noted that he has also visited a number of UGFs in the United States. Even though they are older facilities, they reflect a very high state of the art. After visiting many underground sites, Gen. Curtin has concluded that existing UGFs offer a number of advantages over above-ground sites: they are secure, adaptable, relatively inexpensive compared to some options, and already available because of cutbacks in other government programs.

Gen. Curtin discussed some of the cost benefits compared to surface locations that could accrue as a result of moving infrastructure underground. First, the land at the surface can be used for other purposes. In a country like Norway, where flat terrain is at a premium, this is an important consideration. Second, energy costs are lower because temperature and humidity underground fluctuate very little. Third, from the commercial point of view, taxes and insurance tend to be low because underground space is not exposed to the same weather conditions and hazards as above-ground facilities.

Gen. Curtin concluded by outlining his expectations for the workshop: identifying the missions and functions for which UGFs may be useful in supporting infrastructure; assessing the costs and benefits of going underground; flagging issues that need further evaluation; and, most important, bringing together government and the private sector to propose initiatives to the National Research Council and the PCCIP's successor organization.

Findings of the President's Commission on Critical Infrastructure Protection

Frederick Struble
President's Commission on Critical Infrastructure Protection

Dr. Struble's summarized the findings of the PCCIP, which he hoped would be helpful as background information for the workshop's deliberations on the uses and applications of underground facilities (UGFs). The PCCIP report was submitted to the President on October 13, 1997, with the understanding that key federal agencies would be given the opportunity to review it and submit comments, which would also be presented to the President.

Dr. Struble observed that, even though the Cold War is over, the people and properties of the United States, both inside and outside our borders, remain at considerable risk from terrorists, both domestic and foreign, hostile nation states, and various malcontents. Recent events have made these threats abundantly clear; bombings of the World Trade Center in New York, the federal office building in Oklahoma City, the Olympic grounds in Atlanta, and the U.S. military base in Saudi Arabia. Weapons of mass destruction, including chemical and biological agents, pose comparable, if not more, lethal threats. Some nation states are probably working to develop small atomic bombs, and not all of the nuclear weapons that were part of the arsenal of the former Soviet Union have been accounted for. These weapons pose the most serious danger to our country in the immediate future.

The PCCIP focused, however, on another type of weapon, which has the potential to match, or even exceed, the damage and disruption caused by physical weapons. Cyber-tools and techniques that use sophisticated telecommunications systems can be used to disrupt or gain control of computer-based information and operating systems. These information technologies and systems have been credited with major scientific and technological advances, enhancing technical capabilities, and improving the efficiencies of almost every type of activity in our society. At the same time, our growing reliance on them has created serious vulnerabilities in our critical infrastructures and other vital functions of society that depend on them. As infrastructure sectors become more and more interdependent, a malfunction in the information and operating system of one sector can have cascading effects onto other sectors. For example, a failure of the power grid could disrupt many other infrastructure sectors.

Recent events have underscored the vulnerability of our information and control systems. Hackers, with apparently no more motivation than proving how smart they are, have on many occasions broken into the control centers or impaired the functioning of many systems, both governmental and private. An exercise carried out by the U.S. Department of Defense (DoD) last year, Operation Eligible Receiver, demonstrated the alarming potential of cyber-threats. The exercise showed that cyber-tools, used with other sophisticated

procedures and techniques that are well known to intelligence communities, could disrupt and impair the functioning of information, operational, and communications systems of defense agencies and other vital infrastructure sectors. The PCCIP concluded that the United States will be increasingly at risk from the use of cyber-weapons.

The PCCIP described the following scenario. A well-financed and knowledgeable adversary, not wishing to test the military might of the United States in conventional conflict, could seek to undermine our strength and security by using both cyber-weapons and physical weapons in a coordinated way to cause death, damage, and disruption. Part of the attack might involve sophisticated cyber-tools to invade and interrupt the electric grid system in the Northeast, for example. Given the worldwide Internet, this attack could be controlled from a foreign country. The disruptive effects of the attack could be enhanced by using the same cyber-tools and techniques to undermine DoD's ability to communicate over the Internet, which is used to transmit all but the most sensitive messages.

If physical weapons were also used, such as chemical sabotage of the water system of a midwestern city coupled with the bombing of public facilities on the West Coast or the introduction of lethal gas into the subway system of a major eastern city, the resulting death and destruction would cause a widespread loss of morale, if not panic. The tendency to panic would be even greater if our defense and law enforcement authorities were not able to respond effectively to such events.

This is not an unrealistic scenario. Given the clandestine nature of the attack, it might take some time to determine whether a foreign or domestic source was responsible or even to decide if all of the events were related. Thus, there could be considerable confusion as to which agencies, defense or law enforcement, should take the lead and organize a response. Also, if defense communications systems were disrupted, defense agencies would find it difficult to mobilize their forces and to organize an effective response. In addition, efforts by federal agencies to mitigate the effects of the attack and to help in the cleanup and reconstruction could be handicapped by the lack of enabling legislation. State and local authorities could also be hampered in their efforts because most of them lack the necessary training and equipment.

In short, the PCCIP concluded that if this scenario occurred it would present a serious challenge to our overall national security. The commission's strongest recommendation was that it is imperative for the United States to act now to protect itself. The commission recognized that this is not just a question for the federal government. Although the federal government has overarching responsibilities for defense, law enforcement, and intelligence, private firms and state and local governments that own the infrastructure systems also must act to protect themselves.

The infrastructure systems considered by the commission were limited to telecommunications, electric power, oil and gas, transportation, banking and finance, water distribution, emergency services, and government operations at

all levels. The principal owners of these infrastructures have the immediate responsibility of providing security for their employees and properties and for ensuring that they have the capability to serve their customers under adverse circumstances. Thus, joint actions by the government and the private sector will be required to address our national security needs; some actions should be undertaken in parallel by the federal government and the private sector, some in partnership, and some individually.

The PCCIP recommended that concerted efforts be made to heighten public awareness of the risks facing our country, particularly cyber-risks, which are not adequately appreciated, and to strengthen educational programs to deal with these risks. The need for education in this area is apparent. Dr. Strubble noted, for example, how often employees, both within and without the government, react to computer malfunctions by assuming that the machine or its programs are responsible rather than a hostile agent acting over an Internet connection. People must become conditioned to recognize and suspect the potential for outside threats. Information security consciousness by senior infrastructure management was observed to be uneven across firms and sectors. Training at all levels of our education system must be improved to raise security consciousness and to provide a cadre of people with security expertise. Finally, the commission found that young people, many of whom have better technical skills than judgment, need to be made to understand that the invasion of information systems, whether government or private, is a serious offense comparable to breaking into a business or home and that offenders will be subject to prosecution and punishment.

To achieve these objectives, the PCCIP recommended that the White House sponsor a series of conferences for leaders in the business and academic communities and state and local governments. In addition, the commission recommended that the National Science Foundation provide research grants for university faculties and scholarships for students to promote research on ways to protect the security of our information systems.

A second set of recommendations focused on the federal government's management of the security of its own information systems. From reports by the Inspector General and other sources, it is clear that many of our government agencies have not taken appropriate measures to secure their information systems. Thus, the PCCIP recommended that the federal government take decisive steps to get its house in order and lead by example. To that end, the commission called for the National Institute of Standards and Technology and the National Security Agency to establish standards and best practices for safeguarding the government's information systems. In addition, the commission recommended that clear and unequivocal specifications for complying with these standards and practices be built into the planning processes for federal agencies. The planning goals should be stated in a way that makes it easy to ascertain whether or not they have been met.

Third, the PCCIP report called for a major increase in federal R&D funding. Although both private industry and federal agencies have increased

their spending considerably in recent years, the commission concluded that much more remains to be done to promote security. Specifically, the PCCIP called for an immediate doubling, to more than $500 million, of federal spending on R&D in the coming year, and for a further increase of 20 percent per annum in the following five years. Expanded R&D for technologies and procedures is expected to pay direct dividends for the government as well as the private sector. Federally funded R&D will also be a catalyst to encourage private efforts.

Fourth, after reviewing the existing legal framework, the PCCIP recommended that key laws be changed so that cyber-threats can be addressed and potential attacks managed more effectively. A few of the recommendations the commission made in this area are that (1) owners of infrastructures should be authorized to screen potential employees being considered for sensitive security positions more thoroughly; (2) our law enforcement agencies should be authorized to investigate suspected criminal activities that cross the jurisdictional lines of federal district courts by obtaining an order from only one federal court rather than from each court involved; (3) computer crimes should be deterred by making sentencing parameters stricter; and (4) the federal government should provide greater financial and other assistance to municipal, state, and local firefighters and police to prepare them to deal with the effects of natural disasters and other destructive forces.

Fifth, the commission recommended that actions be taken to promote information sharing within each infrastructure sector, across infrastructure sectors, and among all sectors and relevant government agencies. Shared information should include reports of all attempts to intrude into information systems. Government efforts to stop these intrusions would be more effective if the techniques used and the number of occurrences were known. Many entities have been reluctant to report such intrusions, even to law enforcement agencies, because they are concerned that disclosure might be embarrassing, attract further attacks, or expose their operations to disruptive criminal investigations. Information must flow in both directions, with government agencies informing private firms of plans by potentially hostile parties, as well as making information available about technologies that can be used to make information systems more secure.

Finally, the PCCIP recommended that organizational structures be established to facilitate the sharing of information and to promote cooperation between government agencies and private firms. The commission attempted to avoid, as much as possible, recommendations for the establishment of an extensive new bureaucracy or added regulations. The commission's recommendations include the following:

- An Office of National Infrastructure Assurance, to be located in the White House as part of the National Security Council and staffed by a small number of people drawn from relevant government agencies, would serve as a focal point for efforts to protect critical infrastructures.

- An Infrastructure Assurance Council, composed of prominent corporate leaders, representatives of states and local governments, and cabinet officers, would address infrastructure policy issues and advise the President.
- An infrastructure assurance support office, composed of staff from both government and the private sector, would provide functional support to the Office of National Infrastructure Assurance and to the National Security Council and would carry out other activities for promoting the security of our information systems.

The PCCIP also recommended that several other entities help organize and facilitate the sharing and analysis of information and general cooperation between federal agencies, private firms, and state and local governments. First, the commission recommended that each infrastructure sector organize itself in the way best suited to facilitate information sharing and be authorized to designate its own infrastructure assurance coordinator. Second, federal agencies with supervisory and oversight responsibilities for each sector were directed to assist them. Third, the PCCIP recommended the establishment of an information and analysis center in the private sector to receive information from each infrastructure sector and use it to analyze the progress of each sector and to disseminate the results of their analyses to both government and private users. Finally, the PCCIP recommended the establishment of an early warning center within the government that would be responsible for analyzing information and assessing threats from all sources. This center would provide warnings as quickly as possible of a concerted attack on our country. The Federal Bureau of Investigation is already working to establish such a center.

Since these recommendations were submitted to the administration in October 1997, national defense and law enforcement agencies and other key government departments have had them under review. The review has been supplemented with advice from a presidentially appointed committee of industry leaders. Former Senator Sam Nunn and Jamie Gorlick, past assistant attorney general are cochairs. The committee was established to advise the commission as it formulated its recommendations. Many aspects of the recommendations have complicated implications, and some create, at least at the margin, jurisdictional problems for various agencies. As expected, the deliberation process will take some time, but the essentials of the recommendations, if not every detail, will probably be endorsed by the departments and agencies now reviewing them.

Dr. Struble concluded by reemphasizing the threats facing our nation today and in the future. He cited the need to improve the security of critical infrastructures as we move into the twenty-first century, and UGFs would seem to help achieve that end in many situations. Not only are UGFs suitable for this purpose, some are also available now. Dr. Struble challenged the workshop participants to identify the advantages of existing UGFs, determine how they could be modified to be of most benefit, and make them known to infrastructure owners. In short, he said the workshop should focus on stimulating demand to match the existing supply.

Key Issues in Going Underground

Donald Woodard
Underground Developers Association and Park College

Mr. Woodard contrasted commercial underground applications with infrastructure assurance applications. The advantages offered by underground facilities (UGFs) in commercial applications are purely economic, while advantages for infrastructure protection depend on the application and involve more factors than simply cost per square foot. From a commercial perspective, Mr. Woodard emphasized, UGFs compete quite well against surface facilities. The experience in Kansas City shows that existing premined underground space is cheaper to build out and operate than above-ground space.

Mr. Woodard discussed several disadvantages of UGFs, acknowledging at the outset that some applications are not well suited to underground locations. For purposes of comparison, he made the point that a UGF can be thought of as a surface facility with a thicker roof. In this case, some underground locations pose problems with structural integrity and groundwater not encountered with surface structures. In addition, UGFs depend on the surface for some elements of their support, including communications, power generation, and ventilation. There is a security advantage to decentralization in any protection scheme. An underground protection plan where a single location becomes the critical hub would not be the best design. On the positive side, Mr. Woodard thought that UGFs offer definite physical security advantages. Life-cycle cost savings make them economically attractive for infrastructure applications, and UGFs can be a major benefit in reconstituting infrastructure capability following an attack.

Mr. Woodard emphasized improving public awareness of UGF capabilities for infrastructure assurance. He made a number of recommendations, which included:

- implementing a thorough study to foster understanding of underground capabilities vis-à-vis infrastructure protection needs;
- facilitating government-industry partnerships to provide R&D funding for underground applications. The Underground Developers Association has endeavored to do this, but available funding has been insufficient to sustain long-term research;
- creating a center for underground studies to examine and promote the use of UGFs and to attract new talent into underground disciplines; and
- considering requiring government at all levels to include underground locations as an alternative in their site selection process.

Infrastructure Protection in the United States: A Norwegian Perspective

Arnfinn Jenssen
Norwegian Defence Construction Service

Mr. Jenssen addressed the use of underground facilities (UGFs) for the protection of critical infrastructures from a Norwegian perspective. He presented Norway's extensive experience with UGFs, including 200 hydropower stations, thousands of diesel generators, and one nuclear power station. He encouraged the primarily American audience to think in larger terms, challenging people to consider a crisis situation where 10, 100, or 1,000 buildings are at risk. The Oklahoma City bombing involved only one building.

He addressed several important issues:

- *Needs and requirements.* Food, clothing, and shelter were described as primary human needs, which must take first priority.
- *Legislation, protection, and organization.* Make participation in a total defense system compulsory where a condition for businesses is to protect their critical assets and keep a certain amount of goods and spare parts in stock (e.g., 10 to 30 percent).
- *Hardening.* Look at hardening in the broadest possible sense, to include standoff, disbursement, supply from abroad, and so forth.
- *Force protection.* Armed forces must be kept at standoff distances from potential terrorists. Trucks and cars must not be permitted to come close to a building that houses critical assets.
- *Use a generic, future threat.* Use a generic threat for planning purposes, not the current or approved threat. The approved threat is always old and lags behind the future threat. Changing an approved threat can be difficult, especially in NATO.
- *Design facilities for multipurpose use.* Design UGFs for many purposes. This means they may have to be large.
- *Use manual backup systems rather than computer-controlled backup systems.* Newer computer-controlled systems are more vulnerable than older manual systems. Knowledge of the architectural and engineering design of a UGF can facilitate an attack, thus making a facility more vulnerable. The most vulnerable part of an underground system is the air duct/air conditioning system.
- *Design UGFs that use water for internal climate control.* If climate control is maintained by a forced-air system instead of water, this is a built-in mechanism that can transport chemical and biological agents and other hazardous and toxic substances throughout the facility.
- *Keep control of personnel and vehicles.* Have daily checks and searches.
- *Role of the private sector.* Do not tell the private sector how to run its business but make use of it in time of crisis and war, without changing company

organizations. Give private-sector companies specific tasks that must be fulfilled if they want to stay in business. This has been done through legislation in Norway.

The question-and-answer session emphasized that infrastructure assurance requires diligence and, perhaps, elements of a program similar to that in Norway to cover these problems. Mr. Jenssen noted that going underground is not the only solution to infrastructure assurance and that it must be looked at from a much broader perspective. Since industry does not want more regulation, one option would be a simple declaration that, if judged to be a critical infrastructure element, there must be an alternative or a protected system. The government could conceivably subsidize that portion—whether it be underground, mobile, or disbursed. Mr. Cicolani observed that AT&T's program involves a mobile backup system for their switching centers. Mr. Jenssen agreed that a government policy is absolutely necessary and must start from the top. The nation must be made aware that protection of its critical infrastructures is necessary.

Panel Discussions

PANEL 1: INFRASTRUCTURE PROTECTION ISSUES

Moderator: George Baker, Springfield Research Facility Defense Special Weapons Agency

James Werth Federal Bureau of Investigation

Mr. Werth provided a brief history of the FBI's involvement in infrastructure protection in the United States. In 1992 the FBI created the National Computer Crime Squad at its Washington, D.C., field office. Since then, the number of computer intrusions investigated by the FBI has increased significantly, resulting in the establishment of regional computer squads in New York and San Francisco in 1995. Other computer squads were then established in Boston, Atlanta, Dallas, and Los Angeles, and computer investigative teams have been established in 56 field offices throughout the United States.

Expansion of the national computer crime squads was accompanied by creation of the National Security Threat List (NSTL). Addition of the NSTL made it possible for the FBI, working within its foreign counterintelligence program authority, to investigate infrastructure-related incidents perpetrated by foreign intelligence services. These attacks might be directed against the U.S. government, corporations, establishments, or individuals. Targets could include physical facilities, personnel, information, computers, cables, satellites, or telecommunications systems. Attackers range from teenage hackers to members of organized crime to domestic or international terrorists to individuals or groups intent on sending a political message by misinforming or disrupting or denying service. Also, foreign intelligence services may attempt to obtain proprietary data or sensitive government information.

These computer squads were responsible for criminal, investigative, and national security implications of computer intrusions. In 1996 the FBI created the Computer Investigations and Infrastructure Threat Assessment Center (CITAC) at FBI headquarters. CITAC operations encompassed counterterrorism, foreign counterintelligence, and law enforcement. CITAC was made up of the two operational investigative divisions of the FBI and focused on potential threats and assisting authorities with warnings and technical support.

In the interim between the establishment of the President's Commission on Critical Infrastructure Protection (PCCIP) and presidential action on the matter of infrastructure protection, the FBI has been designated as the chair of the Infrastructure Protection Task Force (IPTF). The IPTF is an interagency body charged with the coordination and management of

infrastructure protection. In July 1997 the Office of Computer Investigations and Infrastructure Protection was established to bring computer intrusions and infrastructure protection under one umbrella organization at the FBI that would continue to report to the national security and computer investigations divisions.

Establishment of the National Infrastructure Protection Center (NIPC) by the FBI in February 1998 will facilitate a government-industry partnership by providing mechanisms for assessing, warning of, investigating, responding to, and preventing attacks on our nation's critical infrastructures. The NIPC incorporates and expands the mission and personnel of the FBI's former computer investigations and infrastructure threat assessment center, the CITAC. The NIPC is an interagency public-private partnership comprised of representatives from the FBI, U.S. Department of Defense (DoD), the intelligence community, other federal departments and agencies, state and law enforcement groups, and private industry. NIPC's critical objectives are:

- investigations of incidents,
- emergency responses to incidents,
- coordination and application of technical tools,
- analysis and information sharing,
- monitoring and warning,
- providing training and continuing education,
- conducting outreach and providing field support.

Mr. Werth noted that the number of pending investigations that represent many major potential national and economic security risks to the United States has increased. The investigations involve exploitation of technologies that threaten both the public and the private sectors and that are both national security and criminal in nature. Investigative cases and successful prosecutions also have increased. In fiscal year (FY) 1997 the FBI noted the following changes:

- a 120 percent increase in pending cases (from 263 to 453 cases); a 254 percent increase from the beginning of FY 1996 (from 128 to 453 cases);
- a 950 percent increase in arrests in cases involving cyber-intrusions; and
- an 88 percent increase in convictions.

Mr. Werth identified the following future FBI initiatives:

- increasing the number of computer crime squads at field offices throughout the United States;
- improving the ability of computer squads to analyze and respond to conflicts and threats to telecommunications and information systems;
- developing technologies that assist the NIPC in responding to high-technology investigations;

- developing watch and warning capabilities for threats to the nation's critical infrastructures, with real-time alert capabilities for both the public and the private sectors;
- coordinating and developing a trusted communications network for the exchange of threat and warning data with government and the private sector; and
- operating the NIPC program at full speed by October 1998 (Michael Vattis will be the director).

Robert Minehart Army War College

Mr. Minehart' s presentation focused on the issue of infrastructure protection in the future. He began by crediting the PCCIP with defining the issue of infrastructure protection and information warfare, which would have been very difficult to do just three years ago. Mr. Minehart said that he would present some findings to support an argument for using underground facilities (UGFs) for the protection of critical infrastructures.

Mr. Minehart has helped the Army War College develop advanced courses on information warfare. In February 1998 infrastructure owners participated in a war gaming exercise that showed that the infrastructures the government must protect are owned primarily by commercial entities (63 percent of the participants were infrastructure owners). Owners and operators at this exercise were adamant that the responsibility to protect the infrastructures was theirs. Except for government regulations that are already in place and that must be enforced in the areas of detection and the disclosure of attacks, private owners had a knee-jerk response against the imposition of more regulations or being told how to conduct their business. They stressed that industry is completely focused on meeting customers' needs and that government regulations would inhibit their ability to be responsive to their customers.

Mr. Minehart cited an example of the variety of threats facing infrastructure owners. In March 1998 two teenagers in California broke into government and DoD databases. About two weeks later, it was learned that they had received help from a mentor in Israel known as "The Analyzer," whom they had met via the Internet. Many computer hackers have outsiders helping them and the identities and affiliations of these mentors cannot always be determined. The threat posed by mentoring networks and their supporters is an issue that requires evaluation.

As systems become more secure against outside threats, adversaries will look for other ways to break in. If a network is difficult to hack into from the outside, whether because of a fire wall or isolation, an easy way to gain access to the system is to recruit someone on the inside. Training workers to be aware of this possibility can be difficult. Individual infrastructure owners do not have the money, time, or resources to monitor such threats, from a foreign

intelligence service for instance. A policy of requiring polygraphs and rejecting workers on the basis of the results is difficult to implement in the private sector. Even though the screening programs used by government for classified programs have proved to be effective, industries have had a hard time adopting similar screening processes.

Turning to the issue of UGFs, Mr. Minehart suggested that the workshop participants consider an attack on a large manufacturing company that relies heavily on robotics and CAD-CAM (computer-aided design, computer-aided manufacturing) machines. The attackers would first corrupt the backup system. Once they have corrupted every tape in backup, they would attack the main system and delete all the programs that automate the machines. All of the machines would simply stop working and the cost to reprogram them would be enormous. In a coordinated strategic attack the first targets would be the backup databases, and they would be corrupted in a way that was not immediately detectable. The World Trade Center attack showed that many companies have built-in backups, but they are kept in the same building. In fact, backup services may be contracted to multiple customers in the same building. The upshot is that in an attack the backup service either cannot restart everyone at once or the backup service also would be attacked.

Mr. Minehart noted several potential benefits that UGFs offer for system protection:

- *Physical access is controlled.* Controlled-access areas prevent casual access to systems.
- *Workers are well trained.* Workers in secure facilities are generally well trained to understand and respond to threats.
- *System architecture is protected.* After a physical attack, whether it be a sprinkler system going off or an explosion, the way a system is designed or a network configured is just as important as the data on it. Having the system architecture well protected is critical to returning to operation. UGFs can provide this protection.

One of the challenges to using UGFs or any remote backup facility is finding a way to secure data, so that only the owners have keys. This would protect the data and provide security to both the information owner and the storage provider. On balance, UGFs offer a potentially interesting and useful approach to meeting the needs of both industry and government.

John Reingruber Office of the Assistant Secretary of Defense Special Operations and Low Intensity Conflict

Mr. Reingruber noted that because the workshop had an unclassified forum, he could present very little information about deep underground (DUG) facilities. Instead, he focused on threats to infrastructures in general terms. The good news, he said, is that the probability of a terrorist attack on a DUG facility is quite low. Therefore, he could state that a DUG facility would be a very effective foil to terrorist attacks. Mr. Reingruber acknowledged that some of his colleagues might disagree with him, but he believes that terrorists would be more likely to look for an easier target.

In a global sense, terrorism now includes acts by both criminals and disaffected employees. Traditional terrorists have had political motives and used terrorism to influence peace-loving governments. Ad hoc terrorists, however, may be trying to make a personal statement, such as showing their anger at an oppressive government or a former employer. No terrorist, however, will select targets that are very difficult to bring down. A DUG facility, for example, would only be attacked during a war.

Mr. Reingruber identified several factors that must be taken into account in considering the use of UGFs for the protection of critical infrastructure:

- *Threat.* The threat is a function of capability and intent. The capability to disable an infrastructure does not mean that the infrastructure is threatened. Capability must be coupled with intent to do harm.
- *Cost.* Does the threat to the infrastructure justify the cost of protecting it, and who is going to pay to protect it?
- *Effect on the American psyche.* Americans would reject the idea of building a "Fortress America." Therefore, we can protect some infrastructures using DUGs, but the costs of protecting all of them would be astronomical.
- *Other options.* The first obvious option is to increase security measures to protect existing infrastructures. A second option would be to design infrastructure architectures that are less vulnerable to terrorist activities, such as, supervisory control and data acquisition (SCADA) systems that are designed to mitigate the effects of attack. The design philosophy of SCADAs builds in fire walls and redundancy. A third option would be to reconsider which of our infrastructures should be made invulnerable (e.g., national security information.) Hackers who breach national security systems should be punished, but sabotage by an insider remains a risk.

Mr. Reingruber described the group he cochairs, the technical support working group (TSWG), which conducts the national interagency program for combating terrorism and coordinates government R&D. One of the eight subgroups of the TSWG is the infrastructure protection group, which is

currently developing a capability road map that will recommend useful projects in the area of infrastructure protection that can be funded over the next few years. The road map is being developed by Booz Allen, Inc., and will be ready in June 1998. Although the TSWG will probably not have an effect on big architectural schemes, it could influence some aspects of infrastructure protection.

Raymond Daddazio Weidlinger Associates

Dr. Daddazio described Weidlinger Associates' involvement with UGFs and infrastructure protection as well as the central artery project in Boston. The company has developed analytical methods for hardened underground structures in particular and UGFs in general, for both the military and civilian sectors. Many of Weidlinger's projects in the field of protective structures involve blast-hardening conventional buildings, and Dr. Daddazio outlined some of the differences between the protection afforded by UGFs and modified above-ground structures and suggested that a case could be made for protecting infrastructures in shallow-buried facilities.

He identified cost as a major factor in the decision to locate facilities underground, particularly in a densely populated urban area. These costs include:

- *Buried utilities.* Municipal electrical and telephone lines are sometimes as shallow as 18 inches, water supplies are typically located below the frost line, and sewers are generally a bit deeper. These utilities must be moved or protected during construction.
- *Trenching and backfill.* The major costs of putting a distributed system underground are excavation and backfill. The cost curve from a 4-foot trench to an 8-foot trench is not linear (i.e., unit costs increase more rapidly with depth). Other costs include sheet piling and protecting construction workers.
- *Safety and maintenance.* Stringent Occupational Safety and Health Administration requirements, shoring and underpinning of adjacent structures and utilities, and maintenance of existing utilities during excavation and repair all add to the cost of burying a distributed system.
- *Geology.* The cost of burial can be complicated by geological conditions, such as groundwater and rock.

An above-ground building is a more centralized system. The following measures designed to protect buildings from large vehicle bombs and small external devices can add to the costs:

- *Glazing protection.* Flying glass is a major cause of injury in an explosion. Putting films or blast net on glass may reduce the danger of flying glass.

- *External site planning.* Most buildings are located on sites about twice as large as the floor plan of the building itself. This extra area can provide standoff distance, room for defensive bollards, and reduced access to the site (the White House is a example of this approach).
- *Facade detailing.* Generally the amount of glazing should be minimized to reduce cost.
- *Internal planning.* Critical internal areas such as control centers and utility rooms can be blast-hardened. Such structural hardening requires the use of additional structural steel and reinforced concrete; internal walls also can be constructed of reinforced concrete to minimize the vulnerability of critical systems.

In a typical seven-story, 100,000-square-foot building constructed to the specifications of the General Services Administration (GSA), a reasonable level of blast protection would increase the cost of the building by 8 to 10 percent for these types of structural considerations. About 60 percent of the cost increase is for glass and glazing, either for films or higher-quality laminated or tempered glass.

Locating a building or a critical system underground can reduce the need for and cost of blast hardening. With the exception of physical site planning, all other protective measures are minimized or eliminated for a UGF. There are no glazing or facade issues, and the internal planning considerations will be the same. A less robust underground structure would be required to provide a similar level of protection as a hardened above-ground facility because of the energy attenuation offered by the soil cover and backfill material. Simple reinforced concrete burster slabs also can be used to protect underground structures.

Dr. Daddazio concluded by stating that the protection of infrastructures by UGFs has advantages and disadvantages:

- No single issue, either financial or physical, should preclude the use of a UGF for infrastructure protection.
- Every application must be considered individually from a risk and cost standpoint.
- Locating critical infrastructures underground, especially a centralized system, should always be considered an option.

Questions and Answers

Dr. Baker began by asking the panelists to identify the benefits they thought UGFs offer against cyber-threats. Mr. Daddazio noted that the PCCIP report had described the most effective terrorist threat as a combination of cyber-terrorism and a physical threat. A cyber-threat coupled with a well-placed

physical attack against a target could be very damaging to an infrastructure. Therefore, locating electrical substations, for example, in remote areas or underground could definitely offer protection. Mr. Werth questioned whether a UGF in itself would serve as a defense against a cyber-attack, because if communication went out at three or four different points in the system, the entire system would be vulnerable. But he agreed that attacking a UGF would require a highly sophisticated operation. There are good reasons to vary the locations of infrastructures to defend against physical attacks.

Mr. Minehart restated the importance of backup systems and of storing data in locations separate from operations. The expense to industry could be prohibitive, but if government provided a location where backup electronic tape could be held safely and protected with cryptography, a coordinated attack that would place backup data at risk would be much more difficult. The costs to industry would be reduced and a national asset—UGFs—would continue functioning for a new protective purpose.

Dr. Sevin observed that UGFs make the design process more manageable, greatly easing the job for architects, engineers, and security design professionals. The potential for injury and death to personnel is decreased, and recovery in the event of an attack is improved. The UGF presents a difficult target and probably directs the attacker to a less secure site elsewhere. So UGFs may provide a cost-effective solution along with other advantages.

Mr. Jenssen did not agree that all UGFs are difficult to attack. If they are badly designed, they are easy to assault; if well designed, a strike is difficult. There is a vast difference between good and bad designs, and experience is required to ensure a strong design. Mr. Cicolani concurred with Mr. Jenssen's observations. The Springfield Research Facility has reviewed many poor designs for UGFs worldwide, and its conclusion is that poorly designed facilities are fairly easy targets.

Dr. Baker observed that the PCCIP also identified specific physical threats, including high explosives; small-scale nuclear weapons; chemical, biological, and radiological agents; and electronic weapons designed to attack computer-based systems. Mr. Reingruber said it is difficult to guard against all potential threats and that efforts to rank threats by importance may not be productive. Explosives are still the weapon of choice for terrorists, but there is concern that this will not always be the case. Weapons of mass destruction could be a greater problem in the near future. Dr. Sevin countered that from a design point of view threats will have to be prioritized because comparable design solutions cannot be made for a small truck bomb versus a nuclear weapon. Dr. Daddazio pointed out that a blast engineer would rely on intelligence or statistics from government agencies to help determine the design threat for physically protecting a facility. At present, the greatest danger remains a conventional weapon, and this is the area in which most efforts toward a solution should be directed.

Mr. Ryall emphasized the hazards posed by fire and smoke in UGFs. An arsonist can breach the security of a UGF and start a fire, especially one that

generates a great deal of smoke, and can take down a mission. Many people could be killed in an event that appeared to be an accident.

Mr. Smeallie, who is experienced with embassy security, noted that no glazing or facade treatments are required in unoccupied buildings (e.g., electrical substations), and questioned whether the 60 percent increase in glazing costs cited earlier was a realistic figure. Dr. Daddazio responded that even if glazing and facade requirements are eliminated, the hardening costs in a typical $100-per-square-foot, 100,000-square-foot GSA office building are 8 to 10 percent above the cost of a building without hardening. Reinforced concrete walls above ground will necessarily be thicker than the walls in a UGF. An above-ground building would have to be more strongly constructed than one below ground, but this would be offset by the additional costs of building a structure underground. He emphasized that overall this is a site-specific issue.

Dr. Baker questioned the technological sophistication of the individuals and groups that pose threats to this country's critical infrastructures. Mr. Werth responded that most groups are not highly sophisticated when it comes to UGFs. While that may be a good reason to investigate UGFs and their advantages, he cautioned that a cyber-attack on UGFs was certainly possible. Dr. Baker also asked whether the panel thought UGFs would help reconstitute systems after a cyber-attack. Mr. Minehart concurred that any structure that had been hardened would be critical in such a case.

Dr. Baker concluded the question-and-answer period by noting that a controversial issue in the infrastructure community is whether or not protecting systems can be a deterrent to attack. Dr. Daddazio stated that a mix of solutions should be available for those facing potential physical threats against their infrastructures. Owners and operators must be aware of threats from the very beginning of the process; sometimes a small investment can be made in up-front planning that can ultimately result in large savings. Mr. Reingruber agreed that there is a deterrent value to protected systems, but noted that, if an attack is diverted from one target, it most likely will carried through against another. Mr. Werth agreed that, while deterrence may be enhanced by putting key infrastructures underground, a high priority must be placed on educating employees to be more aware of how infrastructure can be protected.

PANEL 2: NEEDS AND REQUIREMENTS OF THE INFRASTRUCTURE COMMUNITY

Moderator: Richard G. Little,
National Research Council

Michael Brandenburg AT&T

Mr. Brandenburg described the ways in which AT&T has used either underground placement or underground construction to protect vital company systems. Many of these facilities presently have available capacity since today's equipment is much more compact than earlier systems. He then detailed the use of UGFs to support a major DoD communications program as one strategy for protecting critical systems. A second strategy is a robust program for patching and routing around network problems. A third is development of mobile assets for emergency response.

Mr. Brandenburg noted that AT&T has been burying cables (i.e., critical infrastructures) for over 100 years. At the height of the Cold War, AT&T maintained 20 key switching centers for DoD's Automatic Voice Network (AUTOVON) in hardened 25-foot-deep underground sites. The AUTOVON network also contained hardened buried cable routes. The buildings housed noninterruptable power supplies, emergency generators, and emergency provisions. These structures are still in place but are underutilized. AT&T continues to work with buried cable routes and has in place the largest fiber optic network in the United States. The company has mechanisms, including computer-controlled restoration systems, for quickly patching and routing around any switches that go out of service. AT&T's strategy also allows it to field mobile assets that can respond quickly to an emergency. The company maintains a fleet of large semitrailer trucks with telecommunications equipment at strategic locations across the United States. These mobile assets can be deployed in hours and have been used over 20 times in the past four years.

Mr. Brandenburg explained the ways in which AT&T might respond to a problem in the context of risk assessment and management and noted that organizations need to conduct a risk assessment to determine their vulnerabilities. AT&T carries out such exercises four times a year. In closing he pointed out that UGFs are just one of many tools available that can help protect critical infrastructures.

Paul Rodgers President's Commission on Critical Infrastructure Protection

Mr. Rodgers began his remarks with a historical account of how ancient cultures used UGFs. History provides a solid precedent for the use of UGFs to protect critical infrastructures against natural disasters, the explosion of

bombs, and the deployment of weapons of mass destruction. The existing surplus of UGFs today represents a huge investment that should be relatively inexpensive to occupy, operate, and maintain for new purposes. The vulnerability of critical infrastructures has grown markedly in recent years as a result of a number of factors, including increased competitive pressures from deregulation and globalization and the use of information technologies to improve competitiveness. Another element is the widespread concentration of operations for many organizations in a smaller number of facilities to decrease costs. This has resulted in less redundancy and reserved capacity. Together these trends have created vulnerabilities where none previously existed. Until now, these infrastructures have been protected from attack by distance, effective defenses, and the near certainty of retaliation. Adequate parallel capacity has usually been available as assurance against all but the most serious outages.

Today, the computers that control critical infrastructures can be attacked through the Internet from any point on the globe. Military forces are not organized or deployed to defend the nation's vast infrastructures from physical and network-based sabotage. The threat of retaliation is less effective against small and elusive groups that strike anonymously and have no territory to hold at risk. Clearly, the owners and operators of today's infrastructures should assess the risk to their physical facilities and determine whether placing critical facilities underground is appropriate and cost effective. Prime candidates for this kind of protection are the supervisory control and data acquisition (SCADA) systems and other computer processes and their backup facilities for use in emergencies. These systems work from a remote location to monitor, maintain, and manage financial services, electric and gas systems, petroleum product pipelines, telecommunications, transportation operations, and a host of other infrastructures.

The U.S. banking and finance infrastructure is the most advanced and robust in the world. Critical aspects of it are the key funds transfer and messaging systems, and the securities and commodities exchanges and their supporting clearing, settling, and depository infrastructures. The New York Stock Exchange, because of its prominence in the financial community and its close identification with U.S. capital systems, is an attractive target for a physical terrorist attack. As illustrated by the 1993 World Trade Center bombing, which caused many Wall Street firms to add backup locations, there is a need for contingency data systems, centers for key systems, and trading locations for the exchanges that can survive such attacks. Surplus UGFs would be a cost-effective means to enhance security. The use of remote secure locations would eliminate the risk of concentrating resources in one place.

The electric power system is critically important to the operations of all other infrastructures in the United States. Electric power uses the ultimate just-in-time delivery system, since electricity cannot be stored at the point of consumption but must be used at the time of delivery. Unfortunately, electric power is also our most vulnerable infrastructure because of the multitude of above-ground, high-voltage transmission lines and towers that crisscross the

nation. They are easy targets that cannot be defended on any kind of comprehensive basis. The United States will have to cope with this vulnerability until such time as it may become technologically and economically feasible to place them all underground.

The practicality of building electric generating plants underground should be assessed, particularly those to be constructed under the new concept of distributed generation, owing to the abundance and low cost of natural gas. This concept includes the construction of small electric generating plants close to the customers they serve. The natural gas and petroleum industry has 1.4 million miles of pipelines that are already underground, except where they are suspended above ground for major river crossings. Many key assets are above ground, such as control and processing centers, pumping and compressor stations, refineries, storage facilities, and receipt and delivery points. The need for and economic feasibility of placing critical facilities underground must be examined, especially in the case of new construction.

The U.S. telecommunications industry alone generates more revenue than most nations produce. The potential of explosive, chemical, and biological attacks against the country's telecommunications infrastructure has increased, as service providers have concentrated operations in a smaller number of facilities. Remote access technology has reduced the number of staff facilities needed to operate the network. New technology also permits cost-saving consolidation of switching equipment and transmission paths. Consolidating network control in central offices and megacenters lowers building, real estate, and labor costs. Key assets, such as switching facilities, should be reviewed to determine whether placement of existing or planned installations underground would increase their security. A 1988 fire in Hinsdale, Illinois, demonstrated the widespread and long-standing effects associated with the destruction of a major telecommunications network's switching facility. Half a million customers lost service, air traffic control at O'Hare International Airport was disrupted, and ATM banking networks were shut down. Full recovery required installation of a massive new switch, a process that took several weeks.

Another means for assuring the operation of our critical infrastructures is to stockpile replacement parts needed to restore service and antidotes to chemical and biological attacks. Here, again, UGFs should be considered as alternatives in the selection of secure and convenient locations for stockpiling.

Mr. Rodgers concluded by observing that there is a compelling case for increasing the use of UGFs to protect critical assets. Existing facilities represent a huge investment by the public and private sectors, such as federal and municipal UGFs, mines, missile sites, and tunnels that have been abandoned, and many are available for multiple uses. In the interest of carrying forward the national infrastructure assurance program, Mr. Rodgers stated his personal view that a federal agency should be designated as the matchmaker to inventory available UGFs, identify the terms and conditions governing occupancy, and promote their use by those seeking to protect critical facilities. The American Underground Construction Association should be helpful in this regard, since its goal is to promote the development and use of UGFs.

Daniel Schutzer Citibank

Dr. Schutzer focused his remarks on the threats to and current operating environment of the financial services industry. Of all the daily financial transactions in the United States, only about 5 percent can be termed on-line, but by the year 2000 that figure could reach 15 percent. On-line brokerage transactions may be as high as 25 percent but the bulk of financial transactions today are still face to face and paper based, approximately 80 percent of 350 billion transactions a day. Approximately 15 percent of all transactions represent paper checks, and 5 percent are credit card and other on-line transactions.

The advantage of using the Internet and on-line capabilities is that they are global and can reach anybody with appropriate access equipment. The Internet's disadvantage is that it is a very attractive target because it is widely distributed. Loss of privacy and identity theft also are serious issues today. Much work in the financial services industry is done remotely, so it has large problems in terms of authentication.

Another key point raised by Dr. Schutzer was that financial institutions are service providers that do not really control their environment. Their users, whether they are companies or individuals, select the access devices of their choice. These access devices are general purpose (and include personal computers, workstations, telephones, hand held devices, and television sets.). This technology is open and widely known and is available over public networks. The problems that are paramount here are loss of privacy, fraud, and identity takeover. Attacking the system by flooding communications lines and thus denying customer service is an additional concern. This is rapidly becoming a global concern because temporary cash-flow imbalances can cause businesses to fail.

Dr. Schutzer also discussed security and the integrity of transactions. As money is spent on security, performance slows and inconvenience rises for customers. Customers are less likely to accept this situation. This is critically important because "point-of-sale" cryptography is not yet available, and although financial institutions will not pay for such security now, they will make up for it in processing costs. The financial services industry will not provide as much security on the retail side as it will in other areas. In this way the losses can be absorbed rather easily at present.

The financial services industry is concerned about making sure services are up and available at all times. There are some backup facilities and alternate sites. Multiple alternate sites located both in the United States and in other countries are a part of the industry's security strategy. This includes backup power and alternate providers and routes. The industry does not make widespread use of UGFs, except for the storage of documents and tapes. Instead, it worries substantially about the activities of insiders and emphasizes intrusion detectors and anomaly detection among the tools for identifying attacks and

intrusions. Biometrics, sophisticated passwords, and other high-security tools also are being used.

Michael Shannon Oklahoma City Fire Department

Mr. Shannon spoke about the difficulties encountered by rescuers when entering a damaged facility. Hazards, risk, and protection all play a role in how help can be rendered when needed. A structure that is heavily compartmentalized can better survive a fire, but escaping such a structure can be a problem for rescue operation teams.

One person's protective measures are another person's obstacles, and the same defense mechanisms for protection from attackers can also keep rescuers out of a structure. There is a trade-off between knowing about hazards and developing acceptable protective measures to mitigate them. It is absolutely essential to address protective measures in either above-ground or underground construction during the engineering design process.

The controlled environment within UGFs is advantageous. UGFs face the problem of access points becoming possible avenues for an attack, but proper engineering can mitigate the impact. Even when attacked, UGFs still their structural integrity. Protective measures should be based on risk analysis and on the specific hazards identified.

Mr. Shannon recounted his experience supervising rescue efforts in Oklahoma City after the bombing of the Murrah Building and some of the special problems faced by rescue teams there.

Questions and Answers

Mr. Little opened the question-and-answer session by summarizing the viewpoints expressed by the panelists. UGFs are essentially a physical solution to a problem, but there is debate as to which infrastructure vulnerabilities are physical issues. He alluded to Mr. Brandenburg's discussion of choosing between hardening and mobility for increasing the survival rate of an infrastructure. In the banking industry, very few threats are directly physical, although there is a need for better backup facilities. The question is to what extent these backup facilities need to be located underground. Mr. Rodger's comments made it clear that there are sectors of the energy industry for which physical solutions are necessary and that users and suppliers must be brought together. Finally, Mr. Shannon urged that these facilities be engineered with rescue and recovery in mind. Mr. Little highlighted the enormous need for coordination between service providers and the infrastructure community for development of the physical solutions to infrastructure protection problems.

Mr. Brandenburg noted that AT&T has underutilized UGFs and that AT&T's attempts to interest federal agencies in them have met with limited success. Mr. Rodgers stated that one PCCIP recommendation was that critical infrastructure owners and operators in the private sector conduct periodic vulnerability assessments; this could lead to greater interest in UGFs. A federal matchmaker could catalog underground capacity and promote its use when economical and feasible. Mr. Schutzer mentioned two key issues for the financial services industry: many critical facilities are unmanned and can be checked out from remote locations, and such facilities must be connected to the outside world.

Several questions were raised concerning the psychological impact on workers of being in underground buildings. Mr. Brandenburg said that going underground has never been a significant personnel issue at AT&T; he noted that there is an awareness of heightened security among those working in an underground environment. Mr. Shannon commented that not everyone is comfortable working underground and that those who do must understand the changes it will require.

Other questions focused on how to safely communicate information on vulnerability and reduce the number of critical local points where assets are at risk. Mr. Schutzer stated that the financial services industry generally shares criminal alerts, particularly for money laundering, computer intrusions, viruses, and fraudulent activities. There are well-established connections between banks, financial institutions, and federal law enforcement institutions, such as the FBI. Systems can also be run outside the United States to increase security. Mr. Brandenburg added that AT&T also participates in computer emergency response teams. He noted, however, that the competitive marketplace has real barriers in place that inhibit the exposure of unique operating systems; some proprietary information will not be shared. In answer to another question concerning attacks against both primary and secondary switches, Mr. Brandenburg responded that, although he did not know if that particular scenario has been evaluated, AT&T has 130 switches throughout the country, and thousands of software and database changes are occurring daily.

PANEL 3: EXPERIENCES WITH UNDERGROUND FACILITIES: CAPABILITIES, LIMITATIONS AND APPLICATIONS

Moderator: Angelo Cicolani,
Springfield Research Facility, Defense Special Weapons Agency

Angelo Cicolani Springfield Research Facility

Mr. Cicolani presented a history of UGF use for defense purposes in which they were likened to DoD structures built for protection against an acute threat, such as conventional weapons, nerve gas, or nuclear weapons. The idea that UGFs could be used for infrastructure protection against terrorist threats is now beginning to get more attention. The threat against infrastructures is pervasive and it is difficult to know where it will originate. However, UGFs are useful for nonprotective reasons as well.

Mr. Cicolani gave several examples of how hardened UGFs have been used throughout history and explained that an attacker will go to extraordinary lengths to destroy, capture, undermine, or neutralize a hardened facility. The history of underground and hardened facilities is represented by centuries of conflict between the defender and the attacker. Examples include:

- *Massada.* In ancient times, a group of 900 Palestinians protected themselves from the Roman army on a plateau called Madder, a facility that still exists today. The men, women, and children—not all of whom were fighters—held off 15,000 Legionaries. The Romans developed a special battering ram to attack the structure.
- *Middle Ages.* Fortresses played a significant role in protecting their masters in the Middle Ages and often included underground tunnels.
- *World War II defensive structures.* There are several examples of World War Il-era underground defensive facilities. The French constructed the 235-kilometer Maginot Line to stop any possible German invasions. It included defensive bunkers that were six or seven levels deep and stored ammunition, bunking, messing, emergency supplies, electric generators, and other essentials. A very large defensive structure was built on Gibraltar from which the allies could control the entrance to the Mediterranean Sea. It also provided a platform to mount attacks against Nazis in the area. It included miles of tunnels and hospitals, ammunition storage, ship supplies, repair shops, workshops, and headquarters space.
- *World War II industries.* During the war, the Germans began to use worked-out mines to relocate some of their military industries because of intense allied bombing. They were also trying to build weapons of mass destruction underground. The V-2 missile was assembled and launched from an underground facility with a hardened concrete dome 5-meters thick. In addition

to the V-2 launch sites, many of the German submarine pens also were hardened. The allies developed 12,000-to 22,000-pound bombs to attack such hardened facilities.

- *Cold War era.* In the Cold War era, the Swedes deployed soldiers underground—a Scandinavian response to the probable exchange of nuclear weapons between the Soviet Union and the United States. These facilities were similar in design to fallout shelters. Sweden publicized its reasons for going underground, and Scandinavia in general developed a defense-oriented underground construction industry. Consequently, there was a great deal of momentum for this program and an infrastructure for underground construction. After having met defense requirements, the Scandinavians had an industry in place that could work for two purposes. Consequently, there are many UGFs in Scandinavia that have nothing to do with defense. Some were built in response to aesthetic, environmental, or space utilization issues. Specific examples include UGFs for air traffic control; telephone exchange; sewage and wastewater treatment; and storage of solar-heated water, archived material, oil, food, and radioactive waste.

Mr. Cicolani stated that the only countries that have significantly utilized UGFs beyond defense purposes to include critical infrastructures have been Norway, Sweden, and Switzerland. These countries have significant UGF programs and are eager to share their expertise and experience. Should the United States find compelling reasons for using UGFs to protect critical infrastructures, there are lessons to be learned from the experts in these countries.

Paul Ryall, ENSCO, Inc.

Mr. Ryall opened by noting that he had recently retired from the Air Force as a civil engineer. He spent four years as the director of Public Works for Base Civil Engineering inside the Cheyenne Mountain Complex (CMC) and was instrumental in implementing the Cheyenne Mountain upgrade, which consisted of replacing the Integrated Tactical Warning and Assessment System. It began as a $1.8 billion program, which grew to $2.1 billion by project end, and took 13 years to complete.

Mr. Ryall discussed the CMU in significant detail. The assessment of missile, air, space, space control, intelligence, and all the other systems, including drug interdiction, had to continue while Cheyenne Mountain computers were upgraded from early 1970s technology to late 1980s technology. Additionally, the CMC complex has various commercial customers, making it a dual-purpose facility. Key considerations taken into account during the CMC upgrade included:

- *Utilities.* Ensuring that the utilities and support remained operational throughout the mission and that those putting in new systems, utilities, and HVAC were allowed to test their systems to bring them up on schedule.
- *Planning.* Making certain that initiating a new mission was well planned through constant interaction and communication with all members involved. Meetings were sometimes held on a daily basis.
- *Security.* Assuring adequate security for both workers and visitors.
- *Environment.* Understanding the environmental processes that a new mission produces.
- *Government-customer interface.* Maintaining contact between government officials and customer representatives is imperative. If a customer is in the middle of a very critical operation and the power is turned off, it can cost millions of dollars.
- *Space requirements.* Never underestimate the amount of storage space needed by a customer. Make sure storage space requirements are known in advance.
- *Utility Load and interference.* When customers reduced their utility loads and required uninterruptible power, CMC had 7.3 megawatts of it and was able to meet the customers' needs. It must be clear where critical utilities are to be located.
- *Classified versus unclassified operations.* Red and black systems should not be mixed.
- *Other Support.* In a facility housing 800 people, the dining facility must maintain a close relationship with the food service contractor.
- *Modifications to an existing layout.* Rearranging walls is not as easy as it is in a soft facility. The customer may not understand all requirements, such as the need to maintain walls that have been hardened against electromagnetic pulse.
- *Resources.* An operator of a hardened facility must invest considerable resources to ensure that a new customer does not upset the existing operation.
- *Government design review.* Make sure there is an accounting for all possible drains on the operating budget; assure that contract termination expenses are considered.
- *Execution.* Coordinate on such items as schedule, safety, fire protection, security, notifications, daily shutdown, and after-hours notification. Other issues include escort for workers, waste removal, asbestos removal, and utility outages.
- *Daily operations.* Know the schedule; there will be changes, and flexibility will be needed. Consideration must be given to housekeeping, food supply, and appliances.
- *Special Periods.* Exercises will occur on a predictable basis. Coordination is important because a new customer may not participate in exercises. With respect to higher defense conditions, contracts should very plainly state that at a certain defense condition (DEFCON) level a contractor's operation ceases and the contractor must depart the facility.

Mr. Ryall concluded that initiating a new mission is very complex. There will be problems that cannot be anticipated. Daily activities will be disrupted, but the mission cannot be shut down nor can excessive governmental resources be expended. The primary mission always comes first and everything else is secondary.

Donald Woodard Underground Developers Association

Mr. Woodard began by noting that underground development in the commercial sector is fairly routine compared to the military and that its main competitor is above-ground facilities. With a background in engineering, Mr. Woodard has spent 20 years as an urban planner in the public sector. His view is that underground space provides a new third dimension for land use and density.

Mr. Woodard reviewed the history of commercial underground development in the Kansas City area. This region is ideal for underground development because of widespread limestone mines, and Kansas City has, in fact, pioneered commercial use of underground space. Initially, the real estate community in the area was not interested in underground development. There were no zoning ordinances, building codes, occupancy permits, or construction standards. There also were no taxation practices, government support, paved roads, power, or fire protection. Insurance was very expensive and virtually unavailable, and there was no bank financing. The few UGFs operating at the time were not built to consistent standards and leases were not marketable. Most important, there really were no clients of quality. Underground development was considered a novelty —an inexpensive place to use temporarily before moving onto the surface for a quality environment.

In some places, above-and below-ground uses are only a few feet apart, so there are conflicts concerning land use. In Kansas City, residents and industry on the surface constituted a problem, since plats above ground dedicated public rights-of-way and easements as part of property sales. The mining below the surface did not recognize these plats because most plats flow to the center of the earth and the top of the sky. So it became a question of who owned the surface rights and how the surface was zoned. The legal descriptions included in the plat and titles to the land had to be worked out before underground development could continue to grow and flourish. As permits and clearances were obtained, the concerns of banks and lawyers were satisfied and development prospects improved. Much is really owed to those who kept investing in the underground, despite all of the problems. Underground development was a secondary use for them; they had paid for the space when it was mined and they made a profit. Now they are collecting dividends and are again making profits.

Kansas City is now the most significant pioneer in the development and use of commercial underground space in the world, and people go there to study

the precedents established. These are the relevant facts about Kansas City's underground developments:

- Roughly 90 percent of the world's developed and leased commercial underground space is in the Kansas City area.
- Over 30 million square feet is leased at this time, and 2 million square feet is added each year. There is over 300 million square feet of mined space available there to develop. About 6 million square feet is added each year in new mining.
- There are 16 facilities around the metropolitan area, and 10 new underground developments are on the drawing board.
- There are about 50 businesses that operate underground in Kansas City now, with nearly 10,000 employees.

Mr. Woodard described several commercial underground facilities in the Kansas City area and noted that underground operators have developed their own marketing expertise. The Kansas City underground is just starting to attract tenants from industrial parks because of reduced costs that are reflected in rental rates. Mr. Woodard described the benefits to relocating underground:

- *Cost.* Annual energy costs are about 15 percent of that for a building operating on the surface, a tremendous savings.
- *Construction time.* UGFs can be built out in three to five months. There is no concern about the weather. Construction can be done on three shifts a day, if need be.
- *Location.* In Kansas City this provides a cost advantage. The mines are, for the most part, in the corridor of intensive surface development. Because mined rock is very expensive to transport, the available space is in the development corridor.

Mr. Woodard noted that an Underground Developers Association was established and organized mainly for mutual support. Forums were provided for surveys of underground space, publications, symposiums, and operating and development guidelines. Classes were held in underground developments. Construction guidelines were written in conjunction with the fire departments. Building codes were developed with the city, and Mr. Woodard personally wrote the zoning ordnance covering underground space for Kansas City. Issues were resolved with insurance companies and tax assessors, and UGFs were able to get favorable rates and financing. The jurisdictional authorities have promoted UGFs as a local resource. Environmental issues that have been raised have been well handled.

The success of the underground development industry with respect to surface developers is directly related to its ability to provide:

- a higher degree of security and safety;

- lower construction costs, lease rates, and operations and maintenance costs;
- faster delivery time;
- economy of operation;
- a better environment;
- innovative uses of underground space; and
- better locations relative to the market and psychological acceptance.

Foreign countries, such as Norway, Sweden, Japan, and even China, have an advantage over the United States in terms of experience with highly technical geological underground applications. But their developments rarely compete in the free market or with surface activities. Mr. Woodard proposed that a Center for Underground Studies be created and funded to promote the use and occupancy of underground space and the identification of UGF needs. Its jurisdiction may be national or international, and he thought approximately $1 million a year would be a viable starting budget.

Arnfinn Jenssen Norwegian Defence Construction Service

Mr. Jenssen emphasized that the basic needs for the survival of human beings are food, clothing, and housing. To provide these basic needs, modern society has created an infrastructure problem because we depend more and more on transportation, communication, information, monetary, and energy systems.

He stated that a first principle of civil engineering is to avoid problems. Norway learned this the hard way during World War II and managed to survive. Today, if important resources are lost or disrupted, it can result in a disaster. This was recognized by the Norwegian government and the Defence Commission, and in 1945 Norway began developing a total defense system that integrated military and civilian elements to prevent critical situations from developing into catastrophes. This was repeated from 1992 to 1993, but by then the program stressed cyber-attacks and disruptions to the banking system more strongly than physical defense.

Norway has established emergency requirements and organizations to address them. Mr. Jenssen advanced the Norwegian model, which emphasizes that critical infrastructures be protected by hardening against enemy attack, shelters be provided for the public, bomb damage repair be organized, and preparations to receive supplies from abroad be made. Service should be compulsory in the overall defense system. The emergency preparedness organization should undergo a minimum of changes from peacetime to wartime. In response to the Berlin crisis in 1948, all of these programs were implemented by legislation. Six main preparedness categories are considered by the Norwegian parliament every year: emergency, information, economic, medical emergency, police, and civil defense. The Norwegian Ministry of Justice takes

the main lead in this national organization. Civil defense is very well organized at the national, county, and municipal levels. Preparedness includes the following major areas:

- food supply (up to a 12-month supply is required for some goods; sugar, for example);
- water;
- sewer;
- environmental warfare (e g , attacks on a dam);
- clothing;
- shipping;
- energy;
- industry and trade;
- communications;
- telecommunications; and
- coordination of civil defense, information, radio, news media, police, and construction.

Mr. Jenssen provided significant details about Norway's use of UGFs. About 75 percent of the population has access to a proper shelter. Much of Norway's energy resources are stored underground. Norway has more than 200 underground hydropower stations, including transformer stations. Many petroleum, oil, and lubrication facilities, pumping stations, and gas stations also are located underground. In addition, water, fresh food, deep freeze, and cold storage supplies are stocked for several months, while telecommunications and air traffic control systems are protected underground as well. A few factories for ammunition and food are below the surface. The 5000-seat Norwegian Olympic underground ice hockey rink has a span of 62 meters.

In time of war, Norwegian contractors do not change their organization; they just change their hats. Provision has been made for the use of UGFs for war headquarters of political bodies, civil defense authorities, communications control, and road and rail authorities. If military or civilian activities need communications, today's modern equipment extends the range for many miles to the antenna sites. In Norway, UGFs exist for the army, navy, air force, and coastal defense but also for some of the NATO allies, such as the United Kingdom, United States, Netherlands, and Germany. Coastal surveillance is provided through retractable underground antennas and cameras. Missiles can be located above ground and then can be moved below the surface in eight to 10 seconds.

There are many dual-purpose underground installations in Norway. In peacetime, sports and swimming pools are used for recreation; in wartime they can be converted into a shelter or facilities for other purposes. In the city of Govik, a UGF houses an ice hockey rink, police and civil defense headquarters, and a telecommunications center. All of these facilities have sophisticated ventilation and heating systems. Finally, Norway's topography requires that it

make extensive use of tunneling technology. Norway has been constructing up to 75 kilometers of modern tunnels per year in the past 10 years. There is also extensive underground construction activity in the mountains.

Questions and Answers

Mr. Jenssen responded to several questions on the capital costs for above-ground versus below-ground structures. Using the average for all kinds of underground installations, the capital cost for a military facility underground is about 90 percent of that for an above-ground structure. There are at present about 3,000 military UGFs in Norway. On the civilian side, the difference can be greater. For a hydropower plant the cost is probably 50 to 60 percent of surface structures, while the operations cost is about 12 to 25 percent, much less for an underground than for an above-ground facility.

A question was posed from the floor concerning experience with fires, evacuation, and ventilation. Mr. Woodard said that there had been some experience with fires in Kansas City UGFs. For those facilities that have sprinklers, fire is not a great threat. Americold Inland, one of the largest underground installations in the Kansas City metropolitan area, had a significant fire that burned for over two months. This was partly due to the lack of a sprinkler system, but there also were no backup plans for how to extinguish a fire in the structure. A room was breached where the fire occurred, and smoke contaminated the UGF. Even though Americold Inland was still operating in the facility while the fire was burning, the smoldering and smoke contamination caused other problems. The insurance settlement was the largest that ever resulted from a fire and totaled billions of dollars.

Mr. Ryall noted that the Cheyenne Mountain Complex is classified by Colorado as a nonproducing mine. The code stipulates what type of vehicles can be used, how much explosives can be stored, and what type of airflow is needed. However, there is no code requirement for sprinklers, so the buildings did not have them. The computers were protected with Halon, but those systems have been removed due to the Montreal Accord on CFCs. Where applicable, carbon dioxide/water systems are now being installed each time a room is renovated in what may be a 20-year process.

Mr. Cicolani commented that a number of people at the workshop are working with fire codes, particularly Bill Jacobs of the U.S. Fire Administration. The National Fire Protection Association has been working to develop a code for underground commercial operations.

PANEL 4: FACTORS INFLUENCING THE DECISION-MAKING PROCESS

Moderator: Paul Byron Pattak,
PME, Ltd.

John Copenhaver Federal Emergency Management Agency, Region IV

Drawing on his experience at IBM and Bell South, Mr. Copenhaver provided the workshop attendees with his views on how decisions are made in corporate America and on what factors influence the approval process for funding new initiatives. If he were to try promoting the use of UGFs to top management, he said, he would begin with an objective risk analysis. This would be used to project the impact to corporate managers of an attack against operations infrastructure. He then would estimate how frequently such an event might happen, followed by a request for phased funding to address the threat. He stressed the importance of not seeking all of the money needed up front.

His message was that executives want to see two things: first, they want their reasons for saying "no" eliminated; second, they want to be given reasons to say "yes." Executives typically do not gather such information themselves; rather they depend on others to make a case with relevant information and to present it to them. Corporate executives encourage competition from those requesting a larger piece of the corporate budget. Arguments about "what if" scenarios can be anticipated by providing executives with information and statistics from which they can evaluate a range of informed choices based on realistic options. If presented with only one option, it becomes easier to say "no." Presenting a number of options for implementation, such as multiyear budgets as compared to significant up-front funding is better. Asking for a large part of the project money in the beginning makes it easier for executives to say "no."

There is inherent competition within companies, particularly when someone requests funding for new initiatives or attempts to change procedures. This is partly because corporate shareholders are always looking for more revenue-generating activities. A protective feature like UGFs can be perceived as an unnecessary expense; therefore, the business case has to be very strong.

Mr. Copenhaver described the environment in the corporate world with respect to security and disaster recovery as inadequate. Few corporations have a genuine commitment to emergency preparedness. Instead their emphasis is on stockholders and return on investment. That process is beginning to change, however. Talking to executives about their fiduciary obligations to protect and conserve corporate assets is a good strategy.

Derek Long BT Syntegra

Mr. Long began by stating that the issue of UGFs must not be addressed in isolation. Global connections make infrastructure protection everybody's problem, and interdependence of systems is total. Throughout the world economic growth is reliant on a consistent and interdependent communications infrastructure, which in turn is dependent on electric power, natural gas, and many other systems.

European countries have just begun investigating this issue in a collective sense. Mr. Long related how he had recently represented the European telecommunications industry at the first meeting of the European Union Commission, which is now beginning to study dependability and survivability, in which UGFs do come into play. The conclusion of the participants was that the interconnectivity of systems is now total.

Mr. Long described how the British telecommunications monopoly was broken up and forced to allow its competitors access to billings systems, traffic routing, and so forth—even those competitors owned by foreign concerns. Thus, a vision for increasing competition has led to unexpected vulnerabilities. He also spoke about the vulnerability of British telecommunications, which failed when a pile driver accidentally broke a main fiber optic cable, cutting power to 50 percent of all users.

BT has a directive from the British government to protect its systems, and all BT staff must have security clearances. BT Syntegra has just finished a £300 million project to totally upgrade the Ministry of Defence's core network. Also, competing contractors are now precluded from working in large parts of the BT organization for security reasons.

From the decision-making point of view, Mr. Long and his colleagues in information warfare won approval for some of their programs by showing senior management that their company could be put out of business in less than two hours. This was a powerful incentive. He believes that one area in which UGFs might engender general interest in the commercial sector has to do with the year 2000 computer issue.

The British telecommunications experience is broader than simply studying UGFs for solutions. If facilities are going to be underground to guard against current threats, engineering must be conducted with possible future threats in mind. A good example was the former TEMPEST program for communications. Mr. Long noted that there are advantages and disadvantages to UGFs. Fire is a potential weakness; one example is the fire in the English Channel Tunnel that destroyed fiber optics and power cables, putting it out of business for six months. Nonnuclear radio frequency attacks also are a concern and could potentially endanger lines of communication that lead into tunnels.

Carl Peterson NADET Institute

Dr. Peterson described the National Advanced Drilling and Excavation Technologies (NADET) Institute, and its work. He noted that the NADET Institute does not actually conduct research but rather facilitates it. He believes that neither individuals in various industries or government agencies have the power to solve large problems when looking for long-range innovative solutions. The users and those with funds must come together and take advantage of their combined resources to achieve results. NADET once surveyed various industries to develop a listing of barriers to major progress in the mining industry. Of the approximately 20 items on the list, not one was technical. One item named was the lack of leadership, and another was the lack of a road map for success.

Existing underground spaces do have limitations such as having been originally designed for military purposes with fairly large budgets or having represented mining space that was paid for out of mining company profits. Either way, cost was not a factor at the time of construction but is today. Even in Norway, for example, government policy is to build underground and the economics work out very well, but it required a regulatory policy to make it happen.

Dr. Peterson maintained that in this country the cost of new underground construction is very limiting. In the United States, underground space is much more expensive than above-ground construction and that new technology and perhaps new contractual arrangements are, therefore, required. Policy controls the technical effort that is put forward, and the technical effort or, more likely, the lack of it controls the options available to policymakers. One problem with existing underground spaces is that a user has to find one that is in the right shape and in the right location for their needs. In light of this, refurbishing existing UGFs can be a good value. Dr. Peterson described the current situation with respect to the utilization of UGFs as one of gridlock. The problem is not so much research as it is development. In times of tight budgets it is sometimes hard to gain support for projects clouded in secrecy, and a public works project might be easier to sell. To break the gridlock, government might have to take the lead for a broadly based program because industry will not do it alone.

Those needing solutions outnumber those funding solutions, and those who want to do the research far outnumber those who want to fund it. There is a need to improve underground technologies as a way of lowering the costs, such as a device called a universal tunneler, which reduces much of the risk and associated costs of civil projects. No one entity really has the incentive to fund this research, but there is a collective need, and there should be an organized effort to do so. Dr. Peterson closed by indicating that the most important thing to do is break through the barriers that are inhibiting progress and that events such as this workshop might act as a catalyst.

Irwin Pikus President's Commission on Critical Infrastructure Protection

Dr. Pikus focused his remarks on the various threats to critical infrastructures. While individual organizations and some industries know where they are vulnerable, there is no national perspective on the potential range of threats. Infrastructures are vulnerable and attractive targets, and attacking them can affect enterprise profitability, national security, economic health, living standards, public confidence, and many other concerns. Physical attacks include destroying targets, altering them so they cannot function correctly, and contamination. Cyber-attacks include denial of access, corruption of information, destruction of data, and theft of information. The overriding national need is to be able to deter, detect, deflect, respond to, and recover from an attack, and to mitigate or control its consequences. Dr. Pikus emphasized that we must raise public awareness of the problem, train people to deal with such situations, address the relevant security issues, and increase R&D to get the tools we are currently lacking.

A great advantage of UGFs is their controlled environment, which makes them ideal for certain uses. UGFs are isolated, and activities can be conducted in this environment without affecting neighboring installations. A range of facilities and amenities can be maintained underground, and key assets can be housed there. UGFs need to be evaluated in terms of best, intermediate, and worst choices for particular situations.

Perhaps an ideal use for UGFs is as infrastructure protection R&D centers and as useful testbeds for promising approaches. Other potential good uses include training exercises for first responders in dealing with chemical or biological agents and suggested training exercises using simulated chemical or biological agents in these facilities. Dr. Pikus also noted that it is conceivable to use UGFs for assessing the vulnerabilities of systems (e.g., sub-scale modeling) which can be done out of the public view.

Dr. Pikus advised that before beginning such a program the costs and vulnerabilities associated with relocating key infrastructure elements underground must be understood. He closed by highlighting the importance of evaluating whether UGFs are the best choice for a particular situation or just one of many options. This must be taken into account with solid cost data, so that corporate executives can make sound business decisions.

Eugene Sevin DoD Consultant

The focus of Dr. Sevin's remarks was that, to move forward seriously on UGFs as a viable solution to infrastructure protection problems, the government in general, and DoD in particular, must play key leadership roles. Security is DoD's principal but not its only concern. DoD's experience with

UGFs and other hardened facilities has been to design them to resist a massive nuclear threat. DoD's historical perspective on UGFs partially accounts for the conservative design philosophy related to the scale of that threat. As a consequence, UGFs were often judged to be too costly in relationship to alternative solutions, such as mobile assets. Additionally, there were cultural obstacles to be overcome, and this history is discouraging. Dr. Sevin noted that the primary threat to our infrastructures today seems to be cyber-attacks, which UGFs do not address directly because the principal use of UGFs over the years was for protection against nuclear (i.e., physical) threats.

A National Research Council (NRC) study on design and building applications of hardening technologies ruled out the use of fortress-type structures and UGFs as protection from bomb threats and blast damage. Dr. Sevin noted that the NRC and its Board on Infrastructure and the Constructed Environment need to be involved in the protection of the constructed environment.

DoD has a mixed view of its responsibilities for protecting the civilian population as it contributes to national security. Dr. Sevin did not think that protecting the civilian population as part of national security is an accepted mission of DoD. This will have to be resolved if the agency is to provide leadership on this issue.

Questions and Answers

During the question-and-answer period, Mr. Pattak mentioned his experiences talking about infrastructure assurance to federal agencies, and how they advised the PCCIP to get executive guidance signed by the President to establish the policy. Otherwise, agencies will be reluctant to act. He emphasized the political implications of many issues and that, ultimately, decisions rest on the cost of a facility and who pays that cost. Political implications at this level also affect the relationships between individuals. While the use of UGFs for infrastructure protection appears to be a good idea, this alone is not enough to effect change. People must be convinced of the advantages in order to make progress.

Mr. Pattak also noted that the panel represents a cross-section of government, industry, and academic professionals and that each has had a distinguished career in two out of those three areas. He pointed out that from his PCCIP service he learned that, although the problems presented in the area of UGFs are technical, the solutions are cultural, social, and political. Developing sound policy recommendations to complement technical solutions is absolutely essential for success.

Dr. Sevin stated that he thought the Federal Facilities Council of the NRC should take an active role in protection issues and encouraged the National Academy of Sciences to take a longer view as well. To this Mr. Eastler

expressed the concern that information technology and information warfare are still the top priorities and that UGFs and physical protection are not considered critical. Dr. Sevin commented that UGFs, if properly designed, have one large attribute: at whatever depth of burial, they enforce the standoff of a threat.

Dr. Schroeder asked whether the $500 million the PCCIP recommended for R&D would go solely to the cyber-threat, as opposed to physical threats. Dr. Pikus answered that, while it was stated to address infrastructure assurance across the board, the bulk of the additional R&D will be spent on information security. Derek Long encouraged additional research on tools for detection analysis to identify an attacker and determine whether it is a real attack or a deception. The draft Presidential Decision Directive (PDD) will assign to the Office of Science and Technology Policy the responsibilities for conducting an interagency working group on R&D. While UGFs have not been mentioned there, that might be a forum in which they could be discussed.

Mr. Scanlan asked the panel participants if presidential requirements are currently at a very broad level or if they had become departmental requirements and policies within the U.S. Department of Commerce and DoD. Dr. Pikus said that during the PCCIP's deliberations it was thought that there was not adequate work being done within the departments and agencies; therefore, the commission recommended additional effort on their part. He expects the draft PDD will state that agencies and departments will be responsible for conducting serious vulnerability assessments, primarily but not exclusively on information systems. Mr. Pattak added that when the PCCIP went out to the various agencies it was underscored that presidential guidance is absolutely necessary if funding priorities and spending allocations are to be changed. A PDD states unequivocally that this is the President's view.

Dr. Nelson of the National Science Foundation (NSF) reviewed the initiatives that organization has taken to deal with infrastructure investment and planning. NSF has established an institute for civil infrastructure systems to support the decision-making process and identify research needs. Mr. Copenhaver noted that business impact analysis methodology is now being used in the private sector to investigate the consequences of the interruption of critical functions.

Mr. Minehart had reservations about suggestions that the government cooperate more with industry on indications and warning as well as on tools to detect infrastructure attacks. Industry may not want to be forthcoming with a disclosure that it has been attacked, as this becomes a customer confidence issue. In response, Mr. Long noted that in Britain industry will not accept mandated standards. What it wants from the government as taxpayers is advice as to what standards it should be applying. He noted that in the United Kingdom there is a defense science advisory council similar to the U.S. Defense Science Board that studies the civil infrastructure and its impact on the Ministry of Defence's ability to carry out its mission. Britain also has a unified reporting system. It was found that various infrastructure sectors felt free to talk to the council; what they will not talk about is passing this information into the

government system. They concluded that a way around the problem was to approach the insurance industry to obtain alternative reduced premiums if, in fact, an industry is meeting a particular standard and thus reducing its risk. Mr. Long strongly recommended the use of this commercial route for those infrastructure sectors that are not supplying information directly to the government. When the government procures services, these standards can be applied to their contractual activities and can be more easily mandated.

SUMMARY

Dr. Baker concluded the session by thanking the keynote speakers and clarifying the important potential value of UGFs in the cyber-arena. He made the point that cyber-warfare or information warfare, as defined by the military components in the United States and NATO, includes both electronic and physical attacks. While UGFs do not improve infrastructure survivability against electronic attacks, they do protect against physical attacks on information systems. Even in the case of electronic attacks, UGFs can be used to provide safe havens for network nodes and the storage of backup media and systems. Thus, UGFs can greatly further the ability to reconstitute information systems and networks following an electronic or physical cyber-attack.

Dr. Baker then recapped several important calls for action from workshop panelists.

- Mr. Woodard called for the establishment of an academic center for underground studies.
- Mr. Rodgers advocated a designated clearinghouse organization to hold and distribute information and serve in a "matchmaker" role for interested users in search of suitable underground sites.
- Dr. Sevin stated that DoD will need to take the lead in moving forward seriously with underground applications.
- Mr. Brandenburg indicated that, although DoD is one of the biggest infrastructure customers, its procurements lack requirements for protecting against threats other than cyber-threats.

Breakout Sessions

TECHNICAL SESSION SUMMARY

Moderators: James Beck and Gary McIntire
Defense Special Weapons Agency

Mr. McIntire summarized the technical and operational issues associated with UGFs used for the protection of critical infrastructures that were raised in the technical breakout session:

- Threats to infrastructures are both physical and cyber; an overriding concern is that most infrastructures reside in the private sector.
- Many solutions, and any overall solution, will require a partnership between the private sector and government. The current private-sector record in infrastructure protection is mixed.
- It is essential to define what infrastructure is critical.
- There is a lack of tools for exploring the long-term trade-offs between UGFs and other solutions. Data must be developed that can be used by decision makers in considering various means of protection, including UGFs. There are clear benefits to going underground, such as improved security and dual-use opportunities.
- Cost is a major issue at the technical level. In the United States, if not in Scandinavia, the initial construction cost of new UGFs can be considerably higher than that of above-ground facilities. Cost will be considered a barrier by some infrastructure owners and operators considering underground relocation. Over time there are operations and maintenance cost savings, and the financial trade-offs tend to improve. Over the entire life cycle, UGFs can be considered very cost competitive. Specific factors that should be included in the cost equation are location, geology, construction depth, and the presence of groundwater.
- A well-defined facility makes an attack more difficult. Generally, UGFs provide improved physical security and are at least neutral on the cyber-threat.
- Other technical issues include external connections, fire, and the ability of the facilities to be protected against chemical, biological, and radio frequency weapons.

UGFs are among the tools in the arsenal of those who would protect critical infrastructures. In reality, a combination of protection methods for most system-type architectures is probably the best approach. This would include mobile units, alternate routing, improvements in training and procedures, and the development of rapid recovery teams. All of these are important when

discussing critical infrastructure protection. The perceived threat ultimately will drive the solution. The psychological impact of UGFs on workers is not a major problem but must be considered. Dual-use facilities present their own set of challenges. Having disparate users with different requirements and cultures in a single facility must be considered in developing a satisfactory working arrangement.

POLICY SESSION SUMMARY

Moderators: Paul Byron Pattak, PME, Ltd., and Wayne A. Schroeder, Logicon/RDA

Dr. Schroeder discussed the top issues affecting the use of UGFs for the protection of critical infrastructures that were raised in the policy breakout session. Those attending the session believe that compelling arguments must be developed to communicate that underground relocation reduces the risks to a specific threat. Public opinion and the American psyche also are of concern. While the Norwegians are very comfortable using underground facilities, there is an entirely different attitude in the United States. There would be a need for a psychological adjustment if UGFs are to be used more aggressively, and ultimately there would be political costs for doing so.

Session attendees perceived that affordability would be a problem in the United States, and this is an important issue for the underground community to address. If the underground community is to publicly advance the use of UGFs for the protection of critical infrastructures, it must first have a better understanding of the costs. Up-front construction costs certainly are a major part of that equation. Other issues include the perception that there is little direct relationship to the more visible information warfare problem, consolidation issues in which fewer facilities present more lucrative targets, and the need for a clearinghouse for data on UGFs.

A number of different challenges were discussed, including:

- increasing public-and private-sector awareness of UGFs,
- creating a government-industry partnership,
- obtaining industry support,
- assisting infrastructure owners in determining if UGFs can meet their requirements,
- defining the role and extent of government support, and
- implementation.

The policy session did not extensively address implementation, but it is something that the PCCIP has addressed in terms of whether implementation would be through direct support of R&D, tax incentives, or simply an education and awareness campaign.

In conclusion, the top policy issues were identified as follows:

- Public perception is the key issue. Corporate America needs to be made aware of the benefits UGFs offer.
- Education is needed to make the uses and benefits of UGFs for infrastructure protection better known to the public. A number of different ideas were broached, including continued work with the Underground Construction Association and a more integrated effort with the NRC and its Board on Infrastructure and the Constructed Environment.
- Cost is a major policy issue. The apparent differences in comparative costs for UGFs relative to above ground structures presented at the workshop are cause for concern. Before a more aggressive public effort is mounted, more definitive cost data must be developed.
- Dual-use opportunities were emphasized in the policy breakout session, as throughout the workshop. Workshop participants learned a great deal from the Norwegian dual-use experience with UGFs, and this issue should be given a higher priority in future programs on UGFs.

There was considerable discussion concerning how to proceed in the future. Two approaches were considered. The first involved evaluating a broad selection of infrastructures to determine where UGFs might be of use. A second approach was to narrow the focus and identify a few suitable projects. A good approximation of the design and cost data for going underground would be developed for those particular infrastructure elements, and then the specific audiences for which the projects apply (e.g., corporate executives, government) would be approached. A longer-term program would be adopted to test how the projects were received. The second, and more focused approach was considered the appropriate course to pursue.

Mr. Pattak concluded the policy breakout session by reminding the group that it is never easy to propose new policies, new initiatives, and new ways of doing things. People are naturally skeptical of change, and it is incumbent on those who are knowledgeable about UGFs and committed to their use to make the case for their use. The key points he raised were:

- In the pursuit of saving money, industries may be making themselves more vulnerable.
- Cost analyses on UGFs need to be divided between construction on the one hand and operations and maintenance on the other.
- Ninety-five percent of U.S. critical infrastructures are owned by organizations other than the federal government.

CLOSING REMARKS

Dr. George Baker provided the following summary observations from the workshop presentations and breakout session discussions. He noted that, although UGFs may not be a panacea for critical infrastructure protection, workshop participants believe they offer many important benefits in the areas of physical protection and security controls. UGFs would have deterrent value against both terrorist and military threats. The initial impression of many workshop participants was that UGFs offer no benefits for protecting infrastructures from cyber-attacks. UGFs, however, can indeed play an important role in reconstituting networks following a cyber-attack because they provide a safe haven for the storage of critical backup media and systems. In addition, the military view of information warfare is that it includes both electronic and physical attacks. Although UGFs may not improve survivability against electronic attacks, they do mitigate against physical attacks on information systems and can speed recovery following a cyber-attack.

Serious consideration of UGFs as an option for protecting critical infrastructures will require cost comparisons with above-ground facilities that afford the same level of protection. There is good reason to expect that UGFs will provide cost benefits with respect to blast hardening and long-term maintenance. Europe has the most comprehensive data on life-cycle costs, but these data must be carefully evaluated to determine their applicability to the United States.

Education and consensus building in the infrastructure community regarding the capabilities and utilization of UGFs will be essential. The underground technical community must get its message across to both corporate America and the American public. Within the government, DoD is in the strongest position to organize a coordinated effort. A designated clearinghouse organization is needed to hold and distribute information and serve as "matchmaker" for users in search of suitable underground sites. Furthermore, establishment of an academic center for underground studies would enhance the visibility and encourage the acceptance and use of underground construction in the United States.

In the future a useful pilot project might begin with the selection of two infrastructure applications as a point of focus. These applications would be the basis for discussions between government and industry on cost-risk benefits and an implementation approach. If convincing arguments were forthcoming, with proper government incentives, the exercise could lead to a demonstration project for a prime infrastructure function.

Dr. Baker noted that UGFs appear to be an important tool for protecting critical infrastructures by providing physical security and the capability to reconstitute critical infrastructure functions. The technical feasibility and benefits are well established, with many precedents of underground infrastructure applications, most notably in Scandinavian countries and Switzerland. The biggest remaining challenge is to establish the cost and risk benefits to the United States.

Dr. Baker thanked the members of the Underground Site Infrastructure Working Group which was largely responsible for planning the workshop and the National Research Council and Board on Infrastructure and the Constructed Environment for convening the workshop and expressed his hopes for a future association in this area. He recognized the keynote speakers and all of the panelists for their presentations and expressed his pleasure at having Arnfinn Jenssen, Derek Long, and Ben Vretblad here from Norway, the United Kingdom and Sweden, respectively. Dr. Baker concluded by saying that the workshop was a defining moment, that resulted in some excellent ideas and that the challenge now is to act.

Mr. Little extended his thanks to everyone on behalf of the board. He stated that the use of UGFs for infrastructure protection is an important issue and that going forward requires that the discussion begun during the workshop be continued in the infrastructure community at large.

Appendix A Speaker Biographies

George H. Baker III Dr. Baker is currently chief of the Springfield Research Facility, the national center of excellence for underground technologies of the Defense Special Weapons Agency. He began his career at the Harry Diamond Laboratories in nuclear electromagnetic effects protection and instrumentation design and later transitioned to the Defense Special Weapons Agency, initially managing survivability programs for the Air Force Peacekeeper and Army ballistic missile defense systems. He developed the agency's source region electro-magnetic pulse program and launched several associated underground test programs. He also developed new models to explain global fallout dispersion from U.S. and Russian atmospheric tests. In 1983 Dr. Baker chaired the working group that defined the U.S. high power microwave program. In 1987 he was appointed team leader for the agency's integrated electromagnetic effects program. During 1994–1996 he served as chief of the Innovative Concepts Division overseeing space nuclear power technology, the electrothermal chemical gun program, and the agency's university grants programs. He assumed leadership of the Springfield Research Facility in 1996. Dr. Baker currently cochairs the Nonproliferation and Arms Control Technology Working Groups, Underground Focus Group and the Underground Site Infrastructure Assurance Applications Working Group. He is a member of the Technology Panel on Directed Energy Weapons, the New York Academy of Sciences, the Institute of Electrical and Electronics Engineers, and Who's Who in Science and Engineering.

James E. Beck Mr. Beck deals with structural engineering issues at the Defense Special Weapons Agency's Springfield Research Facility and is a member of the Underground Site Infrastructure Assurance Applications Working Group. He has over 26 years of experience in structural mechanics; structural dynamics; matrix-computer analysis; concrete, wood, masonry, and steel structural design; and analysis of structures. His capabilities have been used to examine the effects of nuclear and conventional weapons on structures; to design structures to resist accidental explosions at gas-handling facilities and oil refineries; and to evaluate the capabilities of structures to resist the effects of natural disasters, including high winds, hurricanes, tornadoes, and earthquakes. He holds B.S. (University of Maryland) and M.S. (Stanford University) degrees in Civil Engineering.

Michael Brandenburg Mr. Brandenburg is director of AT&T's Special Government Services, located in Oakton, Virginia. He leads a 150-person

organization in AT&T government markets that provides government industrial security, engineering, and operations support to DoD and various other agencies. He has worked at AT&T for 27 years in assignments that included computer systems development, systems engineering, and operations, in Washington and at AT&T headquarters in New Jersey. Mr. Brandenburg has a B.S. degree in electrical engineering from Iowa State University.

Angelo Cicolani Mr. Cicolani is technical director of the Defense Special Weapons Agency's Springfield Research Facility. Mr. Cicolani served in the U.S. Navy from 1950 to 1975 in the last of the all-gun ships, amphibious forces, first of the all-missile ships, fast attack and ballistic missile submarines. A graduate of the U.S. Naval Academy, he was one of a few chief reactor operators of both nuclear ships and submarines. From 1970 to 1975 he was special assistant for systems analysis at the Polaris, Poseidon, and Trident Strategic Systems Program Office. Since 1975 he has been a program manager for survivability studies of command, control, communications, and information systems and has been involved at SRF in developing many of the techniques for improving survivability or exploiting the vulnerabilities of underground facilities. His specialty in underground facility analysis is damage control and recovery operations. He has degrees in marine engineering and operations research.

John B. Copenhaver Mr. Copenhaver was appointed as director of the Federal Emergency Management Agency's Region IV office in Atlanta, Georgia, in late 1997. As regional director, Mr. Copenhaver is responsible for administering a variety of federal emergency preparedness, prevention, and disaster relief programs for Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, and Tennessee. Mr. Copenhaver is a long-time Georgia resident with extensive private-sector emergency management experience. Prior to joining FEMA, he was team adviser for the Worldwide Crisis Response Team of IBM's Business Recovery Services. He also worked as director of business continuity services for Bell South Business Systems and earlier served as that organization's marketing manager with responsibilities for development and deployment of Bell South's Emergency Preparedness Program. Mr. Copenhaver holds a bachelor's degree in planetary geology from Brown University and a law degree from the University of Georgia School of Law. He is a member of the state bar of Georgia and is a certified business continuity professional.

Maj. Gen. Gary L. Curtin Gen. Curtin has been Director of the Defense Special Weapons Agency since mid-1995 after long experience in intercontinental ballistic missile (ICBM) operations, arms control, intelligence, command control, and international affairs. As a young officer he filled positions as an ICBM missile launch officer, an intelligence targeting officer and politico-military affairs staff officer. Gen. Curtin served as commander of

the 90th Strategic Missile Wing, Cheyenne, Wyoming from 1986–1988, commanding 200 Minuteman III ICBMs and managing the deployment of 50 new Peacekeeper ICBMs. He was director of Command Control of Strategic Air Command (SAC) in Omaha, Nebraska from 1988–1989, responsible for the SAC underground command center and the Looking Glass airborne command post. He also managed the construction and activation of SAC's new underground command center, now used by the U.S. Strategic Command. From 1990–1991, Gen. Curtin was the senior US military member of the Strategic Arms Reduction Talks (START) during negotiation of the START I treaty in Geneva. He subsequently became the Joint Staff's deputy director for international negotiations during conclusion of the START II, open skies, and chemical weapons treaties. Gen. Curtin also served as director of Intelligence for U.S. Strategic Command from 1993–1995, dramatically downsizing and refocusing that organization in light of changes in the post-Cold War threat. Gen. Curtin holds a B.S. in aerospace engineering from the University of Maryland and an M.S. in economics from South Dakota State University. He is a graduate of the National War College and Harvard University's Program for Senior Executives. Gen. Curtin wears the Command Missile Operations badge and the Senior Officer Aircrewmember badge, reflecting his 2500 aircrew flying hours and 105 combat missions in Southeast Asia. He has been awarded the Defense Distinguished Service Medal, the Defense Superior Service Medal, the Legion of Merit, the Bronze Star, three Meritorious Service Medals, and three Air Medals.

Raymond P. Daddazio Dr. Daddazio is director of the Applied Science Division of Weidlinger Associates. He is a registered professional engineer with 23 years of experience in elastic and inelastic analysis of structures. He is a developer of the first principles, finite element computer program EPSA (elastic-plastic shell analysis) used to perform large-deflection elastic-plastic structural analysis of structures subjected to dynamic loading. He is the principal investigator for structures programs sponsored by the Carderock Division/Naval Surface Warfare Center, Office of Naval Research, Defense Advanced Research Projects Agency, and Naval Sea Systems Command. He was codeveloper of several innovative approaches for quantifying the effects of uncertainties in structural systems. Dr. Daddazio received his Eng.Sc.D. degree from Columbia University in 1982. He also received his B.S. and M.S. degrees in civil engineering from Columbia in 1975 and 1976, respectively.

Arnfinn Jenssen Mr. Jenssen joined the Norwegian Defence Construction Service (NDCS) in 1957 and served as chief of test and development from 1964 until his retirement in 1996. He was responsible for research and development of all military and NATO installations in Norway, including many underground facilities. During the same period, he was a member of committees such as the KLOTZ Club (an international explosives safety committee), the NATO committee to establish criteria for War Headquarters, and the NATO ad hoc

committee on protective construction measures. He retired in 1996 but remains an adviser to the NDCS.

Richard G. Little Mr. Little is director of the National Research Council's (NRC) Division of Infrastructure. In this capacity, he develops and directs a program of studies in building and infrastructure research related to the social and technical interactions that occur between people and the built environment. The NRC's current activities in infrastructure are focused on the provision, performance, surety, and sustainability of constructed facilities. Mr. Little is also a consultant to the private sector and government agencies, prior to joining the NRC, served as director of the planning division in Fairfax County, Virginia. Mr. Little has over twenty-five years experience in the planning, management, and development of policy relating to public facilities and holds a B.S. in geology and an M.S. in urban-environmental studies from Rensselaer Polytechnic Institute.

Derek M. Long Mr. Long has been a managing business consultant with BT Syntegra since 1993. Following a 30-year career in the Royal Navy, initially in aviation and then with the Intelligence Service, Mr. Long served as a principal security consultant with ICL Defence Systems. An authority on information vulnerability, information assurance, and the impact of the new digital environment on the management of enterprise structures, he has been advising the Ministry of Defence (MoD) in the research and development of United Kingdom and MoD strategies and policies for information warfare (IW). Mr. Long was the founder of the BT corporate defensive IW program and currently provides advice on corporate strategy and the impact of IW upon BT development. He has developed the concept of a National Information Assurance Center for use by Her Majesty's Government (HMG), commerce, and the public. He is also a Board member of HMG's Defence Scientific Advisory Council, where he has served on various working groups.

Gary McIntire Mr. McIntire is a program manager at the Defense Special Weapons Agency's Springfield Research Facility and is a member of the Underground Site Infrastructure Assurance Applications Working Group. He currently specializes in infrastructure survivability and vulnerability assessments. He has worked on systems survivability issues for over 20 years. Mr. McIntire served in the U.S. Air Force for 27 years in a variety of worldwide tactical aviation, research, and staff assignments. He has degrees in aeronautical engineering from Saint Louis University and psychology from the University of Northern Colorado.

Robert F. Minehart Mr. Minehart is visiting professor for information warfare at the Army War College, Carlisle, Pennsylvania. A license professional engineer, Mr. Minehart's experience includes work at the National Security Agency and at Boeing as a flight test engineer. Mr. Minehart has conducted

extensive research in the fields of modeling, laser remote sensing, numerical analysis, computer programming, and engineering design. He received his B.S. and M.S. degrees in mechanical engineering from West Virginia University in 1979 and 1982, respectively. Mr. Minehart continued his education in electrical engineering at the University of Wisconsin, Georgia Tech, and George Washington University.

Paul Byron Pattak Mr. Pattak served as a senior consultant to the President's Commission on Critical Infrastructure Protection and is currently working in the same capacity for the PCCIP Transition Office (PCCIPTO), which succeeded the commission. He currently coordinates the PCCIPTO outreach effort to brief various executive branch organizations on the work of the PCCIP and is involved in the editing and review process of PCCIP supporting documents to the Commission's report. He also serves as a resource to the PCCIP Advisory Committee. Mr. Pattak is a consultant, educator, and entrepreneur for corporate and government clients and has also served in the Bush administration as special assistant to the associate director for national preparedness at the Federal Emergency Management Agency. Previously, he was the transition office contact for FEMA in the office of the president-elect. He has also worked on the personal staff of the Secretary of Defense and at the Fogarty International Center of the National Institutes of Health.

Carl R. Peterson Dr. Peterson is professor emeritus of mechanical engineering at Massachusetts Institute of Technology and director of the National Advanced Drilling and Excavation Technologies (NADET) Institute. His industrial experience includes employment at Ingersoll-Rand Research; Foster-Miller, Inc.; and his own company, RAPIDEX, Inc. Most of that work was associated with the design and development of advanced drilling, mining, and construction equipment. His academic work was largely in the teaching of design, with emphasis on encouraging student creativity, and he was an active member of the department's new curriculum development committee. He received a B.S.E. from the University of Michigan in 1956, as well as S.M. (1958) and Sc.D. (1963) degrees from MIT, all in mechanical engineering.

Irwin M. Pikus A member of the President's Commission on Critical Infrastructure Protection, Dr. Pikus's career focus has been on the role of science and technology in addressing national goals and objectives. A charter member of the Senior Executive Service, he began his government career in 1975 with the U.S. Department of State. Since 1987, Dr. Pikus has been with the U.S. Department of Commerce's Bureau of Export Administration, where he led an office that collected and analyzed information dealing with foreign technology comparable to the advanced technologies whose exports are controlled by the United States. Prior to his government career, he was an individual contributor and project manager in applied research with the aerospace and electronics industries. Dr. Pikus holds a Ph.D. degree in physics and a J.D. from Temple University.

John K. Reingruber Mr. Reingruber is currently the assistant for science and technology in the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. In 1984 he established the Congressionally mandated Special Operations Special Technology Program to help revitalize Special Operations Forces through the rapid development and fielding of prototypes. In 1987 he was selected as a staff assistant to the director of special operations technology, Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. Later he became as acting head of the Munitions Countermeasures Department at the Naval Explosive Ordnance Disposal Technology Center, in Indian Head, Maryland. In 1989 he returned to direct the Special Technology Program Office, which is now the Office of Special Technology. In 1992 Mr. Reingruber was assigned to his current position where he oversees special operations, low-intensity conflict, and interagency counterterrorism and counterproliferation technology development programs.

Paul Rodgers A member of the President's Commission on Critical Infrastructure Protection, Mr. Rodgers was the executive director and general counsel for the National Association of Regulated Utilities Commissioners (NARUC) in Washington, D.C., from 1965 to 1996. NARUC includes all state and federal agencies engaged in the regulation of public utilities and carriers. While at NARUC Mr. Rodgers was influential in strengthening the role of NARUC as an organization known and respected in Congress, the executive branch, and federal agencies. From 1960 to 1965 Mr. Rodgers served as assistant attorney general for the state of Georgia, during which time he represented the Public Service Commission and other state agencies and argued three cases before the U.S. Supreme Court. From 1957 to 1960, Mr. Rodgers was an attorney for the Atlanta Gas Light Company. A member of the District of Columbia and Georgia bars, he holds a J.D. degree from Mercer University.

Paul B. Ryall Mr. Ryall is a staff civil engineer with ENSCO, Inc., working with the Springfield Research Facility on hardened facilities issues, with a focus on fire protection and customers' mission recovery after an incident. A career Air Force officer, he was the base civil engineer (director of public works) of the Cheyenne Mountain Air Station in Colorado Springs, Colorado for four years. He commanded a 200-person organization that provided real property, utility, and emergency response functions to support NORAD and U.S. Space Command missions in the Cheyenne Mountain hardened complex. By converting to 100 percent commercial electric power, he helped the Cheyenne Mountain Complex reduce its annual operations and maintenance budget by over $2 million. His first experience with hardened facilities was in Europe as a safety engineer. He ensured that the facilities constructed through the NATO infrastructure construction program complied with life safety codes, and he designed and constructed numerous revetment projects to provide splinter protection for aircraft and facilities. Mr. Ryall has a B.S. in civil engineering

from Rutgers University and is a registered professional civil engineer in California. He also holds an M.B.A. in business and marketing.

Wayne A. Schroeder Dr. Schroeder, a senior research specialist with Logicon RDA, provides support to the Defense Special Weapons Agency's Springfield Research Facility on infrastructure assurance and is a member of the Underground Site Infrastructure Assurance Applications Working Group. A member of LRDA's systems engineering team since 1986, he has provided technical and analytical support to DSWA on counterproliferation, nuclear arms control, verification R&D, and test programs and policies. Over the past 20 years he has written extensively on defense planning, arms control, and international security in such publications as *Strategic Review, Policy Review, Comparative Strategy, Military Engineer, Amphibious Warfare Review* and the *National Security Record*. Dr. Schroeder received a B.A. in political science from the University of Oregon (1974), an M.A. in political science from Portland State University (1976) and A.M. and Ph.D. degrees in international relations from the University of Southern California (1979, 1981).

Daniel Schutzer Dr. Schutzer is vice president and director of external organizations, standards, and advanced technology, at Citibank and the president of the Financial Services Technology Consortium. He previously held positions as technical director, naval intelligence, technical director, of the Navy's command, control, and communications and program manager at Sperry Rand. He also worked at Bell Labs, Syracuse University, and IBM. He currently has responsibility for interfacing with external organizations and standards bodies and for directing company-wide research. This includes coordinating research with business goals and priorities and keeping Citibank up to date with the latest technologies. His research projects include electronic commerce, risk management, customer behavioral modeling and mathematical marketing, and new product design. Advanced technology projects under investigation include agent technology, machine learning, multimedia, image and voice processing, and high performance computing. He has authored seven books and over 65 other publications. Dr. Schutzer received a B.S. degree in electrical engineering from the College of the City of New York and M.S. and Ph.D. degrees from Syracuse University.

Eugene Sevin An independent consultant, Dr. Sevin's research interests are in nuclear and conventional weapons effects, hardened facility design, and computational structural mechanics. Dr. Sevin has served as chief of the Strategic Structures Division of the Defense Nuclear Agency and as assistant to the deputy director for science and technology for experimental research, DNA. He joined the Office of the Secretary of Defense in 1986 as director, space and missile systems. Previously, he served as professor of mechanical engineering at the Israel Institute of Technology and was head of mechanical engineering at Ben Gurion University of the Negev, in Israel. Dr. Sevin is a member of the

National Academy of Engineering and holds a Ph.D. in applied mechanics from the Illinois Institute of Technology, an M.S. in mechanical engineering from the California Institute of Technology, and a B.S. in mechanical engineering from the Illinois Institute of Technology.

Michael Shannon Mike Shannon is chief of special operations, for the Oklahoma City Fire Department. He began his hazardous materials work in the U.S. Navy with nuclear, chemical, and biological warfare in 1972 and continued through 1976. Mr. Shannon has over 20 years of service with the Oklahoma City Fire Department. During the bombing incident in Oklahoma City in 1995, he served as rescue operations chief for 288 hours over a 16-day period. This placed him in charge of all technical rescue and recovery operations in the Murrah Building. He was the first firefighter to enter the building and made the recommendation to cease recovery operations.

Frederick M. Struble A member of the President's Commission on Critical Infrastructure Protection, Dr. Struble has served as a member of the commission's Banking and Finance Sector Team and its Economic Team. He has insight and knowledge gained over several decades of professional service in banking and regulation, financial analysis, and economic policy. Dr. Struble worked for more than 25 years in various positions at the Federal Reserve Board, serving as deputy associate director responsible for the work of the government finance and the capital markets sections. He also served in the Division of Banking Supervision and Regulation. Previously, he worked as a financial economist at the Federal Reserve Bank of Kansas City and as a teaching assistant in the Department of Economics at the University of Colorado. Dr. Struble received a Ph.D. in economics from the University of Colorado in 1965 and a degree in business administration from the University of Kansas.

James A. Werth Mr. Werth is a supervisory special agent with the Federal Bureau of Investigation (FBI), where he has been worked for more than 26 years. Most of his investigative/operational experience has involved matters concerning foreign counterterrorism and counterintelligence. He has been stationed at a number of field offices in the country and has been FBI representative to U.S. embassies in Belgium and Switzerland. He is currently assigned to the Infrastructure Protection Task Force and National Information Protection Center at FBI headquarters in Washington, D.C. Mr. Werth received a B.A. degree from St. Benedicts's College and a Master of Public Administration from the University of Missouri, Kansas City.

Donald P. Woodard Mr. Woodard is director of underground planning and development at Park College, Parkville, Missouri. He previously held similar positions for the Garney Company and Hunt Midwest. He has been in underground development for many years and is also currently the executive

director of the Underground Developers Association in Kansas City. Prior to focusing full time on underground development, he served as director of planning for the cities of Kansas City, Missouri and Tulsa and the state of Missouri. He is familiar with all 16 operating commercial undergrounds in the Kansas City area.

Appendix B Workshop Agenda

Monday, April 6, 1998	
8:45 a.m.	**Welcoming Remarks**
	Richard Little
	National Research Council
8:50	**Introduction to the Workshop**
	Maj. Gen. Gary Curtin
	Director, Defense Special Weapons Agency
9:10	**Keynote Address**
	Frederick M. Struble
	Commissioner President's Commission on Critical Infrastructure Protection
9:35	**Panel 1: Infrastructure Protection Issues**
	Moderator, George Baker
	Defense Special Weapons Agency
	• James Werth, Federal Bureau of Investigation
	• Robert Minehart, National Security Agency
	• Raymond Daddazio, Weidlinger Associates
	• John Reingruber, Office of the Secretary of Defense for Special Operations and Low-Intensity Conflict
10:50	**Break**
11:00	**Panel 2: Infrastructure Community Needs and Requirements**
	Moderator, Richard Little
	National Research Council
	• Michael Brandenburg, AT&T
	• Paul Rodgers, President's Commission on Critical Infrastructure Protection
	• Daniel Schutzer, Citibank
	• Michael Shannon, Oklahoma City Fire Department

12:30 p.m.	**Lunch**
1:30	**Panel 3: Experience with Underground Facilities: Capabilities, Limitations, and Applications**
	Moderator, Angelo Cicolani
	Defense Special Weapons Agency
	• Arnfinn Jenssen, Norwegian Defence Construction Service
	• Paul Ryall, ENSCO, Inc.
	• Donald Woodard, Underground Developers Association and Park College
3:00	**Break**
3:15	**Panel 4: Factors Influencing the Decision-Making Process**
	Moderator, Paul Byron Pattak
	PME, Ltd.
	• John Copenhaver, Federal Emergency Management Agency, Region 4
	• Derek Long, BT Syntegra
	• Carl Peterson, NADET Institute
	• Irwin Pikus, President's Commission on Critical Infrastructure Protection
	• Eugene Sevin, Logicon/RDA
5:00	**Recess for the Day**
Tuesday, April 7, 1998	
8:45 a.m.	**Key Issues in Going Underground**
	Donald Woodard
	Underground Developers Association/Park College
9:00	**Infrastructure Protection in the United States: A Norwegian Perspective**
	Arnfinn Jenssen
	Norwegian Defence Construction Service
9:15	**Guidance to Breakout Groups**
	George Baker
	Defense Special Weapons Agency
9:30	**Breakout Sessions**

	Technical Group (The Lecture Room)
	Moderators: James Beck and Gary McIntire
	Defense Special Weapons Agency
	Policy Group (The Board Room)
	Moderators: Paul Pattak
	PME, Ltd.
	Wayne Schroeder
	Logicon, RDA
10:45	**Break**
11:00	**Synthesis of Technical and Policy Issues**
	Breakout Session Facilitators
11:45	**Synopsis of Workshop**
	George Baker
	Defense Special Weapons Agency
12:00 p.m.	**Adjourn**

Appendix C Workshop Participants

Mark Allen	
George Baker	DSWA/SRF
William Bearden	ANSER, Inc.
James Beck	DSWA/SRF
Brenda Bohlke	Parsons Brinckerhoff
Michael Brandenburg	AT&T
Robert Brannon	
Jasey B. Briley	OSD Facilities Management
Carl A. Bunche	OSD Facilities Management
Joseph R. Carter	Center for Disease Control & Prevention
Angelo Cicolani	DSWA/SRF
Bron Cikotas	Consultant
John Copenhaver	FEMA Region IV
Maj. Gen. Gary Curtin	Director, DSWA
Raymond P. Daddazio	Weidlinger Associates, Inc.
LCdr. Michael Daly	DSWA/SRF
Kenneth deGraffenreid	National Security Research, Inc.
Ralph Easley	898th Munitions Squadron (AFMC)
Thomas Eastler	DSWA/SRF
Joan Erwin	DSWA/SRF
Robert A. Flory	ARA, Inc.
Carl Fuetsch	
Victor Gehman	
William Graham	National Security Research, Inc.
Michael J. Guarracino	DSWA/SRF
William J. Harris	PCCIP
Brian Hayes	US Army
Kathleen M. Hickman	OUSD(A&T)/AW
John Hill	DSWA/SRF
Kris Indseth	
William F. Jacobs	FEMA/US Fire Academy
Arnfinn Jenssen	Norwegian Defence Construction Service
William J. Kane	DSWA/SRF

Cyrus P. Knowles	JAYCOR
Col. Harlan A. Lawson	Field Command, DSWA
Richard Little	National Research Council
Derek M. Long	British Telecom
Lt.Col. R. Thomas Lutton	DSWA/SRF
Rudy Matalucci	Sandia National Labs
Gary McIntire	DSWA/SRF
Robert Minehart	Army War College
Charles T.C.	Mo RDA/Logicon
Peter A. Mote	Nevada Testing Institute
Priscilla Nelson	National Science Foundation
Vayl Oxford	DSWA
James Papineau	US Army
Paul Pattak	PME, Ltd
Lt.Col. Paul J. Perrone	DSWA/OPSF
Carl R. Peterson	NADET Institute, MIT
Robert Phillips	System Planning Corp
Irwin Pikus	PCCIP
William T. Porter	Center for Disease Control & Prevention
John Reingruber	OSD, SO/LIC
Paul Rodgers	National Regulated Utilities
Paul Ryall	DSWA/SRF
David H. Scanlan	NCCS
Gerard K. Schlegel	Logicon RDA
Wayne Schroeder	RDA/Logicon
Daniel Schutzer	Citibank
Gene Sevin	DOD Consultant
Michael Shannon	Oklahoma City Fire Dept
Peter Smeallie	Research Opportunities Management
Frederick Struble	Former Commissioner, PCCIP
Ralph L. Tindal	DSWA/SRF
William T. Todd	DSWA/SRF
Bengt E. Vretblad	Sweden
David Walther	US Army
James Werth	Federal Bureau of Investigation
Fred Wikner	Jaycor
Lt.Col. Michael D. Williams	OASD (SO/LIC)
Charles A. Williamson	OASD (SO/LIC) CT/SA
Donald Woodard	Park College
Rowland Worrell III	ARA, Inc.

Appendix D Underground Site Infrastructure Applications Working Group

George Baker, Chair
Defense Special Weapons Agency

Jim Beck
DSWA/SRF

Brian Berry
RPI

Brenda Myers Bohlke
Parsons Brinckerhoff, Inc.

Jason Briley
OSD Facilities Management

Carl Bunche
OSD Facilities Management

Joan Erwin
DSWA/SRF

Bill Gunnells
DoD/OSD

William F. Jacobs
FEMA/USFA

Richard G. Little
National Research Council

Gary McIntire
Facilities DSWA/SRF

Paul Pattak
PME, Ltd.

Wayne Schroeder
Logicon/RDA

Steve Sherwood
DoD/OSD