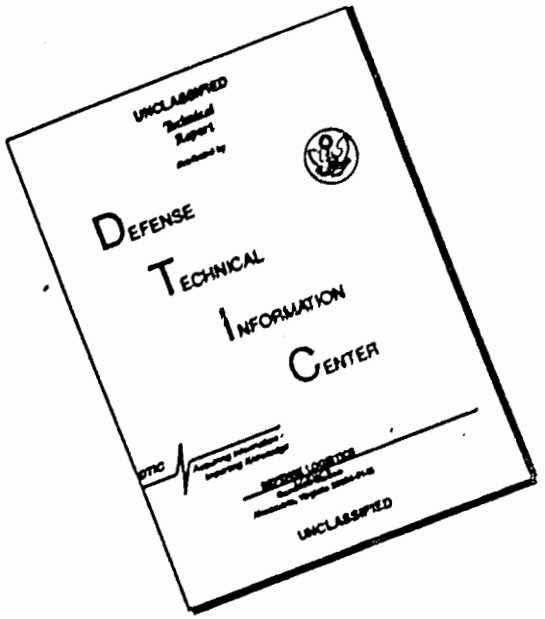
Issues of Command and Control

Edited by Thomas P. Coakley

DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

BLANK PAGES
IN THIS
DOCUMENT
WERE NOT
FILMED

C^3 I:

Issues of Command and Control

C^3 I:

Issues of Command and Control

Edited by

Thomas P. Coakley

1991

National Defense University
Washington, D.C. 20319-6000

National Defense University Press Publications.

To increase general knowledge and inform discussion, NDU Press publishes books on subjects relating to US national security. Each year, in this effort, The National Defense University, through the Institute for National Strategic Studies, hosts about two dozen Senior Fellows who engage in original research on national security issues. NDU Press publishes the best of this research. In addition, the Press publishes especially timely or distinguished writing on national security from authors outside the University, new editions of out-of-print defense classics, and books based on conferences concerning national security affairs.

 This book was prepared with partial support from the Command and Control Research Program of the National Defense University in fulfillment of the contract DAHC–32–89–C–001 between NDU-CCRP and the Harvard Program on Information Resources Policy.

Editorial Research Associates, Rockville, Maryland, designed, proofread and indexed this publication under contract DAHC32–90–M–3257.

NDU Press publications are sold by the US Government Printing Office. For ordering information, call (202) 783-3238, or write to: Superintendent of Documents, US Government Printing Office, Washington, DC 20402.

Library of Congress Cataloging-in-Publication Data

Coakley, Thomas P.,

C³I: Issues of Command and Control / Thomas P. Coakley.

p. cm.

On t.p. "3" is superscript.

Includes bibliographical references and index.

$10.00 (est.)

1. Command and control systems—United States. 2. United States—Armed Forces—Communication systems. 3. United States—Armed Forces—Organization. 4. Military intelligence—United States.

I. Title.

UB212.C6 1991

355.6—dc20 90-49793

CIP

First printing, June 1991

To
Thomas M. and Catherine R. Coakley,
in appreciation for their
command, control, and love (C^3L).

Contents

Foreword

It is axiomatic that the command and control of military forces is of utmost importance to all military operations. Dozens of books and articles address what professionals in the field refer to as "command, control, communications, and intelligence (C^3I)." But the esoteric perspective taken by these publications is usually intended for a professional audience, leaving a need for a work that places the subject in the overall context of operations, decisionmaking, and planning, so that the interested layman can understand its vital and often complex functioning.

To write such a book about C^3I, the National Defense University joined forces with the Program on Information Resources Policy of Harvard University. Since 1980, a series of seminars on command and control have been held, attended by senior government officials and leaders in industry. These meetings often produced illuminating and lively debate. Over the years records of these exchanges, which contain the best of what has been thought and said on the topic, have accumulated in the archives, accessible only to scholars who can carry out their research at Harvard.

Lieutenant Colonel Thomas P. Coakley, USAF, Associate Professor of English at the US Air Force Academy, during a sabbatical as an NDU Visiting Fellow, took on the task of editing, organizing, and presenting this archival material so that it might be accessible to a wider audience. Screening thousands of pages, he has arranged the best of the material in chapters on the central issues of command and control, introducing each chapter with an instructive summary, and then presenting the most informative extracts from the Harvard papers and transcripts. This book can serve both the general reader and the specialist. Moreover, Dr. Coakley has made the wisdom of senior leaders and experts, whose experience is irreplaceable, available to those who must cope with the fast-moving communications revolution.

J.A. BALDWIN
Vice Admiral, US Navy
President, National Defense University

Acknowledgments

This book draws on publications of the Program on Information Resources Policy at Harvard University. The Program has a unique method of operation, aimed at providing research for policymakers with a non-partisan perspective that permits an impartial overview of the subject. For that reason, a short description of the goals and methods of the Program will help put this work in context.

In order to do impartial policy research, the Program was established in 1972 with a novel funding mechanism. Because it would be dealing in areas of high stakes and corporate and political self-interest, it set out to establish a broad base of financial support from all sides on an issue that the Program addresses. (Contributors current to publication of this book are listed below.) The Program has participants from all segments of the information business, as well as organizations that are consumers of information. Competing industries and competitors within industries are represented.

The preparation of this book, as with the Program's other publications, was undertaken on the Program's own initiative and on its own terms. During preparation, the editor, Lt. Col. Thomas P. Coakley, was on sabbatical leave from the United States Air Force Academy and serving as Senior Research Fellow with the National Defense University. The excerpts are drawn from proceedings of the Harvard Seminar on Intelligence, Command and Control conducted at the John F. Kennedy School of Government since 1980 by Anthony G. Oettinger, Professor of Information Resources Policy, and John F. McLaughlin, Executive Director of the Program on Information Resources Policy. The proceedings were prepared in collaboration with editors and editorial assistants from the MITRE Corporation, and each speaker approved the text of his or her remarks before printing by the Program.

National Defense University's Command and Control Research Program, directed by Dr. Thomas A. Julian, provided instrumental assistance to the publication of this book.

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University Center for Information Policy Research Affiliates
(December 1990)

ABRH Consulting
Action for Children's Television
American Newspaper Publishers Association
American Telephone & Telegraph Co.
Ameritech Publishing
Apple Computer, Inc.
Arthur D. Little, Inc.
Auerbach Publishers Inc.
Bell Atlantic
Bell Canada
BellSouth Corporation
Boice Dunham Group Inc.
Bull, S.A. (France)
Centel Corporation
Chronicle Broadcasting Company
CMC Limited (India)
Commission of the European Communities
Communications Workers of America
Computer & Communications Industry Assoc.
COMSAT
Cox Enterprises, Inc.
Data America Corp.
Dialog Information Services, Inc.
Digital Equipment Corp.
Dow Jones & Co., Inc.
France Telecom
Gartner Group, Inc.
GTE Corporation
Hitachi Research Institute (Japan)
Honeywell, Inc.
IBM Corp.
Information Gatekeepers, Inc.
Information Industry Association
International Data Corp.
International Resource Development, Inc.
Invoco AB Gunnar Bergvall (Sweden)
I.T. Direction Ltd. (UK)
Knowledge Industry Publications, Inc.
Korean Telecommunications Authority
Lee Enterprises, Inc.
John and Mary R. Markle Foundation
MCI Telecommunications, Inc.
Mead Data Central
MITRE Corp.
National Telephone Cooperative Assoc.
The New York Times Co.
NEC Corp. (Japan)
Nippon Telegraph & Telephone Corp. (Japan)
Northern Telecom Ltd. (Canada)
Nova Systems Inc.
NYNEX
Ing. C. Olivetti & Co., S.p.A. (Italy)
OTC Limited (Australia)
Pacific Telesis Group
Public Agenda Foundation
Research Institute of Telecommunications and Economics (Japan)
RESEAU (Italy)
Revista Nacional de Telematica (Brazil)
Salomon Brothers
Scaife Family Charitable Trusts
SEAT S.P.A. (Italy)
Southern New England Telecommunications Corp.
State of California Public Utilities Commission
State of Minnesota Funding
TEKNIBANK S.p.A. (Italy)
Telecommunications Research Action Center (TRAC)
Tele/Scope Networks, Inc.
Third Class Mail Association
Times Mirror Co.
Tribune Company
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of State
  - Office of Communications
- Federal Communications Commission
- General Services Administration
- National Aeronautics and Space Administration
- National Security Agency
- U.S. General Accounting Office
- United States Postal Rate Commission

United Telecommunications, Inc.
US West
Williams Telecommunications
Wolters Kluwer

Introduction

"Information is power." The notion echoes through the ages, from Proverbs to the lips of Gordon Gekko, an unscrupulous character in the movie *Wall Street*. Measures of that power range from the political influence wielded by shamans and priests who were well informed about the processes of the natural world to the immense fortunes accumulated by Gekko's real-life counterparts, the Ivan Boeskys who thrive on insider information.

Wall Street's embrace of the information-power equation is reflected in the frequent appearance of books with titles such as *Corporate Intelligence and Espionage: A Blueprint for Executive Decision Making* and *Monitoring the Competition: Find Out What's Really Going On Over There*. *The Wall Street Journal*'s status as a major US paper is yet another indication that information and power go hand in hand.[1]

Primacy of information holds for battlefields as well as board rooms. In the context of national defense, the acquisition and use of information underlie the concept of "Command, Control, Communications, and Intelligence," represented by the cumbersome acronym "C³I" (pronounced "c-cubed-i" or "c-three-i").

Use of the term "C³I" in casual conversation about defense issues elicits a variety of responses. By far the most common is a quizzical look. On the faces of those who pride themselves on their interest in things highly technological and avant garde, the speaker will observe the blank, embarrassed smiles of people who can't quite place something they know they've heard before. If the listeners include members of the military, one should be prepared to see at least a few grimaces of knowing disgust. Electrical engineers and their associates will respond with enthusiastic nods when they hear the term. On very rare occasions, it will draw the furrowed brow and slow, sagacious nod of the C³I theorist. The latter is normally encountered only on the fringes of social science circles.

That most citizens are unacquainted with the term C³I—or its translations: "command, control, communications, and intelligence"; "command and control"; "command systems," and so

on—is surprising, given the fact that C³I has, throughout the 1980s, been "a growth industry," even in the face of Gramm-Rudman-Hollings and other restrictions on federal spending.[2] Both President Carter and President Reagan made improving C³I a top priority, according it, in the words of Senator John Tower, "equal value with the weapons systems in the competition for dollars and the attention of senior Defense Department management."[3]

So the concept of C³I is important and increasingly visible, but what exactly is it? Debates about terminology abound in this area. Though an inelegant phrase, C³I carries with it allusions to timeless elements of support for commanders as well as contemporary connotations ("C³I" looks mathematical or "high tech")—advantages lacking in the otherwise attractive alternative of simply using "command" in an all-inclusive sense.[4] More importantly, "C³I" has the advantage of currency: while many experts dislike the term, they all recognize it.

The concept of C³I probably originated in an attempt to apply systems analysis, with its connotations of mathematical precision and efficiency, to command and other functions which directly support command. Take away those things usually thought of as the substance of defense—weapons, ammunition, fuel, logistics, spare parts, buildings, people—and C³I is what remains. Ideally, C³I is what melds the "stuff" of defense together into an effective fighting machine.

A useful way to look at the concept of C³I is in terms of an analogy with the human body (Table 1). The central nervous system

Table 1 C³I and the Human Body

	Body	Function	C³I	
1	Central nervous system (brain and spinal cord)	Sorts out information and issues appropriate orders to the muscles or glands	Command	Central nervous system
2	Motor nerves	Carry outgoing information to the muscles	Control	Peripheral nervous system
3	Sensory nerves	Provide information about the outside world or the state of the body	Intelligence	Peripheral nervous system
4	Action potentials (electrical charges)	Format information to and from central nervous system	Communications	"Instrumentalities"

exercises the body's **Command** function: receiving information from the sensory nerves, processing that information, making decisions—some conscious, some automatic—based on that information, and sending orders by way of the motor nerves. The motor nerves themselves are analogous to a commander's **Control** function which consists of channels—organizational structures or "lines of command"—through which the commander's decisions, in the form of orders, pass to the forces charged with carrying them out, just as the orders of the central nervous system are passed to the body's muscles. The sensory nerves provide information about the outside world and the state of the body, just as the **Intelligence** function provides a commander with information about enemy forces and the state of friendly forces.

In Table 1, the motor nerves and the sensory nerves constitute the "peripheral nervous system." Direction differentiates the two elements of this system: one is directed toward the central nervous system; the other, away. Some experts on C³I see the control as "friendly intelligence," the means the commander has for keeping track of the status of his or her own forces.[5] While control is used in a slightly different sense here, the C³I-Body analogy fits both views.

Messages to and from the central nervous system take the form of minute electrical changes—"action potentials."[6] They are the means, the "instrumentalities"—to use Anthony Oettinger's term for the **Communications** function of C³I—by which information and orders move to and from the central nervous system.[7] Though the body's action potentials and C³I's communications are subsidiary aspects of their respective systems, neither system could function without them.

The advantage of using a systems approach when studying either the human body or national defense is that one is less prone to leave out something vital. Just as some body builders seem to slight the intricate system that develops and coordinates all those well-formed muscles, some defense advocates are inclined to slight the systems that make something useful of the "stuff" of defense. Fascinated by the latest developments in jets, ships, and tanks, they forget the C³I systems vital to using those weapons effectively. The bottom line is that a body without a nervous system is a useless lump of rapidly decaying matter; a defense program without good C³I is just as worthless.

Perhaps the breadth and significance of C³I may be best understood by examining the concerns encompassed by each element of the term. In a defense context, **Command** covers the range of organizational levels from the National Command Authority (NCA)—the President and those who succeed the President in command—to the soldier in charge

of a small patrol. At each level, it involves receiving and assessing information about the environment (enemy, friendly forces, intentions, positions, capabilities, and so on), generating and considering options, selecting a best option, and sending out the orders to implement that option. Thus, the exercise of command can cover everything from devising a strategy for nuclear deterrence to getting a patrol back to friendly lines. Persons in positions of command must concern themselves with how much information they want to receive directly, how much they want filtered before it reaches them, and who is to do the filtering. They must also resolve how much leeway to give subordinates, how quickly or slowly to respond to changes in the environment, how to allocate resources, and a thousand other issues.

Control, as used here, describes the channels or "lines of command" through which a commander's orders, advisories, admonitions, queries, and so on, pass to his or her forces. Such lines reflect responsibility as well as authority: "You're in charge. If the job doesn't get done, you'll be fired." Unfortunately, the concept of control is often clearer in theory than in reality, a problem demonstrated in the Department of Defense's *Dictionary of Military and Associated Terms*. That publication defines "control" as

> That authority exercised by a commander over part of the activities of subordinate organizations or other organizations not normally under his command, which encompasses the responsibility for implementing orders or directives. All or part of this authority may be transferred or delegated.*

Further nuances come into play with the application of adjectives such as "administrative," "operational," and "tactical." In Chapter 4, extracts from General Cushman's presentation highlight some of the practical difficulties that result when the lines of control are not clear-cut.

The higher the level of the commander is, the more attenuated control becomes and the greater the risk of information loss or distortion as it moves to and from the commander. At the low end of the spectrum, a commander will probably be able to establish control according to his or her individual requirements; at the high end, a commander will be obliged to use the lines of command established by Congress or the Department of Defense (DoD). If a commander isn't comfortable with the established control channels, he or she may be tempted to supplement or circumvent those channels through the creation of informal ones. It will also be up to the commander to determine when it's appropriate to adhere closely to established lines of command and when to skip one or more echelons.

Communications are the means by which information is carried back and forth between the commander and the commander's forces, sensors, allies, and perhaps even the enemy. The term "communications" includes everything from runners and carrier pigeons to the most sophisticated and secure electronic transmission devices. A commander will want communications to be dependable; secure from enemy interception or interruption; interoperable—able to connect his or her own force elements with each other and with allied forces; and easy to use, especially in the heat of battle. Seldom having equipment that will satisfy all of those criteria, the commander will have to use tradeoffs to determine the best mixes of available communications systems.

Intelligence is the collection, analysis, and presentation (to the commander) of information about an enemy, potential enemy, or the commander's own forces. When intelligence insiders toss about terms such as "HUMINT," "SIGINT," "COMINT," and "IMINT," they're referring to various sources of intelligence: spies, intercepted telemetry or communications, pictures taken by "spy satellites," and so on. Intelligence sources may also be classified as open (newspapers, TV and radio broadcasts, public data banks) or clandestine. Major intelligence issues concern the allocation of resources between collection and analysis and between human and electronic sources; the legitimacy of covert action as a function of intelligence agencies; and the role of Congress in overseeing intelligence activities.

Further contributing to the complexity of C³I is the matter of perspective. Different "communities" of experts have very different perspectives on C³I issues. Historically, members of the military services have tended to downplay C³I, emphasizing instead the "stuff" of defense: "Give me the right stuff—better bombers, better fighters, better tanks, better ships, and I'll get the job done. Don't waste those precious defense dollars on radios, or telephone lines, or command posts when we don't have as many weapons as we need."

Engineers—the "techies" or "wireheads"—are often inclined to put all of their emphasis on the mechanics of C³I—radios, computers, satellites, local area networks, and so on. Describe a problem and they'll immediately start looking for a technical fix. Say "C³I" to techies and they'll hear "communications"; in fact, the techies often refer to themselves as "communicators." That's ironic, because many people outside the engineering community find the language of the "communicators" incomprehensible. That language, of course, reflects their backgrounds in mathematics, science, and engineering. They belong to what experts in cognitive development call a "specialized

community of discourse," a group which shares vocabulary and usage patterns not readily understood by the less technically-oriented.

C^3I theorists approach the subject with still a different perspective. They insist on modelling as the first step in the complicated process leading to improved C^3I. Start anywhere else and you risk losing sight of important requirements for your system. To many theorists, members of the military community seem hung up on traditional ways of approaching problems, on "school solutions"; they see techies rushing about with no sense of direction. In turn, the military and techies see theorists as irrelevant, lost in abstraction.

One's position in the hierarchy can also affect perspective. The fact that modern communications will allow the President to talk directly to the soldier in the foxhole may be perceived as a plus by the President, while the soldier (or the soldier's commander) sees it as a distraction. The military services may see a new approach to acquiring communications equipment as streamlining, while Congress sees it as an invitation to fraud. A restriction an intelligence officer sees as necessary to protect sources may be perceived as an obstacle to thorough planning by an operational commander. While the White House is focusing on how to improve information flow upward, from the field to the Commander-in-Chief, the military may be more concerned with getting the battlefield commander the information he or she needs. In short, the C^3I area offers many opportunities for honest men and women to disagree about what constitutes an improvement.

While such a variety of perspectives can be fruitful, being so requires that adherents of the various perspectives interact with each other. In the old story of the blind men and the elephant, each man fooled himself into believing that the part of the elephant he had in his grasp was the key to the elephant's essence and that his peers were both literally and metaphorically blind. Thus, in the absence of real dialogue, differences of perspective can lead to long and fruitless pursuits down multiple blind alleys. That has often been the case in the domain of C^3I.

The fruitful development of that domain requires the participation of the military, with its knowledge and experience of operational conditions; engineers, with their grasp of what is possible; and theorists, who can provide insights into the functioning of the human elements in C^3I systems, as well as the broader picture of what such systems should be designed to do and how their elements should fit together. It requires the participation of decision makers, procurement and intelligence specialists, and operational commanders as well. The exclusion of one or more of these perspectives can result in costly, tragic failures such as the

devastation of Pearl Harbor; the loss of the USS *Pueblo*; the needless loss of life in the *Liberty*, *Mayaguez*, and *Stark* incidents and in Grenada; the bombing of the Marine barracks in Lebanon; and the USS *Vincennes*' downing of the Iranian airliner. In a nuclear confrontation, the costs of C³I shortcomings would likely be far worse.

In 1980, Harvard University's Program on Information Resources Policy began a series of annual seminars in which policy makers, military leaders, government and business executives, scientists, engineers, and theorists involved in the design, testing, procurement, and use of C³I systems and concepts presented their insights and participated in discussions with a select group of graduate students. Under the guidance of Anthony G. Oettinger, Professor of Information Resources Policy, and John F. McLaughlin, Executive Director of the Program on Information Resources Policy, the seminars became an occasion for dialogue among the holders of various perspectives on C³I. Each discussion explored the ways "institutions draw on systems of people, policies, and technologies to gather and use information for survival and growth."[9]

The transcripts of seven years of seminars (there was no seminar in 1983) amount to roughly 1300 pages of unclassified material, a fascinating variety of insights from an impressive group of C³I experts.[10] All of the material is readily approachable for an intelligent reader, regardless of his or her background. Based on spoken presentations and discussions, and edited for coherence, the transcripts offer an excellent foundation for the kind of interaction among experts that has long been needed.

Unfortunately, 1300 pages is a lot of reading. It is enough to put off many of the people who could benefit most from the insights contained in the transcripts, which are in chronological, not topical, order. Each presentation covers a wide variety of issues, making the task of focusing on a particular subject a demanding one. Furthermore, finding a set of the transcripts may be difficult for the individual who lacks ready access to a major library.

Hence, this book—a compilation of the extracts (1980–82 and 1984–87). Each chapter is devoted to a single topic, with the extracts within the chapter arranged chronologically. Acronyms, a major distraction of C³I-speak, and other terms and references that may not be immediately familiar to all readers are **boldfaced** and explained in "cut-ins." Informational cut-ins are also used to provide information about the speaker at the time of the presentation. Appendix A gives a brief career summary for the speakers whose comments are included in these extracts. Appendix B lists all of the seminar speakers and the titles of

their presentations. Not all are represented in these extracts because some of the seminars focused on topics not germane to this book.

Chapter 1 is concerned with "C³I in Crisis Management." It covers issues as diverse as protecting the National Command Authority and controlling the information flow to the President and other decision makers. Chapter 2, "C³I Structures," examines the links between C³I and nuclear strategies, perceived strengths and shortcomings of existing C³I arrangements, and the directions C³I planning should take. Chapter 3, "Improving C³I," deals with the special problems associated with designing, acquiring, and modifying elements of C³I—from communications equipment to computerized decision aids. The fourth chapter, "C³I and Organizational Structure," explores the relationship between recent emphasis on C³I and the Defense Reorganization Act of 1986. "The Eyes of C³I," the final chapter, is concerned with intelligence issues.

One may, with Moshe Dayan, lament the passing of "the good old days of the simple wars when, as the hour of battle approached, the commander got on his white horse, someone blew the trumpet, and off he charged toward the enemy."[1] But gone those days are, and today's leaders must be willing to exchange their white horses for C³I systems that enable them to function effectively on modern fields of battle—places where specialization, complex technology, and unprecedented mobility leave the inflexible behind as footnotes to history. This collection of extracts is intended to help decision makers—from battlefield commanders to business and government executives—sort out the issues involved in establishing a C³I system that gives them the flexibility needed to survive and lead.

Notes

1. Richard J. Levine, "Electronic Publishing for Business Intelligence," *Seminar on Command, Control, Communications, and Intelligence*, Spring 1986 (Cambridge, MA: Harvard University Program on Information Resources Policy, 1986), p. 121. The books referred to in this paragraph are Richard Eells and Peter Nehemkis, *Corporate Intelligence and Espionage: A Blueprint for Executive Decision Making* (New York: Macmillan Publishing Company, 1984) and Leonard M. Fuld, *Monitoring the Competition: Find Out What's Really Going On Over There* (New York: John Wiley & Sons, Inc., 1988).
2. Philip S. Kronenberg, "Command and Control as a Theory of Interorganizational Design," *Defense Analysis*, Sept. 1988, p. 229. Though usually referred to as "Gramm-Rudman," the deficit reduction bill of 1985 had Democratic Senator Fritz Hollings as a main sponsor along with Republican senators Phil Gramm and Warren Rudman.
3. Francis W. A'Hearn, *The Information Arsenal: A C³I Profile* (Cambridge, MA: Harvard University Program on Information Resources Policy, 1984), pp. 1-22, 1-25, 1-28.
4. Martin Van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), p. 1.

5. A'Hearn, p. II–6.
6. "Nerve Conduction," *Encyclopaedia Britannica* (Chicago, IL: Encyclopaedia Britannica, Inc., 1971).
7. Gregory D. Foster, "The National Defense University's Command and Control Program," *Seminar on Command, Control, Communications, and Intelligence*, Spring 1987 (Cambridge, MA: Harvard University Program on Information Resources Policy, 1988), p. 2.
8. "Control," Department of Defense, *Dictionary of Military and Associated Terms* (Washington, DC: Government Printing Office, 1979).
9. Program on Information Resources Policy, "Proceedings," *Seminar on Command, Control, Communications, and Intelligence*, Spring 1987 (Cambridge, MA: Harvard University Program on Information Resources Policy, 1988), p. vii.
10. All speakers were advised that the seminars were unclassified and open to the public. The speakers edited the typed transcripts prepared from tape recordings of their sessions.
11. Quoted in Van Creveld, p. 17.

C^3I:

Issues of Command and Control

1

C³I in Crisis Management

The earliest extracts in this chapter bring out some startling facts about deficiencies in US crisis management capabilities. In the 1970s, despite nearly a half century of Cold War experience, we were in some ways as naive and our methods as primitive as they had been in 1945. Once capable warning and response systems had been outdistanced by technological change as administration after administration focused on developing the muscles of US military forces, rather than creating a nervous system to enable and control those forces, as well as the other elements of national power.

In the late 1970s, the Carter Administration began to examine the implications of these changes. The Reagan Administration continued the examination and attempted to remedy some of the shortcomings. The extracts presented here in chronological order reflect the accumulated wisdom, shifting concerns, and improvements between 1980 and 1988. Unfortunately, not every shift in concern reflects a remedy discovered. Sometimes such a shift is the result of frustration, a movement of attention from that which cannot be fixed to that which can. As a result, none of the questions about crisis management raised here are irrelevant today, and none of the answers are final.

The questions asked reflect the broad scope of the topic. When a crisis arises—be it a nuclear attack or a revolution in Yemen—will the President of the United States have available everything he or she needs to respond rationally? If sensors detect a missile aimed at Washington, D.C., will the President and other decision makers hear about it in time to do anything? Will they know where the missile is coming from? Or who launched it? Or whether the launching of that missile is part of a coordinated attack or a freak accident? Once the decision makers select the appropriate response, will they be able to communicate their decision to those charged with carrying it out?

If the decision makers learn the government of Yemen is under attack, will they know whether that's good news or bad? Will they know who is behind the attack and whether it's likely or not to succeed? Will they know how Yemen is linked with US security interests? What interests our closest allies have in Yemen? Where Yemen is?

How do we protect our National Command Authority (NCA)—the President, the Secretary of Defense, and others with access to the codes required to launch nuclear weapons? How can we organize the flow of information—including intelligence—so that the NCA has all the data necessary to make informed decisions? Should the President assume he or she will have the means—communications as well as weapons—to choose options—including the option of fighting a "sustained" nuclear war?

Such questions, in turn, suggest subsidiary questions. In protecting the NCA, should the focus be on protecting individuals or functions? When do we reach a point where there are too many fingers on the "button"? At what level does a crisis demand NCA attention? How can the President use modern communications, which allow him or her to talk directly with the soldier on the scene, in ways that provide positive control without "micromanagement"? How dependable are our facilities for warning? Do they provide enough time for rational decision making? What information sources should be available to the NCA? How do we avoid overloading decision makers with too much information? How do we avoid bias in filtering information for the decision makers?

Some might argue that the phrase "crisis management," with which all of these questions are concerned, is itself an oxymoron, that an efficient manager heads off a crisis before it occurs. Such an argument, however, assumes not only that the manager has all the information he or she needs to spot a crisis in the making, but also that he or she wishes to avoid the crisis.

The latter assumption is probably safe if the crisis in question relates to nuclear weapons. Seldom will a rational decision maker be tempted to foment a nuclear crisis. However, the vast majority of crises do not involve nuclear weapons. It is, therefore, certainly conceivable that a decision maker might see advantages in having a particular crisis arise at a particularly favorable time—perhaps to avoid having it crop up on a less auspicious occasion in a less manageable form, or to draw attention away from another issue.

The first assumption—that "the manager has all the information he or she needs to spot a crisis in the making"—would be valid if all the popular myths about contemporary intelligence capabilities were true. However, what emerges from these extracts, as well as from extracts in subsequent chapters, is that the US intelligence gathering apparatus—like that of the USSR—is impressive but not perfect.

Most experts admit there has never been and will never be a perfect intelligence system. Every system will have its technological and procedural blind spots. Some things or activities may be hidden or disguised well enough to frustrate the efforts of the most sophisticated satellites and sensors. In other cases, habit, policy, or unwarranted assumptions may keep the intelligence apparatus from being directed toward the right place at the right time. Even if the required data is picked up, it may not reach the decision maker in time or in a form that will allow him or her to respond appropriately. Plenty of examples, from Pearl Harbor in 1941 to the attack on the USS *Stark* in 1987, underscore this possibility.

Crises occur and will continue to occur. And every crisis must be managed—or submitted to. Decision makers, recognizing they will never have all the information they need, nor infallible communications, must build flexibility into their crisis management systems and must exercise those systems in ways that nurture adaptability.

Extracts

1. WILLIAM ODOM, "C³I and Telecommunications at the Policy Level" (1980, pp. 1–23)

Military Assistant to the President's Assistant for National Security Affairs

[N]o staffer can manage crises. Once a crisis starts you can bet your life that, if you are the crisis manager's staffer, you will be kicked aside and all the principals, the President, the Secretaries, will take over and run it, and you might as well go home. During the crisis—that's the time to be away—that's your staff responsibility.

. . . [W]e became intimately involved in rigging the President up for **SIOP** execution. . . . I was very proud of that effort, because it led to the President becoming personally involved in exercising command and control of the strategic forces. I don't think that has ever been done before. Kennedy may have played around with it a little, but the President's attitude toward command and control, particularly of the strategic forces, has typically been one of benign neglect. But President Carter opened up his decision handbook, he really got into the procedures, ran through numerous scenarios and became very comfortable with it. He wanted to be able to be awakened at three o'clock in the morning and not be confused, and understand what he was going to have to see, or what he was about to hear, what the voice would sound like on the other end of the line, and that sort of thing. We covered that particular aspect of command and control over a period of about a year, or a year and a half, and we achieved a fair amount. (1–3)

SIOP—Single (sometimes Strategic) Integrated Operations Plan, here the targeting plan for nuclear weapons

2. RAYMOND TATE, "Worldwide C³I and Telecommunications" (1980, pp. 25–47)

former Deputy Assistant Secretary of the Navy and Deputy Director, National Security Agency

I believe the era that began when John Kennedy was President during the **Cuban missile crisis** has led to many of the activities we will discuss today. Kennedy's ability to negotiate and carry out a big portion of the President's responsibilities failed during the Cuban missile crisis because of communications. He was, for example, totally unable, in the time period available at that time, to advise every South American ambassador through the Department of State that he was going to invoke the Monroe Doctrine—that he was going to take positive action against Khrushchev's introduction of missiles that he thought were offensive into the island of Cuba. That system literally fell on its face, not only to his chagrin, but to his outright rage, I have been told.

Cuban missile crisis—October 1962

... [M]ore and more of the decision-making process—the coordination of the process and the business of decisions themselves—depends largely, and in some cases even totally, on communications. For example, the law now says that *before* the President can actually use troops, even though he has the authority in some cases, he must consult with key members of Congress. Since the Watergate crisis Congress has injected words concerning **advice and notification** of the leadership of the House and the Senate. I know of examples under President Ford (the ***Mayaguez* incident** was one) in which hours were spent trying to find a key senator on a Sunday so that the President of the United States could comply with the current law and notify him that he was going to take action. I think things like that need to be understood in context. So we have recognized in many forms the utter essentiality of these communications, even in the decision-making process of this country. Their availability, timeliness, security and effectiveness are critical.

advice and notification—refers to the War Powers Act of 1973. The Watergate crisis resulted in President Nixon's resignation in 1974.

Mayaguez incident—In 1975, communist forces from Cambodia seized the US-flag freighter Mayaguez. A small force of Marines was sent to recapture the ship and its crew.

... The *Liberty*, to refresh your memory, was one of the seven World War II Liberty Ships that had been reconfigured as intelligence collectors, much like the Soviet trawlers which you have been aware of for quite a long time. The USS *Liberty* was monitoring the Egyptian-Israeli war of 1967 when the Israelis dispatched a flight of tactical aircraft and came very close to sinking the ship. Some of our people suffered casualties, both military and civilian. The Israeli Intelligence Service knew that the ship was there, and knew what was being done with it, a fact which has made this event extremely

controversial for a long time. The context in our terms here is that the commander of the Sixth Fleet was informed by the Washington intelligence apparatus that it had evidence that the *Liberty* was going to be attacked and to provide protection for it. That message was never really acted upon, and the ship was dead in the water when it was hit. So the end result was no accident.

You are probably more familiar with the ***Pueblo* case**. There has been a Congressional investigation, the results of which are in the public domain. I was a first-hand participant in one small phase of the *Pueblo* operation; the National Security Agency notified the National Reconnaissance Center in the Pentagon of the danger of an attack more than two days in advance. The Center notified the Naval Command in Japan of the likelihood that the North Koreans would take offensive action against the *Pueblo*, and that they should take that into consideration. The *Pueblo*'s deployment schedule itself was a function of the local fleet command, not the National Command. This turned out, as the investigation indicated, to have been a snafu through the command and control system. Several different commands were blamed, but the bottom line is that it did not work. The ship was not notified, and we had not only a physical disaster to a United States Navy ship—the first one ever hijacked on the high seas—but personal embarrassment to the government of the United States.

Pueblo case—*USS Pueblo, an intelligence-gathering ship, was seized by North Koreans in January 1968. The ship's 82 surviving crew members were released 11 months later.*

In 1969 something very similar happened to the EC-121 aircraft, a converted propeller-driven Constellation on an intelligence mission in South Korea. It's almost a carbon copy of the other incidents. The North Koreans' intentions were known to the military system; yet the EC-121 was not notified, and was shot down with total loss of life.

Another case: the Saigon evacuation in 1973. We had very good clear-language communication to the end of the evacuation, but there were a lot of problems because it was unsecured, and in fact the North Vietnamese had total monitoring going on and knew exactly what was occurring during the entire period. Another example is the communication during the *Mayaguez* incident. From a command and control standpoint they were significantly better than in any of the other crisis periods I have mentioned. Yet from my point of view (at that time I was the senior cryptographer for the United States) it was a disaster, and needlessly cost the lives of a number of Marines. I will show you exactly how that occurred and why in a moment.

Now in the Lebanon crisis the Sixth Fleet actually landed Marines, and the command and control of that operation was much better. We still had crypto problems, but the President had virtually constant touch with the military force involved.

So we have gone through six major international crises, plus of course the **present hostage problem** which is really of a different nature. But the Presidents even by 1976 have had improvements in their ability to act as Commander-in-Chief and direct command operations through the system—a great deal better than they had in previous years, although there still are some problems, as in the *Mayaguez* case, that while the President had command and control, the enemy knew everything he was going to do at about the same time as the commanders on the site, and took some direct actions against them. The White House issued orders in the *Mayaguez* incident down the National Military Command System, which went through a borrowed satellite, the NATO IIB. (The point where the security broke down was the Naval Command at **Clark Air Force Base**, under the Commander of the United States Seventh Air Force coordinating to the Seventh Fleet, which was in Japan but deployed units all over this area.)

the present hostage problem—On 4 November 1979, militant Iranians invaded the US Embassy in Teheran, taking 66 hostages. The hostages were released on January 20, 1981, Inauguration Day for President Reagan.

Clark Air Force Base—Base in the Philippines used by the US Air Force under the terms of the Security Assistance Program agreement

The forces that transmitted the orders were using **HF voice, all in the clear**. Orders to the helicopters to take the islands were passed from the Air Force to the Navy. Over the circuit the two commanders revealed how many helicopters and how many men were involved, where they were going, at what time, and the replenishment rate. I don't know anything more an enemy commander needs to know in order to defend himself against an operation. Even if uneducated, he had the information to take action against our force, and he did. A number of the helicopters were shot down—the most dangerous part was the retrieval. We did not have the helicopter force to retrieve the Marines as close to simultaneously as possible, so there was a delay of several hours between one wave of retrieval and another. There was quite a battle going on there and both sides were fighting hard. Once the first wave of Marines was evacuated, that left the remaining ones very vulnerable. The forces were very greatly diminished, and that was when the Marines took the heaviest casualties and actually lost a full helicopter load of Marines. All

HF voice, all in the clear—insecure High Frequency voice communications

the information, the plans for that retrieval, were passed through those unsecured nets. I know two men, now Major Generals in the Marine Corps, who went through that operation and are still extremely bitter about that involvement; it was their units that took the losses. The point is, we talk of command and control as a method of using communications to carry out the will of our command authority. But I can tell you, unless those communications are secure, many times it is better not to have them.

... [T]he Situation Room at the White House has a direct line to the **NSA**. And the warnings in the crisis periods I talked about did not, in fact, go serially through the chain of command. They go in parallel. Therefore the Situation Room in the White House is notified immediately when NSA decides there is a serious problem. So this is a short-circuit for what is called critical intelligence that goes directly to the President of the United States; and nobody can stop it unless they physically do not show the President the warnings. This system was set up after the Cuban missile crisis, largely by John Kennedy, and it still works today. If you think it is a sterile system in which everybody works together and it works without flaws, forget it! It is a human system that has personalities.

NSA—National Security Agency

... [L]et me tell you that one of the biggest complaints the senior military people in all three Services have today—they are going to be faced with it forever, and they know it—is that nuclear weapons have changed the concept of warfare in a lot of subtle ways. One of the ways is that there is no absolute military command authority. Mainly it's the President, in my view, who is going to detonate a nuclear weapon with great devastation. He must exercise as much constitutional authority as he has over any facet of his office, and it's probably more important than most.

In the early days of **nukes and ICBMs** I participated in a study to determine how to control the weapons centrally. At the time we didn't know what was going to develop, but I'd get violent reactions, because what we were talking about was planning command and control over nukes—not downward from the headquarters of the United States Air Force through the Fifth Air Force to a wing commander to a squadron commander to a captain to a sergeant or a lieutenant; but from the White House. The military has not yet changed substantially from a basic resentment of this fact. Fundamentally

nukes and ICBMs—nuclear weapons and Intercontinental Ballistic Missiles

the system—During 1961 and 1962, Permissive Action Links (PALs), electronic locking systems, were installed on US nuclear weapons in the United States and Europe to prevent unauthorized detonation.

JCS—Joint Chiefs of Staff

the system still works as it did. I've been in the White House many nights and seen Lyndon Johnson anguished and seldom going to bed, selecting between two or three targets. The **JCS** gave him all the targets—but the decisions on how many civilian casualties, or the potential of this or that, were all made by the President. And that wasn't even a nuclear exchange. Whether it is right or wrong is a different matter; all I am telling you, after watching this system for better than 25 years, is that's the way it works. I don't think anybody is going to change it, particularly with respect to nuclear weapons. No Soviet commander, thank God, without overt, direct, violent disobedience of orders, can make the nuclear decision himself without the **Politburo**'s approval. And nobody in this country, or **NATO**, can do it without the President of the United States' approval. Talk of the **"NATO nuclear capability"**—forget it. It's an American capability that can only be released by an American officer. And this has changed the military structure. It's just that the structure hasn't caught up, or chosen to align its command structure to demonstrate that. But that's the real world.

Politburo—supreme executive body of the USSR's Communist Party

NATO—North Atlantic Treaty Organization

NATO nuclear capability—Both Great Britain and France have independent nuclear capabilities. The French are known to have a locking system in place. No public knowledge of a British PAL-type system is available.

[STUDENT] You mentioned how centralized nuclear authority is. Can you comment on the methods or techniques by which this sort of authority is reserved to the President? Because I think one of the dangers is that, by making it impossible for the subordinate commander to illegally use nuclear weapons, you are very narrowly restricting the number of targets the Soviets need to hit to "decapitate" the command authority so that we are unable to respond with nuclear weapons.

[TATE] No. My activity made all of the devices and codes that create a chain of command for nuclear release. The way it is designed is that the President, the Vice President and the Speaker of the House on the civilian side, and the Secretary of Defense, the JCS, the Military Command Post and the Alternate Command Posts all have the capability of acting as the central authority, in some sort of succession. The codes and devices are set up to allow that. So if all else goes, the airborne commands can take over and be the central authority, with all the capabilities—**CINCSAC, Looking Glass**, etc. (26, 29–30, 34, 42, 43)

CINCSAC, Looking Glass—Commander-in-Chief, Strategic Air Command (SAC); SAC's airborne command post—always in the air, commanded by a general officer who has authority to launch nuclear weapons

3. **ROBERT ROSENBERG**, "The Influence of Policy Making on C³I" (1980, pp. 49–65)

Policy Assistant to the President for National Security Affairs, National Security Council Staff

So in parallel with one Presidential Directive and countervailing strategic posture, a lot of real things were happening which started getting the attention of the leadership policy makers. Early in the administration President Carter became the first President ever to fly in an Airborne Command Post. He said, "I don't understand what good this multimillion-dollar affair is. You say we are going to buy six of them? Well, why not two or three at the most?" He was immediately struck with its mammoth size, the fact that it can't stay in the air forever, that it is not nuclear-hardened, that a 747 takes a runway capable of withstanding very considerable loads. We all fly on 747s and L-1011s, but you would be surprised how few airports in this country can take the landing loads of the 747; and when you stock it full of computer equipment and electronics the way the Airborne Command Post is, you can imagine the tremendous load. When the President questions the viability of such a thing, it leads to a very interesting exercise. A couple weeks later, **Dr. Brzezinski** got on the telephone and called the man you all have heard about who carries the little briefcase with all the codes inside, and said, "This is an exercise. I am the President of the United States. We have just gotten warning that a raid of nuclear warheads is en route to the United States. Get me out of here. This is an emergency exercise. We are going to war." The helicopter that is supposed to be on alert at all times, to land on the White House lawn and whisk away the National Command Authority, almost got shot down by the Secret Service. (By the way, this was kept secret for quite some time until it got blown in the newspapers, which is the only reason I am able to tell this story. I think we were ashamed of the horrible state of readiness we were in.) The sum and substance is that the exercise of trying to evacuate the National Command Authority and set up his communications was a nightmare, just a complete disaster. (60)

Dr. Brzezinski—Zbigniew Brzezinski, President Carter's National Security Advisor

4. **LEE PASCHALL**, "C³I and the National Military Command System" (1980, pp. 67–86)

Consultant, formerly Director, Defense Communications Agency and Manager, National Communications System

Our structure, our strategy, our military forces are trained and will obey the order that says only the President can release nuclear weapons. Seventeen

minutes is the time of flight from the normal Soviet submarine ballistic launched missile patrol distance off the Atlantic Coast to the White House. So from the time somebody sees something launching on one of those satellite sensors, or one of the radar sensors along the shore, seventeen minutes is decision time. That's a very short time indeed. Moreover, people don't want to believe news like, "They have launched, the world is coming to an end, it's time for you to launch in return." President after President has called for options, more options. Each option called for imposes an enormous demand and strain on the command and control system. So how are we to solve decision time problems? How can we make warning completely credible to the President or to his successors? How do we ensure that the successors can communicate, can establish contact with the force commanders to execute the retaliation or the strategic reserve, or continue to negotiate, or whatever? There's a very difficult task. Technocrats talk about computer-based executive aids, about making warning more and more credible, and they tend to forget there's a man who's got the world's fate in his hands, and he's got seventeen minutes, and that's just not very long. That's why military doctrine is so emphatic about building a force structure that will deter war. Deterrence is simply a state of mind, and a command and control structure capable of absorbing a strike and functioning thereafter, or being reconstituted to execute the strategic reserve, is a very important part of that deterrence state of mind. The enemy must believe he could never decapitate us, in the sense of killing the decision maker and preventing the decision to launch from being transmitted. That's why command and control systems are so important to the military, and that's why we've learned so many lessons over time. (84)

5. **WILLIAM E. COLBY**, "The Developing Perspective of Intelligence" (1980, pp. 115–39)

Counsel, Reid & Priest; former Director of Central Intelligence

[T]here's very little you can do about that tendency to reach for more raw material and subject it to multiple and even public analysis. The fact is, you know, it's the way we've been operating in crisis all along that's the tragedy. The theory is that the analyst is the screen, thinks about intelligence and then gives a judgment. But every time you hit a crisis, bang! It all short-circuits. I've seen the President of the United States pick up raw reports right off the cable line, cutting out of the circuit the very person he should turn to at exactly the time he's most valuable. Now, how do you get the analyst back into it at a time of crisis? I think you get him back into it by

making the material more broadly available beforehand, so that the thought process has already gone into the material and the President doesn't think the raw data is the only source he had—he's aware that he has a lot of other centers of analysis working with him. Then I think he'll pay more attention to intelligence analysis. (128)

6. **B.R. INMAN**, "Managing Intelligence for Effective Use" (1980, pp. 141–61)

Director, National Security Agency and Chief, Central Security Service

I went to the staff of the Navy's Commander in Chief, Pacific Fleet to head the current intelligence operation. From there I watched a series of events, including the seizure of the *Pueblo* and the loss of an EC–121 off Korea. I began to spend a lot of time examining how our government had structured the flow of information. A system had been established years ago so that, on anything that might be a crisis, information should flow from the point at which it was detected to the highest levels of government and be available to the President within ten minutes. But no comparable attention had been given to what pattern of flow should be orchestrated to insure that information is available to support the conduct of military operations. As a sideline observer with the time to take notes and analyze, I found that in each of those two major crises the Washington decision makers did indeed have knowledge, widely spread among the departments, within ten minutes of the event. And in a very uncoordinated way they went about making telephone calls to various places around the world seeking individual pieces of information. Those who had command of forces got the information no sooner than an hour and five minutes after the event, because it had to stack up behind all the other reports that were coming at flash precedence.

... But in crisis monitoring the flow of that information up to the principal decision makers has never been a problem. The problem you get is in the US structure for deciding plans based on policy. There you can run into all kinds of bureaucratic approaches and priorities. The Joint Chiefs of Staff will not want to discuss their detailed contingency planning with other departments. They believe they have the expertise, and they don't want to spend much time being critiqued by the other departments, where they think there's less expertise. Or the President and the Secretary of State will insist that all information about negotiations flow only to them and not include the Secretary of Defense, the Joint Chiefs, etc. Inevitably, in instances where I've seen that occur, it is not because they don't trust them, it is simply a question of limiting the possibility of leaking the information. The basic rule

is that the more communication centers and administrative personnel you flow through on the way to the principals, the greater the danger of that information being leaked by someone who either is simply trying to curry favor or disapproves of policy. (142, 150–51)

7. **CHARLES W. SNOIDGRASS**, "Funding C³I" (1981, pp. 119–46)

Vice President, Electronic Data Systems Corp; former Assistant Secretary of the Air Force for Financial Management

[T]he compression of time because of technology has become so dramatic that there is no longer the luxury of just doing it by the numbers and through the organization chart. Indeed in my experience, while the organization chart is still followed in times of stability and relatively low-level issues, when it came to the *Mayaguez* and **Bay of Pigs** crises, the **evacuation of Lebanon** or something like that, the organization chart was thrown out and the personal structures started to become the real C³ backbone of the government, and the fact that **Harold Brown** had established a relationship of confidence with the President was a more important influence on whether his advice was followed than what the National Security Act of 1947 says. Indeed you can find nothing in the National Security Act that says the President should speak to the commander of the **Iranian raid** in the middle of the desert after they hit the planes and blew them up, and discuss whether the raid should go on or not—but indeed they did talk to the President. In the Lebanon evacuation Harold Brown, after it was all over, used to brag about the fact that he was in direct secure voice contact with the Marine second lieutenant on the first landing ship that went in, and he knew as soon as the Marine did when the bow of the LST opened up. That's a technological revolution thanks to communications satellites, secure voice scrambling and all the things that interest the codebreaker. And it does dramatic violence to the concept of organization charts, statutory responsibilities, that sort of thing. (121–22)

Bay of Pigs—the failed attempt by 1500 Cuban exiles to invade Cuba, April 17-19, 1961

evacuation of Lebanon—June-July 1976

Harold Brown—Secretary of Defense under President Carter

Iranian raid—the failed attempt to rescue hostages in Iran, April 24, 1980

LST—landing ship, tank—A ship designed to transport and land men and equipment in amphibious assault.

8. **B.R. INMAN**, "Issues In Intelligence" (1981, pp. 193–214)

Deputy Director of Central Intelligence

The popular literature holds that we gave up human intelligence collection assets to buy technical collection capability. I stress: that's a myth. We really gave up manpower-intensive technical collectors; and we did not buy the manpower to process the huge volumes of different additional information which were made accessible by a whole range of technical sensors. If you scan the notes of last year's talk you will know that I picked up much of my interest in the information flow part of this information-need/information-flow equation through watching the government's difficulty in dealing with crises, beginning with the capture of the *Pueblo*, and the impact that slowness in the flow of available information had in restricting the government's options in trying to respond to that crisis. We made very little progress, at least through the first half of the '70s, in dealing with that problem. We had lots of studies and a fair amount of investment in command and control systems that—from this critic's vantage point—too often were focused on ownership questions rather than on the degree to which the systems would accelerate the movement of information to a whole range of people who might be able to make effective use of it. We really did not get any change in the general attitude toward dealing with information-need/information-flow until the end of the 1970s. Now, I believe, we have again crossed a major obstacle: the attitude is moving toward "What do you need to know," not "What can you do without," and there is a growing awareness that much more has to be done than has been done to date in facilitating information flow. As one approaches that, one needs to keep in focus why you need the information, and what are the time limits dictating the speed with which you must be able to move information and assimilate it for decision-making purposes.

... Whether the President changes or not, much of the leadership at the next level tends to change every four years if not sooner. And there is always a learning curve. In some cases you're fortunate—it's only a few months—other times it runs at least a year; and particularly if they stop to study organization you can be sure that it will run longer than a year. There is a tendency to get fascinated early with the nuclear command and control procedures, and to learn how to operate that mechanism. But they do not tend to deal as quickly with command and control problems for contingencies or for crisis monitoring. Frankly, every administration that I've watched since the 1950s has had to get involved in its first crisis before it really focused on how it could get the system to perform, either to really refine its needs, or to decide how it would operate the process.

This is an area where worries about leaks do enormous damage to effective human communications, which is a major factor in making this process work better, faster, more smoothly. A new administration's people come in, they've either looked with horror on, or have benefited from leaks by, the previous administration. They get started; they suddenly start reading about their agenda for the National Security Council sessions, or the results of a meeting which only five or six people attended, whose details they consider classified. That does not encourage them to involve as many people as might be able to contribute to contingency planning or crisis management. When you limit the number of people you involve, you run a high risk that you will fail to consider elements essential to the plan. This is not a forum where I really can get into any great detail on the **hostage rescue**, but I believe very strongly that the extreme compartmentation in the planning involved exacted a pretty severe price. Some of the command and control information flow portions worked very well, but that was fortuitous. (194–95, 205–06)

the hostage rescue—See "Iranian raid" above.

9. **RICHARD H. ELLIS**, "Strategic Connectivity" (1982, pp. 1–9)

former Commander-in-Chief, Strategic Air Command (SAC)

Let me first talk a little about C³ as I've seen it over the years. I'd like to go all the way back to World War II. I was a combat pilot and I was on the receiving end of orders. I was in the mission execution business, but at the same time my comrades and I were a very key part of the decision-making process, because we were the ones who reported what we did. And that is one of the first uncertainties that enters into the whole C³I problem: what did you do and what else has to be done?

I can speak from first-hand experience. We were engaged in low-level attack. We were right down on the targets, bombing and strafing them at treetop level. There were certain things we saw and reported, and yet it turned out, when we got the photographs back, that we were wrong. And if you think that's changed today, you're wrong, because it hasn't. What is reported about the battlefield or the airspace, and the actual fact of the case, may be two entirely different things. And that's why this is an iffy business, and it's why, when people talk about firing on warning, or launching on warning, they're in a very risky area. It's dangerous, in my opinion—very destabilizing. (2)

18 Ionian, 1981

10. **HILLMAN DICKINSON**, "Planning For Defense-Wide Command and Control" (1982, pp. 11–55)

Director, Command, Control and Communications Systems, JCS

The most important message I have is that the command and control network has got to have a systems approach. There is a pretty good analogy to a living system. A living system has sensors—eyes, ears, nose—it has a nervous system which carries those sensings to a decision making brain, and it has an operating system which carries out the decisions of the brain by means of the fists and the feet. We mean the same kind of organic interconnection when we talk about C³I systems. There's no way to disassemble that, and have a living organism that can evolve successfully. Equally, there is no way that a living organism evolves into all fists and feet. And the message that I have from each of those **unified**, and to a lesser degree, **specified CINCs** is that my system is out of balance: I've got more fists and feet than I've got the rest of the system. (21)

unified—command that involves more than one US Service

specified—normally a single Service command with a broad, continuing mission, e.g., SAC

CINCs—Commanders-in-Chief

11. **THOMAS H. MCMULLEN**, "A Tactical Commander's View of C³I" (1982, pp. 57–76)

Deputy Commander, Tactical Air Command (TAC)

So we have to have a good plan, good information, good ability to control the force to get them where we want them, and then we have to be able to sense what's going on and adjust. C³I really is the sum of the things done to achieve proper, effective employment of tactical air. (59)

12. **GERALD P. DINNEEN**, "C³ Priorities" (1982, pp. 77–93)

Corporate Vice President, Honeywell, Inc.; former Assistant Secretary of Defense for Communications, Command, Control, and Intelligence

I personally don't think it's rational to think of a limited nuclear exchange. Deterrence is deterrence, and as I said at the very beginning, the primary

objective of your strategic command and control is to establish that deterrence in order to prevent nuclear war. I don't think it makes any sense the other way—or only in that you would like to have the capability (though I can't foresee what the situation might be) for the chief executive to have some other option than letting everything go. The Soviets have written about that, too. (81)

13. **ROBERT T. MARSH**, "Air Force C³I Systems" (1982, pp. 95–114)

Commander, Air Force Systems Command (AFSC)

In very candid terms, C³I is a tough business to understand. It's tough to validate the requirements, it's tough to estimate what it's going to cost, and it's always been sort of in the range of the unthinkable. You don't have a C³I problem until you really know that the bell's gone off; that's when C³I gets tough. Now I would suggest that there are a lot of other arenas we haven't addressed about how we're going to behave and operate when the real bell goes off. When the **EMP** gets so tough that it destroys Ma Bell, and we've got to have other means of connectivity, for instance.

EMP—Electromagnetic Pulse. Current and voltage surges triggered by a nuclear blast above the earth's surface

[OETTINGER] Those unaddressed problems come in smaller sizes, too. As, for example, in the *Mayaguez* crisis where the absence of adequate secure communications, even in a non-apocalyptic situation, cost a number of lives.

[MARSH] I found out that I could narrow down all my software difficulties to the decision aiding systems, where we were trying to assist the commander with his decisions. That opens up a whole Pandora's box. Where the commander had tried to foresee what his information needs were, in what order he would want them, how he would rank them, how you'd correlate them, and what do you do then with all the fancy correlation schemes, how you'd fuse the information and all—that's where we really met our nemesis. We just hit off way, way too much in trying to automate human decision making.

... [H]ow many times have you all gone and looked at a big computer demonstration, or an advanced **ADP** demonstration? They'll tell you all the things it'll do for you, and you're just flabbergasted; you can put your whole income tax on it and all that kind of thing; it's striking what it will do for you. But the thing that never comes to mind is what it won't do for you. My guys invented a big procurement database, and I went down the first day to view it. They were going through the magnificent things it would do, and I said, "Well, ask the damn thing what my seven biggest overruns in the command are." "We haven't got a program for that, General." "Well, what are the top values of all the cost reimbursement contracts, those are the dangerous contracts." "It's not arrayed that way." And so on and on. My problem was that those guys invented a system that evidently suited their purposes, but didn't suit my purpose at all. So I suppose managers are somehow going to have to sit down and articulate their needs. I don't think people out there inventing those ADP systems know what the hell management needs. And I'm not sure management has ever sat down and gone through whatever it takes to articulate its needs. Maybe if we did that we'd get systems that are responsive to our needs.

ADP—Automated Data Processing

[MCLAUGHLIN] Let me pursue that for a minute because I think it raises a higher-level problem. Over the last couple of years this seminar has collected a number of war stories about someone in the national command authority at some point asking, "Where is the ship?" or "What are the forces closest to that point?" and finding that **WWMCCS** and the other systems weren't programmed to answer that question. So the deputy secretary of defense, or the secretary, walks out of the room. At the **ESD** C³ symposium last October, I believe it was **General Scowcroft** who was saying that the national command authority does not exercise the system. The problem is how to get a president to play the game. It seems to me that unless the game is played we'll never anticipate what they are going to need. (103, 107, 109)

WWMCCS—World-Wide Military Command and Control System

ESD—Electronic Systems Division

General Scowcroft—Brent Scowcroft, National Security Advisor to President Ford

14. **RICHARD G. STILWELL**, "Policy and National Command" (1982, pp. 115–45)

Deputy Under Secretary of Defense for Policy

There's a whole range of crises—some more military, some more politically charged, some very transient in nature. Our military command structure is designed for major campaigns in terms of its vertical organization, its planning structure and the like; but, of course, crises have been more in vogue. We have a minor crisis action center in being right now in the Pentagon as a direct outgrowth, as you might expect, of the **Falkland Islands**. This administration has a very embryonic crisis management organization at the White House level, headed up by the Vice President. It doesn't have much sinew at the moment. There is a national counter-terrorist cross-management structure, also, without sinew. The JCS has a crisis action setup, again tempered to the large operation rather than the smaller one, although they're working on the latter. **OSD** doesn't have any real capability, being a policy, planning, review and analysis organization for the most part. It's not adapted to operational responses, although it has enormous contingent responsibilities in a military crisis. . . .

Falkland Islands—focus of 1982 war between Britain and Argentina

OSD—Office of the Secretary of Defense

We're trying to drill parts of the OSD staff in how to man battle stations for a crisis, to develop a cadre of people from the assistant secretariats and so forth who would be marshaled at the appropriate time. They would be known to one another, would have specific assignments, would be furnished with the requisite data bases with decision packages of major actions likely to be required, including the implications of any of those actions; with our legal authorities and our constraints; the priority aims, and data on all the other government agencies involved. Next to dealing with an actual crisis, nothing is more important in developing professionalism and know-how than exercise, whether it be tabletop or sophisticated. That's basic.

Another phenomenon of crisis: because the information is sketchy, because of the time and sensitivity, because of the nature of the initial report, which may come from elsewhere than our embassy or a military command, there's a tremendous impetus at the national level to search in all directions for more information, to flesh out the issue as a basis for developing the plan. Usually the plans that are on the shelves are not applicable to the situation. And so the NCA has a tendency to violate the chain of command. That's okay from the standpoint of information request, but it could be pretty disastrous if com. al is involved.

[OLTINGER] You are the first one in all the discussions we've had here who has explicitly stressed the distinction between searching for information and the downward flow of orders. Could you comment on why the distinction seems so hard for the rest?

[STILWELL] I don't know. If I'm a full commander and the President or the National Security Advisor or the Secretary of Defense makes a legitimate request for information that skips my echelon, and goes direct to subordinates to get what information he can, I have no problem. If I have any evidence that suggests he'd better not depend too much on that initial report, or if it should be modified, though, I'm going to tell him. I have a responsibility to correct him. We've provided all these command, control and communication systems; we should exploit them. Information is intelligence, it's germane to the decision-making process. But I don't want seniors bypassing the chain of command when it comes to application of force unless it's been prearranged for good and sufficient reasons.

... [M]y deputy, an Air Force three-star general, J.J. Burns (now a vice-president for advanced development at McDonnell Douglas), had been the nominal on-site commander for the *Mayaguez* operation and, during that crisis, watched the NCA, the theater commander and everybody else try to talk to the little guy on the ground. He told me that this confused everyone. So I informed **Admiral Gayler** and JCS that I had looked over all the **commo** assets, and there was just no way we could arrange communications below my headquarters. We had a remarkable secure teleconference that morning that linked everybody who was anybody in Washington and the Pacific with my headquarters, so that they could ask questions, and give advice, which no one elected to do. So it worked all right. (130, 135, 145)

Discussion here refers to communications during the American response when two American officers, clearing a tree in Korea's Demilitarized Zone, were killed by North Korean soldiers, August 1976.

Admiral Gayler—*Admiral Noel Gayler, Commander-in-Chief of the Pacific Command at the time of the incident.*

commo—*communications*

15 **RICHARD S. BEAL**, "Decision Making, Crisis Management, Information and Technology" (1984), pp. 5–191

Special Assistant to the President for National Security Affairs and Senior Director, Crisis Management Systems and Planning

As Special Assistant to the President on the National Security Council, I am responsible for all the crisis management assets within the White House. This is a new position. Formerly the crisis involvement was handled by one member of the NSC in support of the Assistant to the President for National

Security Affairs, with the basic managerial support of the Director of the White House Situation Room. But in the last two years, at the President's directive, we have been involved in a major upgrade of the White House crisis management assets.

What I am about to say is based largely on a premise you will recognize, if you know anything about the interplay between the White House and various elements of the bureaucracy. It is a very common Washington proposition: the White House should have comparatively low participation in many if not most crises. As a matter of principle I find that a good operating premise. In many cases it clearly does not apply, for a variety of reasons. But most everything that has occurred in the last two years has not presupposed that the White House should have a more active role.

I want, first of all, to describe an incident that occurred about a year and a half ago between the National Military Command Center and the White House. The military leadership, with **General Vessey** in the National Military Command Center (NMCC) in the Pentagon, was briefing the National Security Council including the President, Secretary of State, and other participants in the Council. This incident has shaped, as very often is the case, this President's view of what he could and couldn't do.

General Vessey—*General John W. Vessey, Chairman of the Joint Chiefs of Staff*

There was a discussion about what was going on in Lebanon. The Chairman of the Joint Chiefs, briefing by video from the NMCC, mentioned the constraints that the President was under due to the rules of engagement (ROEs). Then he pointed to a map to show the President where a particular Israeli activity was, and where the **Druze** were. The President was very surprised—this is not uncommon for Presidents—that he was constrained by the ROEs. Also, when the Chairman pointed to a location on the map, the President, using the various secure video links, could not see what the Chairman was pointing to. The briefers thought it was important to have the President pay attention to what they were talking about. But the President's reaction was, first, why should he be constrained by these rules of engagement, and second, he couldn't tell what they were talking about. The President turned to **Judge Clark** and said, "This is ridiculous. I not only don't know what they are talking about, I don't know where they're talking about it, and I don't have anything in front of me that helps me understand or give context to it."

Druze—*a left-wing group among the warring factions in Lebanon*

Judge Clark—*William P. Clark, National Security Advisor to President Reagan*

Now, this anecdote ought not to be surprising to any of you. Indeed, it isn't intended to be a surprise story. It is to confirm that decision making at the highest levels of the American government is not a good system. The participants in it are all well-meaning people; still it's not that good a system for the decision makers. We spend billions and billions of dollars to collect information, to get it from the field to an analyst in the bowels of the bureaucracy. Don't misunderstand me—that is very, very important. But having spent a lot of money to sustain an information collection, dissemination and analysis process, we spend virtually nothing on direct support to a senior-level policymaker. Virtually nothing. This is a major theme I am going to talk about: we spend very, very little and we have very few analytic tools for the very high-level people. That leads me to my first major observation. I believe this society pays dearly, every single day, in terms of policy, for its failure to teach truly systems-oriented people to synthesize at the macro level. I dare say we could go through the length and breadth of this land and not find twenty people who have that capacity by virtue of training. A lot of people develop capacities by virtue of experience, but I'm talking about those who are both experienced and trained to synthesize information at the macro level. In my judgement the biggest problem in information processing is not sensors, not telecommunications, not **CPUs**, not even analytic procedures. Very little work has gone into the synthesis process. I'm not talking about a partial system, a little economics and rational decision making and let's throw a little more in the budget. I'm talking about big pieces.

CPUs—central processing units (of computers)

Furthermore, Presidents, engaging in the decision-making process, where you have a very stressful situation, experience high levels of fatigue. People get worn out, they are harraged, there's a lot of pressure on their time. Very few tools exist at that level to relieve the pressure while supporting their synthesizing activity. I'm repeating myself, but I want to make sure I'm understood: the tools are not there. I think that is so serious that it affects my views on technology. What differentiates man from all the rest of the creatures is that man goes out and builds a tool to do his work for him. He builds tractors and plows to take care of the land, he builds relay stations to take care of signals, he builds computers to process data. Yet the tools for doing synthesis don't exist. In stressful situations, as the principal crisis manager for the President in the White House (I have actively worked every single one of the recent ones), I have to process, to synthesize, megabytes of data in very short periods of time, to give descriptive clarity to what's going on. For instance, we receive situation reports (we get at least ten of them) varying in length from short to quite long, and we have very little time to

take those data and crunch them using some data compression technique, and then tease from them the essence of the messages. Believe me, that is not an easy trick during a crisis.

[STUDENT] Could you give us an example of that kind of situation? You say it happens every day.

[BEAL] Certainly: the most serious conflict facing the United States today is the Iran/Iraq war. You may think it's Lebanon, it's not; it's not El Salvador, it's not US-Soviet relations, it is Iran/Iraq. Right now the number of cable messages the White House receives about Iran/Iraq—and that is a smaller pool than the total messages within the national security community—is substantial, around 600 every 24 hours. That pool includes situation summaries coming from at least nine different sources, teasing out economic, political, military, political leadership aspects of what's happening, on a daily basis.

We probably will get something on the order of a minute to two and a half minutes with the President. Try thinking realistically about what is required. We have to take that pool of messages, those summarized reports, the expertise of human beings on hand or out in the community, and prepare a message. You have to know what on earth to tell the President. The synthesizing, integrating process goes through that volume of data, those already synthesized pieces, to put through your final window a page, two pages, five pages, of very, very crystallized information.

To do what? To just inform him? No. Decision makers whom you only inform are not worthy of your effort to inform. Decision makers have to form impressions and act—or else not act, which is a form of acting (I'm not saying that Presidents or their advisors act only by doing something specific; non-action can also be very worthwhile—in fact, as a superpower, we ought to learn to do it more often; it's probably the number one rule of a superpower. Superpower behavior is not to act). So action, or inaction, is the essence of the message. Then you have to weigh all the different factors.

For example, there is a very large British convoy in the Gulf of Oman this morning. I guarantee you that is going to raise all kinds of questions: why is it there, is it new, did we know it was going to happen, all those kinds of things, which for us is a ratcheting up of the question of how we put it together in a context.

Now, a word of caution. Everything I say today is about crises. We can talk about general decision making in a non-crisis sense some other time. The

essence of information during a crisis is that it has a very short half-life. Therefore, every time you put information on a piece of paper and imply to your boss—in my case, **Bud McFarlane** and the President—that this is the way it is, when you know you're dealing with information that has a very short half-life, you are on a precarious edge. So Law One is: if you've got a piece of information that is so perishable that it will not survive the evening, then don't send it up. If your best estimate is that it's that perishable, you've got to be very, very careful about processing it. I know very few tools except experience and judgment that are going to help you in that area.

Bud McFarlane—Robert McFarlane, National Security Advisor (after Clark) to President Reagan, 1983-85

[OETTINGER] It seems to me that the background against which to interpret a crisis, against which the decision maker evaluates what he gets fed for two and a half minutes, is an important element at risk. Would you touch on that before we close?

[BEAL] All right. First, however, let me make a few general propositions. Number one, I would describe crisis decision making, at least in my experience and as I have now come to conceptualize it, as organized anarchy. Sometimes it is an organization, sometimes a decision setting and sometimes a set of decision makers. But its primary characteristic is that in crises it is always very difficult to establish a set of goals—of preferences. Crises, by their very nature, are like playing Scrabble. When somebody tosses the board and everything is initialized to zero, and most of the pieces are far-flung and in disarray—that's the anarchy. And when confronted with that, a person who makes decisions must decide how to establish preferences. For somebody going back and analyzing it, it's very difficult to elicit, from a set of decisions, what those preferences were. The reason is that most preferences are not someone's will during the period of anarchy, but rather a consequence of a loose collection of ideas and acts. The preferences are functions of action rather than drivers of action.

This in my judgment is very important. In **our current situation in Lebanon** (which in my judgment is a very clear policy reversal) our preferences and our goals have been derived from a set of actions ever-so-loosely formulated over time. Derived from those acts—not the drivers of those acts. Secondly, in crisis situations, with this

our current situation in Lebanon – aftermath of the bombing of the Marine barracks in October 1983

organized anarchy, the tools available to you are very unclear. You don't always know what you have.

For example, I hope the military is always a political instrument—that it never has strictly military purposes. That's why I find the Lebanon situation just bizarre. Commentators say, "Our forces have been given a mission for which they weren't designed; they were well equipped to do military things, but they were given a political role." The day that isn't true, when that is not what we want from our military capability, is the day we're going to just shoot each other up, because then we will have nothing but military purposes. So, in my judgment, the public discussion on this is absolutely upside down.

That's what happens in a crisis. Your tools become unclear to you. And their uses become unclear, and you apply them inappropriately.

[OETTINGER] Just so we will be clear: tools, for you, are animate? Inanimate? People? Institutions? Things?

[BEAL] A tool is an **Ambassador Rumsfeld**, Special Envoy of the President of the United States. As an instrument in the hands of the President, he has a particular characteristic that makes him very different from **Ambassador Walters**, who is also a troubleshooter. Ambassador Walters reports to the Secretary of State, and he basically is what I call the "bad news boy." He goes out to tell President Marcos of the Philippines, "Look, you're in real trouble," or, "You know, that foreign military assistance is going to drop from $100 million to $25 million." That's what Walters does, while Rumsfeld reports to the President, not the Secretary of State, and he's the special envoy to a region, not to a specific conflict. He's not out there all the time, he's specially deployed, and he is a tool. And the President has to figure out, with his advisors, how that particular tool is going to be used.

Ambassador Rumsfeld—Donald Rumsfeld, White House Chief of Staff and Secretary of Defense under President Ford

Ambassador Walters—Vernon Walters, appointed US ambassador to the UN in May 1985

We may want to know how a particular country feels about something we do—we may employ a particular kind of information collection system—and use that to watch how another nation reacts. That's also a tool. For example, if we went to a new alert status, we'd probably use some of our collection techniques to learn how country X responded to our increased alert. Or if we

have some forces out of garrison, and we want to see what the other country thinks of that, we have an instrument to measure it. We may call up **Ambassador Kirkpatrick** and say, "Would you float the following notion? Maybe we ought to substitute the multinational force for a U. N. force." So she becomes, in a sense, a tool.

Ambassador Kirkpatrick—Jeane Kirkpatrick, President Reagan's ambassador to the UN (Walters' predecessor)

But in crises it becomes unclear which assets you have available, which ones will work, who's going to use them, who actually controls them. I cannot tell you how often I have heard somebody say in a conversation with the President of the United States, "But sir, we can't do that. It's not within the DCI's prerogative." That means that the Director of Central Intelligence, in his other hat as director of the intelligence community, is telling the President of the United States, his boss, that he, the DCI, has a charter that is independent of the will and preferences of the President. If you read the **1947 act as amended in 1958**, that can't be. And yet the assets are appropriated, given by law to the DCI, and they are his in the mind of everybody who manipulates them.

the 1947 act as amended in 1958—the National Security Act of 1947 and the Department of Defense Reorganization Act of 1958

[OETTINGER] It's not unique to the Presidency. We're talking about decision makers in a very generic way, through these focused observations.

[BEAL] Yes, and not being unique, it's very critical during times of crisis. Why? Because you've got very compressed decision time, whether in reality or simply in the mind of the decision maker. He or she can't tolerate that sort of element being fed into the decision—it puts tension into the process, that makes it very difficult to come to some sensible set of decisions.

The third major characteristic I'd like to emphasize is that all crises involve what I call fluid participation in the decision-making process. That is, in this organized anarchy, each time the President and the National Security Council meet, it may involve ten people—and in three successive meetings not even three of them will be the same. People are constantly sending their substitute, while somebody else gets dragged away. Why? Because a superpower is involved in managing all kinds of things in a non-crisis area while it handles a crisis.

That will always he the case. In 1973 it meant that there were major elements of the State Department having nothing to do with the Middle East, processing other kinds of matters and demanding the attention of the Secretary of State. Furthermore no one set of participants is hoth analytically competent in the region or the specifics, and also high enough in position in the government to be in the meetings. So the experts who really know Iran/Iraq (generally they only know Iran and not Iraq) hrief a boss who hriefs a boss, who goes to the meeting with the President. He may not know a single thing ahout this particular issue.

This may touch on your question of hackground. The critical thing is that analytic, competent people are not that valuahle to you in the decision-making setting—this is going to strike you as a little perverse and a little upside-down—because they do not control the assets of the organization they are members of. So you have to have somebody in the meetings who can speak for the agency, allocate its resources, and make commitments to the President during the crisis decision making—not the expert on Iran/Iraq. No matter how much the expert knows about the foreign minister or whatever, that's not what is frequently critical in those settings.

You also have what I call the integration-of-knowledge prohlem. By the time you reach decision making settings, you've already had to go through the analytic stuff and have cast this problem in its decision making macro terms. That's not where you need analytic smarts, you need integrating smarts, and people capahle of allocating the resources and assets of the society.

Fourth proposition: every piece of analysis I have ever seen is incomplete, because the bureaucracy and the political element (I don't want to imply anything other than a very positive approach) never know anything about Blue (Red is the enemy and Blue is you). Nohody ever analyzes Blue. Nobody ever finds out what this country will support, accept, tolerate—what Congress will tolerate. They leave out major portions of what the law will permit a President to do, what the Office of Management and Budget (OMB) will permit a President to do, what Congress will permit—so they don't complete the total analysis. We could have a posture as to what we intend to do with the West Europeans and the Japanese if the Iran-Iraq war goes into the Persian Gulf—yet it might be perfectly impossihle to get that done domestically. And we would never know it, because neither the Defense Department nor the State Department is permitted or mandated to know anything about America! I have the greatest possible respect for all of them, but they don't analyze America domestically.

[OETTINGER] Conversely, the domestic folks are not permitted to get into national security. So synthesis becomes extraordinarily difficult.

[BEAL] That is one of my major points. One of the fundamental questions in foreign policy is, is your foreign policy driven by domestic sources, or is it derived from the interaction between the two or three nations involved? Well nobody has ever decided to have a Bureau of US Affairs in the Department of State. You have to have certain specialized tickets if you want to play in national security affairs, and one of them is: Don't know anything about America. Of course I've overstated, but not unfairly, I think.

An article by Bill Bundy, from *Foreign Affairs*, talks about how American foreign policy is conducted. It always turns on four elements. First, the central views, style, and characteristics of the President. Well, Ronald Reagan is still an enigma to everybody. Second, coordination of policy within the executive branch, including the relative influence of key advisors, is never analyzed; it's never even a part of analysis; it would be inappropriate if somebody wrote it down. It's outrageous if somebody raises it. Third, relations with Congress. Well, Congress is never in on it; in fact, the people who conduct legislative affairs knew zero about **Grenada**, for example. Intentionally, they were never even given a piece of the knowledge ahead of time. Fourth, the level of popular support for the administration, especially the President personally. I think that's remarkable for William Bundy or anybody to say. I have spent a lot of my academic and professional life doing surveys, but if **Richard Wirthlin** in the current administration uttered a word to the Secretary of State on what the public will tolerate, you would have the longest discussion about the fallacy of polls. Few people are as good at the balance between domestic and foreign as Wirthlin is, but he wouldn't be permitted to speak.

Grenada—the US invasion, October 1983

Richard Wirthlin—President Reagan's pollster

Another principle. There is no domestic/foreign interface. It is not there, and that is very, very serious. In my judgment it is the single most critical factor in being unable to sustain foreign policy. It's not really our difficulties with one nation or another, but the problem of not being able to sustain domestically almost any policy you can name in a crisis. You have to remember that a characteristic of a crisis is generally high public tolerance for a President, his advisors, and Congress as they work through the problem. That's one of the things we know about crises: there is a suspension of immediate criticism about what you are doing. During Grenada, for example, it was

decided that we could do the action, that it was correct, we could finish it, pack it up, and return—all before we had to truly defend the policy. Invasion of an island—and I don't see any point served in altering those words—invasion of an island for the specific purpose of overthrowing the government did not have to he sustained as an argument over the long term, hecause you could put the forces there, clean it up, and take them home before you had to really dehate the policy. During crisis you have to think of the sustainahility question as much as you possihly can.

Next is what I call Gray's Principle. **Gray** is a Marine General, commanding officer of Camp Lejeune, and a remarkahle man in many respects. To get understanding about some of the problems we had, I visited General Gray at Camp Lejeune. I did not understand why there was miscommunication hetween the President and some of his military advisors about use of the MAU force in Lehanon—the Marine Amphibious Unit, one of the hasic elements the Marines use for certain kinds of actions.

Gray—Maj. Gen. Alfred M. Gray, Jr., Commanding General, 2nd Marine Division, Heet Marine Force

General Gray and I were going over some of the concepts that the Navy and the Marines were going to use, and I asked him, "How do you keep all this coordinated?" It was a very large landing on a beach front with lots of forces and lots of firepower and lots of other things. And I was interested in the information questions, the command and control.

Now this is my proposition, though you may disagree. I believe command and control structures are always pyramidal. They have to be; otherwise they can't possihly sustain command and control. By contrast, all information structures are, in my judgment, initially horizontal. And they are horizontal all the way up and down, because for a variety of reasons they have to be. Command and control, however, and the information in a command and control structure, always have to run up or down, pyramidally through the structure.

But, as I have said, the information systems that support command and control are always horizontal and they are characterized by network flows more than by vertical action. And what General Gray said to me I found very interesting: that in times of stress, every echelon in the organization must understand the organization's immediate goals and act to fulfill them, without further information. That means that there is an information suspense period in a command and control structure. The horizontal flow is not active

during certain restrictive periods. Especially in stressful conditions, you cannot expect the same kind of information network flow across the horizontal planes and up through the various echelons. Another point: much of command and control information is punitive. It has to be. A directive: you do this; you send me feedback that you've done it. If you haven't done it, get your butt out there and take care of it. And that's why the command and control structure passes what is not passed in a horizontal structure: how we are doing on the intelligence side.

Now, in crisis decision making most presumptions about the highest level are that it is pyramidal. But in organized anarchies it is anything but pyramidal. Why? To go back to my first notion, nobody knows what the preferences are, so nobody can act to meet the intermediate goals. How do you ever know what the preferences are? By inferring it from actions that are very difficult to interpret. And during a crisis this is one of the things that gets interrupted.

The next proposition I want to give to you is what I call the theory of night operations. During the **Gulf of Sidra incident**, when Navy aircraft on the USS *Nimitz* shot down two Libyan fighters, you may remember that there was discussion in the press about who woke up the President to tell him. Well, I'm one of the lower players in that loop. And my opinion is that it is dumb to wake up the President to tell him that two Libyan jets have been shot down and everybody else in the Libyan air force has gone back to their bases and they are sitting on the runways. There is nothing to say. What are you going to wake him up to tell him? That's like saying, "There are a lot of stopped-up toilets in Milan." What are you going to do about it?

the Gulf of Sidra incident—1981

To make sure we had all our facts straight, I was sent to the USS *Nimitz* to have a discussion with Captain Ilg and Admiral Martin, then the admiral of the Fourth Task Force. Martin's a POW from Vietnam, and both are very remarkable people. While I was there they were doing maneuvers and night operations. For a person who didn't spend any time in the Navy, this was to me a remarkable experience. During these night operations the *Nimitz* was moving during the night moored to two replenishment vessels—taking on food and supplies on one side, and petroleum on the other. Although the *Nimitz* is a nuclear-powered vessel it still needs petroleum for a variety of things on board.

So we're going through the ocean, three ships hooked together. It is an incredible experience to see them doing this with the ocean rolling. All this time they were landing aircraft on the deck and taking off, at night. Night operations are very different from day operations. One characteristic is that pilots are trained to disregard most of the information available to them to land an aircraft. They are told, "Keep your eye on the meatball"—the lights on the left-hand side that have to be kept horizontal. The pilots are trained to focus not on the ship, not on their instruments, not on what they are hearing, not on what they are seeing, not on how the ship is tossing. This is an aircraft they have to get down, one of the most complex manned machines. I'm not telling you this because I like stories about the military; we're talking about technology, information, decisions during short, compressed periods of time; and to get that aircraft down they had taken the volume of information that one might pass to that pilot and reduced it down to "Keep your eye on the meatball."

[STUDENT] But you know what the pilot's preferences are: to come down in one piece.

[BEAL] That's the preference not only of the pilot but everybody associated with him. The guys who clear those planes want very much for that pilot to get that aircraft down. But within the context of my own observations, I know very well that keeping your eye on the meatball works—and this is my point: you can have information reduction and compression only when you know preferences. All the other characteristics of night operations and crisis decision making are very much alike, but the crisis decision maker can never say "Keep your eye on the meatball" because he doesn't know what the meatball is.

You go through all the other processes: data reduction, data compression, short periods of time, high risk—let me tell you, putting that aircraft on that flattop is high risk. Somebody has worked out a manned machine, the technology is clear, the instruments that you have available to you are clear. But they are successful in landing that aircraft only to the degree that they get all that coordination.

If you apply all those pieces to the pre-crisis stage, you discover that people who say to the President, "Sir, keep your eye on the meatball and we'll get through this," are deceiving him. Advice-giving during crisis periods, for precisely the reasons I have alluded to, is very dangerous. In crises most of the advice the President receives is inaccurate and fallacious. Everybody will be telling the President, "Keep your eye on the meatball, sir, and we'll

make it," because that's their job. But since they are likely to be wrong, the President is denied the number one thing he personally needs: high confidence that the advice given to him in the privy council is correct.

[STUDENT] The word "correct" troubles me. Instead it is really incomplete, isn't it?

[BEAL] It is incomplete, incorrect, and inadequate.

[STUDENT] Isn't the advisor saying, "Based on my experience with you, Mr. President, I believe your preferences are thus, and therefore I think this indicator is the only one that will do it." Isn't that an effort to distill in some meaningful way . . .?

[BEAL] It is. But my proposition to you is that, in all probability, whether it is the Secretary of Defense or the Secretary of State, whoever it is, he's wrong. In my judgment you have to operate from the premise that when you are in a crisis condition, he is likely to be wrong. That's the risk you run because in the circumstances anarchy can surround everything they do, and it simply makes almost everyone's good advice not that good. The conditions no longer permit them to concentrate on one thing. In a crisis a lot of the effort goes toward finding a path to solve the problems; they have to meet, they have to bolster each other and get a certain kind of consensus to get the thing resolved. That's the basis of Irving Janis' "group think" theory. They have to build consensus and get the President on a path, then they have to do the proselytizing and cheerleading. And in my trivial way, I keep records about who says to the President, "This will work." I red-flag that, since if anybody is convinced, in my judgment, that is likely to be dangerous—because in a crisis you just don't know.

What do I conclude from this? I do not have a prescription if you are a weak nation. But as long as you are the United States, because of the conditions I have described, you need to act very, very slowly. Short of a nuclear exchange, there is no crisis that this nation ever has to respond to in very compressed time, either real or psychological. I think that is one of the major problems we face: advice given under stress to a leader of a superpower causes that superpower to act precipitously and unnecessarily, without the basis of consideration that you fundamentally need. Am I arguing for "give-it-a-week"? No, but any time you get in a crisis, the major thing is, let's not go too fast.

I will give you a case in point. I think in the **Korean airliner incident**, from the time we knew the plane had gone down to the time the Secretary of State went on the air, and the President's first public statement about it, did not exceed 24 hours. In my judgment it caught the Soviets so ill-prepared for the speed at which we were processing information that that very thing boxed them into a corner—first to deny it and then coming back and saying, "Well, yes we did it, but we had every right to do it, it was the correct thing for us to do." That is a response we didn't really need to evoke, had we not been moving the issue too fast on them. Not that we weren't correct on the moral aspects or the other dimensions of the situation.

Korean airliner incident—the shooting down of a Korean airliner by Soviet aircraft in September 1983

Now, if our larger concern is not to beat the Soviets bloody over an issue but to foster US-Soviet relations, we could take all the measured response we really need. Moving too rapidly is probably the single most significant error we make.

[STUDENT] To what extent were there really confrontations with the Soviet Union? Before we really did anything, did we really try to figure out what they knew?

[BEAL] I think the direct answer is that we did not sit down and discuss this with the Soviet Union at any length, at any time, because our initial evaluation was that, in every way we could determine, we knew more about what was going on than they did. We were absolutely convinced that they had shot the airliner down, and that we probably had all the information we needed. This was never seen as an opportunity for us to have a good congenial talk with them.

[STUDENT] If the incident were to occur today, do you think things would be handled differently?

[BEAL] Yes, I think that we would do several things today that we did not do at that time. The delicate issue from the NSC's perspective, and, I believe, from State's perspective, is that we could not have done what we did had we not had the verifying evidence from the Japanese. It was not possible to go forward with what we alone had even though we had evidence. We are not a credible nation—not the President, not the nation. There are all kinds of reasons why we could not have sustained the debate in the various international forums where it has been discussed without the collaborative

evidence of the Japanese. And if it were to occur again, the fact that they had it and we eventually got it from them would make that process go a lot more smoothly than it did.

This is the first time I knew anything about it at this kind of level; in fact, I am sure it is the only time when a third party has truly and genuinely helped us make a case about Soviet complicity in a horrible act.

[OETTINGER] That is a theme worth taking up again with **Leo Cherne**, under the heading of the role of public opinion in both the U.S. and foreign countries in crisis for long-term national security management.

Leo Cherne—Vice Chairman of President Reagan's Foreign Intelligence Advisory Board

[STUDENT] It appears to me that what you are saying is that the President shouldn't be involved, because when it goes up to that level, you don't want to just give him a series of briefing papers so that his reaction is just "What am I supposed to be doing with this?" By involving the President you make more likely a precipitous decision that may be inappropriate and based on inaccurate or incomplete information. Is that right?

[BEAL] I wouldn't necessarily infer that by bringing in the President you are much more likely to commit a precipitous act. But I would thoroughly agree that most people—including many people in the NSC—do not understand what it means to get the President involved in anything. The White House only has one asset: the President, and his attention to anything. This is the single most important asset the White House allocates. Symbolically it means the most. If you know anything about open pluralist systems like ours, the asset we have is whether or not the President will pay attention to an issue; and everybody in the society who wants to get his or her issue acted on has got to get that issue on his plate. I guarantee you that when **Mr. McLaughlin** worked for the Post Office, the number one issue, when he had a big enough one, was to get the Postmaster General to take the issue as high as he could. The Secretary of Defense constantly has pressure from within or from without to get issues before the President. That is the number one game in Washington.

Mr. McLaughlin—John L. McLaughlin, Executive Director, Program on Information Resources Policy

Now to get a President into a situation means that you have to understand how to control that situation a lot better than when he is not in it. In that

sense I thoroughly agree with your point. In fact, most White Houses have, in my judgment, basically been brought in as part of what I would call their default political considerations. It is by nature a political issue whether you bring in the President, but it has been a default issue; that is to say, it was largely a question of time, or having met with a group, or is he giving proper treatment to some department or agency compared to some other. It has basically been a default balancing act; it's paying everybody off.

Most administrations try to focus on the big domestic issues of the time. But then invariably the national security items start to take over, and they run around scratching their heads and wondering why this happened. I'll tell you why it happened: because every White House in modern times has allocated the National Security Advisor time every day to brief the President. No domestic counselor has ever been granted, to my knowledge, that separate, independent allocation of time—and believe me, we plan it and manipulate it and control it, and it is the number one thing we have to deal with. The second major factor is that we have kings, presidents, prime ministers, foreign ministers as power leverage. The NSC leverages that against the President through the time in his calendar to get him involved.

Now, let me get specifically to crises. The presumption is that the President is involved if it's a crisis. **Sam Donaldson** says, "Hey, when did you tell the President?" It doesn't matter how low-level a crisis it is; it can be a terrorist attack in southern Sudan (there have been three). "When did you tell the President? When did you notify him?" It is a public issue. We even get calls from Senators: they read it in the press. "Is the President aware?" So, in my judgment, the expectation is that in all crises you put the President in the loop and then that makes the scale of the game very different.

Sam Donaldson, news correspondent for ABC television

I think this is a fascinating problem, because I am a big believer in management of time. That's "upward boss" management. We had some interesting feedback from the Soviet Union on the Korean airliner incident, from people in the Institute for US and Canadian Studies, who told us "When Secretary of State Shultz announced it we didn't think it was a big deal." Just imagine. They can shoot an airplane down with civilians on it, and after the fact they knew what it was—that's not a big deal; the Secretary of State goes on TV. It was a big deal only after we got the President involved.

Now, having said "default/political," having accepted the proposition that it really matters, my contention is that in crises one of the things you have to

manage is whether the President is in or out—because if the President's in, then this nonsense that the Secretary of State or Defense will run the crisis is not possible: the President has to. Even if he delegates it to the Vice President just to manage the meetings, that creates a tremendous public hullabaloo. So, no matter what you do, once you put the President in, that says, "All right, Secretary of State, you now play not the coordinator of the crisis, but diplomacy, foreign affairs—that's your job. Secretary of Defense, or DCI, yours is intelligence."

I'll give you a case in point. Recently the **Libyans invaded the northern part of Chad**. The first issue we dealt with was, "Is this a matter worthy of Presidential involvement?" The NSC made the decision that it was not, that there was only a very limited role for the President of the United States. It was determined that he would only have a role if we had to have president-to-president relations with **Francois Mitterand**. This was largely not an American issue, and there was little we really could do about it, but if it did involve the French, it might involve president-to-president contact. Otherwise it was a problem for the Secretary of State, and he turned it over to the director of P/M (political/military). Admiral Howe, and Admiral Howe ran the crisis. The President played only one role in the Korean airliner crisis. After the strategy was laid out as to what we would do and how we would do it, it was decided that we would not use our first gun up front. We would bring in the President later, and then only in a way that would enable us to sustain the international momentum.

the Libyans invaded the northern part of Chad—The Libyan involvement in the civil war in Chad led to French intervention against Libya in 1983.

Francois Mitterand—President of France

[STUDENT] Something really bothers me: you said the US is not a credible nation. What do you mean by that?

[BEAL] There are so many elites and people around the world who will not believe us when we make a case—for example, about use of gases and toxins in the various fighting zones around the world, or **KGB** activities. We basically can't convince anybody. And we can't convince many of the leaders of the third world about positions we take in international forums. Many people believe that the CIA is the root of a lot of things.

KGB—USSR's Committee for State Security

What is the evidence, by the way, that the Korean airliner was shot down? The ocean eventually yielded some debris. But when we first made the accusation nobody knew the aircraft had been shot down by the Soviets. Furthermore lots of documents are forged; it goes on all of the time. We are just not able to use international forums like the United Nations to make a case. I lived a significant part of my recent life in India, and I guarantee you that the Indian government would not have accepted our explanation of the shootdown.

[STUDENT] Is that something we just have to live with for the next few decades, or could we do something about it?

[BEAL] I haven't really thought about that. I don't think it's something you consciously do something about. We need to be a more credible player across the board, in my opinion. Ask Leo Cherne about that when he is here.

[STUDENT] You mentioned a consolidation of crisis management functions within the White House. Could you describe that in more detail?

[BEAL] Yes. The White House decided, as a result of the President's directive, that we really could not use the situation room—which is a very small place, smaller than this classroom—as our single location for management of crises. During the last year or so we have built some additional capabilities, largely to support the NSC, the Vice President and the National Security Advisor in the analytical role in which the senior members of the NSC staff support the President. The room holds additional telecommunications, computer capabilities, and a few other things.

[STUDENT] High tech. But the policymaking team hasn't changed?

[BEAL] Well, it has changed in the sense that once you build an instrument, that causes you to change the players, the team, even the rules of the game. So there now are, internally within the White House, a lot more rules of the game, as to how you play, who plays, and under what conditions.

[OETTINGER] To go back a bit, your statement about putting the President in or out—compared with the last three or four years' record of this seminar, and much of the other literature—is probably the most eloquent and pithy statement of the impact of modern technology on decision making. That was an option that didn't exist in the old days. You sent off Ben

Franklin, or the Ambassador, or the European Sales Chief, and that was that. It was some time before you could even get new instructions from the boss. Flexibility began increasing with the telegraph, increased with the telephone, and is so greatly increased now that it even raises the question whether you need the top of the pyramid. It is, I think, at the heart of some of the questions of modern management under conditions of high technology. Flexibility makes that question possible.

[STUDENT] That worked in reverse, too. We lived through a period when with this apparatus, for the first time in history, there was a crisis called "the Vietnam War." And it was a continuous crisis. And the President could read the newspapers and get detailed information from the wire services faster than the official apparatus could provide it to him—faster even than it could decide whether to involve him or not. So he decided.

[OETTINGER] LBJ was the prize first example, sitting down there in the situation room saying, "I'm going to run this stuff myself at a distance." But the funny thing is that the staff people learned to stop him and others from doing that. There's a whole history of that—and it's exactly the point I'm trying to make, which is that the flexibility is there. So there is a whole new set of conditions under which people either play, or protect themselves from that game—either from the President downward, or upward. That set of possibilities is an important element.

[BEAL] When **Dave McManis** gets here he can tell you all about Johnson sitting there and moving I-Corps around in the sandbox, and I think that will reinforce the point you're making. But most people don't understand the difference between information structures and command and control structures. I don't want to appear to defend President Johnson, because I think he had a propensity to do this no matter what. However, there is a tendency for the bottom to say, "We will not send this kind of information to the top because it would tempt that echelon to come back down, make tactical decisions, and turn all the tactical knobs." They don't want that to happen at all: they'll do everything they possibly can to prevent it.

Dave McManis—National Intelligence Officer for Warning

Now, that confuses the pyramid and the horizontal structures—because the number one thing everybody up the various echelons has to contend with is uncertainty, and information denial creates higher degrees of uncertainty than necessary. Instead, if you understand the horizontal information structure, the tendency will be to pass more synthesized, properly integrated

information, which reduces uncertainty. It also encourages the real process, which is for a President or a person at whatever echelon to delegate the authority, establish accountability, and then get feedback as to what is happening in that loop. That is the delegated authority accountability loop, which is the thing a decision maker wants to know most about. But once you start snipping up those pieces on him and denying information, he will be looking into tactical matters every single day, and in my judgment he ought to be. Why? Because he's ultimately responsible, and without thorough synthesized information that enables him to make macro-level synthesized decisions, he is going to make the ones he can make, and they will be tactical. In short, a decision maker will be strongly tempted to make tactical decisions if he is being denied strategic, integrated information.

[OETTINGER] And this is the gentleman who is three years plus into an administration. That was my second point. I don't know when you learned that, but every four years all that knowledge disappears and a brand new set of players moves in. So another set of the dynamics is institutional, having little to do with modern technology, which is global, with different degrees of use, different degrees of awareness and so on. This is a matter of continuity of understanding. Every once in a while a Soviet leader dies, and it's international news. But our leaders routinely disappear! Not only the President, but all the others—a whole administration. And what's more, they clean out the files before the brand new team comes in. The continuity rests in support people like McManis, who bridges the Johnson-era situation room to the Reagan-era national intelligence scene. It takes each new administration months to reconnect and find out where those people are. They're certainly not among the initial team the new President brings in. They are a lucky accident, or an unfortunate one, depending. I'm not trying to give theories of government here—clearly there are different patterns, but that's the United States.

One last thing, then I'll break off this interruption. You said something about how difficult it is for the White House apparatus to get resources, and about all the information gathering going on at the lower echelons and nothing at the top for synthesis. There's a poignant record of some of that in a book by a man who was in the White House Communications Agency: Gulley's *Breaking Cover*. Though it has the appearance of a backstairs gossip piece, his stories of his administration—Johnson's I think—raiding Navy funds to pay for Number One's phone bills and so forth make interesting reading.

[BEAT] I should pick up on that. It is not in the interest of a lot of resource people to allocate much of their resource's power to the White

House. White Houses have enough resources and power by virtue of their sheer overbearing character—so that if they were really endowed with all the assets they need to do their business, it might be a real problem. However, the White House is the least well-supported front office I've ever worked in, bar none. I mean, they think a big deal is getting a parking pass. It is not properly supported and in my opinion the law to provide telecommunications to the President is being circumvented. An example is the White House Communications Agency under Brigadier General Tuck—he worried every day whether he was within the law in his support to the President as Commander-in-Chief. We support, with our communications, the President of the United States in his Commander-in-Chief role, and really in no other role. The law doesn't provide for communications support to his role as chief executive, as party leader, as political leader—nobody cares one iota about that, and Congress would never appropriate funds to him, and probably shouldn't.

Presidents have to go hat in hand. A little while ago it dawned on me to compare when technology was introduced in this society and then when it was introduced into the White House. I had my staff look it up, and the lead-lag relationship is staggering. Think of the telecommunications-computer revolution that has gone on in this society, penetrating educational institutions and corporations. When I arrived, the White House had a great big corner office, room 200, utterly without technology. I found a pencil. But I had ten times the technology when I was at the University—much more than ten times, because it's a factor against zero. I find that absolutely terrible. In many respects the White House is the hollow center. And when people contend with the White House to keep it the hollow center, they are unwise, because then it all depends on the personal assets of the President. And that's how you keep presidents at bay.

[OETTINGER] As a checks and balances question both vis-a-vis the Congress and the games within the Executive Branch, that phenomenon bears study. You couldn't have started us off better. When I invited you, I didn't know you were going to so eloquently echo the theme we began with: that the fragmented learning students get elsewhere in this school does not begin to address central problems of synthesis, and what it is like to be a CEO, not just of the United States, but in organization X,Y, or Z. The rest of the information you're getting here is for slaves, not for CEOs. The main thing you can get out of this course is: maybe you can't all be bosses, maybe you can't all be President of the United States, but if you want to serve the President of the United States or any organization's CEO, you've got to think like one, and not like a slave. Mr. Beal is doing a fantastic job of making clear just what that means.

[STUDENT] You said there were two categories: nuclear confrontational decisions, and the others. And in the case of a nuclear confrontation you automatically involve the President, which makes sense. But how does that translate into a different magnitude of the problem? How does that change the analysis? It seems to me to be a whole different category of problems.

[BEAL] I'll admit a certain bias in my answer to your question. I believe my work generally involves what I hope will be the 99.9999 percentage of non-nuclear crises we're actually going to deal with. When we get into nuclear decision making, the characteristics of the decision making, the number of people who are already in that loop, all the factors are a quantum jump. I'm not saying we're ready for that. A lot of work has gone into it, theoretical approaches are on the books. An awful lot of things would have to be factored in if we were ever really confronted with that rather tense, to say the least, kind of decision making. We have adopted crisis-management procedures that will allow us to transition into it if we are ever actually involved in an eyeball-to-eyeball issue. I must confess though, in terms of all we have done in the last two years, that has not been our focus—based on the belief that we would have many more of the other kind of crises before we ever got to any nuclear one. Moreover, people who have dealt with crises have learned their lessons of history out of Berlin blockades, the Cuban missile crisis, Middle East tensions—and people do study the **Quemoy and Matsu** experience, though very few have ever learned any lessons from it.

Quemoy and Matsu experience—1958 diplomatic confrontation between the United States and China over the latter's heavy bombardment of these two fortified outposts of the Nationalist government on Taiwan

So, in my judgment, in a nuclear crisis you have a "takeoff," by which I mean that the magnitude of the data categories you have to deal with just gets staggering. It's handled in many departments and agencies by **SOPs**; they are out there, they exist. How good they are qualitatively we would have to have the right security level to discuss, but they are all in place. The other dimension in a nuclear crisis is all the verification issues, authenticity and accreditation.

SOPs—standard operating procedures

In non-nuclear crises we have something similar, but on a different scale. For example, the bombings of the Embassy and the Marine Headquarters

immediately raised authenticity and accreditation questions. Who did it, and how do we know they did it, and what can we say about that publicly? What should we say, even if we can say something? In a nuclear crisis you have that category of problem in spades. Because the moment you go outside the crisis management early warning or warning identification question into emergency management procedures, the number of agencies involved increases, and that's a whole different ball game.

[STUDENT] But if the other crises are barely manageable, a nuclear crisis would seem to become unmanageable in terms of information overload. Presumably, the preference of any NCA would be just to postpone the decision to use nuclear weapons for as long as conceivable. At least his objective would be to slow things down.

[OETTINGER] Which is precisely why, among other things, there is all this attention to the lower-order crisis. We really would rather not let any of these things escalate to that level; and—I echo what Dr. Beal has said—not enough attention has been paid to the lower-level crisis. As a consequence, the risk of getting to the higher-level ones is greater. After all, there can hardly be anybody left around the world who doesn't agree that one would really rather not enter into nuclear confrontation.

[BEAL] Let me make one observation. The work in crisis management we're doing now involves looking at the other side. Certain assumptions and certain scenarios about the world would lead one to conclude that we generally think of crisis management as dampening. That is, you have a problem out there, you want to avert its adverse consequences, so you try to dampen the prospects of the crisis—or, once you get one, you try to keep its negative consequences down.

But the whole other end of that spectrum has to be considered: sometimes you want a crisis. A crisis can serve as a firebreak for you, burning against the forest fire itself. So you may want to precipitate one. You need to think what that might mean; so having an amplifying as well as a dampening strategy is an essential part of understanding crises and their value to you.

Surely you all know that the Chinese character for crisis has opportunity in one part and danger in its other part. I think that's quite true. We tend not to be as manipulative as we might—at least we tend not to admit to manipulating the opportunity side of the character, but the opportunity is there.

[STUDENT] I wanted to ask you about one of the characteristics of crisis decision making. You mentioned fluid participation. A lot of analysts have written that in crisis decision making the big characteristic seemed to be that the number of decision makers gets smaller. So in the majority of cases a few top policy makers isolate themselves more from incoming information. That doesn't seem to fit in with what you're describing here.

[BEAL] It doesn't fit because we've read that too, and we'd like to avoid that problem. Item one: we probably have as many errors in our crisis activities as you can imagine—but not because we isolated the decision makers. Two: in very tense settings I believe presidents will have privy councils. I think this is really very important. I don't believe you can deny any sitting President the right—without any of our technology or anything we can provide him—to go into a room and receive counsel privately and have the assurance that it is the best judgment he can possibly get.

Now, I have some problems with that. I think the most dangerous products can come out of the privy council process. Comparing certain activities we've been involved with over the last year, some privy councils are better than others, and you can examine the differences in structure and membership of those groups. But privy councils tend to be small. I do not believe you can have a large group that's very fluid. The group has to be fairly small, with considerable diversity, and you have to cope with the fluidity problem I mentioned earlier. This is absolutely serious: you cannot, in the middle of a Central America or Grenada crisis, have the Assistant Secretary for Inter-American Affairs or Latin American Affairs coming in one session and his deputy the next, sitting in with the President of the United States. It just doesn't work. They're not confidantes; in fact the President may not even know who that guy is. And when you go into that meeting you can feel the chill: this is the wrong mix of people. And you just pray the President has the good sense to end the meeting early.

[OETTINGER] You're veering again to the question of the role of background and earlier input at the time of crisis. Obviously you can't have a President memorize the geography of every place, so that when you tell him about it he knows exactly what it is. But what is the role of fact-finding?

[BEAL] Maybe Dave McManis could talk to this more appropriately than I. But the departments and agencies have enormous access to the President, and during crises we have constant contact with them. You learn to use these departments and agencies, and they can give you all kinds of information, fast and analyzed. It's a question of knowing how to ask them the right

questions and get to the right people. You can get confused. The first premise is that, by virtue of its contact with the operations centers in each of the departments and agencies, the White House can have almost instantaneous high-quality information on warning conditions, possible threat areas and background. When the Chad crisis broke, the intelligence community had been talking about border buildups, incursions and other border problems for a long time. We had more than enough strategic warning to know this was a hot spot we needed to worry about. But what kind of information should the President see? You can go through a whole litany of questions about what you should have the community prepare for you.

In Chad, for example, it took us about two days to find anybody truly competent to know where the oases were and where the roads ran in the middle of Chad around the 15th parallel. You get out the list and count up how many Americans you know who are competent to tell you where the oases are in Chad. And that was no trivial issue. The only truly competent person we had was an American military officer who had spent time with the French in Africa. And as it turned out, the information we received geographically and demographically was the number one thing to know in the Chad case, because it led us to conclude that the Libyans could invade in the north. The population is in the south, but in between are very few roads, airstrips or oases, making for very difficult logistic problems for anything coming through there. So if they were to invade in the north and came down to one of the critical oases, neither we, nor Egypt, nor France, nor any central African nation could get any forces a hundred or so miles up through that area to resist the rebels and the Libyans. But if they then went further down, through the area crossing the 15th parallel, then the Libyans and the rebels couldn't sustain an attack against the capital, because then their logistics problems would be horrendous. So if you didn't resist them in the north you would have a natural partition. What we decided to do was resist the natural partition of Chad if we could avoid it. (Not that Chad's boundaries make any sense to anybody, but put that issue aside.)

So, if you follow me, concerning the question of background information, resources and what we should know, we had one of those scenarios that say, "If the knife drops tonight, what do you know?" And our work in the Crisis Management Systems and Planning Directorate, which I head, is to take all such areas around the world and ask ourselves how to maintain "threat situation files" on them.

Your information strategy is "high-burst." It's also high-video; if you don't understand that the channel is video, you're going to lose. By that I mean that in a short period the best way to communicate the highest data rate to a

high-level decision maker is to pump to him the equivalent of a sequence of video images with very compressed data. Most of the community is still working in words, writing things down. We don't write things down; we take written things, transform them into what I call video frames, and high-burst that through to the President and the National Security Advisor largely in video form. That way the President can quickly picture where the crisis area is and what is germane to it; and the technology is fairly simple. You identify the area in terms of geographic base, and build windows of information into everything. Then you theoretically touch the screen for additional information. That way the President can interact with the data. Now, that's a wish list more than an accomplished fact but it's as specific as I can be.

[MCLAUGHLIN] Let me pursue the background issue a little further. Maybe a crisis, a pre-crisis, or a contingency is a matter of definition. The Iran/Iraq situation has been a crisis for 2½ to 3 years or so, and we know it can go critical very easily with a lot of different scenarios. Does your staff worry about when that goes critical? What the options are? Are you trying to define options now?

[BEAL] Yes. You don't have to be a great warner to pick up on Iran/Iraq. You have to be pretty good analytically to know all its features. Basically we are using the notion of strategic warning. We have an inventory of the parts of the world where the community has alerted the National Security Council that there is a potential threat area that could go critical any time. Then we are constantly soliciting from the community what I call tactical warning. And tactical warning always has to be timely. If a guy says, "I'm glad you called, because tonight it's going to happen," he hasn't really helped you very much.

It's a question of the liaison between the policy maker and the analytic community, the intelligence community, to keep up that constant exchange over those potentially critical areas of the world. I think we learned during the Iranian crisis that we have to have a critical exchange about who is looking at what, and why. It's our job, we think, to build the inventory, and look at the dimensions of strategic warning and what they tell you you ought to know about the particular situation. Then draw out the community proactively for the more immediate warning.

Now, there's another category, where we sit around and say, "What could we be surprised by this afternoon?" We do that every day. Tonight before I go home I will have a little pow-wow with the people who work for me, and we'll go over a hundred and seventy-odd places. Some of it is fairly trivial;

some of it isn't so trivial. The question is tactical: has our time period changed?

Now, we are trying throughout the crisis management area to arrive at a better planning process for that. That brings up the question of options. First of all, the White House is not the place where you carve out most of your options. If you can't get that in the bureaucracy, then you've got real troubles. And that's our problem. I don't know what your experience is, but I know of very few elements of the bureaucracy that, unless specifically tasked by the President, will offer him (not me, him) options. The courses of action are generally preselected. How? Regardless what books you read—they are all fallacious in my experience—they do not bring forward those options. Often the lower levels of the State Department may pass options forward to somebody else who then passes them to the Secretary, but by the time I see them there are very few options. They don't want us to have a lot of options. I think that's a competency question, a trust-of-government question. After so many people have analyzed something, a certain policy determinacy sets in. The guys who know everything there is to know about every ideographic piece of information will drive you absolutely crazy with facts—they know about this, that and the other thing, but they haven't got a concept. A concept is an alien notion. It is not something to be dealt with.

So concepts and options don't come forth. If we got a set of options, would we know what to do with it? I wouldn't necessarily jump on it with both feet. Why? I come back to my central premise: this society pays dearly for its inability to integrate information.

Let me make one other observation about information processing. Technical, highly specialized information rises without being integrated right to the top. So that presidents truly are not, and their advisors are not, competent to deal with the pieces they frequently get. This is the great problem with the parts of the intelligence community. They collect a kind of data that is tremendously important, but which must be integrated in the total wehhing of knowledge about a particular problem. Yet it is so hot, and sometimes so specialized, and so much a question of the sources and the methods. You don't buy the data unless you know those sources and methods—and it causes them all kinds of grief if you're going to know that, except in the most general of ways. Yet you must act on it—and that's what the presidents have done. That very President we talked about acted on highly specialized knowledge he was getting, and it was called "raw" but it wasn't raw. Johnson couldn't have acted on raw data. It could not have happened. It has had an initial processing. A decision maker who is living in high levels of uncertainty reaches out there and says, "Give me something I can act

on, some piece of information on which I can comfortably take the step of allocating enormous resources."

[STUDENT] What's your prescription for data integration? How do you go about teaching people, or pushing that to happen in an organization?

[BEAL] I'm going to leave you disappointed on this; I plead first of all not being competent on the question. It is an issue we really would have to spend some time on. I've thought about it for years. I used to run an international relations program and had sophomores, juniors, seniors, and graduate students asking, "How do I do all this?" That's why I think this particular program is important: you're combining substantive issues with technology information. You know you've got to step across a lot of knowledge domains to be able to handle that probability. It is a basic philosophical question about education that starts very early. I have a lot of thoughts on it, but it really is well beyond what we could cover today. (5–19)

16. **DAVID MCMANIS**, "Warning as a Peacekeeping Mechanism" (1984, pp. 21–34)

National Intelligence Officer for Warning and Director, National Warning Staff

Now, when we talk of warning, we're talking about it as communication of a potential threat to national security interests—a communication that is given to the decision maker or the policy maker sufficiently in advance of the event so that the decision maker or policy maker can take steps to avoid or mitigate the threat's consequences.

. . . Half of the warning equation is the recipient: the decision maker and the policy maker. We in the intelligence community have been guilty for many years of periodically opening the door and yelling "Here they come!" and then quickly slamming the door, not even worrying about whether anybody on the other side of the door heard the message. I am stressing to our analysts and to the mid-level managers that they have a responsibility to identify who has to hear the information, and then to put it in a form that is usable, understandable—maybe even tailored to the recipient, particularly the more naive recipient. That is a lot of responsibility.

. . . Another area we are trying to illuminate is all the paradoxes of warning. We don't understand them well; there is a lot of room for more research.

An example of paradox is that the earlier we try to provide warning, the more ambiguous that warning may be. And ambiguity is hard for our decision makers and policy makers to cope with. It is particularly hard because for so many years we talked about unambiguous warning. From my viewpoint, the only unambiguous warning today is when you see that the missile has been launched, or the bullet has been fired and is on its way toward you. That sure isn't much warning. . . .

Another paradox is a problem we deal with constantly in our estimative work: consensus versus sharpness of decision or analysis. For years and years we based our estimates on consensus, coming forward with a draft position that was massaged by a room full of intelligence gurus until it had little or no significance but certainly was not offensive to anybody. We have had to find ways to get away from that. And even though our estimative process today still uses consensus, we have encouraged alternative analysis, development of alternative scenarios, and publication of dissenting views. So no longer do we feel compelled to go forward with the national estimate which has only one—usually very safe—view of what the future may bring.

. . . Most of our postmortems have shown us that the information has usually been there. It has not necessarily been pulled together or synthesized properly. Often it is not recognized. (Often, too, the decision maker didn't want to hear that particular message on that day, and so ignored it.) But the information is usually in the data.

. . . We have to keep from falling into the trap of the warning becoming too familiar—maybe changing the color of the paper, or putting a microchip in the corner that emits a klaxon when it hits the decision maker's desk. I am not quite sure how we do that, but we have to keep working at new solutions.

. . . In the Washington area today there are some 14 or 15 principal crisis management centers. They are tiered. The "big six" of the National Security area are the National Military Command Center, which has operational responsibility; the National Military Indications Center, which is strictly intelligence; the State Department Operations Center (operational); State Intelligence and Research (intelligence); the National Security Agency's Operations Center (intelligence); and the White House Situation Room.

The next tier, primarily operational, includes the Service operations centers—Army, Air Force, Marine Corps, and Navy. Below that is another tier which is

getting a lot more action these days: the crisis centers of the Department of Commerce, the Treasury, the Federal Emergency Management Agency, the FBI, and in terms of nuclear terrorism, the Department of Energy. These people are the front line in terms of crisis containment and subsequently crisis management. We've been working with them to try to strengthen their bonds.

You probably don't recognize how unusual it is to have those people working together—having an operations organization like the J-3 working closely with a bunch of intelligence people, with very few boundaries between them, and complete sharing of information. When you throw in the Department of Energy as another separate but equal player, that's a pretty potent force. Then if you realize what each single node represents in terms of our ability to literally encircle the globe, putting tentacles out to the other military and civilian watch centers throughout the world; it's a damned impressive network.

The problems lie in making sure that the players themselves understand what it is they have—that they understand the capabilities of their counterpart centers, and know how to marshal all their selective assets to work a crisis without tripping over one another. In the conventional scenarios—nuclear attack or even a non-nuclear event, say a collision of a US destroyer and Soviet submarine, we handle things well, because we have a limited set of players. But let's say a group of terrorists successfully captures the nuclear generating plant at Hanford, Washington, and holds it hostage. The community responsible in that situation has at least four people in charge, maybe more. How well have they worked out the operating procedures to deal with that problem? They really haven't yet.

. . . I want to stress the criticality of the old-boy net. Not only does it exist, it is viable and should be nurtured. There really is nothing better in terms of warning than to have a **Bill Casey** pick up the telephone and tell the President, "That estimate on its way over to your office represents a very serious threat for national security." (22, 23, 24, 26, 27–8, 31)

Bill Casey—William J. Casey, Director of Central Intelligence under President Reagan, 1981–87

17. **Robert A. Rosenberg**, "Strategic Defense: A Challenge for C³I" (1984, pp. 63–86)

Vice Commander-in-Chief, North American Aerospace Defense Command and Assistant Vice Commander, US Air Force Space Command

I'll tell you about a couple of threats that my boss and I worry about every day. One of them is a crazy threat, **a Khaddafi-type threat**. You know, about the best the boss can do in that kind of case is tell the National Command Authority, "Here comes one." Even more serious than the crazy terrorist threat is what I call inadvertent (or advertent) attack—it's not an accident. A **Yankee boatload of 16 tubes** comes heading toward North America, and the Washington-Moscow hot line lights up, and a message comes through from **Chernenko** that says, "Mr. President, it's a crazy sea captain, he got the code, he launched them, we are not responsible, we didn't do it, don't retaliate; after they land and you clean things up, we'll agree to mutual retribution. Don't do anything; it was all an accident." And in fact it wasn't an accident. It's the leading edge of a decapitation attack. With a strategic defense program—not a 100-percent leakproof program, just a reasonable strategic defense program—those two threats will disappear forever. And those are the threats I worry about very much today. (86)

Khaddafi-type threat—refers to the Libyan leader's links with international terrorism

Yankee boatload of 16 tubes—a Soviet submarine carrying 16 ballistic missiles

Chernenko—Konstantin Chernenko, General Secretary of the Central Committee and President of the Presidium of the Supreme Soviet (died March 10, 1985)

18. **STUART E. BRANCH**, "C³I and Crisis Management" (1984, pp. 87–102)

Deputy Assistant Secretary for Communications, Department of State and member, National Communications System and US Communications Security Board of the National Security Council

I'm convinced that we will be successful in moving more information faster than ever before, and getting it closer to the user. That's "ho-hum" technology, even with the requirement to make it secure. It's a function of how many people we can throw at installations and logistical support. However, my concern is this: having done that, I don't think we will have accomplished a thing for the decision maker. If anything, I think we're going to frustrate that process. If we're looking at command, control, communications, or the National Command Authority and we're talking about avoiding hostilities or a cessation of hostilities, and all we're doing is building the pipes bigger, have we really promoted our national security? . . .

Users are just beginning to experience the problem of too much information flowing from embassies to Washington, or from Washington to embassies. It is very difficult to sort through that and find out what is important, what's

timely, and what ought to be on that desk. We are building the technical capability out there that's encouraging movement of information, and it is moving. In fact, in some cases, it's looping. I spoke to one ambassador who mentioned this problem. He said, "I'm getting too much information. I'm even getting information we generate! Our political counselor writes a report that deals with military activities, sends it to Washington, where it is sent to the Defense Department, where it is sent back to us because it divulges military actions here in this country. And the report originated here." That's an example. I'm not suggesting there's a lot of that, but it's an example.... [W]e're going to see more and more centralization of the formulation and the execution of foreign policy. I don't know if that's by design or if it's accidental. I think that technology is encouraging centralization because information can flow back and forth.

It's not just in the State Department or the diplomatic service—the Washington managers are involving themselves in the decision-making process as they never have because they are on a much shorter leash than ever before. We used to beat that by saying, "I can't hear you," or "I didn't get that memorandum." Now you've got them right on the other end of your system. I think that concept is contributing to this shift of centralization of control to Washington, but I think there are also a number of other things that cause it.

Clearly, the interrelationship of issues across our government demands that information be shared, and that inputs from the defense, intelligence, and other sectors of our Executive Branch be factored into that decision-making process. Also, it limits the occasions in which an ambassador can act on his own and then report back after the fact. Of course, the argument continues about whether there's too much or too little control from Washington, whether the coordination is good or bad. (92–93)

19. **LINCOLN FAURER**, "The Role of Intelligence Within C³I" (1985, pp. 17–32)

former Director, National Security Agency and Chief, Central Security Service

I don't think, at the present time, that we have adequate national intelligence survivability to guarantee flow to our decision makers. I think, perhaps, our greatest failing lies in our cultural reluctance to accept the imminent possibility of war starting. That probably is not only big war with the Soviet Union, but war at almost any level in a crisis. I think we will be reluctant to

accept the indications that say someone is going to start shooting shortly. Therefore, we will lose the advantage of action that might precede that first shot, for fear that by taking action we will worsen the situation and encourage hostilities.

... You see, even the most well-intentioned of the intelligence community, as they prepare estimates or advise the policy maker, must have an eye on the policy maker's interests. That is, not what conclusions he ought to reach, but in what he ought to be interested, or in what he is interested. As an estimate is put together, it is essential that certain aspects not be overlooked in regard to a problem that the policy maker clearly needs to confront. In doing that, one occasionally provides the policy maker with exactly the kind of information he wants, because he's made up his mind in advance about what he wants the answer to be. And just as often that does not happen. When it does, the screams go up about playing into the hands of policy makers....

[STUDENT] What are your first priorities for improvement?

[FAURER] Our first priorities? We can be more selfish than others and, at the moment, we are and have been for a long time. Our approach is to ensure adequate communications for moving our data in peacetime, to try gradually to make that more robust so it can survive some encroachment in wartime, but our real hope lies in reducing the essential. And the lesson we preach on this subject isn't how much more communication to buy, although we're happy to do that even though the figure is large, but rather our lesson is the essentiality of reducing identification of the requirements. (28, 32)

20. **RICHARD G. STILWELL,** "Structure and Mechanisms for Command and Control" (1985, pp. 33-65)

Chairman, DoD Security Review Commission

[I]n controlling the operation, stick to the chain of command. Don't hypass or skip echelons.... It's one thing to hypass in a request for information down below, but it is something else again to try to hypass channels in order to give instructions to people two or three echelons below, because that's a recipe for disaster.

... [T]he more people operate on common doctrine and standard procedures, the more you're likely to get a disciplined, automatic reaction—even

under great stress—on the part of everyone. Procedures, in my view, are more important than sophisticated hardware.

[OETTINGER] If I may interject a linkage to what you heard from General Faurer, he commented toward the end of his presentation that what is desirable under stress is not necessarily hardening all the Coms, but reducing the requirements. This remark is intimately linked to our discussion here because the flip side of communicating is standard procedures and doctrine, where the communication has been done beforehand.

[STILWELL] When you get in a crisis, you have a terrible compression of time; large events are occurring in a very constrained time frame. You're dealing with a tremendous number of concurrent issues which become all the more difficult to prioritize, and we'll come back to this. You've got incomplete information and you have to make big decisions, and you'd better be right because decisions are irreversible. Therefore, you'd better have a lean, well-schooled organization that can handle that type of crisis.

. . . You will find, if you've been through war games (and most of us have), that when the crisis comes, a lot of things are happening very quickly, and your interest is not in your data bank behind you, except very peripherally. Your interest is in what is happening currently. And the search for that information, the precision of that information, the prioritization, and the reduction to the real essential concerns are very important. (48, 57, 63)

21. DONALD C. LATHAM, "A View From Inside OSD" (1985, pp. 103–23) *Assistant Secretary of Defense for C³I*

The strategic problem that we are faced with is then summarized in the new Defense Guidance, for FY 1985 to 1986. It states that since we're committed to a defensive use of power, we are always going to be reacting to what is known as ambiguous warning, or after the enemy has seized the first initiative. Everybody talks about unambiguous warning, but we'll never have such a thing. Either there will be warning indicators on some pending attack that will be ambiguous in the sense that you're really not sure what's going on—so it will be a very difficult problem—or else the enemy will go first with no warning at all. This situation puts a very heavy burden on the C³I system.

... Another favorite topic of people in terms of enduring C³I is denying the decapitation of the NCA. And that has to do with people claiming that a terrorist attack or something in the night could come in, kill the President and all successors and the other national command authorities, and as a result, prevent the U.S. from ever using its strategic force. We've taken major steps to deny that possibility. There was an announcement made in June 1982 of a major Continuity of Government program by a special advisor to the President. We have worked on that problem very hard.

We also say we will let no "cheap shots" succeed. This means that the horror stories about some sort of an attack that could disable the whole command and control system with just a few weapons do not come true. The favorite one is the high-altitude electromagnetic pulse (HEMP) attack or a few cruise missiles sneaking in and taking out a few command centers in the dead of night.

[OETTINGER] If you accept the point that people are very much in the loop, then one of the critical elements ... is this fundamental balance in terms of how much gets up to decision makers. If you let too much through, they haven't time to digest it, causing problems of absorption, limited attention span, understanding, etc.; you overload. If you don't let it all through, there's a selection problem. The minute you start selecting, there are people doing the selection, and the minute people start doing the selection they acquire a certain amount of bureaucratic and/or other power, and so you have a constant instability in that.

The question of how to organize to do this almost becomes a contradiction in terms. The minute you organize there's somebody who sits on top of the pile. Everything you've heard, both last year and this year, about the little word "through" in the role of the Joint Chiefs in the chain of command becomes an issue. So much of the problem of where that balance is in the flow of information, in the flow of warning and so on, rests on that question of "Whom does it go through?" "Is it formally organized?" "Is it not formally organized?" If you organize too much you have sources of independent powers tending to thwart lines of communications, but if you don't organize enough, everybody gets snowed, and nothing happens. There is no permanent solution to that problem, because it depends on who is on top—the commander-in-chief—and that position varies with each administration. (104, 107-08, 118)

22. **CLARENCE E. MCKNIGHT, JR.**, "C³I Systems at the Joint Level" (1986, pp. 1–30)

Director, Command, Control, and Communications Systems, JCS

When most people start talking about architectures, they like to start drawing circles, and then lines and arrows between the circles, and connecting everybody up before they ever understand what it is that they want the system to do for them. It's most important in the creation of any system, in my opinion, that you should design it as a pyramid so that all the actions that are down at a lower level stay at that level, and only a few go up to the next level, and very few go up to the top. But in a system where everything is moving massive amounts of information to decision nodes too rapidly, you get mass confusion as more and more information is being generated and then distributed at a higher and higher level.

If you look at the genesis of C^3 networks, they deal with sensors, correlation, analysis, decision making, and the posturing of either military or diplomatic forces, all of which constitute a feedback loop that comes back and forth but is primarily centered around that human intelligence in the center and the experience of that decision making node—be it the President and his advisors, or the Chairman and his advisors, or the duty officer and his people on the floor. You've got to design your systems so as to take into consideration the experience of those people who are in the system; yet this is one thing we forget, and we put in last.

... You have to keep the decision maker in the loop and you shouldn't have to climb a ladder to hand him a piece of paper. But there are tons of information that flow back and forth from local area networks that keep the worker bee, so to speak, informed. That doesn't mean that you shouldn't have trap doors or crisis management equipment going through. But in one of your earlier presentations, Dr. Beal talked about how to boil down 600 messages on the Iraqi-Iranian War into two minutes to tell the President. I defy anyone to do that very intelligently. I have seen the Chairman get intelligence briefings from a whole battery of subject matter experts. A lot of this stuff needs to be correlated by subject matter experts, because otherwise it is premature many times. Now, that's not to say that you can't have information go all the way up to the top. But 600 messages in one day? Trying to force a correlation with all that? What I say is that you have to have hedgerows of competent people; but what we have done today is to build bigger and bigger staffs. Washington has absolutely turned that pyramid upside down. They're running back and forth from the Hill to the Pentagon, and it's a constant interchange of information at the highest levels, most of which needs to be trimmed down and pushed back to where it can be processed closer to the source, in order to get a better flow upward of critical information....

What I'm trying to say here is that I believe many of our systems lack the discipline they need in order to tap that action officer traffic off without just putting everything in the hopper. (13–17)

23. **LIONEL OLMER, ESQ.**, "Intelligence and the American Business Community" (1986, pp. 59–71)

Member, Paul, Weiss, Rifkind, Wharton & Garrison, an international law firm; former Under Secretary for International Trade, Department of Commerce

It is impossible, at the present state of the art, to design a system that will satisfy all decision makers. They're different. The Under Secretary of State for Economic Affairs may he a very different person from his Commerce counterpart. It would not be appropriate to design a system for the government that would make Commeree happy if it wouldn't be useful to State, and vice versa. The same could he said of others in the policy process. Of what use is this judgment? Well, maybe it tells you not to invest a lot in something that is not easily adapted to individual personalities.

I've had the experience of hriefing three Presidents. I can tell you that they're all very, very different. It would do no good whatsoever to deliver to President Reagan a big, fat, hrieling hook every day with just two pages on the 154 countries of the world, or to pick six suhjects that you're going to cover, because that just doesn't suit his style. Well, I don't actually know what the procedure is now; hut there was a time when you had to fit all that you needed to say on the entire world every 24 hours into four pages. It didn't matter if it was the holocaust in Cambodia or a Soviet missile test. You had to fit everything in four pages. That requirement helps you design your system: You develop printing presses that produce four pages more rapidly and at greater cost efficiency than anything else could. But don't confuse the ahility to prepare intelligence in an efficient way with getting through to the persons you're trying to reach. (64)

24. **MARK LOWENTHAL**, "The Quest for 'Good' Intelligence" (1986, pp. 103–20)

Acting Director, Office of Strategic Forces Analysis, Bureau of Intelligence and Research, Department of State

A crisis is the worst time to get something done in the government, because everyone's critical faculties begin to drop off; everyone's living on adrenalin, and everyone wants to be involved. A classic example was Grenada. There were troops in action. Everyone really gets excited about combat. Lots of people were trying to get into the Operations Center in the department to "be there," including Assistant Secretaries for regions that in no way, shape, or form had anything to do with Grenada. I had to do a

postmortem on how we handled that situation and several other "crises." The director of the Operations Center told me that what he really wanted to do was to stand on a table and yell, "Will everyone except for the two **GS–9s** who are supposed to be in here please leave the room." But you don't do that to an Assistant Secretary of State when he's in the Operations Center.

GS—general schedule, a pay and ranking system for Civil Service workers

During a crisis things don't work as well. People start doing things for really bizarre reasons. Civilians, for example, often tend to be much more willing to use force than the military. The civilians have much less sense of what these operations are really like, even one-time veterans. (108–09)

25. **JOHN GRIMES**, "Information Technology and Multinational Corporations" (1986, pp. 135–49)

Director, National Security Telecommunications and Director, Defense Programs (C³), National Security Council

In a corporation, it is not unusual now for the chief executive to have a terminal next to his desk, which gives him direct access to the corporate data bases or allows him to communicate directly through electronic mail to all levels. You may categorize this process as command and control if you wish, but it has a major impact on management's control in the corporation, allowing the CEO in some cases to bypass middle management. Some layers of what we know today as middle management may vanish because of the advent of information technology.

Satellite communications is another of those technologies that permits both the military commands and corporations to "skip echelon," and communicate directly from the corporate head or commander down to a division-level organization. General Motors has installed a pervasive satellite system that will reach down to depot level. In the national sense, we can do the same thing today—go from the White House, or from the Secretary of Defense, right down to the foxhole. Satellite and information technology have made communications flow transparent from top to bottom of an organization. There is an excellent example of this. Back in the mid-1970s, during the *Mayaguez* boat incident in Cambodia, a two-hop satellite transmission path was established over which President Ford was able to talk to the battalion commander under fire on the ground. Here you had the Commander in Chief

of a nation talking to a guy right on the ground or, as they say, to the foxhole. This skipped the chain of command from the Chairman of the Joint Chiefs of Staff, the military command in the Pacific area, and the intermediate command in Thailand. Multinational corporations do the same thing today, especially overseas operations.

I want to elaborate on how we use computers and communications satellite technologies for crisis prevention. Information is received quickly from various intelligence and diplomatic sources; it is processed and made to control or prevent a crisis from escalating. Today, I think you would say that in a *controlled crisis*, whether in a corporation or the government, the CEO (or, in our case, the President) is able to be directly involved at all levels of the units involved in that crisis because it's no longer beyond his span of control.

. . . One aspect to which many of us give little thought and rarely use, and that I mentioned earlier, is *feedback*. Computer-based communications systems and decision support systems provide an excellent real-time accounting record or result of the sequence of steps that take place during an event, whether in a corporation or the government. Feedback not only helps to complete the record of what transpired, but also drives future policy or changes. In our case, we've learned that when decisions are made in a major crisis and certain actions are taken, standing policy will change.

Computer-based decision support systems, including videotext, video teleconferencing, facsimile, and other visual aids, give more efficient capabilities, and enhance crisis management decision making. Before we had computer-driven display boards, we used to track aircraft by having individuals put radar tracks on Plexiglas boards. Today, those tracks and decisions are made on a real-time basis with computer-based technology. Gaming and modeling of economic situations in a multinational corporate setting illustrate the advantages that technology provides for decision making tasks.

Real-time video teleconferencing is seeing increased use in the government for day-to-day operations and we're seeing it explode within the private sector. The cost of travel and the fact that people don't want to get on airplanes because of the terrorism threat in themselves increase the demand for this technology. Not only does it improve the use of time but it also lets you see individuals' expressions and gestures during conversations. We're going to see more of this technology used in command and control and even in intelligence operations. The intelligence community can transmit a map or

drawing from one country, or one state, by facsimile machine, which is pretty efficient, or can display the material via video teleconferencing, and then record it. I might mention that facsimile technology is used to improve the accuracy and speed of information flow over the Hot Line between the Soviet Union and the United States. Facsimile or video teleconferencing is real. The reason being, getting back to satellites, the efficiency of transmission systems operating on T–1 carriers at 1.544 megabits, versus what we used to run, 2400 baud. Today, we multiplex video teleconferencing, telephone conversations, and data transmission all on the same wideband digital circuit for efficiency and reduced cost.

There is a major *vulnerability* to all of this. We have become so dependent on some of these tools that when we do lose the capability under certain circumstances or for a certain function, it causes chaos. The banking industry is concerned about the financial information they transfer, to the point where they put error detection and correction capabilities (redundant paths) in their systems so that the information is transmitted in two different ways. In any decision process, from a corporate decision to a national decision, you can soon see that if you don't do some smart things with this technology it can get you in trouble; it's like putting all your eggs in one basket.

... Once they learn how to use a system, they continue to get more and more messages regenerated. I know that General McKnight has been having a terrible problem, because people have adulterated the military system. When they send a message out, they not only send it to the individual addressee, but they also give an information copy to the world, without realizing the burden it puts on the system. A smart staff person knows how to use a system like that, because sometimes the guy actually receiving a message does not have the authority or ability to react as well as one or two of the information addressees. It's a very interesting point to play. Once again, technology gives you that opportunity to use or control information.

... In recent years I've read some books, right out of this school, indicating cases where upper management goes in and gets reports on production, product lines, delivery times, etc., and just bypasses all of the middle management. The question is how to control that process of blending technology with management. Well, again, as individuals become more proficient and comfortable with it, I think it's going to become more pervasive in time. You will find that it will change organizational management schemes for those companies that use it.

... It takes on the character of the guy at the helm, though. You've got to remember that. If you want to talk about a *Mayaguez*, I don't think

this President would ever do that. He believes in corporate or macromanagement, and leaving war to the experts. He'll make the decision that we're going to take a hill, but not how we're going to take it. Another individual, as we've seen, might assert himself in deciding how we're going to do it. Technology has given you the opportunity to do that. Whatever information is available at the White House today to make those decisions is pretty much just as readily available to the other agencies, only we see more of it. The same goes for corporate headquarters, whether in a domestic company or a multinational corporation. That kind of information is available because you design that data flow into your system so you have some finger on the pulse. You can start seeing if things go awry.

this President—President Reagan

That brings back the point of whether it's a push system or a pull system. People can very subtly cause thresholds to be built. If something happens at the General Motors plant in Spain that exceeds some threshold, you throw the first warning signal back to corporate headquarters. The same goes for the national level; there's some threshold as to whether you're going to wake up the President at night.

[STUDENT] Is there a danger that, because of technology, the information flow is getting faster while there's always a tendency for analysis, being less measurable, to slip behind?

[GRIMES] That risk is definitely there. One of the ways you might overcome it is to improve the decision support capabilities to take in that information, and artificial intelligence is going to help to improve that process. What we're talking about right now is almost on the same threshold as the Strategic Defense Initiative (SDI). When you're trying to respond on a real-time basis, based on your warning, your sensors, there's no human mind that can react fast enough. That's where artificial intelligence will start doing a lot of that recognition for you and giving you options very quickly. Again, you have to play out the various scenarios, whether you're talking about a nuclear conflict versus a national crisis **such as last night**.

such as last night—US bombing raid on Libya, April 14, 1986

You can take the **Bhopal disaster** with Union Carbide as an example of a very major crisis, looking at how they set up emergency operations, collected real-time information, and weighed the decisions they were going to make, including the possibility that the Chairman of the Board might have been locked up and held hostage when he arrived. It depends on the circumstances. In a military situation the primary concern is the element of surprise. The risk is that the information flow is so great and so fast that sometimes the analyst has to go hy intuition. (135–37, 140, 141–42, 143)

Bhopal disaster—In December 1984, a toxic gas leak at a Union Carbide pesticide plant in Bhopal, India, killed 1,762 and injured 200,000.

26. **B.R. INMAN**, "Technological Innovation and the Cost of Change" (1986, pp. 151–68)

President and Chief Executive Officer, Microelectronics and Computer Technology Corporation

[W]hat has surprised me more than anything else about the performance of industry as compared to government in this broad area we're discussing—the ability to gather knowledge or intelligence on the outside world and then integrate it into a decision-making process—is how poorly that is done. I had always held the view, from my 31 years of government service, that industry must be far more effective, far more efficient than government. I'm sure that there are many cases where that is true, but I haven't been exposed to a large number of them in the past four years. (152)

27. **GREGORY D. FOSTER**, "The National Defense University's Command and Control Program" (1987, pp. 1–22)

Senior Fellow, Institute for National Strategic Studies, National Defense University (NDU); former Director, NDU Command and Control Research Program

I think there are in this field, as in other fields, a lot of barriers that continue to exist between different disciplines. For the most part, we have far more mathematicians, physicists, and what I have pejoratively labeled as "wireheads" doing C³-related research. Although there are some parts of the human resources or behavioral sciences community doing command and

control-related research, it's pretty limited. And never the twain shall meet. Typically, the two parties don't talk to each other.

. . . Why is theory important to command and control? I think there are three reasons. In the first place, I would argue that we have witnessed in the modern era a convergence of strategy and tactics. By virtue of significant improvements in telecommunications and transportation technologies, even the most remote tactical activity or action can have almost immediate strategic ramifications.

Similarly, I would suggest that we see before us today a complete reformulation of what war is. The traditional dichotomy between peace and war no longer is meaningful. We are engaged in forms of international interaction and conflict today that suggest to me that we really need to rethink what war is in the context of command and control. This affects how we view, at the grand level, the interrelationship between civil and military authorities and, at a more focused level, how commanders exercise command over forces in being.

[OETTINGER] Is the point complete? The second question will be what does it have to do with "why theory?" The first question is to ask you to sharpen your comments because at the most general level, they don't make much sense to me. The convergence of strategy and tactics, as a new idea, is lacking. I go back to the anecdote "for want of a nail, the horseshoe, etc., etc." It's clearly a parable about the connection between the most tactical of accidents and the most strategic of outcomes. The redefinition of war as carrying out essential diplomacy by other means is an aphorism that simply says that the civilian-military connection is not being made. In some sense, there's nothing new under the sun. I amuse myself by making fun of what you're saying here at that very abstract level. On the other hand, there are some things that have changed that make this more plain. I wonder if you could sharpen up where you see the boundary. What is it that makes this conceptually eternal? What's different now?

[FOSTER] To reiterate a point I just made and then tie this back to some of my earlier premises about the state of C³ in general, I think we live today on kind of a global battlefield wrought, again, by marked advances in telecommunications and transportation technologies. We have witnessed a shrinkage of the globe such that those activities undertaken in what we traditionally have construed as peacetime actually are a form of waging conflict with real-world strategic significance. That is not to say that this is a new state of affairs. The important thing to acknowledge, though, is that our conceptions of command and control, and of how command should be

exercised, continues to hew to a traditional conception of war, i.e., fighting battles and waging campaigns. We need to ask ourselves whether, in the modern era, the assumptions and predispositions that would have been relevant in that traditional conception of war are still pertinent.

For example, consider the proper relationship between civil and military authorities. Although we continue to espouse civilian supremacy, we also tend to adhere to an idealistic notion of giving a mission-type order to a military commander—a la Eisenhower in Europe—and then letting him do his thing. This creates a tension and a paradox of sorts that demands our focused attention because, whether it's Grenada, Desert One, or whatever, we continue to wrestle with this relationship between civilian and military authorities. It may well be that we are in an era now where we have to accept and deal with the idea of having the Commander in Chief, a civilian decision maker, or the National Command Authorities (the President and the Secretary of Defense) directing traditionally military activities that, for a variety of strategic reasons, they are unwilling to turn over to military commanders.

[MCLAUGHLIN] What changed fairly dramatically in recent years is the time span of control. Sure, in the past you gave a commander more general orders, "Go invade the continent." If he screwed it up, and by the time you eventually concluded he screwed it up, you relieved him. Today, it may be that half an hour into the battle you know he has screwed it up to a "fare-thee-well" and you relieve him then. And that's called "micromanagement" by every person who wears a uniform.

[FOSTER] The reason it is important to focus on this particular question, and the reason I want to relate it back to a point I glossed over earlier—the perishability of experience—is that an important consideration is whether, in a non-war situation (call it peacetime or whatever), we are inculcating the sorts of values and the degree of initiative and responsibility in commanders that they would need in a crisis or wartime situation. To relate to your earlier example, Tony, about a simple contract to do all of the software for NASA's Mission Control Center, today we see contracts that contain voluminous details and specifications. This is merely a manifestation of a larger, more pervasive trend in the way we do business, particularly within our military establishment. The question becomes, if you do not instill the sense of initiative, responsibility, and authority in commanders in peacetime that you will expect from them in wartime, are you doing both them and the nation a disservice? The consequences of waiting until a commander loses a battle or a war, or until he gets several thousand people killed, are such that we shouldn't want to wait until that time to deal with the situation.

Business is different, as is coaching or managing a sports team, because you're engaged on a daily basis in your operational mission. But in this age of deterrence, we must concern ourselves with whether we are nurturing the right types of folks to command in war. That is a traditional problem that has existed before every previous war, and it will continue to exist. Unfortunately, there are no school solutions to the problem.

. . . On the research side, there is no focal point for addressing command and control at the national and theater levels of joint and combined operations in peacetime, crisis, and wartime, involving both civil and military decision structures. When I came in, I took the scanty guidance that existed and attempted to fold all of these things together, so that the two principal foci of the program were (a) to conduct and sponsor basic and applied research that looked at command and control along the aforementioned lines, and (b) to develop a program of command and control studies for senior officers and civilians from throughout the national security establishment.

We joined in common endeavor with the other organizations constituting the Basic Research Group (BRG) of the Joint Directors of Laboratories because the foci that we represented were missing. These organizations all focus on uni-service, tactical, military initiatives. Besides our substantive orientation, we have at the National Defense University a wargaming and simulation center. One of my long-term designs was to create there a testbed that could be employed for both experimental and quasi-experimental purposes, looking at various dimensions of command and control. We also could undertake, I believe, what would amount to field research on how student groups acting as commanders and staffs performed in different types of situations. The only experimentation that now goes on takes place at the Naval Postgraduate School. That involves captain- and major-level folks who deal, for the most part, with naval tactical problems. That leaves a big range of issues that are not addressed.

The types of things I set about doing when I created the program included establishing NDU as a legitimate actor in the command and control community. One mechanism for doing that was a series of publications, of which there were two types. Two edited volumes were commissioned that attempted to deal with different dimensions of command and control. One volume, titled *Toward a Theory of Command and Control*, was kind of a living experiment in which I commissioned 10 different authors to address the same set of questions: What is command and control? What are its constituent elements? What is the state of the art in command and control theory and research? What work outside the military domain has been done that might be relevant? And where should we go from here? The idea was that if

I could get 10 reputable individuals with expertise in the area and stature within the community, who could look independently at these questions, we could determine where natural divergence or convergence exists.

Another volume, titled *The Dimensions of Command and Control*, looks at command and control from different perspectives: the technological dimension, the behavioral dimension, the legal dimension, the historical dimension, the socio-political dimension, and so forth. The idea was to get individuals with expertise in each of these areas to look at command and control from their different perspectives, and thereby to see where we have areas of commonality and complementarity.

Then there was a series of occasional papers. The intent of the occasional papers was to elevate the level of discourse and expand the bounds of inquiry on command and control. So I commissioned papers which deal with such issues as command and control in a democratic society. One paper I commissioned was titled, "Toward an American Philosophy of Command and Control." Another looked at the Soviet philosophy of command and control. I commissioned General Paul Gorman, former Commander-in-Chief, US Southern Command, to provide a theater commander's perspective on command and control.

On the educational side, I established a network with the other military educational institutions to try to see where NDU should be focusing its efforts in developing a course of instruction for senior officers and civilians. That is how the program came into being, and that is what the initial thrust was and continues to be. (5, 9–11, 12, 18, 19)

28. **RODNEY B. MCDANIEL**, "C³I: A National Security Council Perspective" (1987, pp. 107–24)

Executive Secretary, National Security Council; former Senior Director, Crisis Management Center

I got into the National Security Council (NSC) business by inheriting the job of Richard Beal, who was a one-time participant in these proceedings, and as a testament to the work that you do, I think one of the reasons that Tony and I met was I was really trying to find out what it was that Beal had in mind. One of the few places I could ever find that out was when he was up here and spoke to the seminar and subsequently created a transcript.

I think I'll begin at that point by giving you my observations about the direction in which I've tried to go relative to the direction in which Richard Beal had been going. My sense is that what Richard Beal was trying to do was to create within the White House a room where decisions are made in the context of a crisis, or fast-breaking events.

Senior people are brought in, kind of late, to a problem that's crashing about them. The perceived need, as Beal saw it, was to harness the power of modern technology, information processing technology, to assimilate all this mass of fast-breaking information. Perhaps you could pull up some history besides and squash that into some form that could be more readily assimilated by decision makers than is possible in the conventional setting, which is what he found when he took the job. There was a room like this with a little more security, probably no windows, and a bunch of people coming in with notes and papers, a few of them may have briefing charts, and that's it. Somebody in the corner takes notes. A traditional committee meeting. A room where decisions are made in the context of crisis.

My belief, then, and it's my belief now, is that that plan had some fundamental flaws. First of all I'll stipulate that that's what I think he had in mind. He's not here to defend himself, I may well have grossly misinterpreted, but that seemed to be what he set about, and what he had done. It was a non-trivial exercise in bureaucratic terms. He had gotten hold of some very hard-to-get-hold-of space in the old Executive Office Building—a room which had been the Secretary of State's office in the original design of the building, which as you know was the State/War/Navy Building and literally held the total departmental apparatus of those three departments at the turn of the century. He converted that into a high tech conference room which had screens to project all forms of media: television, computer screens which could be processed to video and shown on a screen, as well as slides and regular TV.

He created a database, hosted on some **VAX** machines, and he hired some junior intelligence officers to be database analysts. They were regional specialists, for the Near East, the Soviet Union, etc. There were seven of those fellows who were supposed to be up to speed on what's going on in those regions, and they would be the action officers who, when a crisis went down, would begin to pull the information together and put it in a form where it could be processed and presented on the screen. In 1985, Beal got a serious heart ailment and subsequently died. There was

VAX—a family of minicomputers produced by the Digital Equipment Corporation

subsequently a gap of six months or so from the point in time when he effectively became disengaged from the White House Crisis Management Center until the time I arrived on the scene. I had the problem of both rebuilding the staff, which had kind of drifted off because the leadership was no longer there—the more energetic folks lost interest and went looking for jobs elsewhere, as well as trying to reconstruct what the guy really had in mind. Given my sense of what Beal was up to, I think there was one major problem with it. It ignored the fact that the larger issue is, there's a process out there that's going on all the time. It's going on right now, this minute; that is, gathering information, digesting it, and analyzing information, and moving that up a series of kind of semi-hermetically sealed chambers to the Secretary of State, and the Secretary of Defense, and the Chairman of the Joint Chiefs of Staff, and the Director of Central Intelligence, who are the major members of the NSC. When these fellows or their principal subordinates meet in this room to make decisions, they're simply not going to live off the information that Beal's guys would have processed and put up on the screen. They're going to bring the information that they think is relevant right now with them.

How does that fit with the notion of the dynamic of the decision-making process in the room itself? It seemed to me that if you're going to undertake to make the process of decision making in crisis more systematic, and better, you have to enlarge the scope of your sights to take in that total process of information gathering and analysis that the National Security Community—which is a term I'll just coin—by which I mean the Department of Defense, the Department of State, and the Intelligence Community—engage in. That's point one.

[OETTINGER] I think Beal also had in mind that through technical prowess he could have those folks bring their own stuff into that room. The technical, bureaucratic, and psychological problems in that are monumental, but I think he was fairly explicit about having that in mind. Whether it ever got pulled off or not, I don't know.

[MCDANIEL] That's precisely my second thought. The second point is where is the information going to come from that Beal is going to get into his computer, in order to digest it and put it on the screen? The answers are going to come from State, Defense, and the Intelligence Community. Are you going to undertake, essentially, to tap their databases, so that if a crisis breaks in Afghanistan you can immediately reach into Defense, State, and Intelligence and pull out Afghanistan-related stuff with no delay while you hook the wires together, or are they going to send it to you, or what? What is the concept?

There are two obvious problems here. One is a technical problem which is, you're talking about access to a mass of data which is just mind-boggling. It really is a tremendous challenge, technically, to think about tying into the databases: Defense, State, and the military. Frankly that's the trivial issue, the technical issue. The real issue is the bureaucratic issue. There just isn't any way that State, Defense, and the Intelligence Community are going to sit still for some low-level people in the White House to be able to reach in and pull out facts and data from these databases with the prospect of putting it up on a screen in front of the President at some time of crisis without passing it through the chain of command of those respective departments, without the Secretary of State, or Defense, ever having seen it first.

Beal's concept was, in many respects, unachievable without undertaking to come to grips with the absolutely fundamental issue: that our government in the Executive Branch is really better thought of as a federation of agencies than it is of a unified, kind of military, organization with a commander in chief and these other officers as his trusted subordinates. If you will put that in the back of your mind, think of it as a federation, you'll be a lot closer to reality when you actually attempt to deal with these institutions in the real world.

We kind of fell back sharply from Beal's basic concept of tapping the databases and getting into that business. We recognized that what we had on our hands, in the first instance, was essentially a computer-based capability to take the messages that did come into the White House on a daily basis and make them more accessible in times of crisis. The much larger issue of how it is decided that different kinds of information were going to get sent to the White House in the first place hadn't really been touched, and that's what we needed to look into. With that as background, that was how I saw my job as I came in. I think the next thing I'll do is kind of talk you through how the government's organized for national security purposes, both for day-to-day planning, and for the making of policy in crisis.

The National Security Act was written in 1947. That act did three things, two of which, until quite recently anyway, were much more well known than the third. The most famous thing it did was it brought the departments of the Army and Navy together into a unified Department of Defense. Although I am no great student of it and it's my personal belief that the history has not been written very well, I've read a few of the more synthesized histories of this piece of legislation and I find them pretty thin going, actually. Basically, the National Security Act of 1947 was the final congressional output of the "fussing and fuming" over the lessons of World War II. It was thought that the Services didn't cooperate with each other very well,

so the way to fix that was to put the two Services under a common head. That's the first thing the National Security Act of 1947 did. It unified the Army and the Navy.

[OETTINGER] What you just said triggered a thought. One of our colleagues emeritus at the law school, Milton Katz, was in his earlier days one of the lawyers who worked on the drafting of the Act of 1947, and it might be fun to sit down and explore that very question. I think he'd be eager to and remembers enough to put some threads together.

[MCDANIEL] The second thing it did, for which again I have a smattering of historical understanding, is that it created the CIA (Central Intelligence Agency). The CIA was specifically established as an intelligence organ reporting to the President. Actually, under the Act, it reports to the National Security Council, independent of State and Defense—independent of the agencies with responsibility for executing policy and programs. Thus, the President presumably got the unvarnished truth without bias, without a spin being put on it by people who are trying to sell some particular policy line.

The third thing it did, and the area where there's the least legislative history, is, it established the National Security Council itself. The mission of the National Security Council, that title in the law that established the National Security Council, remains unamended to this day. I was pleased to note that the **Tower Commission** recommended that it not be amended. It's a very short act, very readable, and basically it defines the function of the National Security Council as a mechanism to integrate domestic, military, and foreign policy, to effectuate the overall national good. That act, in effect, created the term "national security" which we use so glibly today, a term which really then encompasses foreign policy and defense policy. National security policy, then, is the integration or the fusion of diplomacy and military operations.

Tower Commission—a three-man commission (John G. Tower, Edmund S. Muskie, and Brent Scowcroft) appointed by President Reagan to investigate the Iran-Contra operation

Implicit in the need to create the Council and establish it by law must have been the view on the part of the Congress that the State Department, the War Department, and the Navy Department were not coordinating as effectively as they should have been, although, as I say, the historical record there is kind of thin. It is, according to the history I've read, apparently a fact that in those days the Departments communicated with each other quite

infrequently. The Secretaries of those three departments did not meet on a regular basis, and their staffs, depending on the personalities of the Secretary of State, Navy, and War, were sometimes almost enjoined from talking to each other. In one sense I've characterized the purpose of the National Security Council as to institutionalize the State Department and the Defense Department talking to each other. Indeed, we've come a long way in that regard. So much so, that a great deal of the purpose of the Act is being accomplished totally outside the formal structure of the National Security Council or its staff, because a culture has been created now where State and Defense do talk to each other to a much greater degree apparently than was the case before 1947. That's taken as a matter of routine.

The Act said that the members of the National Security Council shall be the President as Chairman; the Vice President, and the Secretaries of State and Defense are the statutory members. The President is the chairman of a committee that reports to him as President, kind of a quirk in the law, but I'll come back to that because I have my own belief in what that meant. Then that Act or subsequent acts which have come along have defined statutory advisors as the Joint Chiefs of Staff—**that was just changed** to the Chairman of the Joint Chiefs of Staff—the Director of Central Intelligence, and also the Director of the Arms Control and Disarmament Agency when arms control issues are involved, and the Director of the US Information Agency when policy issues affecting overseas information are being discussed. Those individuals are named in the various pieces of legislation as statutory advisors to the NSC.

that was just changed—by the Goldwater-Nichols Defense Reorganization Act of 1986

Although the Act does not say this anywhere, it's my belief that what Congress had in mind was the creation in this council of a body that is somewhat like the theoretical Joint Chiefs of Staff. That is to say, the Secretary of State and the Secretary of Defense come to the table and become advisors to the President. They do not come as the holders of a bureaucratic brief for their respective bureaucracies, but rather as advisors to the President. In conjunction with the Vice President and the President himself, they sit around and talk about policy issues and discuss the pros and cons and the various options, and ultimately make a corporate recommendation to the President. The President, as President then, decides and issues instructions to the agencies to implement. The order, when it goes down, is for the Secretary of State and the Secretary of Defense to implement as heads of executive agencies. The Council exists as a policy body to advise and recommend to the President

When I was giving this explanation to someone who will remain nameless he quipped and said, "Yes, you're right, it works exactly like the Joint Chiefs of Staff works because they don't do that either." Of course, the Army, Navy, and Air Force come to the table and defend to the death their respective bureaucratic turfs and that tends to be what we see in the National Security Council, where you have role playing to a large degree with each of those cabinet heads kind of representing the brief of their respective bureaucracies. The notion that they're there to be personal confidential advisors to the President, while it works to some degree, is perhaps more the exception than the rule.

The Act also said that the President could designate others to be members of the Council. **This President** has designated **Mr. Meese**, and **Mr. Baker**, and the **White House Chief of Staff** to regularly attend meetings. This has varied from administration to administration, although the person occupying the position of Attorney General turns out to be someone who's frequently in the Council. It's important to remember that in this administration the reason Baker and Meese are at the table is not because they're Attorney General and Secretary of the Treasury, but because they started out in the first term being the Chief of Staff and the counselor to the President, respectively, and retained this special relationship to the President.

This President—President Reagan

Mr. Meese—Edwin Meese, III, Attorney General, 1985-88

Mr. Baker—James A. Baker, III, White House Chief of Staff, 1981-85; Secretary of the Treasury, 1985-88; named Secretary of State by President Bush in 1989

White House Chief of Staff—Three men held this position during the Reagan Administration: James Baker, Donald Regan, and Howard Baker.

[OLTINGER] This is James Baker we're talking about?

[MCDANIEL] Jim Baker. When Baker went off to Treasury and Meese went off to be Attorney General, one of the deals they made with the President was they wouldn't lose their seats at the NSC. What you had is that they kept it and the new Chief of Staff, Donald Regan, was added on. Now the Chief of Staff's being a main player in the NSC is definitely something that waxes and wanes. I have talked to a few individuals who were previously closely associated with the National Security Council, who told me that during the Nixon Administration, for example, it was not the role for the Chief of Staff to attend National Security Council meetings or to be involved with NSC staff.

[STUDENT] This is **Haldeman**?

[MCDANIEL] Yes.

[STUDENT] More importantly, it's **Kissinger**.

Haldeman—H.R. Haldeman, President Nixon's White House Chief of Staff, 1969-73

Kissinger—Henry A. Kissinger, Assistant to the President for National Security Affairs, 1969-73; Secretary of State, 1973-77

[MCDANIEL] That is the formal structure set forth in the law. The law, as I say, occupies a couple of paragraphs. That's all it says in the law. Absent from any mention in the law is the position of the National Security Advisor. He is not mentioned in the law, nor in any other law. The only official that is mentioned in the law is someone called the Executive Secretary of the National Security Council, and he is identified in the law as the individual who is the administrative head of the staff. The law says, by the way, that this Council should have a staff and it shall be headed by an Executive Secretary and perform such duties as the President may designate. That's the legal justification for having an NSC staff. The legal justification for the position of the National Security Advisor is actually nothing more than the fact that the Appropriation Act for the White House office says that the President may have 10—I think that's the number—assistants to the President, and just traditionally one of these positions, one of these budget slots, is filled by a fellow who is called the Assistant to the President for National Security Affairs.

In effect, then, the National Security Advisor is de facto the actual head of the National Security Council staff, while the Executive Secretary is the staff administrator. It's undoubtedly done that way for two reasons. By not mentioning him in the law, you're left with the potential to keep his relationship to Congress somewhat ambiguous and more closely related to the White House, so as to fend off the periodic forays that people make that this individual should be subject to Senate confirmation. To some degree you insulate a little bit the fellow who has to go up and testify about the budget of the NSC staff who might be called upon to talk about other things if he were the National Security Advisor. When he's not, generally it's very minor. I've done that and it's a very minor hearing where no substance whatever is discussed.

The staff, as far as I can determine, has been pretty much the same for 40 years. It's an eclectic mix of people reflecting the makeup of the national

security community. That is to say it has military people who are assigned to duty on the NSC staff. It has Foreign Service officers assigned to duty. It has some intelligence officers, and it has civilians who typically are people with a foreign policy background who had some connection with the winning campaign of the President who kind of float in to the NSC as a function of the post-campaign "finding jobs for people" business. In this administration, that is about 50 professionals, although numbers are very hard to track because some of them are detailed, and some of them are on other agency payrolls, and anybody who's knowledgeable about the federal budget knows that that's untrackable.

The only thing you can depend on for doing historical analysis is telephone books, and that only if you had the internal listing that they really used, as opposed to something that might have been prepared for public consumption. I believe that this administration's staff is smaller than Kissinger's under Nixon, and bigger than Carter's. We're talking about a swing of maybe 10 or 15 professionals, total. It's kind of floated around 30 to 50 people for probably 40 years.

[STUDENT] I understand that different administrations, different Presidents, have different management styles and that will have impacts on the NSC staff.

[MCDANIEL] It has an impact on how the staff functions, but it doesn't seem to have that much impact on how big it is. It has a little impact on that. I'll get to how it actually functions in a minute.

[STUDENT] Would you have an ideal model, that the NSC staff should try to be organizationally or functionally flexible to the needs of the President, or should we find an institutional approach . . .?

[MCDANIEL] I recommend to you reading the recommendations chapter of the Tower Commission Report as a good overview of that particular body. A good group of people wrote it—you had a former National Security Advisor, a former Secretary of State, and a member of the Senate very knowledgeable of the political process of this country. They made the observation that if you mandate in law how something that is this close to the President is supposed to be organized, what will happen in fact is some shadow organization will get created to do what the President wants and it will simply cease to be used. The answer then is that you can't, in law, tie the hands of the President on something that is this close to him. If you think you can you're kidding yourself. He's basically going to do with it what he wants. I think the institution pretty much has learned the lessons

with respect to the size and the organizational structure of the staff. I will now describe the staff, and then I'll get into how the whole business really works.

[STUDENT] You mentioned that the Council should be integrating foreign policy and domestic policy. Is that something that you'll address?

[MCDANIEL] I think that's a good question. The law says, "will integrate domestic, military, and foreign policy." Then the law says, "The members shall be the President, Vice President, Secretary of State, and the Secretary of Defense," implicitly recognizing that all of these men are politicians, and when they meet in the Council as councilors, as advisors to the President, they collectively put the domestic implications of making policy into the milieu. That's one interpretation. Another interpretation is, it's the President and Vice President who represent the domestic point of view, and the State and Defense representatives represent the foreign and military policy point of view.

A third observation would be that they screwed up. There are a few people, academics, who have studied the national security process, who think that the procedural injection of the domestic point of view is the least perfect part of the imperfect structure of the NSC process. The sociology of the practitioners of foreign policy, and military policy, in my experience, can only be accurately described as elitists who are most comfortable doing business in a back room, talking to nobody, and then after they've done it their notion of the domestic angle is you call in the public affairs guy and flack it up. The notion that you bring in a bunch of politicians, Congressmen, and you seriously take what they have to say into account is anathema both to the agency professionals, and the "civilian" policy people—many of whom are cranked out of this campus, I might add—who go down to the bureaucracy and become practitioners. That's an interesting comment you made. I personally think that the Act probably didn't focus on that in terms of setting up the structure of the Council.

[DEUTSCH] It's slightly worse also, in that there is a domestic policy council, which functions more or less, which handles some of the purely domestic things. It seems to me that the functioning, whatever the meaning may be of that language, in practice is pretty empty. What is your observation?

[MCDANIEL] I have never attended an NSC meeting where the bulk of the discussion was not devoted to, "How's this going to play in the press,

and how are we going to get Congress to go along with it?" We're talking the domestic content of a national security issue. We're not talking about a forum. It was never the intent of this particular legislation to create a body to make policy for the entire spectrum of federal responsibilities, but rather to inject into the policy deliberation a domestic perspective as well as the perspective of the professional elite.

[MCLAUGHLIN] Which is presumably also one of the goals of a Meese, or a Jim Baker, or a Bobby Kennedy being included.

[MCDANIEL] It's interesting that the law didn't specify that somebody like that would be on the Council, but it's also interesting that all Presidents have always put somebody like that on the Council probably for just that reason.

[STUDENT] Could it be because of the threat perception of the United States—that we see threat as being external rather than domestic? Does that have anything to do with it?

[MCDANIEL] It might.

[STUDENT] Might that have changed over time?

[MCDANIEL] All I know is that the law was written in 1947 with the word "domestic" in it. I think that the people who have actually been practitioners in the making of national security policy have always had to grapple with politics. Probably more so in the post-Vietnam period than the pre-Vietnam period. There's kind of a conventional wisdom that the making of foreign policy was a more bipartisan process before Vietnam. You could cut deals with a smaller number of members of Congress, and the whole thing was more compact and tightly managed then than now. How accurate that assessment is, I don't know, but it's the conventional wisdom held by most people.

Even then, it was recognized that in a political democracy you have to have a domestic consensus if you're going to commit your military force to some act outside the boundaries of the country. That's just something that political democracies don't do without laying a domestic foundation for it.

I was going to just talk briefly about the staff structure of the NSC as it is now, and I think pretty much has been, and then talk about how the process works and then illustrate that with a few anecdotal examples.

The staff itself is organized in regional and functional directorates. The regional directorates mirror-image the State Department, which is organized, if you're familiar with it, with Assistant Secretaries of State for regions X, Y, and Z. Soviet and Europe is one; the Pacific and Asia is another; Africa, south of the Sahara, is another; Latin America is another; and lastly, Near East and South Asia which is the Middle East, basically Africa north of the Sahara all the way over to Bangladesh.

In the NSC staff, a big directorate would be four or five professional people, and a small one would be two. In government terms we're talking about a very small staff. When I left the staff, the Europe and Soviet guy was a Foreign Service officer, a former ambassador to Czechoslovakia, and a Deputy Chief of Mission (DCM) in Moscow, who has just left to be the Ambassador to Moscow, Jack Matlock. The Latin America guy was a Foreign Service officer, a somewhat more junior officer who hadn't been an ambassador yet, and that was a bit of a fluke because it had originally been headed by a political guy who turned out to be a bit of a maverick who wouldn't take direction and eventually had to be fired and the current incumbent wound up getting the job.

The Pacific job was headed by a civilian, professional employee of the Office of the Secretary of the Defense (OSD) who had been the Deputy for Asian Affairs in the OSD International Security Affairs Directorate and came over to the NSC from that job. The Africa office was headed by a CIA intelligence analyst who had headed the Office of African Analytic Affairs for 14 years. The Near East, South Asia was headed by a fellow we recruited from the University of California faculty who had previously been in the Policy Planning Office in the State Department, who would be considered a kind of an academic foreign policy guy, Dennis Ross. That eclectic mix of people, I think, is typical. Carlucci has brought in his people. Many of those people are now gone. But the mix has pretty much been maintained.

Carlucci: Frank Carlucci, Deputy Secretary of Defense, National Security Advisor, and Secretary of Defense under President Reagan

There are also a few functional organizations, all of which have responsibilities that cut across the regional areas. One is the intelligence directorate that looks at intelligence policy and budget issues and also was the office within the NSC staff responsible for coordinating covert action programs. There was another office called International Communications. That was the NSC staff office that looked at the propaganda apparatus of the US government, essentially the US Information Agency, Radio Liberty, Radio Marti,

This office was headed by a former officer from the CIA who had a lot of background in political action. Another office looked at space issues from the intelligence, military, and domestic sides and was the staff officer who was the principal White House official on space issues. Those were the principal staff officers of the NSC. As I say, it all totaled up to about 50 folks.

Now, how did it really work? The key to understanding the NSC is to recognize that what you have is a legislative mandate to set up an interlocking set of interagency committees. These committees have been around with various labels hung on them for 40 years. That's the life blood of how the NSC process really works. An interagency committee will be set up. Each administration has found it necessary to relabel them all as well as to relabel the documents that are used to record their decisions for reasons that don't make a whole lot of sense, but it happens. The last two that I can think of—the Carter Administration used as the title of decision documents PDs, Presidential Decisions. Prior to that Nixon had used NSDMs, National Security Decision Memoranda. This administration uses NSDD, National Security Decision Directive. It's all the same stuff.

There was one interesting difference, though, when this administration came in to set up its organization. Recall that the fundamental issue for the last at least 15 years, the modern era of strong national security advisors, has been that issue of how strong a National Security Advisor do you want? Conventional wisdom quickly throws out on the table two names to represent two polar extremes, and obviously this is a great oversimplification to think about it this way: Kissinger on the one hand, and Scowcroft on the other.

This administration, I think it's fair to say, intended to follow the Scowcroft model, and set itself up that way. Initially, **Allen**, the first National Security Advisor, didn't even report directly to the President. He reported through Meese. The committee structure was set up consistent with President Reagan's concept of "cabinet government" so that the chairmanship of the primary committees was to be vested in the cabinet officer who had principal policy responsibility for the area. There was a Secretary of Defense-chaired committee for Defense Policy, a Secretary of State-chaired committee for Foreign Policy, and a Director of Central Intelligence-chaired committee for Intelligence Policy, and there were no NSC staff-chaired committees, initially.

Allen—Richard V. Allen, National Security Advisor to President Reagan, 1981-82

That evolved over time, so that when I left the staff the Defense-chaired committee essentially wasn't functioning. The CIA-chaired committee was to some limited degree, and the State-chaired committee was fairly active. But a whole host of new committees had been set up on a topical basis. There was a committee for arms control that had been set up outside the framework of this initial structure, which was chaired by the National Security Advisor. There was a space committee that was chaired by the National Security Advisor. There was a covert action review committee that was chaired by the National Security Advisor. The only committee that was supposed to be chaired by the National Security Advisor from the beginning of this administration was the crisis management committee, in effect, which was called the Crisis Preplanning Group (CPPG).

That was the framework, and as I say, State was the most active. There were then established a bunch of subcommittees, in the case of State that essentially took all the different regions, regional groupings, and established an interagency group for each one. The membership would be the State Department desk officer, or the bureau head for the region, as chairman, and then a representative from OSD, from the JCS, and from CIA, and the NSC would have a staff representative on each one of these groups.

Once the committee's structure is established, it's important to recognize that what you've done is you've established an informal communications network, and that IG (interagency group) becomes the network of people who talk to each other about issues. Many people think that what you really should see is meetings, and agendas, and minutes. That's really missing the whole point. On the foreign policy side, where the IG structure was most effectively used, you had a relatively small number of formal meetings where agendas and papers were circulated in advance. What happened was, a decision would need to be made in respect to something, let's say affecting US policy with respect to the Vietnamese ongoing war in Cambodia. There was a need to make some kind of a decision with respect to that. The members of that IG would talk to each other on the telephone most likely, or they might have a short meeting and they would quickly come to grips with the issue and make a rough cut judgment as to whether this is something that is going to have to be run up to the President, or whether we can just agree among "us boys" to just go do it. If they agreed, it was done. The State Department, typically, would write a cable setting forth instructions to some ambassador, or some international delegate to some commission, or some forthcoming vote in the UN, or whatever the issue was, or somebody going to an ASEAN (Association of Southeast Asian Nations) meeting, and the policy would be established and that cable vetted by this group and sent, done. A policy is made, although the output document is a State Department cable

That meant that the stuff that floated up to the formal NSC tended to be either big issues, stuff that you really want to get the President involved in because it was a major decision, or disagreements. I've already mentioned that areas where disagreements were the rule rather than the exception, such as arms control, resulted in a new committee being set up, chaired by the NSC, in an attempt to impose decisions. But the vast bulk in this administration and I'm sure in others, the day-to-day making of national security policy, really goes on over the telephone by three, or four, or five people talking to each other either in a conference call or seriatim, in the context—to use a bureaucratic phrase that we used a lot around the NSC—of clearing a cable. It works. It's so much taken for granted that lots of people actually forget that that really is an NSC process going on. They forget it to such a degree that when I became the executive secretary and got curious about how many IGs there were, there wasn't anybody in NSC who had any central book on how many of these groups existed. I might add that when I sent out a memo to find out, I got resistance; why am I asking? What business is it of mine? Of course, my view was that these IGs really were NSC bodies, they were just operating under delegated authority of the Secretary of State to convene and administer them, because that was what this particular President had mandated when he set up his office.

[OETTINGER] You're getting, in your last remark, to part of the matter which I hoped you'd address. Given that all of that works and so on, it's a sort of a bottom-upward kind of thing in terms of integrating whatever comes out of this process. In terms of independent presidential inquiries, or initiatives, or in terms of presidential check on what the hell these guys are telling me, etc., how does it work?

[MCDANIEL] The last point I was going to make about the NSC role in overall policy formulation was "How does it really work?" I've said that it works to a large degree over the phone. A network of players is defined to work issues. That leaves only the issue of defining an issue. That is where you come into the several roles that the NSC staff are expected to play. Again, this is not really all that well spelled out in the law. They are expected, I think, to play three roles. One, they're expected to be the traffic cop, the honest broker. Nothing more than making sure that State doesn't try to get a cable out without getting Defense's clearance. They're expected to be guys who will blow the whistle in the State Department if the desk officer says, "Well, it's none of Defense's business." To a large degree, that role is a passive one. Your just being privy to the process has, if you will, a cleansing effect. The fact that there is a presumably non-bureaucratically partisan person who's privy to what's going on serves to keep the phone lines between Defense, and State, and the intelligence community working, because they know the NSC staff guy will blow the whistle on the process if

the other agencies aren't accorded their proper role. That's kind of the least exciting one, although a very important one.

The second function of the NSC staff is to he the independent advisors of the President. First they are participants in the interagency process, hut to the degree that the President either hecomes involved or needs to heconie involved, the NSC staff person is the person who will write the memo that transmits the issue to the President. Although you may have had an interagency committee write a paper and produce a consensus product with some options in it—a typical interagency paper v :l have options and a recommendation—that document would go to the President in the form of a memo from the National Security Advisor which will be written hy the NSC staff guy with expertise in the area. In that paper he, of course, will he expected to have his own recommendations, in addition to those of the Secretaries of State and Defense.

The third role of the NSC staff is policy initiation. That is to say, the ahility to say, "Let's create policy in this area," or "Let's cause an interagency policy study to be done with the ohject of reexamining a new Middle East peace process policy, or our Southern Africa policy," to name two where the State Department typically had a lot of trouble getting off the dime and producing anything other than mush.

This is where you have to have an NSC staff that is sufficiently competent, intellectually and professionally, to be capahle of being initiators as well as just honest brokers and traffic cops. At the same time you have to have a process which doesn't overload the circuit with a lot of top-down NSC staff-originated ideas, or you will quickly lose the allegiance and the participation of the other interagency players. There are no hard and fast ground rules here. This is very much a person ality-dependent process. What I'm trying to sketch for you is there's a whole nest of processes going on out there from each one of these interagency communities for Latin America, or for Africa, or for Asia. Each one of them has a se, of personalities that are working on different issues and in different ways interacting to make policy. A key role of the NSC staff has to be the abifity to propose policies as well as simply put the final stamp on the policy that's been proposed hy the Department of State, or the Department of Defense. How much time a particular staff officer spends on any one of those several roles is the function obviously of what the issue is, his own personal competence, and the competence of the other interagency players.

And lastly, something that I haven't said too much about, is the President himself. The NSC staff guys—we need to remember—are the President's

staff for the national security business. These are the guys, either personally, or by receiving detailed direction from the National Security Advisor, who are the people closest to the President on a day-to-day basis. Although it's true that the Secretary of State and the Secretary of Defense, personally, will see the President on a regular basis, on a substantive basis, traditionally the National Security Council staff is the staff that tells the interagency community, "This is what the President thinks on such and such an issue." That gets into the style of the President, and the question you were talking about before.

Where you have a President who comes into office with an extensive foreign policy agenda, you generally are going to find that you have a very active National Security Council staff who are just full of ideas, running all over town imposing these ideas on the interagency process. Where you have a President who has a relatively small number of ideas and is relatively indifferent to other dimensions of foreign policy, then you're going to have a relatively less active staff in some areas, but more in others. This particular President has chosen to focus extensively on the issue of military preparedness and the defense budget on the one hand, and on a policy on dealing with the Soviets from a position of strength, and looking for opportunities to undertake operations where we can do to them what they've been doing to us; the regional dimension which leads to his interest in things such as the Nicaragua-Contra business, as well as Afghanistan and Angola. These are areas where the President has very strong personal views, and where his views to some degree, are not fully consistent with the mainline view of the traditional bureaucratic foreign policy establishment. In those areas the NSC staff, in effect, becomes the President's conscience and becomes the "looker over the shoulders" of the bureaucracy to keep the President's views before the bureaucracy; a role which can produce a high degree of friction and trauma from time to time, and can also be highly dysfunctional if it's done in a rough and crude manner as opposed to a more personal and smooth one.

You're all familiar with how groups of people interact, whether it be this seminar or a more bureaucratic setting, and there's no magic to that. Some people do it better than others. One of the jobs as National Security Advisor is to try to hire a staff that, among other capabilities, has the ability to go and impose the will of the President on a recalcitrant bureaucracy in a way that makes them like it, as opposed to a way that makes them leak to the newspapers and gets anti-administration stories in the press all the time — stories about how Defense and State are at each other's throats about this, that, or the other thing.

[OETTINGER] How frequently do you get the reaction, "We'll send out a memo which will keep the politicians quiet by saying here's what we're going to do, and we're going to take six years to do it, because after all they've got four years at the most," that kind of stuff?

[MCDANIEL] Again, as I say, the NSC staff guy is going to be involved in the group that is sending out the memo. The memo is going to get written in the NSC group. Then he has to be the guy who says, we can't take six years, how about three weeks? What this means is with this going on all the time, you're constantly having issues that I would call the "Please call **Shultz** and make him do so-and-so" kind of issue. Let's talk a little bit about how the staff works on a day-to-day basis.

Shultz—George Shultz, Secretary of State under President Reagan, 1982-88

Every morning at 7:30 the National Security Advisor sits down with the senior members of the NSC staff. The first order of business is "What was in the newspapers today, and how are we going to respond to that?" That's because the NSC staff has responsibility for providing guidance to the White House press spokesman, who in turn provides guidance to the spokesmen of the other Executive Branch agencies. Secondly, "What's on your mind today?" Typically, it will be a rare meeting where one or two staffers won't say, "Well, we're having this problem on such and such and would you please call George and get him engaged." One of the functions of the National Security Advisor is to be on the phone to Shultz and **Weinberger**, and to a lesser degree, **Casey**, fairly continuously getting them engaged in giving top-down direction to what's going on in this interagency process when it's perceived to be off track. Usually there is no real policy difference at the top. I mean, by definition, the President has picked these guys. They are his political confidantes. They are, by definition, going to do what the President wants. If the National Security Advisor calls up and says the President wants so and so, they're not going to argue with whether or not they think that's a good idea, unless there's a good reason. There is that constant "going on over the telephone process."

Weinberger—Caspar Weinberger, Secretary of Defense, 1981-88

Casey—William J. Casey, Director of Central Intelligence, 1981-87

Sometimes it will work the other way. Shultz will call the National Security Advisor and say, "My guys just told me what your guys said, and that isn't right, is it?" That's just an ongoing management process. That's what they

spend their time doing. What I just said probably accounts for 50 percent of the National Security Advisor's time day in and day out.

Let's talk a little bit about the crisis management structure. From the beginning there was an NSC-chaired crisis management group called the Crisis Preplanning Group (CPPG), the title stemming from the fact that if you were doing it right, you would anticipate a crisis and come up with a strategy to avoid it rather than put out the fire after it's already started. That group was chaired by the Deputy to the National Security Advisor and had as members the Assistant to the Chairman of the Joint Chiefs of Staff, a three star; the Under Secretary of Defense for Policy, Fred Ikle—or he would frequently send the Assistant Secretary for International Security Affairs, Rich Armitage; and the Under Secretary for Political Affairs at the State Department, Mike Armacost; and the Deputy Director of Central Intelligence for Intelligence who's called, in the trade, the DDI. He's the principal intelligence officer on the analytic side within the CIA. That core group constituted the CPPG. That group did not meet on a regular basis; they met on an ad hoc basis when they had a reason to meet.

There were two ways they might meet. Somebody might call up, as happened in the **case of the Philippines**, and say, "Gee, we need to have a meeting, because the Philippines are going to hell in a handbasket, and we need to have a meeting and talk about what we're going to do about it." That did, in fact, happen. There was an ongoing series of meetings which resulted in some special analyses by CIA, and studies, and consciousness raising within the bureaucracy that resulted in several special emissaries being sent. The rest is history, as you well know, with respect to **Marcos** stepping down and so forth.

the case of the Philippines—contested election of 1986

Marcos—Ferdinand Marcos, former President of the Philippines, resigned under pressure from the Reagan Administration

[STUDENT] Would you say that was an example of success, because it led to action?

[MCDANIEL] I think so. There's always luck in all of these things. One doesn't want to get too glib about it. The biggest success is when the crisis doesn't happen at all. There was a much more time compressed "mini

success," following the Marcos thing, with **Duvalier** in Haiti. We can't really claim any credit for his having decided to step down, but upon hearing the rumor that maybe he was interested in stepping down, the government moved rather quickly to encourage him along those lines and provided an airplane. The hardest part was finding some country, other than the United States, to take him. We wound up kind of arm-twisting the French in getting him in there, and having them have their noses substantially out of joint. But I notice he's still there.

Duvalier—Jean-Claude Duvalier, President of Haiti, 1971-86

Here you have vested in each one of those standing members as well as the NSC staff person (which was myself for a while) a responsibility to be looking at the process of gathering information and trying to predict crises. The first year I spent was looking at that issue and saying, "How can you do that better? How can you do it more systematically? Do computers help and stuff like that?" The government, actually, is quite good at compiling laundry lists of places where there's a good possibility of having a crisis. One of the more interesting ones is a CIA publication which is the most analytic document that I'm aware of. The problem with it is, it's more than you can deal with. It produces a list of about 20 places where there's a good probability that there might be a crisis, but you can't deal with 20. You're right back to, which ones are you going to try to deal with? Are you just going to hope for the best and just let the normal process work?

I also want to digress and say that everybody in the national security business is in the crisis avoidance business. That is what our ambassadors think they're trying to do. That is what the desk officer in the State Department thinks he's trying to do. That's what the regional military commands and all the port visits and regional military conferences and dialogues we have all over the world are about: all of these individuals are trying to carry out foreign policy objectives, the chief objectives as best they understand them, and to steer around, avoid, crisis. Of course, that also can be translated into a policy of support of the status quo, and a policy of preserving things as they are now.

One of my observations of the professional diplomat is that his experience and training trained him to be a guy who tends to feel that the perfect state of grace is the problem unmolested. Don't screw with it. It may not be perfect, but it's quiet. This is an area where academics and political observers of US foreign policy criticize our policy most, for seeming to align ourselves with totalitarian leaders around the world. The facts are simple to me.

There are more totalitarian leaders than any other kind. If you draw up your own list using normal criteria of democracies and non-democracies, there will be a lot more non-democracies. If you add to that the mind set of diplomats, which is to leave well enough alone, we wind up supporting totalitarian governments more often than we are out actively trying to overthrow them. There are very few that we are out actively trying to overthrow. It's just the nature of the diplomatic process.

I must say that I spent a year looking at how you improve the process of sifting information to predict crisis. One of the more interesting things I did was I funded a panel of artificial intelligence gurus and tried to see whether there was anything to that. I concluded that they need to see a problem as vastly more structured than the very ad hoc and amorphous and messy business of trying to predict instability in the world.

[OETTINGER] They can hardly tell a real missile from chaff.

[McDANIEL] I'm not sanguine that a whole lot more can be done. I personally believe that the NSC should continue to have somebody on its staff who thinks about this issue and tries to plug into people like yourself and others around with different perspectives who are trying to look at the process of crisis management as an academic discipline. It remains an area where I think there will be no breakthroughs in our ability to harness quantitative analysis to predict the outbreak of a crisis with greater precision.

[OETTINGER] You mentioned, over lunch, the ***Achille Lauro*** incident as an example.

Achille Lauro—passenger ship hijacked by Palestinian terrorists in 1985

[McDANIEL] I might come to that in the context of how we organize operationally. I think that fits better there.

[McLAUGHLIN] Let's talk about the CIA forecast, in the context that Sir John Hackett had in *The Third World War*, which starts with the idea that more than half the world's national leaders don't know whether they'll wake up in power tomorrow, or wake up period. If you start with that ...

[McDANIEL] I think that's considerably high. The right number is probably 15 percent or something, but it's a significant number. The world isn't that unstable, I would argue.

[MCLAUGHLIN] This is the difference perhaps, between the 20 perhaps the CIA can predict following crisis indicators: the number of leaders' children being sent overseas to go to school, or whatever one looks for. On the other hand, there are 80 out there who are random shots. If the guy dies accidentally overnight, you may have a crisis on your hands that you never expected. None of the other crisis indicators are necessarily going up, but with the guy out of the way, he may have 17 contentious successors, or would-be successors. It's just a very unstable world out there in that sense.

[MCDANIEL] The other kind of crisis, or the crisis you don't anticipate, is that you wake up in the morning, and you've got one. What are you going to do about it? That's the crisis management mechanism in its most operational context then. You're scrambling in the first instance to find out exactly what happened. This is what Beal was trying to aim at, and to improve on how the system works when you're in that state of grace. You wake up in the morning and you've got a crisis on your hands which you hadn't anticipated and there's no high level planning that's been going on. You've got to get it going and get it done.

How would we work that? We'd convene the group, normally in a room. Only on a couple of occasions did the thing go down so fast that it had to be done over the telephone. If we had any time at all, I would call the CIA guy and ask him to do a quick analysis, and if he could, get it distributed to the other members before he came to the table. Rarely was that done. If we were lucky he'd bring it with enough copies or we'd make copies on the Xerox machine and pass them around. The first item of business was for the CIA guy to provide the current intelligence on what was going on, and then to ask other members of the group, "Who has any additional information on this?" and to make sure that all the players had a common base of information. That's a critical first step, and I feel that that worked quite effectively. I was very satisfied that there was a minimum of withholding information or game playing. There was an honest effort made to share information, and that usually had been shared already, but sometimes because of the pressure of time, people were exchanging tidbits right over the table that they hadn't had a chance to talk to on the phone. In general, it kind of validated the fact that the information sharing mechanism of the national security community worked pretty well. That's the first step.

With that as background then the problem became harder. Then —this was the most slippery part of it— I would always try to have the agenda structured so that we would spend some amount of time talking about "What would we like to see happen?" "What are our objectives?" — before we go down to the action stage. It is an interesting dynamic in the crisis business

how people who are very intelligent, and know a lot, and have been around a long time, will come into a room and after just a few seconds will want to start talking about doing things without having spent any time at all talking about what we want to accomplish before we talk about sending emissaries here, or pre-positioning carriers there, or whatever. I think it's kind of an American trait. We really are an action-oriented people. That's our nature.

This sounds terribly trivial, and in a way it is, but one of the useful functions of having a process guy in this thing who is in charge of structuring the agenda, is that you would at least have on the blackboard, on the screen, the words, "Let's talk about what our objectives are." One of the cliches in the crisis business is "in crisis there is opportunity." It actually comes from an old Chinese proverb. It's very important, when you're kind of in gloom and doom about what a terrible thing this situation is, that you pause and think, are there some opportunities here? Can we take advantage of the situation? Because you certainly want to do that if you can.

Some have suggested that technology might, in some fashion, help parse more systematically through this phase of a crisis management process, ideally, by being able to access and scan history rapidly. There may be something to that. I personally believe that there should be some level of effort funded, preferably sponsored by the NSC for the foreseeable future, to attempt to look at how technology accesses history, and pulls it together and looks for common threads and common elements.

[OLTINGER] I'm not sure that it's initially a technology problem so much as a history problem: namely, to get the history looked at in the first place. The delivery mode may be second. There's very little reliable institutional memory in the crisis management business.

[MCDANIEL] I think we're saying the same thing. I don't want to imply that this is computers and artificial intelligence. I am persuaded by the fact that if doing a job of historical research requires getting in an airplane and flying to the Eisenhower Library to see relevant papers, and you're in the middle of a crisis, you will never look at history. You won't do it at all. If you have some way of getting access to the Eisenhower Library in an hour, and you could even query that library with a subject matter-oriented search routine that says

[OLTINGER] It's worse than that. I recently had a totally unclassified visit to NSA. I'm also on the board of visitors of the Defense Intelligence College. I'm persuaded that there are miles and miles of things to do to get

cases developed, to get as part of the ingrained training of any intelligence officer, any action officer, etc., etc., some sense of "this incident is similar to Crisis X and different from Crisis Y." This is totally missing today. Why worry about gimmickry when you have a very short memory, institutionally?

[MCDANIEL] I don't disagree, Tony. I tend to see the two as somewhat related. The facts are that the way the system works today, history is what the people who come to the table bring to the table. It's just that simple. If they have it at hand, it's there. If they don't have it at hand, there's no external process to add it.

[STUDENT] **May and Neustadt** make the point that quite often the history they bring to the table is incorrect, distorted, mythological, and all the rest of it.

May and Neustadt—*Richard E. Neustadt and Ernest R. May, Thinking in Time: The Uses of History for Decision Making (1986)*

[MCLAUGHLIN] It's all those people in 1964 saying, "Lyndon Johnson doesn't want to preside over another Munich, or whatever"; and the people now—running around and saying, "Well, we don't want another Vietnam in Central America." It's very hard historically to see Nicaragua as not being exactly the opposite of Vietnam.

[MCDANIEL] But at least you have a check on the fact that you've got more than one person in the room. You have the institutions represented, and you have different human beings represented who are going at least to bring six sets of history to the table instead of just one.

[STUDENT] Many years ago there was a thing down in the Navy about trying to do a more analytical job of crisis management, make more use of technical tools. Part of the problem is that when you're having a real crisis under way, nobody involved has any time to help anybody who's studying what is going on and seeing what's needed the most. I don't know if there's a good technologist anywhere on the staff there, but sitting in on a meeting and observing the real event is the starting point of what can be done next.

[MCDANIEL] That was Beal's concept, and that was what the role of the Crisis Management Center as a support agency to the NSC staff was intended to be. You'd have some computer-friendly, junior, subject-oriented analyst who would be the person who would attempt to do the quick crash

job of historical research to supplement, but hopefully in a more objective and systematic way.

[OETTINGER] There was a slightly more modest objective. If the boss doesn't know where the hell the country is, a simple notion of just getting the map up there, so the boss can see it, helps. This applies to this President or any President.

[STUDENT] I think there are a whole bunch of little things like that that can be done, but again you've got to have somebody who knows what can be done sitting down, watching, and that's just the starting point.

[MCDANIEL] That's correct. That was the intent and is the intent of having this Crisis Management Center thing, and it's definitely in its infancy. It represents no more than kind of a token commitment.

[OETTINGER] That brings us full circle to the observation you made at the beginning. The idea is very threatening to all of the normal players, because it suggests then that there might be knowledge accessible to the decision making individual or group that would not be the knowledge brought to the table. The very statement of the problem has in it some of its dilemmas.

[MCDANIEL] It's an interesting thing to watch it as it plays in real time. If you're in a room and the locale of the crisis is kind of obscure, no one in the room cares whether some NSC staffer goes off and gets the map, or the CIA guy brings the map – the guy who by agency charter is supposed to be the map guy—it doesn't matter. If on the other hand you're having a meeting with the President or the senior advisors, the NSC principal advisors' meeting—when they meet in this situation by the way, they call themselves the National Security Planning Group [NSPG], which simply gives a signal that it's supposed to be a more closely held, more sensitive group, but the players are the ones I've mentioned as the National Security Council principals—it turns out it does matter. I would find some sensitivity to having the NSC staff put the map up on the wall, as opposed to having the Chairman of the Joint Chiefs of Staff bring the map. You simply roll with the punches and you call the Chairman in advance and say, "Please bring a map."

That's one of the things Beal wanted—and this leads to foolishness. Because he comes five minutes before the meeting starts, you barely have time to place the map on the easel. What you'd like to do is have a nice color

transparency or something so everybody in the room could see clearly and well, and to do that, you have to have the slides transmitted electronically in advance. When you have a bureaucracy that's unwilling to turn loose any piece of information until Weinberger's seen it, and he won't see it until he's in the car driving over, you have a problem. We created a technology which allowed the instantaneous video formatted transfer of all kinds of data, but we never solved the bureaucratic problem of getting the bureaucracies to turn loose the data without their boss's chop on it, and their bosses wouldn't chop, because they wanted to bring it to the meeting. I think that will alter somewhat over time. It sounds so silly, but it's very real.

As a result, just to finish the point, typically the size of the situation room where they meet is about these two tables, plus half of the third one. What literally happens is the Chairman of the Joint Chiefs of Staff who has the JCS graphic shop, which is one of the faster-response graphic shops in town, will have the map, and some briefing boards, and whatnot, and he'll have them on the easel right here, because the President sits here, and generally Shultz is there, and the Vice President is there, Weinberger is sitting there, and the chairman will stand up to brief. Sometimes they set him over there, and Weinberger does the talking. The National Security Advisor, and Don Regan, and people like that are down at that end of the table, and they can't see the stuff. They literally don't see what the President is seeing.

Surely, technology would allow us at least to have a conference where everybody could see. It's interesting to watch the dynamic. You have to see it to believe it. When Weinberger is briefing the President on a military option, he's really acting as if it's him and the President. These other guys don't really have a real role. That's really what he's saying when he does that, even though it's clear that the intent of the law, and Rod McDaniel's view, is that he's there as a councilor to the President, a co-equal with all these other fellows. The same is true with Shultz in some piece of diplomatic arcaneness. There's no question that the President, personally, must from time to time reinforce the notion of the kind of role he wants his principal subordinates to play, or they're going to tend to act out bureaucratic roles.

Once we have had this preliminary meeting, the next step, which is the crucial step, is generally that the State Department is told to get a working group together and to take 24 hours and develop an options paper. That is the single most important step in the crisis respo[illegible] I say 24 hours, but whatever, if you have 24 hours, you take 24 hours. If you have a little more, you take a little more. If you want it bad, you get it bad. That joke,

The State and Defense and CIA representatives at the **CPPG** are responsible for designating someone from their respective staffs to go to the State Department, let's say, to be in the working group, and out of that will come a paper. Again, if possible, that paper will he reproduced and distrihuted in advance.

CPPG—Crisis Preplanning Group

I guess it's time now to talk about the tension between leak-consciousness and process. That's worth talking about now in the real world.

Almost everything that I've suggested and alluded to, I and others, about how do you mayhe make this hetter, tends to mean more people get involved. Paranoia over security says fewer people involved. One of my colleagues used to joke that if more than four people know, it's gone. Pick your number, but there's no question that there's a logarithmic relationship between the number of people who know and the prohahility of a leak. So you do have a real tension between things you do to promote orderly process in crisis, and things you do to keep secrets in crisis. Laid on top of that legitimate tension is a very pernicious hureaucratic tension. Everyhody who's a real practitioner, and I'm sure you're all not naive in this regard, realizes that there are two uses to which security classification is put: the legitimate desire to protect secrets, and protection of hureaucratic turf. As a practitioner of the real world, it's about 90 hureaucratic turf; 10 legitimate protection of secrets as far as I'm concerned.

One of the functions of the NSC staff is to try to pry this stuff with a crowhar out of the other agencies and spread it around, so that everybody gets a chance to see it. You are fighting against the grain all the time when you do that. It's just a fact of life. It's not going to change. That's just the way the world is.

I left the job on the NSC feeling very uncertain in my own mind about this tension over security. I mean it is a terrihle prohlem to have a meeting where there are fewer people in a room than this and read about th meeting in *The Washington Post* tomorrow. It is precluding options. It's either precluding options domestica y because you're going to have Congress posturing, and taking positions, and making life difficult, or you signal the enemy what your intentions are and make it easier for him to deal with it.

You can't figure out "who dunnit." I assure you, once you've been burned a few times you just are going to want to tell fewer people, and you're going

to join the group of people who say, "I don't want more people." I don't want this honest, objective, graduate student in history that I hired and put on the CMC staff with the thought in mind that he would be the computer-friendly historian who did dissertation work in Soviet-US crisis decision making. My lofty ideal was, here is a real perfect guy who would help pull the history together quickly, but he's a stranger. You can overcome that to some degree in non-crisis periods. You get the group together and you explain what you want to do and they all nod their heads and agree that having this guy in the room is okay. You cannot do this when it hits the fan. It's too late, if you haven't done it in advance.

CMC—Crisis Management Center

The next day the option paper comes back. Hopefully, we've put it out in advance, so that the group has looked at it. There is a very good facsimile system around town—one of the most used pieces of technical equipment we have. It allows you to send document copies on a secure basis through the mail, or through the secure communications rooms, but again code clerks get involved, so if you really are concerned about it you won't use that system. You'll pass it out at the table, denying people the opportunity to read it in advance. Then you wind up spending the first half hour of the meeting with everybody else reading the paper, because no one will have seen it before, which is a waste of time.

Then you have the most important meeting that you're ever going to have, and you talk about that paper. What are the views, the pros and cons, and you try to have the best possible, no-holds-barred discussion of the options. Then you go back and turn the crank on it one more time and you're ready to go up to the NSC, and have an NSPG meeting. What makes the NSPG function is that the CPPG members brief their bosses. They come to the NSPG aware of all the discussion and all the pros and cons and give and take that's taken place in the CPPG, as well as their views of what the options are. They come to the table with the President at the head, and they look at the options and they make their points to the President with respect to the options, whatever they are, and more often than not, there's consensus frankly, but not always.

Normally, this President does not decide things at the table. If there's consensus, it doesn't get said, and the National Security Advisor is responsible for getting things implemented. If there is a disagreement, then the National Security Advisor plays one of the most important roles in this process. He goes in to see the President with a paper, generally, that provides the

recommended decision. That paper will normally not have been seen by anybody before it's seen by the President. If the Advisor is doing his job right, it will be a fair distillation, and he will probably have talked on the telephone to Shultz and Weinberger before he puts it in final form. He will sit down with the President, and he will say, "We had our meeting yesterday and these were the real issues. Shultz thinks this and Weinberger thinks this, and I think this and I think this is what you ought to do." The President will say, "Okay, I'll do it." He'll initial it "RR," and the National Security Advisor goes back to his office, picks up the phone and calls Shultz and Weinberger and says, "The President decided this, do it!" And they do it. Why? Because they believe him. They have to believe him. If they don't believe him, they pick up the phone and call the President themselves, and they only do that once on the average. That's a non-problem. The person who's going to be the National Security Advisor will be trusted and accepted by the Cabinet principals as a guy who faithfully transmits what the President decided.

Then the NSC staff role is essentially a monitoring role at that point, because the operational direction will flow down to either the State or the Defense Department. That then leads me to the last point I wanted to make. I guess I'll close on this. I've a couple of vignettes to show that this process of integrated, political-military thinking still has a lot of rough edges around it when we try to impose political-military thinking either on the planning dimension or on the operational dimension, on what is essentially a federated structure which is what I said it was.

One of the vignettes that we were talking about before lunch was *Achille Lauro*. I personally audited most aspects of *Achille Lauro*, those that I wasn't personally familiar with and involved with, so I'm reasonably comfortable with my possession of the facts on that one. Recall that the cruise ship which had been taken over by the terrorists had sailed back into Egypt. The terrorists had decided to surrender to the Egyptian authorities. The hostages had been released into the custody of the ambassador and the terrorists were taken into the custody of the Egyptian government.

We gained intelligence from a third country, that will remain nameless, as well as from some **SIGINT**, that the Egyptian government was going to return them to Libya. **Poindexter** really had the idea that it might be possible to intercept the plane. He called Vice Admiral Arthur Moreau, who was the Assistant to the Chairman of the Joint Chiefs of Staff, the regular JCS counterpart on the CPPG. This is the network that I've talked

SIGINT—Signal Intelligence: all communications intelligence, electronics intelligence, and telemetry intelligence

about at work. He calls him on a secure phone. He says, "Have you seen this intelligence report? What do you think?" He says, "I don't know. It's an interesting idea. Let me check." He gets hold of the J3 who calls to Europe, the unified command in Europe, who calls the Sixth Fleet, and by sheer chance there was a battle group that was en route to a port visit in Yugoslavia. I believe it was, and just happened to be practically under a flight path—if you got a map out and drew a line between Egypt and Libya, it would go practically over where this boundary was.

Poindexter—Rear Admiral John Poindexter at the time of this incident was head of the CPPG; later, 1985-86, he served as National Security Advisor.

J3—Deputy Chief for Operations

It also transpired that the Commander of the Joint Special Operations Command (JSOC), was in an airplane equipped with a tactical satellite communication device which now, even to this day, in spite of $10 billion a year for C^3, most of our aircraft do not have, but he has it because the JSOC is given special priorities in these matters because it is normally deployed under the direct control of the Joint Chiefs of Staff. He was in an airplane. They had been deployed to the Mediterranean with the thought in mind of preparing to go take down the *Achille Lauro* using the SEALs, which is one of the scenarios the SEALs have practiced for in the Joint Special Operations milieu. That obviously wasn't really needed because the ship had gone in; the hostages were off. Once again the capability had arrived too late to be of any value.

SEALs—sea-air-land team, trained and equipped for unconventional and paramilitary operations

Anyway, they were in an airplane getting ready to go back to the United States and were airborne at the time. The Chairman got hold of the General on the phone and said, "Turn around and land at Sigonella." That then created a command structure where you had a regular JCS chain of command, communications, secure phones, talking through the unified CINC in Europe to the Sixth Fleet battle group, and you had a guy on the ground at Sigonella, which was where they were going to try to get the plane to land. They were going to force the terrorists down at Sigonella, put them in US aircraft and take off. And bring them to the United States and try them under US law. You'll recall that one of the hostages was murdered and the Attorney General was of the opinion that he had the basis for at least indicting them under US criminal law. The basis for claiming jurisdiction was quite clear-cut in this case. That was the plan. The JCS guy came back and told Poindexter, "Yes, it looks like we can do it. Let's give it a try."

Poindexter then convened a conference call, a secure-voice conference call, getting the NSPG principals together: Shultz, Weinberger, Casey, and the Vice President. The President was traveling on a campaign trip as I recall. He was brought in on the conversation. I think he was in Air Force One at the time flying to Chicago. He agreed, but he said he wanted to approve the final operation if it turned out to be feasible. Everybody recognized that the thing might not work. They might not be able to find it, or intercept it, or what not. Subsequently, everything fell into place. Almost miraculously, through special intelligence sources, they were able to gain information that led to knowing what the tail number was of the aircraft and the exact time it was going to take off, and they were going to fly a standard route to Libya. It was quite possible to predict an intercept point.

As you know, the carrier aviators, and the Air Force people routinely practice those kinds of intercepts. If you call up some tactical commander and say there's going to be an airplane with such and such identification, taking off at such and such a time, and flying such and such a route it's easy for him to complete the necessary details and intercept it. It is quite straightforward. They did intercept it and Poindexter called McFarlane who was traveling with the President, and he went in and told the President this. One of the specific things the President wanted to get straight was rules of engagement; that there'd be no shooting. We weren't going to shoot down an Egyptian airplane. If they chose not to cooperate that was going to be the end of it. Of course, we didn't tell the Egyptians that. He approved, "Go ahead."

They did intercept the aircraft and through a combination of hand signals and transmission over the common aircraft-to-aircraft frequency which is used for emergencies they gave the guy to understand that he should follow them and proceeded to divert him to Sigonella. At that point the thing began to unravel a little bit because Sigonella is an Italian-run, US-tenanted base. The Italian authorities were alerted to the fact that something unusual was happening. The Italian commander denied authority. Actually, the Egyptian airplane came up on the circuit and requested to land at Sigonella. They stewed around for about a half an hour with this airplane orbiting. This is kind of unusual, but we had real-time knowledge of this from the battle group guys on the one hand, talking fighter aircraft to carrier; carrier over a secure radio-phone circuit into Stuttgart, and then Stuttgart over secured-landline to the J3 in the Pentagon, who then goes up to see the Chairman who calls up Poindexter and tells him this.

Poindexter calls Armacost at State to get the US Ambassador to get on the phone to the Foreign Minister of Italy to try to explain the situation. Of

course, the Ambassador didn't know anything about this up until this time, so somebody had to explain to our Ambassador what it was we were trying to do. Then he had to find the Foreign Minister and get him on the phone. Meanwhile, **Crowe**, who had served a tour in Naples and was a friend of Spadolini, who's the Italian Defense Minister, checks with Poindexter, and then calls Spadolini up directly. He just places a commercial phone call. Spadolini explains what we're doing to him, and meanwhile, while all this is going on, the aircraft declares a fuel emergency—I think it really was—and lands anyway.

Crowe—Admiral William J. Crowe, Jr., Chairman of the Joint Chiefs of Staff

The next event in the saga, then, is the struggle for physical control of the terrorists. You'll recall the plan was to use US Special Forces to move these fellows into the US airplane and take off. But the Italian force is covering it, which in this case is the Carahiniere, the paramilitary police organization of the Italians who are normally stationed there to provide base security. And these two groups of soldiers have some tension between each other. I've never completely gotten a clear picture of exactly how that was, or why that couldn't have been greased over a little bit more, because presumably they work with each other all the time. But there was no doubt tension there, and in any event, the Italian Carahiniere or the base commander had gotten instructions from the bosses in Rome not to release. This, then, came back through the radio-phone to the Chairman in his office, who notified Poindexter, who notified Armacost, who reenergized the Ambassador again, and then the President was brought in to talk to the Prime Minister of Italy. Somebody on the NSC staff, probably **Ollie North**, had to crash around and put together a few talking points for the President. Then you had to get an interpreter lined up, and get the Prime Minister of Italy on the phone, and all that takes about an hour or so. All this is going on while there's a standoff on the ground at Sigonella. Eventually the Italians decide not to release, but say, "We'll take care of it ourselves." They fly the group to Rome. They put Carahiniere on this Egyptian airplane, and then they actually fly the Egyptian airplane to Rome, and it lands there and the terrorists are taken into custody by the Italian government, as we all know.

Ollie North—Marine Lt. Col. Oliver North, key figure in Iran-Contra affair

Then, Meese was energized and he got on the phone to his counterpart, the Interior Minister in Italy. This was now the next day, and he attempted to get them to hold them long enough to go through normal proceedings for extradition. The Italians ultimately declined to do that. It became a domestic

political issue in Italy. That's true in most countries. Even our staunchest allies have great difficulty being seen to be toadies of Uncle Sam in public. Eventually, the Italians made their own decision as we all know.

That's how it happened. Are there lessons learned from something like that? It was viewed as a success even though the complete operation, meant to spirit them into a US airplane and bring them back and try them in the United States, was not accomplished. It was still viewed as a success. By anybody's estimation, the command and control was a complete and utter lash-up, and complete serendipity that you had a US general on the ground in Sigonella who allowed us to know these problems with the Italians. We'd never have known that because the Sixth Fleet communications obviously didn't extend on the ground to Sigonella. As far as I was able to determine, EUCOM (European Command) had never cut the base commander into the act. That, in my opinion, probably accounts for why there was this tension between the Carabiniere, with whom the US base commander had to have good relations, and these Special Forces guys, who are foreign troops, US troops, not stationed there. That's why there was a problem with the Italians.

How would you have worked that better? I don't know. It has led me to formulate an interesting thesis which I throw out on the table for some of you who might want to pick it up and run with it. Notice there's an interesting dichotomy when you stop and think about it, about how the US government is organized operationally, as between Defense and State. The Defense Department had organized its operational command through a CINC, in this case US EUCOM in Germany, and then through his subordinate commanders, in this case, the Sixth Fleet commander and the battle group.

CINCEUR has under it people who are stationed in the Mediterranean area, on land in Italy, attachés in Egypt. They can pick up the phone and have communication and the capability to coordinate people stationed throughout that region. But the State Department is organized on a country basis with each ambassador reporting nominally to the President/Secretary of State, but in reality to the country desk officer in the Department of State. Their regional coordination is accomplished in the State Department in Washington under the cognizance of an Assistant Secretary of State for the region.

To coordinate EUCOM and Italy diplomatically requires that you come back and work the problem in Washington. We don't have a way to delegate —to say, "Okay, Ambassador and EUCOM, work it out, and let us know if you

need help. The two of you talk to each other." We just don't do business that way. So, you had Armacost on the phone in the Department of State talking to the ambassador while at the same time you had Crowe on the phone at the Pentagon talking to the General in Italy, and EUCOM, to a large degree, playing no role in this particular case except trying to figure out what was going on and be helpful where they could.

In my mind, an interesting alternative would be to consider regionalizing the Department of State and actually have the Assistant Secretary for Europe collocated with CINCEUCOM, and to have those two authorities able, within their respective spheres of influence, to coordinate in the region and then talk to each other directly because here you really did have a real-time problem. You were talking about events like airplanes orbiting at an air base waiting to land. Next to a missile attack being launched, that's about as real-time as you can get. To try to coordinate that out of Washington is just crazy. The military clearly had recognized that you've got to move that kind of coordination problem much closer to the scene of the action or it won't work. Now historically you can do that by having someone, the general on horseback, looking at the battle from the highest hill. It's true that today with communications you may sometimes find that the guy with communications is actually sitting in Washington rather than sitting in Germany, but you've got to have somebody with communications and all the relevant elements who has the authority to effect coordination and resolve these kinds of issues.

29. **FRED R. DEMECH, JR.**, "Making Intelligence Better" (1987, pp. 125–46)

Career cryptologist; former Commanding Officer, US Naval Security Group Activity in Edzell, Scotland

Rich Beal who was here, I guess, three years ago, before he died (God rest his soul), was a tremendous individual. He got to the White House in 1981, and he was shocked along with a lot of other people. There was very little automation. There was little to support the President. The White House Situation Room was like a "horse and buggy." They didn't have access to an awful lot of information that was available to just an everyday person on the street—TV, communications, radio. He went about changing that, based on his experience.

It's interesting to see what happened to him. He built this Center—they called it the Crisis Management Center. It was a crisis management system

where he brought together inputs from all different sources in one place. No one paid any attention to him when he was building this thing, and some of the people I was associated with, Dr. Bill Baker from Bell Labs. Dr. Johnny Foster from TRW, Tony Oettinger, all helped in giving him advice on how to build the center. When people saw what was coming together, that in this one secure room you had information, compressed and displayed in a way everyone could understand, they took notice. Not only did they take notice, they wanted to control it. There was a big power struggle as to who was going to control it. When Beal died and **after the Iran thing**, they almost closed it down because a lot of information flowed through that place, and that was where a lot of information was on record.

after the Iran thing—Iran-Contra affair

A number of comments on that. People from the intelligence community were very hesitant to play because the information was going straight to the center of government. Not to the President, but to the people who supported the President who could gather that information, bypassing the intelligence community, so to speak. The intelligence community had that information, but it was also available at the center and then they digested it and put it together, synthesizing it themselves, and presented it in a form that the advisors and the President could use. Most of it was put together in a video format, pictures. You know the *USA Today* weather page? You look at it, you don't have to read a thing and you can understand what the weather is just by colors. He did that, and it had tremendous implications, and therein was the problem.

One, people saw what was available. They didn't have it. It was bypassing the hierarchy of the intelligence community, and then they could synthesize it and present it in a form that maybe only the President or his assistants who were right there had.

[STUDENT] Who was doing the synthesizing there? The whole point of having an intelligence community is to have a staff, and have a set of organizations who can get together, whether it be on an informal basis as at the analyst level, or on a formal basis when you're putting together an **NIE**, and present a view that the whole community will agree upon. If you have it all bypassing and going to a few folks who work in the Executive Office Building across the street, they have their own little way of pushing the buttons and putting up

NIE—National Intelligence Estimate

their own little product, who's to say that that really isn't a reflection of their own mind sets, and what they think is important?

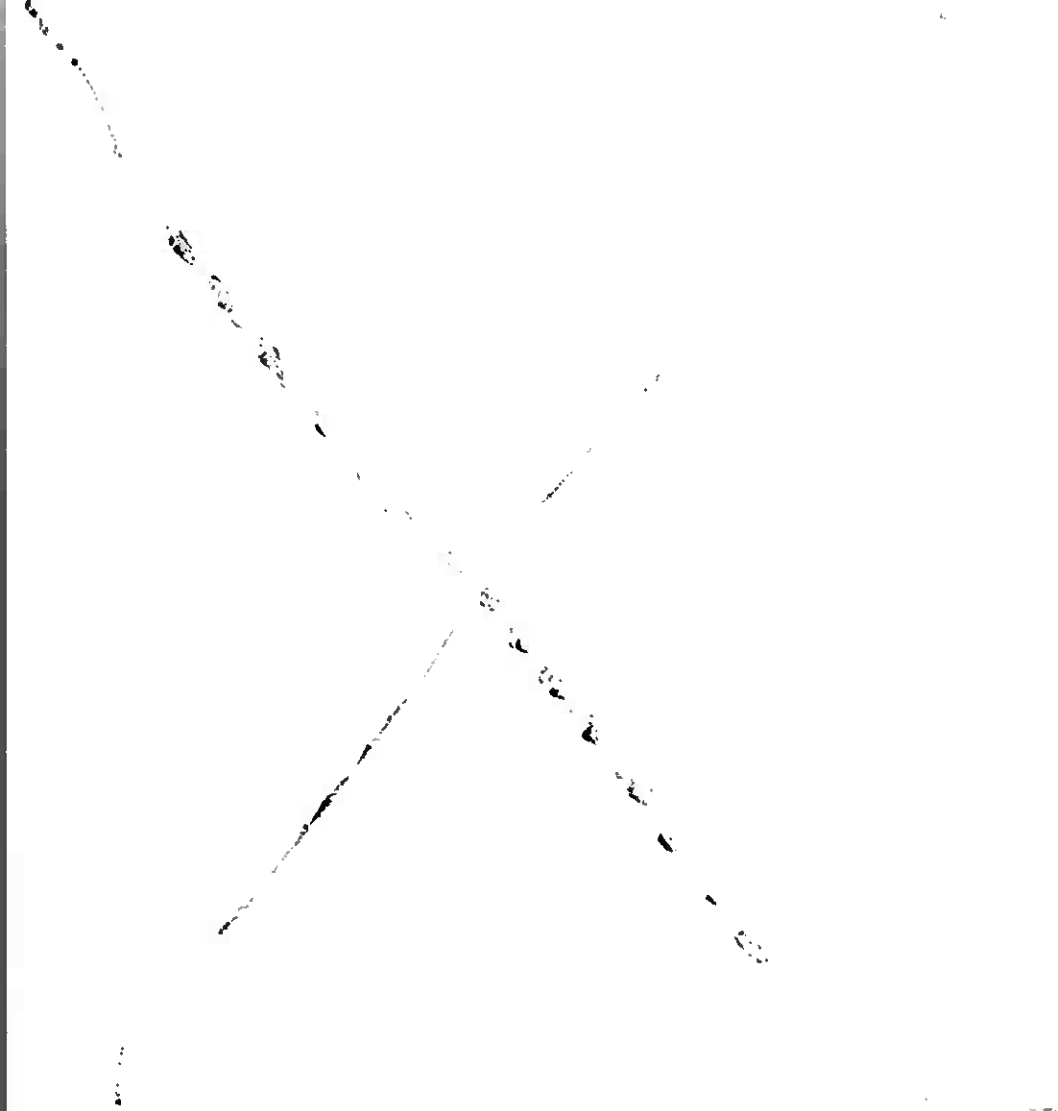
[DEMECH] That's always a problem you can run into. The synthesizing was done in various steps. I'm not saying that the intelligence community was bypassed completely. A lot of the information that was coming into this Center was coming through the intelligence community. They may have gotten the information at the same time. There were people—experts—put into the White House from the intelligence community to synthesize that information and put it together. Biases? They were trying to prevent that by having people who were not beholden to any one community, and were working just for the President. Now, were they putting information together just because the President wanted to hear that? That's always a problem that you run into, and that's what's evidenced in the Tower Commission Report.

... Each set of circumstances is different, and each President, or administration, is going to set its own standards, or its own policy. The people like Rich Beal felt that there was a lot of information available that was not being utilized because, (1) they couldn't get it quickly, and (2) there wasn't any forum where it could be used really quickly. You're talking about a lot of data. You're talking about different circumstances. You're talking about a number of crises, and they felt this was the way to go. The resistance from the intelligence community is obvious, as you said, and that's why they at first resisted it. That's why, to help offset that, they assigned their own people there. Were they coming up with different conclusions than the intelligence community? I would say very little, because the information was the same information. They were looking at it. It was just a time element more than anything else.

[STUDENT] What is the current status of Beal's center?

[DEMECH] The center is still open, but under tight control, until they see what happens as a result of the investigations that are going on. That's where all the information was available that they got so far on what took place. Memos were written and they were stored in a database. The Tower Commission had to have a certain individual who could break the code to get into it to find out what it held, but it was there.

... One of the first lessons I learned was that when the President of the United States signs something, and you think that's what's directed and it's going to happen, it doesn't happen all the time, because you need the people down the line who are going to enforce it. You need individuals or organizations that are going to make sure that that does happen. (129–30, 133, 142)



2

Communications

The generally desired ideal for communications is "transparency." If we want to communicate an idea to another person, we want to be able to "just say it," giving no thought to the specific words we'll use, to the compatibility of our vocabularies, to nuances of accent, and so on. In other words, we don't want to be self-conscious about how we're communicating; we want to be able to focus our attention on the message, not the channel of communication. We want to communicate easily.

Sometimes, however, communicating "easily" may lead to misunderstandings. Because words carry connotative signals—subjectively determined and sometimes emotionally charged—in addition to denotative meanings, the person to whom we're talking may receive a message very different from the one we intended to send. We may discover ease doesn't guarantee successful communication.

In the context of C³I, the term "communications" usually refers to equipment—radios, telephones or other devices. Such equipment converts voices and other data-carrying media into electronic signals which can be transmitted over short or long distances. People who use such equipment don't want to have to think about how to get it started, whether or not it will work, how to link it with the equipment in the hands of those with whom they wish to communicate. In other words, they want it to be transparent, easy to use. Unfortunately, like speakers attempting to communicate with listeners standing next to them, the users of communications equipment may discover they must make tradeoffs between ease and success.

Indeed, a willingness to make intelligent tradeoffs becomes increasingly important as the communications environment becomes less stable. Under normal circumstances, we may demand that our telephones, besides being easy to use, be fully dependable and flexible. We want them to be there when we need them. We want them to be capable of performing myriad tasks—everything from carrying our voices around the world to linking our computers to a data bank across the country.

However, when a natural disaster unsettles the communications environment, we accept intermittent service, degradation of quality, and other annoyances. We accept them because we are realistic; we understand the limitations of technology.

War highlights those limitations even more dramatically than does a natural disaster. War may subject our communications equipment to direct attack (destruction or jamming) or to indirect attack (interception or suppression of important communications nodes). As the intensity of conflict increases, so, naturally, does the stress put upon communications systems. During the invasion of Grenada, Army and Marine Corps forces had trouble communicating because of equipment and procedural differences. In a nuclear conflict, many communications systems may be rendered useless by the electromagnetic effects of a single nuclear explosion.

The tradeoffs enter the picture when we're planning communications systems. Do we want a cheap, efficient system that works well in a benign environment, but is disabled by the first rumble of an earthquake or bomb, or a more durable system that costs billions of dollars more? Do we want a very secure system—i.e., a system less susceptible to enemy interception—or a very flexible system, one that will allow airmen to talk to soldiers, soldiers to talk to sailors, and Americans to talk to Germans? Do we want an old system we know is reliable or a new system that will do more for us? Do we want a system that provides redundancy or one that will handle a greater volume? Should we, in a military context, spend money on new communications systems or on improved training in doctrine—an element which, if thoroughly ingrained in fighting forces, might reduce the need for communications in a combat situation?

Complicating the questions about tradeoffs are the differing perceptions of those involved in the decision process. The user, whether a corporate head or a field commander, will probably place reliability and ease of use at the top of the priorities list. The technician may emphasize state-of-the-art development as top priority, choosing the system with the greatest potential. The procurement specialist may be more interested in lowest price and best contract terms. The security expert—whose voice is increasingly heard in private industry as well as government and military circles—may consider protection of information the most important factor. The president of a multinational corporation or the commander of a multinational military force may give compatibility the edge. The member of Congress may think salvaging a company that produces a particular system is important to

national security. All of these perspectives—and others—are in some sense justified; most are reflected in the extracts included in this chapter.

The extracts also reflect one of the problems with oral communications—language usage. While communications equipment is really the channel through which the other elements of C³I—the command, control, and intelligence—flow back and forth, many of the seminar speakers—consistent with widespread practice—use "C³I" as a synonym for communications equipment. Such usage can be lamented as misleading, but it is probably too well-established to be worth resisting. At any rate, footnoting every "C³I" that *should* be "communications" or "communications equipment" would be distracting. I therefore leave it to the reader to determine whether such translation is necessary in specific instances.

Extracts

1. **WILLIAM ODOM**, "C³I and Telecommunications at the Policy Level" (1980, pp. 1–23)

Military Assistant to the President's Assistant for National Security Affairs

Telecommunications, to foreign policy managers and defense analysts (which all **NSC** staffers believe themselves to be), is a word that causes their eyes to glaze over.

NSC—National Security Council

... Well, I found myself looking at **SIOP**, which is our most well developed and, I would say, staggering war contingency plan. It allows the President, within two or three minutes of tactical warning, to be on the wire, talking to his nuclear commanders-in-chief, and if he decides to, he can send an emergency action message that will do anything from releasing 70 to 80 percent of our nuclear megatonnage in one orgasmic whump, or just sit there and say, "Don't do anything, and we will just take the incoming blow." Looking at the SIOP, you saw the realities. They were right there. All of a sudden we were out of the realm of academic deterrence theory and into real operations—what the real choices were. As I think a member of the faculty at this institution says, you tend to do the things you are organized to do; at least, you are constrained in choices by what you are organized to do.

SIOP—the Single (sometimes "Strategic") Integrated Operations Plan

The more I thought about the way we were organized, the more it reminded me of 1914. We were organized in one big war plan; everybody expected a very short war. There weren't any mobilization plans or any other support—you didn't need it, that was just excess baggage—and you expected to fight the war with your initial onslaught, with all the stocks in being. That is precisely the way the general staffs in Europe entered World War I. They had no economic mobilization plans. They were going to fight the war. They believed they could win it in six weeks. They could do that with the

ammunition stocks in being and whatever other stocks they needed, and they didn't expect to be bogged down. Once they had launched these operations plans, they were extremely difficult to alter or reverse. Probably most staggering is that it was difficult at the start of the war to imagine any politically chosen war aims to which one could harness these great war plans.

Well, I asked myself, what political goals could be achieved with SIOP? That's a sobering question. It's difficult to imagine what you could do besides destroy a lot of Soviet industry, et cetera. There never was much attention to destroying Soviet divisions. It should occur even to the more ordinary of us that if you destroy the industry and leave the divisions alone, they may come to the Rhine and on to the Channel.

So SIOP seemed to create more problems than it solved. I managed to convey these concerns to my boss, **Brzezinski**, and I took him on a trip through **SAC** and **NORAD**. He became very familiar with the operation and, as I said, the President practiced the procedures.

Brzezinski—Zbigniew Brzezinski, President Carter's National Security Advisor

SAC—Strategic Air Command

NORAD—North American Air Defense Command

If you take the things that are disturbing about the way we are organized, and compare that with what you see of Soviet force developments, you see a very large Soviet arsenal, rivaling and in some categories exceeding ours. You see a kind of accuracy which if used selectively, could call into question the existence and endurance of our own command and control systems, our ability to even ride out and respond to the retaliatory shot—to do what we are organized to do. These all seem to me to have been called into question by what we were seeing in the changes in intelligence assessments in the latter half of the 1970s. It was just not the same world as the 1950s and the 1960s, when we had enormous edges in almost everything—in command and control, in weapons—and we felt sure we were deterring.

It became very clear to me that if we were going to move seriously to enhance deterrence, to create a posture which may make opponents more reluctant to take us on, just doing more of what we were doing would no longer be enough. Let me give you an example of what I mean by "doing more of what we have been doing." There was a great hue and cry and an enormous public debate—many of you here participated in it—about Minuteman vulnerability, the vulnerability of our land-based missiles. You can go through a lot of calculations, and you can talk about what you have to do to make them less vulnerable. People developed MX systems, shell games, basing systems. But that's hardware. What I never really understood was

why that kind of vulnerability was so much analyzed when a much easier targeting problem was getting almost no public attention. Now, there are 1,054 missile silos, and people could work up enormous concern about an attack that would get them all in one snap! But I could pick for you a much smaller set of much more attractive targets—the President, the Secretary of Defense, the military operations staffs at the Pentagon and the command and control centers in the major unified commands—whose destruction would do much more perilous damage to our ability to conduct a war, or respond sensibly, or run our system. I don't mean to belittle the Minuteman vulnerability problem; it may be very real. I am merely speaking in comparative terms. I discussed this one day with a journalist (there is enough information in the public domain, you don't have to have a lot of classified information to conceptualize this problem) and he said, "I guarantee I could write about it, and nobody would read it if it were published, and my publisher won't publish it anyway." So that seems to be a psychological reality—it's the kind of problem that just doesn't sell.

. . . "What would it take to manage a conflict, or pursue politically chosen war aims, if deterrents fail?" . . . If you can answer . . . [this] question effectively, then I think you will be able to bargain stably, and you probably will deter. The most distinctive thing about answering the . . . question is to break away from the idea of having only one option—to fire one blast at a lot of predetermined targets—and instead be able to conduct a long campaign in which you may choose new targets, even after the war has gone on. I emphasize choosing new targets because in C³I we have almost no capability to acquire new targets after the start, beyond those already in the data base for the Strategic Integrated Operations Plan. In other words, anything that turns up after the war starts must be found, and you must locate it and determine what kind of weapon you need to hit it with. Unless you can go through that process, you have a really rigid set of choices which within minutes become inappropriate for the realities you will be facing in a campaign. So one of the most important changes we must take to achieve a posture which will deter in this sense in the 1980s and beyond is an enduring, robust C³I system.

. . . If you decide that you want to try to pick up those pieces [forces that survive a nuclear attack] and control and coordinate them, do you have a system that will allow you to do that? I think the answer is, by and large, no. If C³I is going to enhance deterrence in the 1980s and '90s, in my view it has to begin to acquire some of that endurance, and give us somewhat greater probability that we can put it back together as a credible capability, so that our opponent has to take us seriously and realize that one surgical C³I strike by his strategic forces will not be enough to put us out of control indefinitely.

. . . We tried to put an instruction out to the Defense Department, to the Chairman of the WWMCCS Council. We said, "You have this two-dimensional system. It will do the benign business, and it will do the emergency action. Let's get a third dimension, endurance. Start showing us what it is about your present programs that not only gives you these two, but begins to turn the corner and add this third dimension." That was my initial conceptual way to try to put pressure on the NCS and the Defense Department to move in that direction. How you do it practically is a nightmare engineering and analytical problem, and a nightmare bureaucratic problem as well. I don't want to address that now. I just want to bring my doctrinal comments to a close, having explained how C³I becomes very, very critical for deterrence.

WWMCCS—World-Wide Military Command and Control System

NCS—National Communication System

I'll put it this way. . . . If I could choose between great enhancement of a C³I system with a very high probability of control under very adverse conditions, stressed by pretty large strikes, I'd take that over MX. Yet, when you start talking about this, you risk being called a warmonger. The whole logic of deterrence theory is that you are better off vulnerable, and if you want to do anything to avoid vulnerability, then somehow you must be itching for a fight. I think that's an anti-intellectual, know-nothing approach to this kind of problem, but I bring it up merely to try to preempt that kind of cynicism. Given the nature of the Soviet arsenal, you can no longer stay locked in that tidy, rigorous paradigm of thought. You have to begin thinking about what kinds of things you are going to need to deter in a new environment. And one of the first things needed, I think, is ability to ensure, under the most adverse conditions, that we can stay in control.

. . . Now, if you are asking me whether our field commanders would be very able and impressive in exercising . . . autonomy, I would comment on it simply this way. I think we are very far behind in doctrinal developments to cope with the stressed kind of environment and its off-and-on-again kind of command, control and coordination. I think we have a lot of work to do there, particularly in ground forces, which are not at all adequate in that area. In that way, I think, the Soviets are far ahead of us. They have thought these things through and have taken a more down-to-earth pragmatic approach: work out a doctrine, test it under stress and field conditions, and see how it goes. I don't think we have done this nearly to the extent they have.

... Notice that I have talked by and large only about the third C, communications. What about command, what about control, what about intelligence? We have only talked about the signal officer's responsibility. And I think there are some command and control problems, and some very real control problems. The first one is the Services' reluctance to pay for C³I. I think that organizational problem, the command of budgetary program authority, is a very central "what next" we have to do something about. Another command and control question is, can we create a sufficient set of command centers and a sufficient military staff that can survive to support the President under periods of stress, perhaps even in the event that deterrents fail? You have heard me say how vulnerable the National Command Authority and the Command Centers are. Are there different ways to proliferate, harden, or make mobile our command structure so that it can survive? That's a real problem that has to be worked out. The JCS (the only thing that approximates a national military staff) has, as I see it, little or no chance of surviving in its present housing arrangement. For this really is a housing as well as a telephone communication problem.

Then there is another aspect of survival. What about our economic civil mobilization command and control structure? That seems to me to be in a state of total neglect. I am not even sure that what was left over from World War II, if it had been maintained, would be adequate—we are almost in the position of having to start from scratch there. Now, we have made one organizational change which, if it is carried through as it should be, will improve our institutional ability to cope with economic mobilization: pulling back together the Office of Emergency Preparedness into what is now called the Federal Emergency Management Agency. It is having growing pains, but at least the potential is there. (4, 5–6, 7–8, 9–10, 11, 14–15)

2. **RAYMOND TATE**, "Worldwide C³I and Telecommunications" (1980, pp. 25–47)

Former Deputy Assistant Secretary of the Navy and Deputy Director, National Security Agency

I'll run quickly through some tactical systems. There is a significant upgrade of the Navy's Fleet Command Centers, to try to deal with all the data they are starting to get, because you can't do that with grease pencil charts. You would be surprised how many commands in the world are still working the air and submarine problems with circles and a seaman first class with grease pencils. That's not exactly conducive to fast-moving operations. A lot of effort is going into these kinds of things. As for the long haul

communications picture as I see it from the Navy's standpoint: we still have **SHF** satellites and **DSCS II**. Superimposed on all this, I believe the Navy is going to be forced to stay in the **HF** region to the year 2000, maybe forever. They have tried to get out of the business, but they are hurting. The satellites still, when they work, work very well, but when they fail they work very badly. The command of worldwide forces just can't depend on such frailties in the future. So the most modern communications in the world will be overlaid on an HF domain for a long time.

SHF—Super High Frequency
DSCS II—second phase of the Defense Satellite Communications System
HF—High Frequency

[STUDENT] What do you mean by failure in the satellite? I have been at the receiving end of the HF when it occasionally got through; you could never understand it so you made pious noises and ignored whatever they were trying to say; and I have had occasional access to satellite facilities and gotten communication. You can always get noise through HF, but do you really get that much more communications through it?

[TATE] Two points. First, we aren't using the HF media very well, in fact not nearly as well as the Soviets. Second, the satellites work very well when they are there, but we have had problems with the failures of DSCS II, for example. I can remember in 1975, as part of the basic command and control of the ***Mayaguez* incident**, we had a DSCS II failure that caused havoc. Now if the Navy had, for example, been using the DSCS as its only command and control mechanism for the Persian Gulf area or anywhere else in the world (and it virtually did for awhile), we would have been up the creek.

Mayaguez incident—In 1975, communist forces from Cambodia seized the US-flag freighter Mayaguez. A small force of Marines was sent to recapture the ship and its crew.

Going back to my first point, the Soviets have done detailed studies on ionospheric sounding for some 15 years, and studied which part of the spectrum is usable on a 24-hour basis at different locations throughout their interest areas. They do this automatically. They transmit it to their forces all the time. They change their frequencies and go to the usable portions, and they have extremely reliable HF communications. We don't. We can't even change our frequencies except day and night. We do not have any military or other facility in this country transmitting the ionospheric projections, which change on a daily basis, to the operating forces so they can understand what they are supposed to be doing. So a big part of the time we are

operating against the laws of physics. That's understandable. A program I helped foster is going on in the Navy now to upgrade HF. It's, hopefully, going to deal with this on a more systematic basis. But the United States Air Force has the same problems.

Another point.... [A] big portion of the whole globe is not even covered [by satellite communications]—particularly south of the equator. Budget reductions since the Vietnam War, from 1969 until last year when the Congress stopped them, cut out intelligence coverage and did not supply a big part of satellite communications and resources. So what we have is a belt of pretty good communications. But don't think that, if the Cuban missile crisis came again, South America would be in instantaneous touch by satellite over US government communications. We would bridge this by using some of the commercial satellites if the handspace was available.

[OETTINGER] Let me just interject: don't underestimate alternatives. The other night Don Hornig, who was Johnson's science advisor, was telling me how the President heard of the **Eastern power failure**. Hornig himself heard of it through a phone call from his daughter. He started making some phone calls himself, and was prepared when he got through to Lyndon Johnson, who heard on the car radio. But it was quite a while before any kind of official channels had it. It wasn't a military problem, it wasn't military apparatus. It was a command and control problem of the government. But since it was not a military problem there were no established channels. In that situation, the civilian alternatives, including the President's car radio, were the principal means of coordination.

Eastern power failure—electric power failure, November 9, 1965, which affected the northeastern United States and parts of Canada

[TATE] ... Their [Soviet] command and control structure ... is threefold-redundant. They have nuclear-hardened command posts like ours, only about four times as many; at least five are nuclear-hardened and alternate to each other. Each of the major Services have their own, plus national ones that tie it all together. They are connected by very modern communications, and the end result is a very effective C³ system, in my opinion. (36–37, 41)

3. **ROBERT ROSENBERG**, "The Influence of Policy Making on C³I" (1980, pp. 49–65)

Policy Assistant to the President for National Security Affairs, NSC staff

Part of our problem today is that our whole architectural approach to the C³I business stems from an age of strategic superiority, which the United States enjoyed for many, many years. In the current environment of equivalency or parity, however, we can no longer afford to have systems that are capable only of reacting in spasm to an aggressor attack.

... Commerce was also given the responsibility under **PD** 24, and confirmed in the Executive Order, to safeguard significant unclassified government information related to our national well-being—such as data transmitted by the federal regulatory agencies. This is part of our national telecommunications security issue, safeguarding unclassified information and preventing it from falling into the hands of foreign adversaries who would use it to the detriment of our national security. As part of that task, Commerce has the responsibility for public education, in terms of sensitizing the private sector at large to the telecommunications intercept threat to their interests. Commerce also is responsible for regulation within the Executive Branch—as opposed to the **FCC**, which regulates the common carriers et al. Commerce also inherited from **OTP** the responsibility for frequency allocation and spectrum planning for the future. So, with all these tasks, Commerce has a major influence on where our strategic command, control and communications capabilities can go, in terms of both capabilities and restraints.

PD—Presidential Directive

FCC—Federal Communications Commission

OTP—Office of Telecommunications Policy

The Department of Defense is another major player. It is the executive agent for the National Communications System, and the Director of the Defense Communications Agency in his dual role serves as the Director of the National Communications System as well. DoD is responsible for NCS architecture, systems management and operation, procurement and technology development. **NSA**, as I said, has a key role from a protective standpoint, in that it is the US government's executive agent for communications security, that is, protection of classified information.

NSA—National Security Agency

The Department of State has an equally key role in C³I, particularly as it relates to State's responsibility for foreign policy and for establishing the

US position in international negotiations. GSA has a key role as procurer of a tremendously large amount of our telecommunications equipment. The newly created Federal Emergency Management Agency has a key role as a resource manager for working the broad spectrum of telecommunication problems. The Attorney General is also a very important player. And probably one of the most important roles inside the Executive Branch falls to the Office of Management and Budget—not chiefly for its advertised responsibilities in Executive Order 12046, which holds OMB responsible for procurement, management of policy, and frequency allocation adjudication when some department is in a dispute with Commerce. More importantly (as I try to get my own boss to understand every day), budgets drive policy in this government; policy does not drive budgets. Those of you who end up either going back to the federal bureaucracy or going to work in industry somewhere are going to have to deal with the government, and you'll find the power of the budget supreme. I haven't got enough fingers and toes to count for you the number of Presidential Directives that really don't have very strong teeth because the OMB budget examiner managed to make sure there was no money to support the effort.

GSA—Government Services Administration

I have put the NSC down near the bottom of this list of people with responsibility for telecommunications. In the reorganization, the responsibility for all mobilization planning related to telecommunications and setting the architectural policies for the National Communications System was transferred to the National Security Council. OSTP has roles similar to the NSC's.

OSTP—Office of Science and Technology Policy

... The architecture was developed back in the 1950s. The military (as opposed to the civil) side of C³I has most of its foundation in a nebulous entity called WWMCCS—the World Wide Military Command and Control System. WWMCCS arose as a necessary communications command and control system to support spasm response to an enemy attack. And that is all it was intended for, because according to the prevailing view at the time, the world was going to end when that was over. (And interestingly enough, a big part of our problem with the Executive Orders and PDs and budgets and so on is that easily half the people I talk to are still convinced of that.)

... To my knowledge, as long as I have been in government, I know of no other President who actually has conducted SIOP exercises. Jimmy Carter

has. He has participated in a series of what we call **CPXs**, communications command and control exercises, in which there is an end-to-end run-through with different scenarios where the Commander-in-Chief is in communication with the unified and specified commanders—the commanders-in-chief of forces in Europe, the Pacific, the Atlantic, and **CINCSAC**, who is responsible for executing the SIOP by directing the assets of the **SLBM**, B-52 and Minuteman forces. The President actually went through these exercises, and probably the most telling experience they all had was a scenario the **Red** planners (as opposed to the **Blue** planners) developed, in which the Soviets laid down an **RSIOP** at our critical C³I nodes. It was a combination of sabotage and depressed-trajectory SLBM attacks against such things as our early warning satellite ground stations and our early warning radars. The exercise ground to a halt. And we learned that a very important feature of the deterrent posture is to be very flexible, and not just plan a system against an "approved" threat scenario. As I said early on, we know a lot about the enemy's capability, but we know little about his intent; so we had better be prepared for a variety of encounters.

CPXs—Command Post exercises
CINCSAC—Commander-in-Chief, SAC
SLBM—Sea Launched Ballistic Missile
Red—color associated with enemy forces
Blue—color associated with friendly forces
RSIOP—Russian Single Integrated Operations Plan

... The problem is all the players and the structure involved. There's the WWMCCS system, which is the tool by which we get tactical warning of impending attack. We get an assessment. The options of the National Command Authority to execute a retaliatory strike as part and parcel of the WWMCCS system. The authentication process itself, to assure that the National Command Authority, whoever it may be, is the legal executor of the system. The actual strike and post-strike assessments are part of WWMCCS too, and that's where we begin to run into problems, such as how you do post-strike assessment. Assuming that you are going beyond a spasm response, where are the reconstitutable communications? Where are the command and control entities to run them? We have bought, as part of the WWMCCS system, eight running nets, 108 command and control centers, 60 computer systems and 85 communications nets. We face the problem of how to reconstitute them.

But even WWMCCS is only a piece; intelligence is another very essential piece. If I don't know where the empty silos are in the Soviet Union from whence the missiles came, I could expend an unnecessarily large percentage

of my force and my deterrent at random—and we haven't even talked about that. But part of the need to look at the endurance of these functions is that after these nuclear exchanges (God forbid they ever happen), we must make sure we don't find ourselves in a position where an aggressor still has a secure reserve force of such magnitude that he can hold our governmental system hostage because he has blinded us—decapitated our ability to conduct military operations and run a civil entity called government.

... We have designed a C³I system that was built for peacetime operations as a spasm response. We have realized we have to change our focus for mutual assured destruction.

Equally important to this evolving philosophy and its architecture is the use of the information. I am sure you have read many articles that say WWMCCS is a disaster, or C³I is terrible. I neither advocate nor oppose that statement; but I will say that those systems are only as good as the way the decision makers use their information. I assure you that **Afghanistan** was not a surprise to the policy makers in the government. We had intelligence that told us what was going to happen long before it happened. The point is that the decision makers have to know what they want to do with the data they are going to get. So I can build a multibillion-dollar WWMCCS or C³I system, but it will be only as good as the people who are going to use the information that goes back and forth through it. (49, 50, 53, 58, 60, 63, 64)

Afghanistan: Soviet invasion of Afghanistan which began with air support in 1978 and involved massive Soviet troop commitment by the end of 1979.

4. LEE PASCHALL, "C³I and the National Military Command System" (1980, pp. 67–86)

Consultant; former Director, Defense Communications Agency and Manager, NCS

To me, a command and control system consists of an organized arrangement of sensors, communications and command centers. Whether you start with a data entry device, or a sophisticated satellite sensor, or communications, which are probably the critical link of any command and control system, it is at the command centers that all the information comes together, is processed and decisions are made.

... The next thing I would say that's fundamental to understanding C³I, particularly in dealing with C³I justification, acquisition and management, is to know who you're talking to—know your audience. If he is a technocrat you can talk to him in terms of a "C³ system," an aggregate of technical sensors, communications, command centers, people, procedures all tied together to operate in accord with some central directive authority. And the technocrat is comfortable with the idea of a "system" like that. If, on the other hand, you're talking to a manager, the **Gerry Dinneens** of the world, then today you'd best talk about C³I, because you're talking about a program—a chunk of the Department of Defense budget. If you're talking to an operator, the **Bill Odoms** of the world, then you're talking about a process, a command and control process, which is facilitated by the system, all of which is financed by a C³I program. People in Washington, military people very often and technocrats most often of all, make the mistake of talking to people as though everybody were a technocrat and everybody were thinking command and control system. The operators, who think in terms of the command and control process, will die on the ramparts of definitional war—they will define and fight and quarrel about roles and missions until the technocrat is thoroughly confused; and the reason is that they have a differing perspective on what it is you're talking about when you say command and control.

Gerry Dinneen—Assistant Secretary of Defense for C³I under President Carter

Bill Odom—Military Assistant to the Assistant to the President for National Security Affairs

... The other large, unbounded multiple-user system [besides the World-Wide Military Command and Control System] is the National Communications System. A word about the NCS, because it illustrates a couple of things I think will be useful. The National Communications System emerged from the 1962 Cuba experience when President Kennedy tried to consult our Latin American neighbors. He urged the inter-American affairs group to consult their governments, and when all the ambassadors from the Latin American countries tried to do that, the communications problems they experienced were absolutely appalling. Finally, one country had to abstain, another country, whose ambassador couldn't understand over the telephone line what his government was saying to him, nevertheless decided to vote for the blockade, and earned President Kennedy's gratitude thenceforth. Based on that, President Kennedy said we must organize our national communications better, so an executive order was issued. It provided for something called the National Communications System, which was to be a "unified" system. It was to be put together by connecting, or interconnecting, or unifying, all the communication systems of those departments of government which dealt with or could contribute to national security activities.

One of the first interesting things, I suppose, to learn about government is what happened to the word "unified." There was a ten-year debate about what it meant. Did it actually mean a single system, which meant that the Department of Defense and the State Department and the GSA and NASA and all the other contributing agencies would be served by a single system? There were those who felt that way. There were others who felt that what that really meant was that they should all be connected together, so that if the President wanted to talk to Colombia and NASA had a tracking station in Colombia, why, he could use that link through the NCS management structure. All through that ten-year debate, many people moaned and groaned and wailed about what was meant by "unified." I draw two conclusions from that—these are my biases again. First, it's very difficult in a Presidential executive order to get completely unambiguous wording so that people can't argue over what was the intent, what was the meaning. Second, it may not even be wise to write an executive order that's completely unambiguous, so that there is no debate—it sort of forecloses the future and may not be a sensible thing to do.

NASA—National Aeronautics and Space Administration

In any case I don't believe it would have been a sensible thing to do for the NCS. It ended up instead as a federation of communications systems, participated in by the State Department, the Department of Defense, the General Services Administration, the Energy Department now too—and it operates well today without the bureaucratic threat of a single system that you don't control. The Defense Communications System is 80 percent of the National Communications System; it has the dominant role. The director of the Defense Communications Agency is the manager of the National Communications System, and he manages by consultation. He consults, he persuades, he tries to achieve consensus—but he can't dictate, except under certain circumstances. He can dictate in time of war when certain executive orders have been issued; then he becomes a dictator. But up to that time he is a persuader.

It's a difficult way to try to manage something. It's surprising that it works, but it seems to. Every week, somewhere in this country, the President declares an emergency. Whether it's a flood, an earthquake, a tornado, a hurricane, the National Communications System staff, which is in the DCA building, is charged with providing or arranging for communications support as needed by the General Services Administration's Emergency Action Group. When the President declares an emergency, certain loans become available, and certain communications assets can be provided for military or

other resources. So every week in the year, on the average, there's a national emergency somewhere where military equipment may be on loan to a civil agency, or civil agency equipment is on loan to the local National Guard or to an active military unit, and is on the scene. And circuits are extended from the nearest NCS operating agency, whether from a defense installation nearby or from the nearest GSA office. Those weekly disasters exercise the NCS continually and it works quite well. Fortunately we have not had any enormous disaster, like nuclear war, which would further test it. And international communications have improved so dramatically that generally it's not been necessary to use NCS resources other than those of the DCS for that purpose. But it works, every week. Quietly, and without any particular noise.

... Finally, I'm going to list what I think are the major C³I issues today. Anybody who can solve these ... problems, you see, can become a hero in many ways. The first is how to handle the business of telecommunications protection. The way we do it today is to put a cryptographic box on every line, or on one big radio system. Very expensive! You can afford that for military applications, where you have classified military information. But what about all those conversations dealing with unclassified elements and pieces which, however, when assembled even by a relatively inexperienced person can give you a coherent picture of what's happening? Is the size of the wheat surplus in the United States of interest? It would seem to have been when we were negotiating with the Soviets about what price they were going to pay for all that surplus. There's a large amount of information flowing through microwave systems and satellite systems in the country which is readily available to even an unsophisticated interceptor. In Vietnam we found the Viet Cong (not the North Vietnamese professional military, but the Viet Cong—in what they call "spider holes" with Heath-kit radios) were reading our communications. And the problem of protecting against intercept of privacy telecommunication pertains to much more than just classified military information. It extends to point-of-sale things, for example. As I buy an item and the sales clerk punches it in, if that also debits my bank account—in other words, if I pay the bill at the same time I buy it through a fund transfer arrangement—privacy and protection of telecommunications is equally a problem there.

The second problem is survivability. There are really two ways you have to survive. Most people think of survivability as being one thing: you are shot or not shot. Physical survivability is important, and most survivability conversation, thinking, and studies deal with physical survivability. But perhaps an even more serious problem today, given all the electronic systems we use, is electronic survivability—being able to resist an electronic attack. In

the 1973 Yom Kippur War the jamming the Egyptians mounted against the Israeli communications was so severe that the Army had to lay wire out in the desert; and the Air Force, at its bases in Tel Aviv, was forced to use runners to get messages from the control tower to the aircraft. They could not launch aircraft from the control tower. The Israelis literally lost command and control for about thirty-six hours under Egyptian jamming attack. Yet the Egyptians were using, not really hand-me-downs, but certainly second-level electronics jamming equipment.

The Soviets are very candid. Their open literature on military doctrine (not classified stuff) says they intend to physically attack one-third of the enemy's command and control—bombs, weapons, sabotage. They intend to electronically attack—that is, jam—another third of it. With the remaining third they do not feel he will be able to effectively manage his force, and they expect to have a decisive advantage in combat.

So the defense against jamming is a major problem as well as how you survive an attack and, having been damaged, reconstitute what you had in communications, command, and control. Now some of these problems can be solved rather easily by throwing very large amounts of money at them. But that's not a very sophisticated solution, and it's not doable in many ways today. Other problems require engineering advances; some may require some inventions, and a lot of them will be around for a long time. . . .

Software is the next one. First, how do you achieve multi-level security so that your software, your data base, can't be spoofed or changed without your knowledge, or extracted from to get information? It's often called the multi-level security problem. The solutions are hard to implement, and they have an effect on throughput—that is, how efficient your system is. The aspect, though, that's not often talked about is verification: how do you know the computer program's going to work as you want it to when it meets an unexpected situation? There's a classic case. The French had a meteorological satellite up several years ago, and they put into the telemetry a command generated by a computer to reconfigure something, or reposition the satellite, or point the satellite at something else—I don't recall the exact details, but I do know what the result was. A glitch in the software turned the satellite off. This was shortly after it had been launched, and it was a dead loss; they never could get it turned back on again. Now how do you verify command and control systems and management systems, especially as you get more and more into near-real-time situations and people are interacting with the computer? How do you verify software so it won't do something unexpected to you at the worst possible time?

... I alluded earlier to ... [another] problem, the changing domestic communications structure, as being a fact of today's US environment. Ninety percent of the Defense Communications System in the United States is leased; we have very few government-owned communications systems. Ma Bell has provided the bulk of that over the years. They have put transcontinental cables four feet underground in sand and built 50 to 100 pounds-per-square-inch manholes and underground facilities, and they've done all this without charging Defense separately for it. They've routed microwave systems around rather than through cities. They've done many things that are in the defense interest and they say that is because one of the first purposes of the Communications Act of 1934 is to provide for the national security and national defense.

Now there are a lot of new competitors on the street—the MCIs, the Southern Pacifics—and we're going into a competitive, intercity world from a communications standpoint. Most of the new competitors have tried to minimize their investment; they want to charge the least amount possible because they have to compete with something that already exists and is very large indeed, the Bell system. So they're not going to build the additional features of redundancy, restoration, and hardness that we like in military systems. But the Armed Services procurement rules say very simply: you will compete.

So the military people who are acquiring communications, largely leased in the United States, over the next few years have got to learn how to live in a different kind of world entirely. If the catastrophe occurs and we have all these separated communications systems, how can they be interconnected to restore, reconstitute and revive the nation after a nuclear attack?

... First, the WWMCCS is more tightly coupled than the National Communications System, which is very loosely coupled. To answer your question, yes, our system is much less tightly coupled than the Soviet system, reflecting two different styles of government. The Soviet system is hierarchically very rigid, very tightly coupled, but it takes into account the fact that destruction can and will occur. The Soviets make heavy use of something called skip echelon—that is, Moscow can talk to the military district, or it can talk to the missile battery, or whatever. They've spent much more money than we have on hardened command centers; they have them by the thousands, literally. Very little of their capability will sustain a direct nuclear hit, but enough centers will survive collateral damage to give them a very survivable command and control posture. Compared to the Soviet's rather rigidly, hierarchically structured operations, our people exhibit more initiative. In the absence of direction from higher headquarters they tend to

do what they think is best, and it's often better than what our headquarters think they ought to do, too, because they're on the scene. The flexibility and looser coupling of our system is an advantage, I believe, even given the fixes that the Soviets have taken on skip echelon and things like that. (67, 68, 71–72, 81–83, 85)

5. **JOHN H. CUSHMAN**, "C³I and the Commander: Responsibility and Accountability" (1981, pp. 95–118)

Management consultant; former Commandant, Command and General Staff College

I will start off with a very sober assessment. These are convictions of mine. Our performance has been and is gravely deficient. The sad story is that the command and control systems that are in the hands of the deployed US field forces, and of the Allies alongside whom we will no doubt have to fight, are barely marginal for conditions short of war. I'm satisfied that any realistic audit will show that they are, and will be, seriously inadequate for war.

To be specific, they are not well tied together from top to bottom. They are not being exercised realistically under the expected conditions of war. Great sections of them will probably not survive the attack against them that is sure to come in war. For the major operational commander, Allied or US, whose forces must use these systems (I'm talking about theater of operations command) they are largely unplanned, spliced-together, ill-fitting components which have been delivered to his forces by relatively independent parties, far away, who have coordinated adequately neither with him and his staff nor with each other. They do not exploit the present capabilities of technology, nor does the system for their development adequately provide that future systems will. That's essentially my indictment. (95–96)

6. **CHARLES ROSE**, "Congress and C³I" (1981, pp. 169–91)

Member, US House of Representatives; Chairman, Policy Group on Information and Computers

C³I has been paid a lot of lip service. I would like to believe that people are serious about it, but sometimes I'm still skeptical. We hear a lot of talk about the need to harden our satellite systems, to provide for redundancy in our communication systems, but the progress seems to be awfully slow. It

has been so tedious that I wonder how serious we really are. I may not be right up to date—maybe some of you in this class are—but a couple of years ago when I was looking at the status of the NATO/ Warsaw Pact balance in the Central Region, I was shocked to discover that many key communication nodes in NATO had virtually no hardening or protection whatever, so that a skilled enemy using strikes or sabotage could knock out NATO's command and control structure within a few hours of an initial attack.

I'm not sure how far along we are in improving the situation. We need to get serious about hardening our intelligence collection satellites, our communications and relay satellites in outer space, because the Soviets mean business with their anti-satellite interceptor, as they have demonstrated on numerous occasions. They do have the ability to knock out some of our systems. We cannot think of space any longer as hallowed turf where no hostilities will occur. Perhaps the first warning sign of major confrontation will be when we discover one of our satellites out of commission. (174–75)

7. **RICHARD H. ELLIS**, "Strategic Connectivity" (1982, pp. 1–10)

former Commander-in-Chief, SAC

But the problem in Europe then, in the mid-1970s, and to a large extent today, is this. There are some very sophisticated commercial communications nets in Europe, the **PTTs**—all the countries have them, especially in western Europe. But they have difficulty talking to each other, and they could not talk to military systems. One of our challenges was to make arrangements and agreements with the various countries under which we would provide them compatible switching centers and terminals in exchange for permission to use certain frequencies on their nets in wartime.

PTTs—post, telephone and telegraph networks; government-owned commercial communications systems

That's a slow business. You're dealing not only with the nations themselves (a lot of those nets are nationally owned), but with commercial companies that are looking for profit. Our government, of course, added its usual bureaucratic complications. All in all it's very difficult to get the interface we wanted.

I think the best example is the German Grundnetz. It is an underground system, built by the German national communications system, with access

channels into the net throughout Germany. With it one can reach all of the German military. But it couldn't talk to the American military, or to Belgium, or British forces. We made an arrangement with the Germans under which, in return for use of certain of their nets, frequencies, and lines, we provided them certain encryption material. It'll work—but the point of this story is that there's a lot of technology over there, in being, and the problem is to tie it all together into a cohesive net that is available to the NATO military as well as to the national, commercial, and governmental organizations.

Now let me get to strategic connectivity. There are many definitions, but the simplest is that strategic connectivity includes the hardware, the software and the people necessary to get information on nuclear attacks against the United States to the President so that he can get a timely execution order down to the units. That's the mission of our strategic network. Before I describe its different elements, let's look at what we did for so many years before, when it was a relatively simple system. During the 1950s and '60s there was only one mission: to get the word out, to execute. We weren't too concerned about what happened afterward. We had nuclear supremacy, and then superiority—but then gradually that started to fade in the late 1960s. In the early 1970s the Nixon Administration decided that something had to be done. The President couldn't be left with just this one alternative of "throw it all or nothing." **Mr. Schlesinger**'s "**flexible response**" policy was ratified by an **NSDM** in 1974. You might say it was a long time coming. I can recall Mr. Schlesinger's coming in to the air staff when he was head of the strategic section of Rand in the middle sixties and talking flexible response, but it was the sort of subject that people weren't ready for; it was ahead of its time. Besides we still had sizable superiority; we believed all we had to do was let go and that was enough to deter the Soviet Union. In the mid-1970s, however, we realized that that day had passed, and our policy has gradually evolved since.

Mr. Schlesinger—*James Schlesinger, Secretary of Defense under Presidents Nixon and Ford*

flexible response—*nuclear war strategy which called for a variety of options and levels of response to attack*

NSDM—*National Security Decision Memorandum*

Today the latest presidential decisions are spelled out in Presidential Decision Memoranda 53, 58, and 59. Number 59 is actually the policy, while 53 and 58 state the command and control, and the continuity of government, that we must have in order to carry out the nuclear policy. These PDMs are, of course, subjects of some complexity and some debate, and have been since their promulgation in the spring, summer, and fall of 1980; but they are the drivers behind the big advance we have in strategic connectivity

today. They set the policy and the priorities, and, given the right kind of organization to implement them and the resources in terms of money, will provide us with the strategic connectivity we hope to get eventually.

Now let's talk about the elements of strategic connectivity. I say there are seven elements. The first is the attack detection network. That includes the warning satellites, infrared, **SIGINT**, **ELINT**, the **BMEWS**, **PAVE PAWS**, and **COBRA DANE** radars, and other intelligence assets which would indicate that the Soviets are in the process of undertaking an attack against the United States. Some of those systems themselves are very old, like the **BMEWS**, though they have been upgraded from time to time. Some are very new and sophisticated, like our synchronous satellites. But there are things that we didn't think about when we built those that have come under serious discussion in recent months. I'm talking about the atmospheric explosion or detonation of nuclear weapons with resulting **EMP**, blackout and the scintillation that can "blind" these "sophisticated" satellites. That's being worked on. We know they have frailties. You've got to remember too that we don't know as much about any of those phenomena as we would like to know, because we stopped our atmospheric testing many years ago. The Soviets tested in the atmosphere longer than we did, and a lot more extensively than we did, and consequently most knowledgeable people believe the Soviets know more about the atmospheric and exoatmospheric effects of nuclear blasts than we do.

SIGINT—Signal Intelligence; interception of coded electronic pulses

ELINT—Electronic Intelligence

BMEWS—Ballistic Missile Early Warning System: radars at Thule, Greenland; Fylingdales Moor, England; and Clear, Alaska

PAVE PAWS—Phased Array Warning Systems: modern radars on the east and west coasts and in central Texas

COBRA DANE—radar on Shemya Island, Alaska, which uses phased array technology to monitor ballistic missile tests

EMP—Electromagnetic Pulse. Current and voltage surges triggered by a nuclear blast above the earth's surface.

The second element of strategic connectivity, as we define it, is attack characterization: gathering all the intelligence from any possible source, using the most sophisticated and fastest means of collating it, and coming up with a decision on what it means. The information gathered by the detection elements has to be sent back to the place where this characterization is done: NORAD in **Cheyenne Mountain**. Now, just getting it back is a problem in itself. We use satellites, we use transatlantic cable, we use high frequency and very high frequency and low frequency to get

Cheyenne Mountain—site of NORAD's underground command post, near Colorado Springs, CO

the information there. But a lot of things were overlooked as we built those systems. For example, in 1978, when we did a study I'll talk about later, we found that one of the terminals from one of the overseas sites was in an AT&T building in San Francisco that was unprotected. Anyone could just walk in the door to a switching center with the name of the originating terminal on a sign. In other words, it identified the overseas station, and you know right away that this was the United States terminal for that information, highly vulnerable to anything anybody wanted to do to it.

The NORAD commander's job of attack characterization is unique to him. Only one other individual or organization has that responsibility: the President.

... The third step is the decision by the NCA. He's going to have to take the final attack assessment and do all the other things he wants done as part of his decision-making process—political and other considerations that the average military man might not even be aware of. He's going to make a final decision, and his decision could be any one of thousands of choices. People talk about flexibility in the strike plan—there are thousands of alternatives in this plan, any one of which he could pick, but making your selection isn't as bad as it sounds. It is very organized, and people at the far end will know what to do if they get the message.

NCA—National Command Authority: the President or a successor

The most exciting part of this whole sequence to talk about is how this man makes a decision, and I want to forestall any questions on that right now. Let me just say that he's got the responsibility—he knows he's got the responsibility. It's established in law. Obviously a man with that responsibility is going to make provisions for contingencies when he may not be available, or is incapacitated. As SAC commander, I was always satisfied that that was taken care of, and I think that's where we ought to leave that subject. Everybody likes to know exactly who's next in line, and who does what, but that's the President's decision and he's not going to say much about it. I don't know of any President who's ever discussed the subject publicly.

So now there is a decision, and it must be disseminated. The decision goes to a staff that's in constant contact with the decision-making authority, the

CINCs and the fighting forces. They format the message. Much of the formatting is already done. It's the staff's job to get the message out to the forces that are going to execute the plan, and this of course is time-critical because our seat of government is on the coast. This part of the process may have a life expectancy, in some scenarios, of somewhere between 11 and 13 minutes—delivery time from the patrolling Soviet **SLBM** submarines. So these things have to happen fast, and they have to happen accurately. One tends to think about the big parts of the sequence like the decision, but the little parts, like getting out the execution order, are just as important, because if you don't get it disseminated properly and in a timely way, it isn't going to get executed. That's why there is not only an **NMCC** at the Pentagon in Washington, but a national emergency airborne command post (NEACP) which also has the capability to disseminate the decision. It is disseminated through every mode available: landlines, various kinds of radios, satellites, and some others that we probably shouldn't get into at this point.

CINCs—Commanders-in-Chief

SLBM—Sea-launched Ballistic Missile

NMCC—National Military Command Center

The fifth step is execution of the decision. Again every communications system is simultaneously exercised by the people receiving the order—the commanders, whether they are SAC, **LANT**, **PAC** or Europe. For instance, SAC has a primary alerting system, an automated command and control system, **AFSATCOM**, the emergency rocket communications system, to get the orders out in a matter of seconds to the crews. And the crews are in a lot of different places. They may be in airplanes. They may be in the polar reaches of the globe, or sitting out in a silo at a command and control facility in a rocket field in Wyoming. You have to ensure that they get it, that's why they use redundant systems.

LANT—Atlantic Command
PAC—Pacific Command
AFSATCOM—Air Force Satellite Communications Systems

The sixth step is one of the most difficult things to do, if you think we've had problems so far. That is to collect the intelligence and information on what we did to the enemy and what he's done to us; and that, my friends, will be very iffy business. You hope to do it through reconnaissance aircraft,

reconnaissance satellites, ELINT sources, etc. It will be difficult to get any sort of communications back through the environment that's going to be existing during that time. But if we don't get that information, then this business of extended hostilities or enduring nuclear strategy is just so much foolishness—if there was anything to it to begin with.

The final step is reconstitution of forces, to carry out whatever remains to be done with whatever you've got left to do it with. And then the entire cycle starts over again. Now that, theoretically, is what strategic connectivity is, and you can see that it's not something the Bell System is going to solve for us, or that any one person is going to solve. It's an extremely complex sequence of actions that have to take place, and have to come about in very short order.

. . . And there are a lot of anomalies we don't know enough about. What happens when an airburst is 150 kilometers high, for instance? What kinds of things are going to go wrong with our satellites? What's going to go wrong with our ground-based systems?

We built a great big trestle out at Albuquerque, for instance. We can put a B-52 on that trestle and zap it with 50,000 volts. If we can protect against that, we believe we know our C^3 can stand up. But we don't know it for a fact; we don't know whether it's strong enough. It's interesting: the B-52 is actually a pretty hard bird when it comes to C^3, because it's so old. A lot of its systems are old technology—vacuum tubes. While now we're dealing with chips, and this low-power micro-technology burns out when one lights a match a mile away, so to speak. Well, that's a very difficult thing to comment on. I wish I could be more precise.

. . . One of the most destabilizing things that we and the other side will have to live with is the case where one side knows the other side's C^3 system, or weapon system, is vulnerable. That is an incentive for the side living with that vulnerability to go first. (4–6, 7, 8)

8. **HILLMAN DICKINSON**, "Planning for Defense-Wide Command and Control" (1982, pp. 11–55)

Director, Command, Control, and Communications Systems, Joint Chiefs of Staff (JCS)

Our list of goals looks like this:

- Improve survivability of C^3 systems

- Improve joint and combined interoperability
- Improve current C^3 systems effectiveness
- Provide effective wartime C^3 systems
- Provide effective crisis management
- Develop capability to degrade enemy C^3
- Improve management and operation of C^3 systems
- Realistically evaluate C^3 systems

Numbers one and two are by far my most important priorities: to improve the survivability of both the intercontinental nuclear command and control system and the theater and tactical command and control system. And then, secondly, to improve joint interoperability, because the Services have to work together if we have to fight; you can't fight separately. As for the combined interoperability—to explain the jargon for those of you who are not familiar with it—"joint" means among the US Services; and "combined" means between the US and its allies. So we talk about joint forces and combined forces.

... Going back to my list of goals: the third one, improving systems, I would like to print in smaller type. I am much less enamored of all the good things the salesmen want to sell us than I am of telling them: "Let's take the new technology and the new advances and use them to accomplish the first and second objectives." In other words, as we get the wide-bandwidth systems, as we get the tremendous memory capabilities and so on, let's use them for survivability rather than give people ten more telephone circuits. We've too many people talking already. Cutting the total reporting systems down to size is another very important part of that survivability. And we are doing that. There's one particularly onerous report called "Unit Rep," very voluminous, in which there were, in one computer file, some 40,000 units reporting out of our three Services, and up to four hundred pieces of information being reported about each of those units. We believe that probably only a thousand of those units are necessary in wartime, like, say, the 82nd Airborne Division. Not two-man well-digging teams. And about twenty-five pieces of information from each is probably satisfactory. You can see what it does for an **ADP** program if you can cut down to that kind of size, and for the communications that carry that information. We're working on those kinds of things too. That's not a dollar item, but it's a survivability item, I'll guarantee.

ADP: Automated Data Processing

[MCLAUGHLIN] It strikes me that in some of the declassified World War II material, in the battle of the Atlantic, for example, the most valuable

decrypted information for the most part, by some assessments, was that of the individual submarines, U-boats, reporting back nightly to meet standard reporting requirements on status of supplies, crew, and so forth. I think that may just suggest that the problem you're mentioning is not just for efficiency's sake and survivability. We do see the unit reporting, but there might be other considerations. . . .

[DICKINSON] That's survivability. Very much. We're trying to cut down the emissions, because the Soviets do have a very efficient radio electronic combat capability. They will be listening. And emitters will be located.

. . . C^3 system evaluation—realistic evaluation—is very difficult. The reason survivability is up there in the number one position, in my opinion, I blame on the operations research community and the evaluation exercise community. Because it was always too tough for either of them to simulate the damage that would realistically happen to the C^3 system in wartime. And so in all our exercises and almost all our games and studies and analyses, perfect C^3 connectivity was assumed. And therefore the briefings from those studies and analyses were extremely erroneous, by very, very major factors.

Now that is changing. You will see C^3 degradation in exercises, and support for funding is beginning to materialize, because we have gotten into the major war games that are really briefed to the top decision-makers. In all our exercises now we are removing the satellite communications for a period of time. The Navy does that well. Their ships are very dependent on a UHF satellite. They just remove the UHF satellite for three days at a time, so they have to get the message by HF radio or courier it by COD, carrier on-board delivery. That means a small aircraft flying off the deck with a small bundle of papers. Or they signal each other by light. Those are very important exercises.

. . . Another example . . . is our problem with civilian contractors remaining overseas in wartime. Or worse, in the two or three days immediately before, when war is threatening and the question arises whether they're going to take their families and go home, feeling it's more important to evacuate their families than it is to stay on their jobs, and what that will do to our command and control and other sophisticated systems. We're working on that very strongly in this administration. But again, that's the survivability of the system in the biggest sense. Those are the terribly important kinds of things.

. . . One of the nuances of that whole problem [electromagnetic pulse] is that modern aircraft are even more vulnerable than old aircraft, they're plastic

instead of metal, so the electric field penetrates the aircraft more. Also all of our neat, fine computer small parts are in many ways more vulnerable simply because they are small, they can't absorb the same amount of energy that an electron tube could and still continue to function. So we have to be careful as we modernize.

... We will be improving the VLF—very low frequency—communications to the SAC bomber fleet to ensure their reception of orders to continue on course, turn back or whatever, and that will complement their UHF and other modes of transmission. Communications to the deployed submarines are being improved as part of the program. I think you know about the small ELF program, which is important in the pre-hostilities stage, in part as a bellringer so that if that transmission stops, they know they are to go someplace else to get orders by some other means.

ELF—Extra Low Frequency

Communications satellites are very important. The real news in the satellite business, particularly to enhance our survivability, is moving up to the EHF range, which gives us one tremendous bandwidth which can be used for anti-jammer protection even more than it would be used for additional channels. And that's the way we intend to use it, certainly in this system: to improve survivability features that are clearly advisable in the satellite business.

EHF—Extra High Frequency

... The world of high frequency, as a matter of survivability, is coming back. The Services almost stopped their high frequency radio programs in the past—they thought they were going over to satellites. We have seen that that is not the way to go. There are now active programs that are being coordinated so they will all interoperate with each other and can be used together, and I can promise you that this is a very important area. The real-time sounders let us watch the ionosphere and know exactly where it is, those have made a dramatic improvement in performance. High frequency radio, for example: in the 18th Airborne Corps at Fort Bragg, they used to get only about half their calls through the first time on HF radio. Using ionospheric sounders we get 98 percent call completion satisfaction, first time.

Fiber optics is a tremendous improvement area. It has a lot of advantages, not the least of which is mobility. You don't tend to think of plain fiber

optics as being mobile, but look at its weight reduction. The metal cables in the Air Force 407L Tactical Air Control System take about twelve C–130 aircraft loads to transport, one system. It would take about one load with fiber optics, and that's a lot cheaper than buying eleven more C–130s. So fiber optics means less trucks, less truck drivers, less mechanics taking care of the trucks, less cooks cooking for mechanics, and so on. You add that up, it's a magnificent improvement in both mobility and capability, a manpower saving, and a saving in cost as well. Huge bandwidth, relatively secure, a little bit harder to tap than conventional wire lines. It can be tapped, but it's not as simple: it takes a pretty sophisticated fellow to get into a fiber optic cable. It is a lot less vulnerable, it's **TEMPEST**-proof, EMP-proof, and it's got a lot of dramatically improved capabilities. And just as rapidly as possible we're putting in fiber optic systems. You know—two things are happening. We're getting almost unlimited computer memory, so that memory capacity is almost free, and we're getting very wide-bandwidth systems to carry things.

TEMPEST—program to accredit electronic equipment for secure military use

Millimeter wave radios have dramatic possibilities. A typical millimeter wave radio looks like a 35-millimeter camera, and is just about as easy to handle. It's got about a two-degree beamwidth, so you can point it in the direction you want to talk to and get to anything within about four kilometers without laying any cable in between.

. . . Alliance warfare is not easy, especially when you want to work system problems. Since the creation of the directorate, one of the accomplishments of which I'm reasonably proud is that we have become the one point of contact, of approval, for all the positions from US representatives, all the military side of that combination of [NATO] committees—about half of those thirty-two. (23, 24, 25, 31, 35, 42, 49)

9. **THOMAS H. MCMULLEN**, "A Tactical Commander's View of C³I" (1982, pp. 57–76)

Deputy Commander, Tactical Air Command (TAC)

Effective command and control lets us see the situation as it develops; it collects information and presents it in the appropriate way to decision-makers; it lets them decide what to do so they can posture the force correctly to be at

the right place at the right time. Then, when we get into the employment phase, we have to be able to see—we have to see the targets, if not with our eyes, then through some kind of sensors—so as to decide how to use the force. We then have to assess how it's going, so we have to get information on what the situation is and how it's changing. Fundamentally, we need to be able to take advantage of the speed, the maneuver capability, the ability to shift rapidly from one place to another, and the firepower that is fundamental to TAC Air. We have a notion that says we re-role aircraft on the ground; we change them from one of the roles that I mentioned earlier to another role before they're launched; once they are airborne, we can change their tasking, but if they're configured for an air-to-ground mission, that's what we will use them for. We may change the point at which we apply them, but we usually can't change them from an air-to-ground mission to an air-to-air mission in flight, because they would probably not be carrying the right kind of ordnance. Simply said, the key element of C³I is people doing the time-honored military business of leading; they're supported in doing this by a mixture of procedures, facilities, sensors and data processing equipment.

... A good C³I tactical system has to be able to degrade gracefully; that is, it must be able to lose some of the capability that it started with initially, and still not come unglued. And that's a very challenging requirement; in fact, as we concentrate more and more on how best to design the C³I system, there's a tendency to envision one that's centralized—but frequently centralized systems don't degrade gracefully. As one link goes out, it might take with it a lot of force capability. So that's something that we concern ourselves about.

On the other hand, graceful degradation is one of the good characteristics of manned systems; they are capable of reasonably effective independent operations. Part of our C³I training prepares for that. Our training prepares our people not only to use the system when it's fully operating, but to preserve its effectiveness when it becomes degraded. (59, 60)

10. **STUART E. BRANCH**, "C³I and Crisis Management" (1984, pp. 87–102)

Deputy Assistant Secretary for Communications, Department of State; member National Communications System and US Communications Security Board, NSC

This area [communications security] has received a lot of attention in the past and in this administration. The Carter administration recognized the problem and issued Presidential Directive 53. Although not much happened

in the implementation of that directive, it did stress the need for a national security communications system that is restorable, interoperable, and survivable.

... [T]he State Department's communications system is as much a piece of that worldwide military command system as are the defense elements, and ... it has the potential of playing as much a role in command, control, and communications as do a number of the military systems.

... The **Belrut Embassy bombing** is a crisis situation you all are well aware of. We lost our communications center in that bombing. As at most, if not all, of our locations, we had some off-site capability. Our off-site communications capability could handle only a limited amount of information, so we augmented it with certain tactical satellite systems. We were back on the air within 24 hours with full capability in a different location.

Beirut Embassy bombing—1983. A second bombing took place in September 1984—several months after this presentation.

... I mentioned the Presidential Directives regarding national telecommunications and how they came about, and that implementation responsibility went to the National Communications System. It was concluded, however, that as a government entity it alone couldn't do a great deal to improve the system's survivability, restorability, and interoperability. That's because some 90 percent of the communication system the Defense Department depends on belongs to the private sector. So the next step was to involve the private sector in the process. The National Security Telecommunications Advisory Committee to the President was formed. It consisted of 30 chief executives, representing the satellite, data processing, and telecommunications fields. Tasking for the National Communications System, as contained in Presidential Directive 53, was primarily addressed to domestic communications systems, so it was difficult to see a concern about our international communications. When Presidential Directive 53 was rewritten as National Security Decision Directive 97, it specifically incorporated language addressing the international side and asked the State Department to study and manage international services. The National Communication System remains the executive agent but the State Department had agency responsibility for meeting survivability, restorability, and interoperability criteria. The Department then asked the National Security Telecommunications Advisory Committee to put together a task force to examine international telecommunications and give us some thoughts on how we could make the international communications commercial operations more

survivable, more interoperable, and more restorable. That task force was put together with about 13 representatives of industry. Part one of their report was issued in April 1984. It was sent to the White House and accepted. Part two was completed later in the year.

The report includes recommendations that you would expect: greater use of commercial satellites from embassy premises as opposed to terrestrial PTT facilities (recognizing that this would require a lot of coordination with those governments, some regulatory issues, and some legal issues). Also suggested are ways to build in greater redundancy in the communications between the embassy and central offices or earth stations. We should also improve the restoration priority assigned to our critical circuits.

One of the concerns we had was how the divestiture of AT&T would affect our embassies in Washington and overseas. When Bill Hillsman was director of the Defense Communications Agency he used to say who do we call after divestiture? We call AT&T now; who will we call to restore our communications? Think about that a minute—who do the embassy communications officers in Washington call? Are they going to work their way through this maze? We put together an organization called the National Communications Coordinating Center, under the Defense Communications Agency, and that's supposed to be the place where we have industry and government representatives jointly operating. If you have a serious problem, you call there and that's where it comes together.

... My personal observation is that while there is serious concern about the capability of our national security telecommunications assets to accommodate the stress conditions you have examined, and while there are many advocates within the Administration for improving our capabilities—witness **this new Executive Order**—there seems to be a gap between what the policy is and where the resources are to implement it. I'm not suggesting that we cannot revise our thinking, revise our planning, and take national security and survivability into the planning process as we design our systems. But a program of this magnitude is going to span administrations, and it is unclear whether there is a national commitment to this philosophy that would carry through administrations and provide the funding necessary to support it over the long haul.

this new Executive Order—April 4, 1984

It's common to measure the cost of system acquisition, and maybe even system activation, but it's not as common to measure carefully the cost of

maintaining this kind of capability over the long haul—the personnel, training, logistics, facilities, and updating. It's a tremendous effort to keep abreast of the state of the art. If you build a system for emergency purposes, at what point do the funds dry up because the more pressing need is day-to-day? Who makes that decision? I do not in any way suggest that we don't examine emergency needs or fold them into our design process, hut I'm not certain that we have accurately measured the total cost of implementation. (87, 89, 94, 95–96)

11. **RICHARD G. STILWELL,** "Structure and Mechanisms for Command and Control" (1985, pp. 33–65)

Chairman, DoD Security Review Commission

We've done very well at the national level, in my view—except for the exigency of nuclear war—in huilding a fairly rohust communications system.

But that's not true at the theater level. Each theater is different, has different requirements, and in my view, the theater commander should be given the necessary assets to contract or otherwise to design the architecture he needs out there for his theater—**PACOM, EUCOM, CENTCOM,** whatever—and then we ought to hreak our necks to ensure that he's provided with that. So, that's point one. As I said, Boh Kingston, three years after the activation of CENTCOM, still doesn't have the minimum essential communieations capahilities he needs as CINC CENTCOM.

PACOM—Pacific Command
EUCOM—European Command
CENTCOM—Central Command

. . . I guess the last thing I would leave with you is that command and control involves a good many things that you don't normally think ahout: an organization for decision-making; a structure that you hold inviolate for the transmission of instructions downward—although you can skip echelons on the way up for information purposes; and people who understand the mission, who are drilled in the doctrine and the procedures that constitute teamwork. In the last analysis, these people are especially important to the exercise of command and control. Then, of course, you do need the systems—the hardware, if you will, that makes all of those things more efficient. (62, 65)

12. **RICHARD D. DELAUER,** "A Consultant's View" (1985, pp. 87–102)

President, Orion Group Limited; former Under Secretary of Defense for Research and Engineering

The most important feature of C³I is that it is one piece of the President's strategic program that has never taken any flack; that's the real reason for the survival of C³ strategic forces. Congress has supported it fully, and by the end of next year we will have spent as much on strategic C³ as we will have spent on the B-1, about $20 billion. We are getting close to having fully survivable C³ for strategic systems to both the National Command Authorities (NCA) and the Strategic Air Command (SAC). After the authority is given, the SAC link can be used to command the strategic forces. C³ has been one part of the President's programs that we've done correctly and on schedule. In another year or two, C³ will be complete ...

[STUDENT] You talked about improvements in strategic C³ capabilities, but not theater C³.

[DELAUER] Well, theater C³ is mostly being focused on two areas. One, the fusion that I talked about, the Joint Surveillance Target Attack Radar System (JSTARS), which is the joint tactical side-moving target-indicating radar that will be the basis for the whole battlefield management aspects of theater C³I. The Army and the Air Force both are buying it. The Army's radar probably will be carried in an OB–1, with the data stream coming down to Army command posts (which, by the way, are soft and we must do something about making those survivable). The Air Force's data stream will come out of their radar which will be at least in a 707—C–18, we call it—and it will fly behind the forward area portion. And those will be the two tactical sensor integration systems.

The communications themselves primarily depend on to whom you talk. They're not really integrated yet. The Tri-Service Tactical Digital Communications System (TRI-TAC), which is the Army tactical system, has been the world's greatest WPA job for a long time, building all these switches. There's a secure voice communications system that the Air Force will use for its fighters. It should be tied into the Joint Tactical Information Distribution System (JTIDS) which is really a Navy system, a tactical information system for voice and data.

After quite an argument, the Air Force joined with the JTIDS team—that's where Service parochialism comes in—and we're getting the son of JTIDS,

or the enhanced JTIDS (EJS), which is the newest improvement of SEEK TALK, the Air Force's secure, jam-proof airplane-to-airplane system. The only Air Force system that might be tied into JTIDS would probably be the Airborne Warning and Control System (AWACS) because they have to talk to everybody. Now we're looking at putting a JTIDS terminal in an F–15, but the F–16s won't have any in my lifetime.

The Army itself has embarked on a big procurement that will end up costing about $5 billion dollars when it's all said and done. It's called the MSE (Mobile Subscriber Equipment). In a sense it's putting telephone equipment in a jeep. It's the lowest end of the communication link with the foot soldier. That system is compatible with most of the TRI-TAC switches, so for all practical purposes, somebody could call from the White House all the way down to get that guy in that particular jeep just by dialing the right number.

The President actually did it once. His call was quite funny. He went out to visit James J. Kirkpatrick, the conservative columnist who lives out in western Virginia, for Thanksgiving Day. He had this new equipment in the car along with Kirkpatrick. The President said, "This is a great piece of equipment, I can call anyplace." And Kirkpatrick got interested, and mentioned one of his sons was on a ship in the middle of the Mediterranean. The President got on the phone and asked for this kid on this destroyer in the middle of the Mediterranean. Faster than you can get downtown Boston, they answered. And the President said he wanted to talk to so-and-so Kirkpatrick. And this kid told his dad later, never to let that happen to him again. His life was never the same aboard that ship. The President called him right down and said hello to him, then said, "I've got your Dad and your Mom here, would you like to talk to them?" We're getting to that level of sophistication, so now we can do that.

... Integration with NATO forces? We're not doing too badly. The biggest integration would be through the German digital system. For a long time that was a tough problem, because the German Bundespost never wanted to go digital. And once an analog man, always an analog man. Finally they decided to change leadership, and now they're pretty much in the digital system, which means they can be reasonably integrated. If we get the **PTARMIGAN** system, the British MSE, it'll be even more integrated with the British forces. But there is a problem, there is always a problem....

PTARMIGAN—a mobile, digital, trunk-switching network developed by the British

[STUDENT] How do you feel about the survivability of C³ on the **SSBN**s?

SSBN—nuclear powered ballistic missile submarine

[DELAUER] Oh, fine, I think. Of course right now, it's very survivable because they're not yet connected, although almost. But seriously, there are only two nodes to worry about—the submarine on one end and the sender on the other. That's the problem with terrestrial C³: there are a lot of nodes all over the place, and the nodes are the tricky part to make survivable; everything else is handled redundantly. But the only really non-redundant node in the SSBN C³ is the SSBN itself. So survivability of C³ on SSBNs seems pretty good.

Now, if you're really talking about blue-green lasers instead of extremely low frequency (ELF), and blue-green lasers are what we're looking for in real survivability, then how to deploy the laser system becomes an issue. It's possible to have a **TACAMO** aircraft deliver it, such as the **E–6**—they're pretty survivable.

TACAMO—"take charge and move out": acronym for airborne communications link with strategic submarine force

E-6—electronic warfare aircraft equipped with surveillance and control system as well as jamming capability

The big issue is to ensure communication with the submarine when it's submerged. That is not quite possible with the TACAMO now. To talk with it, a submarine has to pop up near the surface. Submarines are very good in regard to knowing what's around them, and they're not going to pop up to the surface with a **Backfire** or something sitting over their shoulder, or three or four destroyers sitting out there, or even another submarine nearby. So, I think the survivability is adequate, but it's a question of effectiveness right now. If we are going to take all these precautions we must advise them so that they really can be timely; I think it's getting better, because with the **D–5**, submarines can cover much more of the broad ocean area that's much rougher to cover, so they can keep a safer distance.

Backfire—Soviet medium range bomber

D-5—newest Trident missile

Survivability should be the least of our worries. First of all, trying to retarget everything will take some time. Then, in terms of surviving capabilities, if at that time the SSBNs have to cover targets that were not

covered by the Minuteman or the bombers or the cruise missiles, then it's best just to save surviving capability. The deterrents have gone down the drain, so it is a completely different situation.

... I think the biggest thing we need to work on in the area of battle management is non-nuclear combat equipment that the Soviets can handle by just jamming. Also, I think the second criterion of the deterrent, the effectiveness, has to be demonstrated. If we come up with a command and control system like the one we have in the shuttle, where whenever something goes wrong we sit down for two weeks, they are not going to consider that much of a deterrent; they wouldn't even bother to attack it. Then they'd really be dangerous, because they'd just ignore it. So you wouldn't even have the benefit of warning that an attack on the system would provide. (87, 95–96, 97–98)

13 **DONALD C. LATHAM, "A View From Inside OSD" (1985, pp. 103–23)** *Assistant Secretary of Defense, C³I*

... [T]he Soviets are spending enormous sums of money in the C³I area—and have been for a long time, are paying a great deal of attention to it, and are quite good at it, especially as it ranges from leadership protection and the survival and endurance of the Communist Party, to heavily fortified shelters, to airborne command posts and submarine command posts, and satellites, etc.

... [I]n order to terminate hostility you've got to know what's going on, you've got to be able to communicate with your adversary, and so on. We are taking steps to be able to do all that. Another major imperative is to limit the damage and then, last, to maintain reserves. This last requirement puts another burden on C³I.

... There are a whole series of NCA sites that have communications to and from the forces by satellites and cables and radio systems. The forces are then under the positive control of the President as the National Command Authority. In all of those areas we're modernizing everything—the forces, the communications, and the sites.

What do I mean by enduring C³I? That's a question that is asked frequently. First of all, the uppermost requirement is having absolute control of nuclear

weapons under all conditions and at every level. There's been a lot written by people saying that in the event of a strategic nuclear conflict, if the system were to go out of control it would be like a control system having too much feedback, resulting in weapons being launched indiscriminately. That is not the case, we ensure that such a scenario could never happen by the way we control the weapons and stay connected to them. That's the first major requirement of the system.

[STUDENT] Can you apply this to the theater as well?

[LATHAM] To the theater and down to a nuclear artillery shell, to the lowest level.

[STUDENT] Why do you say that we would have absolute control of artillery once forces have been dispersed to the field and release authority's been given? Why do you assume that we would be able to maintain control once nuclear weapons have been used?

[LATHAM] Well, first of all, you want to be able to release selectively. You would not tell the artillery it could have everything at its disposal. You would release selectively. Maybe only so many rounds, or only a particular group could be released, and the civilian authorities would know the targets they would engage before the weapons were ever used. Down to that level of detail. It's a monstrous decision ever to use a nuclear weapon.

[STUDENT] But if the release authority isn't granted as weapons disperse, you run into the problem that it may be very difficult to grant the authority—

[LATHAM] That's right. Exactly.

[STUDENT] So then there is a problem with giving selective release.

[LATHAM] That's exactly right. And so you've erred on the side of not being able to do it. There is a problem in the control of nuclear weapons in that you have two conflicting requirements. You want to design your command control system so that there is absolute total control of nuclear weapons in peacetime as well as during a crisis, such that they cannot be used inadvertently or in some way detonated by accident. You want the absolute highest assurance of that possible. Yet at the same time, on the conflicting side, you want to be able to release those weapons some day if

you ever had to, and actually have them detonated if you so commanded. Those two kinds of things are in conflict from a technical and operational point of view. So, you have to and would want to resolve that, in our judgment, by erring on the side of safety, reasoning that I would rather not have the system be able to work than just have an absolutely uncontrollable situation. In the case of the artillery shells, if I couldn't get the word through, they couldn't be used; I probably would err on that side of safety rather than the other way.

[STUDENT] What about a situation where release authority has been selectively given already? For example, we'd like to withdraw it now to terminate the conflict.

[LATHAM] That absolutely has to be part of the system. You must be able to do that.

[STUDENT] Well, is there no problem with jamming or interference?

[LATHAM] Certainly. Getting the word through may be very difficult, but you can have procedures where you have selective release for 12 hours, 10 hours, or three hours. Unless you are otherwise told, you will relock your weapons after that time. That's one precaution. In case you can't get through, you tell them to relock, and not only to relock but to report that they are relocked, to send a message on that. And we have devices such that once the weapons are relocked, they can't be unlocked again without higher authority sending the right unlocks. There are many safety features built in.

[STUDENT] What do you mean by relock? How can you recall release authority?

[LATHAM] You terminate release authority. Believe me, there are **locks**, literally. You relock on the weapon, be it electronically, or via software systems, or by whatever it is, that means the weapons cannot be used. You lock them back up under positive control.

For a detailed, unclassified discussion of the "locks" referred to here, see Peter Stein and Peter Feaver, Assuring Control of Nuclear Weapons: The Evolution of Permissive Action Links (Lanham, MD: University Press of America, 1987).

[STUDENT] But does that rely on the unit in the field implementing that relock? In other words, it's not triggered from a hierarchy, an electronic signal going out.

[LATHAM] Not to every weapon. No.

[STUDENT] You would be dependent on the commander in the field, then?

[LATHAM] Somebody would be in the field doing something to take weapons and to put them back in storage or take them off aircraft, take them out of artillery units, and put them into safe containers and then reset the devices that relock them. We have devices on weapons that lock, so that if a terrorist took a weapon and tried to detonate it, it would not be possible. There are various levels of protection on weapons.

... Now let me summarize where we are on some of the initiatives. I've broken these down into the three areas I mentioned earlier: warning and assessment, command and decisionmaking, and supporting communications. First of all, in the attack warning and attack assessment (AW/AA) area, we've formulated a new architecture that is much more robust and enduring than we've had before. General Herres is the chief architect. We're putting in over-the-horizon backscatter radars (OTH-Bs) for complete continental United States (CONUS) coverage against air-breathing threats. The first east coast sectors are almost completed, and the west coast sectors will start soon. We're also putting in a southern sector. Those radars will provide warning and tracking information against air breathing threats, namely, cruise missiles and aircraft. For the Ballistic Missile Early Warning System (BMEWS) radars, of which there are three, the computers and software on all have been upgraded. And we are in the process of putting in new phased array radars at Thule, Greenland and at Fylindales Moor, England.

Finally, we are constructing two more of the PAVE PAWS radars in the United States. That makes a total of four. They "look" outward for incoming submarine-launched ballistic missiles; the one in the southeast will also perform space tracking. In addition, we've block-changed and improved the DSP program that I mentioned earlier, with new satellites that are more survivable and have enhanced capabilities. And we've started studies on the Boost Surveillance Tracking System (BSTS) that will replace the DSP someday. The BSTS is also part of SDI.

DSP—Defense Support Program
SDI—Strategic Defense Initiative

[STUDENT] What is block-change?

[LATHAM] Block-change means that you move significantly from the previous satellite configuration because it begins to incorporate a fairly major set of design changes.

Now let me address the area of initiatives in communications. We have the Defense Satellite Communications System (DSCS III) now in a multi-year contract. The first of those DSCS IIIs is in orbit, operating. We have 14 of those under contract. The second one will be orbited this year. We also have several reserve DSCS satellites in storage in orbit; we keep four DSCS satellites operating continuously around the globe 365 days a year. Another satellite system is the Military Strategic, Tactical, and Relay Satellite Communication System (MILSTAR); that's the extremely high frequency (EHF) system operating up in the gigahertz frequency range. It is in full-scale engineering development now, and a first launch is scheduled for the late 1980s. It will be a very survivable system. It will allow us to put terminals on bombers as well as on submarines and land combat vehicles. It is the first of its kind.

We also have on orbit the UHF military communications satellite known as FLEETSAT. Four satellites, plus other leased assets, provide vital global coverage. Additional FLEETSATs are being procured to maintain the UHF constellation into the far future.

We also have developed the Ground Wave Emergency Network (GWEN)—a low frequency set of towers using packet switching technology to move low data rate messages across the country into command centers. GWEN will provide assured capability of getting short emergency action messages across the C³ system. Then we have the Miniature Receiver Terminal (MRT), which is a new receiver going on the bombers; it operates at low and very low frequencies.

The E–6A is the new replacement for the C–130 TACAMO aircraft that we maintain on orbit 24 hours a day. Not only do we keep a command and control airplane up 24 hours a day in the midwestern part of the United States, we also keep two TACAMO aircraft up—one in the Pacific, one in the Atlantic—24 hours a day, 365 days a year, for assured connectivity to submarines. We're replacing the C–130 that does that job with a new airplane called the E–6A, which is an AWACS airframe.

Lastly, we're also moving into wide-band EHF to carry more data with higher jam-resistance.

In the navigation area there is the Global Positioning System or GPS. Riding aboard GPS is the Nuclear Detection System (NDS). The GPS side of the system will be an 18-satellite active constellation at around 10,000 miles altitude, providing location in three dimensions in real time. So an F–16 pilot, for example, can determine where he is within about 30 feet in three dimensions at any given instant in time. The system can also be used to verify the time very, very accurately. GPS can be accessed from ship terminals, submarine terminals, manpacks, vehicular terminals, and so on. NDS rides onboard the same satellites and would allow one to know instantly where a nuclear weapon went off with an estimated yield and height of burst. With NDS, in the event anything were to happen, we would be able instantly to perform damage assessment, on ourselves and on the adversary. NDS readout terminals on the airborne command posts and other places will provide this information.

. . . There are also other communications initiatives underway. JRSC, or jam-resistant secure communications terminals, are mobile or movable satellite terminals that operate with DSCS. The one commercial initiative is called the Nationwide Emergency Telecommunications System (NETS). It's an initiative that will upgrade and make more robust the public switched telephone network. We've invented a "box" (or Bell Labs has, with our money) that can be put on certain switches. The way the US public telephone switched networks operate is with very, very large switches, then medium-sized switches, and then some smaller ones. The smaller ones are called class four and class five switches. There are about 20,000 such switches in the country. Now, at the moment, there may be only two or three possible routes to connect points A and B (for example, from here to San Francisco). But when we put this box, which is really a special purpose small computer, on a few hundred of those switches, we'll be able to go by hundreds of routes. So having NETS in place will provide a much more robust communications network using those billions, or tens, or hundreds of billions of dollars, whatever we've got sunk into the local PTT.

In the functional area of command and control, we've built, deployed, and delivered four E-4Bs, the highly modified 747 aircraft crammed full of communication equipment that are called the national emergency airborne command posts (NEACPs) for the President. They are deployed now **in the middle western part of the United States**; they're not at Andrews AFB any more. They sit on five minute alert, or at least one of those aircraft does, 24 hours a day, 365 days a year. We are also modernizing the worldwide airborne command and control platforms, and will continue to do that. They are receiving

in the middle western part of the United States Grissom AFB, Indiana

new electronics, new communications equipment, and things of that nature. We have about three dozen of those. We're hardening systems against high altitude electromagnetic pulse effects and we're doing a lot of special studies on how to do an even better job of providing for a surviving command and control function.

[STUDENT] Do you have any of the E–4Bs at Andrews?

[LATHAM] No.

[STUDENT] Do you have any other emergency aircraft?

[LATHAM] Yes, we keep other aircraft that are on special alert to get the President out, but they're small aircraft.

[STUDENT] They don't have all the command/control equipment?

[LATHAM] We have a Presidential support squadron that has special helicopters and things of that nature for coming in and getting him out of the White House if that were necessary. Now, the probability of something like that happening—that is, if the Soviets or some bad guys could so surprise us that we have to panic in the middle of the night to get the President out of the White House—we consider highly unlikely. The US system provides us with the ability to tell if something is up and take much more measured actions anyway. So, I don't look at moving the President as the most probable situation, and that might send a wrong note anyway. . . .

[STUDENT] I'd like to shift away from the strategic to the tactical. Charlie Beckwith, who was the Delta Force commander on the attempted Iranian hostage rescue, commented on the C³ that he had. I'm addressing the system rather than the particular technology; I guess they were UHF satellite terminal packages at various points, but it's not significant whether they were UHF or some other frequency. He said the communications were basically good, and that the interplay went well between the various elements in the hierarchy, and that the command and control structure was a model for jointness. And yet there have been various allegations that, in **Grenada**, command and control could have been better. Some of the stuff I've read in various articles (all of it unclassified) say the radios for some of the ground forces were too heavy and they couldn't keep up, and there were other things about

Grenada—the US invasion, October 24, 1983

air strikes not being well coordinated. From your perspective what might have, or what should have been some of the lessons learned?

[LATHAM] Well, there's **an interview with me** in the February issue of the *Armed Forces Journal International* that asks that same question. And my answer is that we really didn't do the pre-invasion planning that is normally required by the communications and command and control people in order to get various aspects of the communications plan really straightened out—who was going to have what equipment, what **COMSEC** was needed, and all that. So, it was a planning deficiency brought on by the very high secrecy and the short time that they had to get the job done before they went in there. That was really it. The equipment is designed to be interoperable, and there's adequate equipment around. It just was a very closely held, very short-term planning job done. The commander of the whole task force admitted publicly in a speech not more than a month ago that he'd never heard of the PRC-101 radio until about two days before the invasion. That's a hand-held satellite radio. You must know what you're doing with your communications or you're going to get in trouble. So, he had trouble.

an interview with me—"An Exclusive AFJ Interview with Donald C. Latham," Armed Forces Journal International, *February 1985, pp. 54-70*

COMSEC—secure communications equipment

[MCLAUGHLIN] I can see other situations where one might have more time. It seems to me that any commander going into an operation like this, even if he had more time, will still want to maintain surprise. The secrecy is going to be the continuing problem and the losses entailed are in part the price of that secrecy. This is a problem that comes up time and again.

[LATHAM] That's right. There was a trade-off: they made a judgment that secrecy was more important than anything else, and paid some price for that.

[OETTINGER] But wait a minute. That's the sort of fix one is in as of the week, the month, or the year before Grenada. The real problem is when you're in Grenada. Think of it this way: one of the classic elements of the spy story is the phone booth. Why? Because the phone booth is there, and nobody knows I'm walking up to it, and yet I have the guarantee that no matter what phone booth I walk up to I can talk to some place. So, it seems to me that more fundamental than the matter of either secrecy or surprise is the problem that one cannot count on the notion that whatever piece of

equipment one walks up to, whether it's in the clear or encrypted, one has a reasonable chance of reaching some other instrument in the friendly forces. There is the root of the problem. Why can't one count on walking up to a bit of communications gear in the US military and have reasonable assurance that it'll communicate with another friendly piece of communications?

[LATHAM] Well, I think that we're rapidly getting there in most cases. The mean-time-between-failure rate of the VHF combat radios out there today is unacceptably low. So, when you walk up to a VHF radio mounted in a jeep today, turn it on, and hope you can talk to the brigade commander, it may be that it doesn't work because it's failed for some reason. That is a fact of life of all radio systems, and even telephone systems (although we've made these far more reliable over the years, at least in terms of fixed plant).

Now, the new radio that replaces the VRC–12 has got at least 10 times the reliability, so we're more confident now that when somebody uses the radio, he can make contact with another radio of a similar kind, and using the same COMSEC. In some of our aircraft radios now we're getting a mean-time-between-failure of thousands of hours. So the ability to communicate reliably is getting better and better. We're experiencing exceptionally good performance on our satellites. These DSCS satellites I mentioned are lasting years and years longer than their life design had intended. So you can have some confidence, as Beckwith did, of being able to have a satellite terminal that will in fact work over that satellite. We used those in Grenada, and Beckwith used those—both **SHF** and **UHF**—in Iran, and they were used in Beirut. And they worked pretty well. They had good clear voice, good quality voice. So, it's getting better.

SHF—Super High Frequency
UHF—Ultra High Frequency

Still, if you want to talk across Services (and that came up in Grenada, about cross Service communications with different types of radios, using different types of COMSEC equipment) you're probably going to get in trouble. And that's what happened in Grenada, because they didn't have the right stuff there; they hadn't planned for it. The special forces brought in their own communications, which were unique to them. So, carefully planning this out could have solved a lot of the problems, but again, there was an insatiable desire for information, so people were trying to pass tons of information back and forth both ways, and things got congested and broke down in that sense too.

However, we do have a program called Joint Interoperability of Tactical Command and Control Systems (JINTACCS) which is a joint, cross Service

effort to make sure that tactical command and control systems are, in fact, interoperable. We will spend about $100 million on that in 1986 doing tests, promoting standards, setting up various testbeds, doing simulations, and trying to be the keepers of the interoperability. (103, 105, 106–07, 108–09, 111, 120–21)

14. **CLARENCE E. MCKNIGHT**, "C³I Systems at the Joint Level" (1986, pp. 1–30)

Director, Command, Control, and Communications Systems, JCS

As we move across this increasing spectrum of capabilities and threat toward the 1990s and the Strategic Defense Initiative (SDI) programs, we have to look at the tremendous demand that all of this is placing on command and control systems, recognizing that most of them have evolved from existing systems and are actually just extensions of what is already there today. So if you give a dictum that you want all of that to be surviving and enduring, you're looking at systems that become more and more and more complex as we start our electronic expansion around the world.

... When you look at C³ systems, you have to take into consideration their drivers, all of which have an impact on the national strategy and the elements of the military strategy that were derived from those national objectives. Naturally, technology drives C³ systems. So does where we are in the world, our geographic responsibilities. A big part of the equation as far as the C³ systems are concerned and how they are put together has always been the land mass of Europe. As for architectures, in 1962, when the Defense Communications Agency was created, everyone expected a big metamorphosis, big architectures to be formed. Well, what happened is that they merged the administration and command networks in the Services, and they've been laminating those ever since. The new kinds of architectures are the satellite constellations and we need to look at what we can do to harden those and to move into other arenas that are being forced into being, such as the joint and combined interoperability networks, constantly pushed by the threat. But we have to look at these new architectures in context with what already exists, and that's a big chore because we are heavily capitalized in older equipment, particularly in our analog equipment. It would be nice if it were all digital equipment, but we have an awful lot of analog equipment.

When you look at the connectivity between the National Command Authority and his commanders in chief who are his warlords, if you will,

you have an expansive amount of territory to cover for that connectivity. It's global. And you can finesse it with force structure in other areas but you cannot finesse it with command and control systems. You can do a lot of things with wires and mirrors on a limited exercise, but if you want to have a robust global communications system, you have to make the investment all over the world.

Now, for you gentlemen in the State Department, you know you have the Diplomatic Telecommunications System. There are many crossovers between the Diplomatic Telecommunications System and the Defense Communications System. But neither one of us has the robust linkage that we would always like to have because we are using national and international systems as the connectivity from all of those systems. We do an awful lot of handshaking around the world as we try to create systems that can posture our forces and also accomplish the diplomatic nuances necessary for deterrence.

... [Y]ou can't take one piece of technology like fiber optics or microchips and say, "That's the solution," because they're all part of subsystems; they need to be integrated into a much larger mosaic.

... One of the other key things in our C^3 systems today that I need to comment on, and that I've had to talk to some irate Senators about, is the interoperability issue. I don't believe everything should interoperate. Certainly, our industry does not permit us to make everything interoperate because many times equipment is built on a competitive basis, with some features added specifically to make them unique so they won't interoperate. We really need to ask ourselves the why, how, where, and when kinds of questions so that we get an overlapping of the Services' needs and tie their systems together in such a way that will make us more able to create the entire architectures without having to worry about everything. We tried in **TRI-TAC** to build **"purple" equipment** and we found it's very expensive to do so. It's much better to build equipment that will work together by defining the interfaces because there are so many unique Service requirements that you cost yourself out of the arena very quickly, which brings me back again to the off-the-shelf kind of equipment.

TRI-TAC—Joint (Tri-Service) Tactical Communications Program
"purple" equipment—intended for joint use (Purple represents a blending of the uniform colors of several Services.)

... We really have to look at our master plans and see whether they are achievable across several administrations. We want to try to design things so

that they don't hiccup. We should be as apolitical as we possibly can because our C^3 planning is a national resource. It spawns an awful lot of technological prowess. The military Services have always trained their technicians very well; when they go into the industrial base, they become very productive citizens using that technology. The kinds of architectures that we develop—the master plans of the CINCs (Commanders in Chief), and the master plans that we produce—should be so logical that they are achievable regardless of which administration is in office. As a final shot, I'd like to think that we could get some kind of a balance in the systems that support intelligence and command and control. That is, balanced in the perception of the Russians, such that we have a credible system out there for the tactical forces, a very credible system in the strategic world, and a crisis management system that is second to none, giving us the warning and the time to negotiate ourselves out of an unwanted war. . . .

[STUDENT] Sir, you mentioned earlier that you thought tactical C^3 was relatively neglected as opposed to Department interest in strategic C^3. I suppose you might have in mind something like the correlation between tactical doctrines and C^3 requirements. The newer doctrines, say, of battle in Europe, like air/land battle, would probably have more stress on the requirements in that regard, or is that not the case?

[MCKNIGHT] Most definitely. Air/land battle has tremendous requirements because you need CD (controlled dissemination), you need to synchronize. To give you an analogy, in air/land battle you are no longer in a football game of opposing forces across from each other, but more like a soccer game where you're entwined, and there is a lot more mobility on the battlefield. The essence of air/land battle is flexibility and synchronization, and that requires an awful lot of command and control support systems.

[STUDENT] Is that necessarily reflected in the procurements, the buildups into the organization of C^3 systems so far, or is that only in the offing?

[MCKNIGHT] No, it's in the offing right now. I think you will see far more mobility stressed on the battlefield. We certainly are pretty well tied down like the Lilliputians with the very heavy equipment and the wire systems that today prevent us from having rapid movement of our command centers around the battlefield. The mobile subscriber equipment which they have just started to procure should in the very forward areas give much more flexibility in moving command posts in more compressed time frames. (3, 6, 8, 17–18, 23, 24)

15. **JOHN GRIMES**, "Information Technology and Multinational Corporations" (1986, pp. 135–49)

Director, National Security Telecommunications and Director, Defense Programs (C³), NSC

Because of ... vulnerabilities and demands for ensured connectivity, companies like AT&T have network control centers to maintain the system integrity, and restoral for everything from an earthquake to a regional event, like tornadoes and hurricanes. Other carriers have established so-called operations centers or control centers. Electric power companies are looking at the same thing. They do it primarily for economic reasons, because their profits are based on revenue; when you lose major customers for a long period of time, you lose revenue. Dissatisfied customers tend to switch to a different provider; although the electric power companies in this country still have a monopoly, the telecommunications people do not any more.

As most of you realize, the government does not own a pervasive and independent electric power source or its own telecommunications systems. We get about 95 percent of all our communications from the private sector, i.e., telephone companies. One of the things we've done with both the power industry and the telecommunications industry is to make them aware of the vulnerabilities of their respective industries and encourage them to develop contingency plans and capabilities so that they could restore critical service in case of a major disruption. "Critical service" is defined according to national priorities, depending on what kind of service is being restored and in what situation; the priority may be public safety during a disaster, or service to the Defense Department during a wartime situation.

The electric power grid is now almost totally *computer* controlled over communications links. They have had some brownouts and blackouts due to failures of this technology; while it has improved the overall operating efficiency of the system, it can create tremendous inefficiency when it breaks down. An example—on the West Coast, in the summer, power is shared from the northwestern part of the United States down to the Los Angeles area, to run the air conditioners. In the winter, it is reversed and electric power is shared to the north to run the heaters. The control is done by computers and telemetry flows over communications links.

... Let me first make a point on survivability. Survivability can be regarded as a matter of life and death or as a matter of improvement by degrees. Take the national power grid system. There's a couple of things that you can do. You have single point failures. One of the things we are finding out is that

power plants are not as critical or as vulnerable as substations, which become critical single points. You can do some things today at power plants to take away that vulnerability by using network design. Previously, that kind of solution was not feasible, whether for cost reasons or for regulatory reasons, where the Public Utilities Commissions (PUCs) wouldn't let the companies do that. We have what amounts to a national power grid system.

To come back to your point about integration, the system does become interoperable, but we try to make sure that the loss of one part of it does not take the other part down. We try to take some degradation into account within the integrated system. However, that means that if you do lose a part, you have to have a plan. For example, maybe you're getting power from the Canadians and you lose that as a major source, but you have an alternate plan; in the case of the Northwest, there might be a connection into the Colorado area, for example.

So while parts of what you're saying are correct, I think the systems are so designed in this case as to allow for the danger that you mentioned. We talk about interoperability, rather than integration. A lot of times, integration implies that if you lose one part, it drags another part down. In telecommunications we have some of those kinds of problems, because when you're operating at megabits, synchronization is critical in order to maintain what we call bit integrity. There's a master timing source; somebody always has to be able to clock. We are looking at ways to make sure that the system maintains its integrity because under the new telecommunications industry structure, with so many long-haul carriers—the new MCIs and GTEs, and then the satellites—there has to be one very accurate clocking source, or else you get buffering. It's these kinds of things we have to address to prevent a system failure. In a digital system, if you lose the clock, it's catastrophic; in an analog system it is not. The old frequency division multiplex allowed for slow degradation.

Today, one of the vulnerabilities of a digital system is that it's almost binary: It's either there or it's not. By the way, a very major concern of ours in networks that support national systems is interoperability or alternate routing capability. It used to be that we operated through what we called frequency multiplexing. Today we do time division multiplexing. The difference is that frequency multiplexing worked like your radio; you changed frequency to pass different types of data. Today you code a bit, which is in a serial stream, interwoven with a whole bunch of other information, not even all your own information. When it gets to the other end it's multiplexed out. There's a lot of room today for error and degradation, and you can do things in the system to keep the highest priority systems on the air, whether they're

circuits or customers. Today you can lose everything, so you must plan your systems accordingly. That applies to maintaining telemetry on a hardware system as much as to transferring information for a customer.

[STUDENT] Is there a general theory that ties together all these concerns about system vulnerabilities and integration?

[GRIMES] Well, again, the vulnerabilities can be categorized. A corporation that is revenue-based is looking at it for lost revenue, and will go some distance toward ensuring against failures according to the costs and benefits involved. That's an interesting calculation right now with the increase in terrorist activity around the world. Fortunately, we have had little problem in this nation. Some years ago we had a thing called the Monkey Wrench Gang running around out west. They were environmentalists concerned about the big transmission towers that run across the nation, both the metal and the wooden type trestles, the very tall ones. They took blowtorches out there, in the case of the metal ones, and cut them off and just let them hang. It was a very costly proposition. In another case, they took chain saws and went out where there were telephone pole trestles, and cut those off and let them dangle. They took high-power rifles and shot up transformers and substations. It took quite a bit of time to replace one of those transformers.

Again, that's very localized, and you can do things to get around that loss. If you take a larger event, a tornado or an earthquake in California where you take out a hunk of the system, then you have another type of restoration you've got to consider. In the case of California, for example, communications companies try not to put much cable around the San Francisco area because earth shifts tear the cables. They use a lot of microwave. Also, those shakes "detune" the microwave beam. Companies do various things, like deep piling in the ground, to prevent that. So there are things you can do to guard against some kinds of disruption. But for cases like the Monkey Wrench Gang and terrorism today, physical protection of those facilities has now become a major issue, and corporations are going to have to start doing something about it. Some companies put chain link fences up, with no lights or open gates. Just as you see in Washington with the sandbags, etc., and in airports with the metal detectors, you're going to see that kind of protection as a common practice, unfortunately.

If you carry that one bit further into a wartime situation, we have national policy and plans and organizations in place to handle such things as restoring critical functions or reconstituting the systems. In the case of communications, it's the National Emergency Telecommunications System that works with the 22 federal agencies to set up priorities, so that we can restore those

most critical systems that we need. In the case of the power system, the Department of Energy has worked that out and coordinates with the power companies on a daily basis.

... My point is that with this increased proliferation of computers in every aspect, in the medical area, logistics, transportation, etc., our dependence on them is causing a major strain on our communications capabilities, especially in the tactical environment. When you're operating in a benign environment, your pipe is very large. When there's a disruption in that pipe and you've got to go down to half the size, setting priorities for what is the essential data you need becomes very critical. Unfortunately, people think that they're going to operate in a stressed environment with the same amount of information as they have in peacetime.

The Moscow Hot Line operates in a very controlled environment limited to two individuals, and was designed to pass very critical information on an accident or an error made by either party. Its purpose was not for going to war, but for preventing war. Whereas with these very pervasive systems scattered in 16 divisions or air wings around the world, so much information is flowing out there to sustain that force that the systems now in use during peacetime are going to cause problems when you get into a stressed environment and have to disturb the network.

[OETTINGER] Let me see if I can get you to speculate a little bit as to what the remedy might be. If I go back in history, it seems to me that it is precisely for that reason, among others, that the notion of doctrine evolved in the military: What do you do if the horse and dispatch rider don't get there? There are certain things that you do when you get cut off. To some extent, what you're describing implies having lost sight of some elementary principles. If so, then maybe a correction should be on its way. Or have we not yet had enough experience in stressing these systems, with the pipelines breaking down, for people to have relearned and reinvented doctrine or modes of operating when they're cut off from the pipe?

[GRIMES] I think we're now recognizing the need for doctrine and procedures to deal with stress environments and communications disruptions. The two technologies of computers and telecommunications have merged now to the point where that need has arisen. It used to be that the computer people did not coordinate with the communications people; they just took it for granted that the communications source would always be there. But we got in such dilemmas in the Army and elsewhere that those functions have been merged, because it was recognized that neither one could go without the other in today's distribution systems. I think it's a self-correcting

problem. We're seeing some efforts now, and progress is just a matter of time. We just have to hope we're not faced with a life-or-death situation before we get there. That's kind of the critical point. We do have a propensity for uprighting; we swing one way or the other, and somehow over a period of time, our checks and balances kind of set us straight.

[MCLAUGHLIN] It seems to me that part of the problem is the continual need to reinvent common sense. Your logistics pipeline is not going to be there either if someone's attacking it. That's why you carry certain stores and ammunition with you, on the assumption that you're not going to get resupplied on a daily basis or whatever in certain situations. That logic is basic to contingency planning in general. But it seems as if every time we put in a new technology out there with new opportunities for communicating, we keep forgetting that we won't have all that pipeline available and that we have to plan accordingly.

[GRIMES] Tony used the word "doctrine." Doctrine, of course, is used more in the military than in other federal agencies or in corporations. Doctrines, goals, and objectives are somewhat similar in a sense, but doctrine means, "This is what we're going to do and how we're going to get there." In most government organizations I've been associated with, as computers became available, people never went out and used the computer as a more proficient tool to improve the process. They simply automated the existing one, two, three, four, five steps involved in a travel voucher or transportation form. Now, I think it's generally understood that with all the edit functions and accuracies of computers, you can do away with steps two through 10, because the computer does all that for you. Ten or 12 years ago, I pushed very hard to have the office of the Army Adjutant General at Fort Benjamin Harrison start looking at what office automation computers would do, because they put out all the procedures and regulations on general, common user forms, personnel records, and so forth. If you automate that record-keeping then you eliminate a whole lot of functions; when you do that efficiently you also reduce the amount of data that you have to process or transfer. That's starting from the very beginning: You lay out what you want to do and you take an analyst in there and say, "This is how you do it," and then you write your code around it. That kind of process is starting to police itself. Again, you've got more people who understand computers and their applications, whereas previously there was always just a handful of experts around.

[MCLAUGHLIN] The pattern you described has been very common in industry. It has been our contention for some time that if you went out and did a methods study preliminary to buying a computer, you would wind up

saving all the same money without buying the computer at all; the computer simply provides the icing on the cake. The general pattern is that people tend to start by automating what they've already been doing, and then only later do they rethink the actual process once it's automated.

[GRIMES] Another point that we haven't talked about yet is the trend toward establishing corporate communications centers. It has been brought about by the structural change of the telecommunications industry in this country. As most of you know, about 80 percent of the network out there is owned by AT&T today. Of the rest of it, about 10 percent is MCI, and another eight or nine percent of it, maybe not quite that much, is GTE and U.S. Telecom, while the rest is strewn about. The concept of end-to-end communications changed with deregulation, whether for a computer, a telephone, or any other information system. Corporations have had to change the way they do business. Companies like General Motors and American Airlines have all had to go out now and develop a corporate infrastructure in order to maintain end-to-end communications for the various information systems they use in their day-to-day operations. Cost was one important reason, as I mentioned to you earlier. It used to be that you went to one vendor, AT&T; you told him that you wanted to go from A to B, whether or not you knew anything about 2400 **baud** or 4800 baud, and AT&T would provide that service and just send you a bill. Because of increased costs and rapid change in regulations in the competitive marketplace, people are now out there shopping around for cheaper service.

baud—measurement of the data transmission rate

The result is that corporations not only have added a vice president for these functions, but they've also had to go down and put in what we call control centers, staffed with smart people who know how to order that service. In some cases, they have gone out and built their own systems, or are buying dedicated systems, because it's much cheaper to do that. But if you do that and you want to maintain end-to-end connectivity, you've got to have an infrastructure in order to restore service during an outage. Again, that means you have to build yourself a little control center with competent people in there. You've got to be able to isolate the problem, whether it's the computer or whatever. You're seeing a major trend in the environment for that reason. That's a part of information systems.

A prime example of what happened in government is the case of the Federal Aviation Administration (FAA) at Oklahoma City. Oklahoma City is probably one of the largest nodes for communications for our federal government

for administrative purposes, and the FAA was only getting service from a couple of major carriers. When they were required to go out on a competitive basis and get service from other carriers, and had to operate with the local exchange carrier and install their own modems on the ends of the circuits, they got into some real difficulties to the point that they had to build a control center and staff it with five people 24 hours a day. It's costing us taxpayers a pretty good bundle to maintain that reliability that we wanted from end-to-end service. In the case of the FAA, even though it's an administrative center, it involves some critical things that have to be done overnight, like sending spare parts to radios in a Los Angeles airport. Also, it's the library, if you will, where accident information is deposited and those kinds of things....

[OETTINGER] You've been talking about the cost to the taxpayer for these control centers, network management services, etc. Are you aware of any studies or do you have any impressions as to whether or not, in compensation for that cost, you've gotten more reliability? This goes back to some of your other points about redundancy, etc. The Bell System made a point of having alternate routing and so on, but one could imagine that a decentralized network with these little control centers here and there could be more robust. It could also be more chaotic. Or it could all just be an illusion: everything might rely on the commercial control centers underneath, as a system is no better than the underlying network. From where you now sit and have sat, are you able to form any judgment as to whether we've had a net gain or loss in robustness?

[GRIMES] If you had asked me that question a year ago, I'd have said we had a net loss, but we've grown in that area of expertise and we've put into place some functions to overcome that difficulty in the government. I'd say all things are about equal now with where we were three years ago. I'm talking primarily about the critical command and control type of information systems. Today the federal government gets about 90 to 95 percent of all its communications from the private sector. As I mentioned, AT&T probably owns about 80 percent of that 95 percent. Anyhow, because of that dependency in the federal government on the private sector for what we call national security and emergency preparedness (NS/EP) circuits and services, we have had to establish a capability in Washington such that, in the event that we did have a national emergency, rather than turning to one vendor for end-to-end service, we would have a national coordinating center in Washington to overcome that deficiency that grew out of deregulation. Although the government paid for the facilities, the 12 major carriers of this country have individuals posted there at no cost to the government, to ensure that service is continued or restored, or that a new high-priority service gets installed. That center does not coordinate the total telecommunications

service for the government, only the most critical, and that's a very small percentage.

I haven't seen anything to indicate that we have better or worse service today than three years ago, other than that there's a lot of confusion in people's minds outside of those who deal with telecommunications on a daily basis and understand that relationship between the two technologies of computers and communications. I can't refer to any studies. I will add one other aspect to that: Under the National Security Telecommunications Advisory Committee (NSTAC), we're looking at the network to see where we can do some smart things to restore service between corporations. But, again, that's only for national security; that's not just for anybody's use. Yes, we have done some things to make the system more dynamic, and yes, decentralization may give you some improvement in robustness because it gives you other alternatives. I don't know of anybody who has done any study, or analysis, or measurement of that improvement or degradation. (137, 138–39, 144–46)

16. **FRED R. DEMECH, JR.**, "Making Intelligence Better" (1987, pp. 125–46)

Career cryptologist; former Commanding Officer, US Naval Security Group Activity, Edzell, Scotland

When I first started in the business, communications were less than 100 percent reliable. We depended on troposcatter systems, and it was just horrific. Today we have all these great systems. Is that the answer? Again, I think it helps tremendously, but let me tell you some of the problems which exist today. You don't uncover these until you're part of it. There are certain key installations in the defense establishment that depend on the telephone systems of host countries to pass messages. Messages that say "launch your weapons." Or messages that are in the form of an alert to a unit that says you'd better look out because you're in jeopardy. That is a startling revelation. That is incredible. Once these things are uncovered people start to do something about them, but it's not easy.

•

Then you go to satellite communications to offset that; systems where you have control of your own satellite terminals in your back yard. What about the vulnerability of the satellite itself? So when Donald Latham comes and says we're going to harden the satellites and make them more survivable because they can move and do other things, then you say, "How much does it cost to launch one of those?" It's $100,000 per pound, and you keep adding, and these are some of the problems. But they have to do them to try to have a survivable system.

Will the information be available in time of conflict or war? A problem all the time. Or in business at the time of all these takeovers and stuff like that, are you going to have the information available? I don't know if you will, but a lot of people are trying to do their best to make sure that information is available. Again, not an easy situation and we don't learn well from previous mistakes.

In the 1960s, the Sixth Fleet Commander, Admiral Kidd in the Mediterranean, used to die for information. The system was clogged up. He couldn't get information. Then every day he used to see this plane flying over the Mediterranean. It was an Air Force reconnaissance plane. It used to dip its wings to him. That plane had all the information he needed. They couldn't talk. Simple solution and a couple of young officers got medals. They put a compatible communications system on the plane and the ship. They solved it. The people thought they were heroes. Twenty years later, the same problem. A different part of the world; Air Force planes flying over a Navy ship. They can't talk to each other. You fix it by doing the same thing that was done 20 years ago. We sometimes just don't learn our lessons about communications problems.

One other thing. I remember an exercise conducted by a potential adversary. They must have known something, I think. They didn't practice any emission control. All their emitters were on. Obviously, our system collected all that surge in information. They sent it to the intermediate nodes to be processed and then forwarded on to Washington. So much information was passed that the intermediate nodes shut down. The computers couldn't handle it. You're talking about 2400 baud circuits and things like that, and the information was stuck because they couldn't get it through. It took days to get it to Washington. A big problem. A lot of people were concerned. How do you fix that information? How do you deal with it? Almost as if the adversary knew that we couldn't handle that information, and did it to test it.

Being in the business, knowing a little bit about the Walker espionage case and some other espionage cases, who knows, maybe they knew we couldn't handle it and did it on purpose to test the system. I don't know if that is really the case, but it could be (13:35)

3

Improving C³I

Headlines about waste and fraud—from overpriced toilet seats to million-dollar kickbacks—imply that some common sense, coupled with hefty penalties for wrongdoing, will cure the ills of the Department of Defense's purchasing system. Unfortunately, simplistic approaches and simple solutions tend to compound the system's problems.

For example, if expensive toilet seats are the issue, a "simple solution" might be to set up an office to oversee the purchase of toilet seats. Initially, the office would examine every "system" recommended for DoD purchase to make sure it did not include unreasonably priced toilet seats. However, if past bureaucratic behavior is any indication, eventually the staff would expand and the office would take on additional functions. There might, for example, be a quality control branch charged with designing tests to determine a given seat's resistance to stress; that, of course, would mean that another branch would be needed to do the actual testing.

If one were to take the number of "systems" purchased annually by DoD; multiply that number by the number of components in each system; multiply the resulting product by the number of management levels tasked with oversight functions; and multiply that product in turn by the number of staffers found in the average government agency, one might begin to get a sense of how "simple solutions" grow into massive headaches and how toilet seats developed according to government specifications end up costing hundreds of dollars.

The most critical problems of the DoD purchasing system are the time and cost overruns on the big programs—the multi-billion dollar programs that are obsolete before they reach the field, that don't do what they were designed to do, and that cost ten times as much as they were originally projected to cost.

The extracts in this chapter illustrate the problems inherent in the present DoD purchasing system, highlighting the special difficulties that arise when a C³I system—not a new weapon—is needed. Who in DoD pays for C³I when the Air Force needs more planes, the Army

needs more tanks, and the Navy needs more ships? If you put the responsibility for acquiring new C³I systems at the Joint Staff or DoD level, you must put the funding there too, and doing that will take away money the Services see as critical. Who do you get to prepare design specifications when the users and decision makers don't understand the technologies involved and the engineers are more concerned with state-of-the-art products than the users' needs? How do you sell C³I requirements to congressmen who are awed by the turning radius of a new fighter or the "hard kill" capacity of the latest tank, but are unimpressed by a more secure radio system?

On the positive side, some trends occasioned by rapid technological changes in C³I development might point the way to improving the overall acquisition system. For example, it frequently makes more sense to buy C³I systems "off-the-shelf"—that is, to buy commercially developed systems—rather than to go through the usual acquisition process of determining needs, devising specifications, seeking bidders, and so on. The latter process now takes 10-12 years and almost inevitably results in fielding obsolete systems. Now, if off-the-shelf purchasing makes sense in terms of C³I, might it not also make sense in other areas of rapid technological change? While it's not possible to buy a new fighter off-the-shelf, it may be possible to use that approach in buying the components that go into that aircraft.

Another trend is multi-year procurement, a kind of bulk purchase. If we project a need for 1000 farkles per year for the next ten years, we may save a lot of money by buying 10,000 farkles now, rather than spreading the purchase over ten years. The maker of the farkles saves money by setting his production line up once and keeping it going long enough to produce all 10,000 units—as opposed to setting it up for two months every year for 10 years—and he passes a percentage of the saving on to us.

Bulk purchase is not, of course, a new idea. It's long been popular and productive in the private sector. Government, on the other hand, is understandably and unfortunately more short-sighted: in government, the focus is on this year's budget, not the budget for the next ten years. If we've got $1,000,000 to spend, it probably makes sense to split the money between guns and butter, even if, by doing so, we're missing the savings involved in buying two years' worth of guns. In essence, it comes down to being a matter of priorities.

The rate of change in C³I development can add an additional wrinkle to the question of priorities. If we buy a new radio for the

Army and plan to keep that radio in service for ten years, we may need to buy 10,000 units of a particular chip used in that radio for replacement purposes. If, in order to save money in the short term, we buy 1000 units a year, we may discover in the fifth year that the manufacturer has stopped making that chip. It may be that by the fifth year the chip is so obsolete we're the only ones buying it. And the number we buy each year may not be high enough to justify keeping the production lines open. At that point, we're faced with a dilemma: do we scrap the radio and buy a new one, or do we open our own chip production line? Either alternative will be very expensive. The rapid pace of change may, therefore, force government to look more closely at the issue of multi-year procurement.

While "off-the-shelf" purchasing and multi-year procurement may be useful options in some cases, they're certainly not cure-alls for DoD's purchasing system. If you're not careful about off-the-shelf purchases, you may end up with a lot of advanced systems that won't work with each other. By the same token, multi-year procurement could cause you to buy ten years' worth of a product that will be obsolete next year.

There are no "simple solutions" to our acquisition problems, in C³I or any other area. Procedures are never adequate substitutes for common sense, and, unfortunately, large bureaucracies have little choice but to operate by procedure.

Extracts

1. **WILLIAM ODOM**, "C³I and Telecommunications at the Policy Level" (1980, pp. 1–23)

Military Assistant to the President's Assistant for National Security Affairs

Who do you think pays for the **JCS** and the **CINCs** and the President's command and control—or, to put it colloquially, their telephone bill? The military Services. And this creates enormous budgetary and political strain within the Defense Department. If the Air Force has a choice between buying more airplanes or providing a command and control airplane for the President, and providing more radios and more **ADP** capability for control of the center of the JCS, they prefer the airplanes, not the control. The Army prefers tanks to paying for the President's White House communications system. The Navy has its preferences along the same lines. So there is, in the way the Defense Department budgets are developed, an inherent bias against funding JCS-level, Defense Department-level and, certainly, NCA-level communications. I learned that when I thought I could take two or three enduring elements of the **WWMCCS** program and try to push them through. I fought those right down to the end. Friday night we have the budget issues nailed down, but by Monday morning they were pulled out. Some Air Force staff experts had gotten to the WWMCCS Chairman on Saturday, and I was left with no programs on Monday! (12)

JCS—Joint Chiefs of Staff

CINCs—Commanders-in-Chief; here refers to commanders of the various military operational commands

ADP—Automatic Data Processing

NCA—National Command Authority; the President or a successor

WWMCCS—World-Wide Military Command and Control System

2. **LEE PASCHALL**, "C³I and the National Military Command System" (1980, pp. 67–86)

Consultant; former Director, Defense Communications Agency and Manager, National Communications System

One . . . caution: whether it's a command and control system or a management information system which simply displays from a point-of-sale cash register in the store and makes an adjustment in inventory and billing when the keys are pushed, don't leave it just to the technocrat. If you do, you will get a very exotic system that may or may not do what you want. Incidentally, I speak as a technocrat—those are my biases, and you should know that. But the fact remains that if the user cannot define his information needs and make them understandable to the system designer (and that's not always easy to do), you're in trouble instantly. Defining information needs is the first and toughest task of building an automated system, whether it's a military command and control system or a simple point-of-sale management information system in a department store. And it's not often done very well.

. . . [M]ultiple users' needs often conflict, violently at times. Take the military case, with which I am, of course, so much more familiar. The Army fights from the field, the Air Force fights from its base, and the Navy fights from its ships. So to the Air Force air bases, and the communications connecting them, are very important. The Army is much more concerned with its communication when it deploys into the field. It doesn't care so much about the survivability of its camps, posts, and stations. The Navy, of course, fights at sea. They all fight at different speeds and with different degrees of navigational accuracy. The result is that when you try to build a tri-service system for the Army, Navy, and Air Force, you've got three different speeds to contend with, three different geographical environments, three different doctrines, and indeed, three different languages. So multi-user systems are very difficult.

One other thing about multi-user systems like the Worldwide Military Command and Control System and the Defense Communication System is that since they are joint, the first question that emerges is, who is the sponsor for budgetary purposes? Now the Army, Navy, and Air Force, generally speaking, want to buy, respectively, tanks, ships, and airplanes. They aren't all that enthused about spending a lot of money on the Defense Communication System or the Worldwide Military Command and Control System. DCS and WWMCCS must compete in the Service budgets and with hardware that the Services are obligated to provide under the terms of the **National Security Act**. So first you must find the sponsor for a thing like the Defense Communication System or the National Communication System.

National Security Act—1947 act which established the Department of Defense

... Those rules are built so that DoD spends most of its dollars on ships, tanks, and airplanes; they don't fit command and control systems very well. Now you have the problem of justifying to the Congress a host of little programs: a **VHF** communications system, an **HF** communication system, a **VLF** communication system. And the Congressman sits there and says, "Why do you need three? Why won't one do? Why do you need computers here, why don't you use those computers over there?" So what you have to do is fit all these separate program elements under some sort of umbrella description—and the current title for that in Washington is architecture. So we have a WWMCCS architecture, a military communications satellite architecture, dozens of architectures; and they haven't really met the need yet, because we still think of them as separate little programs that you're acquiring—this particular kind of hardware for that particular use. Its relationship to the other pieces of hardware, and their particular use in the total context of C³I, aren't readily apparent. Last year, in the 1980 budget, 63 separate program elements were submitted under something called the Telecommunications and Command Control Program. Half a billion dollars were cut from those 63 elements. One of the lessons **Dr. Dinneen** drew from that was they had not justified those 63 elements in terms of all the other elements.

VHF—Very High Frequency
HF—High Frequency
VLF—Very Low Frequency
Dr. Dinneen—Gerald P. Dinneen, Assistant Secretary of Defense for C³I in the Carter Administration

It will be interesting to watch. Dr. Dinneen made a speech in December and one in January, and has had an interview in the January *Armed Forces Journal*. It appears to be a very serious, conscious effort on his part to justify all these separate little programs under one overall rubric, so that Congress can see the relationship of each one to the others. Very often if you eliminate one it affects the others in ways that are not readily obvious.

[OETTINGER] There are those who would argue that if you make it all visible it all becomes vulnerable as one unit, while if you put the items on different shelves some may survive even if a couple of them die, and you may be able to recover some of them later on. So that there's perpetual tension, it seems to me, between what you've described and alternative bureaucratic strategy.

[PASCHALL] ... So managers tend to protect themselves. The most successful program manager I've seen in recent years is a close friend of mine. He was a very successful man—since he's a friend of mine I can say this,

and I won't identify him—beyond his intelligence or, really, his capabilities. The reason was that he had a thing called management reserve, and when he went in with his budget for a particular program, he fought for management reserve. He estimated his program fairly carefully, he cranked in inflation and all those things, and then he said: "This is a highly technical, highly complex program, I need a large management reserve," and he fought for that. The management reserve was simply to pay for the cost overruns and schedule slippages he knew were coming. So he devoted his sales effort (incidentally, they don't teach salesmanship in the war colleges and they should, to further an officer's career if for no other reason) to selling management reserve. His **Selected Acquisition Report** went to the Secretary of Defense and to the Congress on schedule, within program. He'd consumed enormous management reserve but it was within program, so he got promoted. That's the kind of games people have to play to defeat the system, survive within it, or succeed within it. And I don't mean that in a derogatory sense. It's practical advice. If you do not include things like management reserve, if you do not take into account the real hard facts of life in budgeting and selling systems, then you should never believe anybody's estimate about what it's going to cost you in time or dollars. I finally came up with another of my laws, which says multiply everything by pi. Somebody once asked me, "Why pi?" I said, "Well, three doesn't sound very sexy and anybody can multiply by two; but pi makes people stop and think, 'He must know something we don't.'"

Selected Acquisition Report—final report in acquisition of a new system

I say that facetiously, but this system forces you to protect yourself in things like estimating—not deliberately overestimating, but you have to provide the cushion, because none of these systems will come in on time and none of them will come in on program in terms of cost.

... Senior decision makers, non-technocrats, get very irritated with the technocrat who's in there with his jargon, pleading for a particular form of spread-spectrum modulation as being absolutely imperative; and how much more does it cost? A couple of hundred million—spread-spectrum modulation for a couple of hundred million is meaningless to many people.

... We've talked about the value of command and control and management systems in improved management—saving money, using systems analysis techniques to make investment choices. It's very hard to quantify the benefit you get by spending a million dollars on a command, control, and

communication system. In terms of numbers of dollars saved in buying **F–15**s, people have subjective views about what it's worth. So anyone who sits down to justify what the trade calls a "soft-kill capability"—well, computers don't kill very much, compared to a "hard-kill capability" like an F–15 or an **A–10** or a tank. The systems analyst can do marvels with the tank—probability of kill, first sighting; add a laser or a laser designator to it and the probability of kill goes up to a measurable degree. It's harder, though, to quantify the benefits if you add another radar which gives you a second way to identify a Soviet missile and decide that it is indeed aimed at you. People who deal with C³I systems analysis and cost-benefits studies would be much happier if they had some way to do that. (69, 72–73, 75, 77, 82–83)

F–15—fighter aircraft
A–10—combat support aircraft

3. **JAMES M. OSBORNE**, "Meeting Military needs for Intelligence Systems" (1981, pp. 1–23)

former Senior Vice President, E-Systems, Inc.

From the viewpoint of an industrialist, the increasing complexities of the weapon systems are drivers to increasing complexity in C³I systems. The C³I systems are reactive to the weapon systems, tactics, doctrines, the military uses. As those systems become more complex, the C³I systems become much more complex in response. The government's changing, and I think decreasing, ability to determine and articulate its needs in the C³I area, and to prepare and manage meaningful specifications, is a very serious problem. The changing and, again, decreasing ability of the government service personnel to operate, repair, and maintain the sophisticated systems which are being delivered to them is a very serious problem too, and I don't see any way out of it at the present time.

I am concerned about the lengthening lapse of time between design/development and production, as a consequence of procurement, reviews, test process, and many other things—for example, **MIL–STD–781C**, which is a very elaborate test program. I call it a statistician's orgy. It has to do with the way equipment is tested after it's developed. There is a proper place

MIL–STD–781C—"Reliability Design Qualification and Production Acceptance Test: Exponential Distribution," October 21, 1977

for tests, no question about it. Certainly systems that have just proceeded through design and initial manufacture have to undergo exhaustive tests. But the government is applying the 781C document to the production of equipment which has been produced in large quantity over a large number of years, whose reliability is well-known, established and entirely suitable. The government, after all, pays the bill; one way or another every dime of this is charged right back to the government. And the government, according to 781C, must buy all these elaborate test machines and facilities and use them, and that, I think, is outrageous. There is greatly increased cost associated with it. And because these tests lengthen the procurement time, we're delivering systems which are semi-obsolete when the user gets them.

... Well, it really boils down to this: what are the real needs? What is it that I really want to do? What are the alternatives associated with the needs, to serve as a framework for preparing the architecture, specifications and the like? Can I pick the alternatives that look the most promising, and from them somehow select the best course? (An endemic problem I ran across in most of the programs was that someone had forgotten to do that.) Can I develop the system specifications, subsystem specifications, equipment specifications, test specifications, in such a way that others can understand what they're supposed to do and I can measure their performance? What are the boundary conditions we're trying to work with, in terms of people, time, money, plant facilities, that sort of thing? I can't imagine that anyone in this group would think that those questions are simple in execution. The overriding consideration—at least it has been to me in managing programs—is to try and determine the forcing functions, to quantify and qualify them, to bring the important items to a level of conscious attention and hold them there. And I think that I've just stated one of the principal problems that I see in C³I: it is exceedingly difficult to develop a focus.

In his book *The Mythical Man-Month*, Frederick P. Brooks describes the problems associated with the development of the IBM System 360. It's a series of software essays, but I found it contained many lessons that were applicable to things other than software. In fact it was required reading for my subordinates. He develops the formula

$$C = N(N-1)/2.$$

The problem in communications: C, the number of communication paths, is equal to the number of people involved times the number of people minus one over two, which of course normalizes to one if you have two people. If you have a third person, the communications problem becomes three times as great; add a fourth, and it's six times as great. That highlights the problem of committees. The whole C³I process is riddled with committees, reviews, and more reviews up and down the line, by people who don't share

a common data base. Another book that I like to have my people read is Justice Cardozo's book: *The Nature of the Judicial Process*. Cardozo, who was on the Supreme Court at the same time as Oliver Wendell Holmes, was a brilliant jurist. He wrote on how a judge goes about making an objective decision, and points out that that is exceedingly difficult to do. The decision a person makes is always run through a set of filters (my words, not his). He's conditioned from birth to pick certain paths, he brings certain mores and standards to the decision process; and it is entirely possible for one judge to make an "objective" decision that is entirely different from another judge's "objective" decision on the same issue.

In the case of C³I, people are developing needs and specifications (particularly with the current United States procurement philosophy) lacking a common data base. Indeed people in positions of authority, though they may believe they think like computers, really have their own different data bases too. And even though all these people are looking at the same facts, they reach different conclusions. As a consequence, it appears to me (and to many of my colleagues) that there is a defense mechanism—an attempt to get something sold through the next level, rather than to address the substantive issue itself.

. . . I was Program Manager of the communication systems for **Minuteman**, the sensitive command networks, support information networks, and permissive action links. Five wings of Minutemen were designed with concurrent manufacture, and placed in operation within six years. I was Program Manager of **Autodin**, whose design was begun in 1965 and the last site signed on in 1969. But now it takes some seven to twelve years to crank out that kind of system. You can't help wondering what's happened to us in the meantime.

Minuteman—Intercontinental Ballistic Missile

Autodin—Automatic Digital Network

. . . But that's a procurement itch I've got, more than a philosophy. The point is that there are all kinds of documents saying that the government establishes and quantifies needs, develops an architecture of specification, and follows a specific procurement process; but if industry were to follow that dictate literally or even approximately, it would be out of business.

[OETTINGER] Can you pinpoint why?

[OSBORNE] Because somebody in industry has been working with some government agency, generally, to determine what the needs are. It's highly

informal activity, but it does happen. Somebody has been in there working on the specifications for the systems and equipments. I still maintain—the government will debate me on this, and so will other people—that you can read a contractor's proposal just like you can the Bible. You can read it as a holy book or as a dirty old man's manual, whatever you like to make of it. At that stage proposals are generally cost-reimbursable instruments. Too often, if you haven't been involved in the process from the beginning (where I don't think you really should have been) you simply aren't the guy who wins the job.

[STUDENT] Are we describing a procedural breakdown? Or, given the changes in systems and technologies, is it realistic to think that someone just invents the need now, specifies it, and then puts it out for bid and gets it?

[OSBORNE] I'm saying that, because the development of needs is now so much more difficult than ever in the past, the government usually (not just frequently) lacks the ability to do it by itself. It doesn't have people current enough in the state-of-the-art to know what can be done, or to assess what should be done....

[STUDENT] It's interesting that you are talking about having no forcing functions to cause you to optimize and support your procurement procedures. Such functions do exist in a couple of operational areas, where special project offices (SPOs), for example in the Air Force, end-run almost every normal channel and procurement practice, **sole-sourcing** nearly everything; they do work with their own engineers in private companies, and it's almost like your description of how things were done back in the '40s and '50s. From that kind of project offices have come certain technologies that were designed 20 years ago, yet are still the state of the art. It is interesting that, in the areas where there are very critical operational needs, that old system still works.

sole-sourcing—designation of one company as only available supplier

[OSBORNE] Another good example of that is **NSA**, which doesn't work under the same kind of requirements that are laid on the Army, Air Force and Navy. They can develop and produce their equipment and systems in a different way. As a consequence, some of the best developments I have seen have come out of NSA.

NSA—National Security Agency

... I guess I feel that with intelligent people on both sides of the fence—trained, intelligent people—the specifications issues and so forth can be resolved. Excessive procedures get to be a problem too; they tend to act as an alternative to intelligent action, and can end up as a straightjacket. For example: in one case I was working with an intelligent **DCA** group and things moved smoothly, both on the contract side of the house and on the technical side. In another case, on a program where **AFSCM-375-5** was invoked, the program was nit-picked to death. I remember that one only too well. I made a film for the Air Force at the end of the program; they hadn't asked for it. It wasn't in their budget. It ran for 33 minutes, it didn't even have a sound track. All it was was a series of forklift trucks going across the screen piled with data, and dumping it into an incinerator. There was a little clock down in the corner registering the millions of dollars that had been poured into the program. It caused quite a furor in the Air Force.

DCA—Defense Communications Agency

AFSCM-375-5—"Systems Engineering Management Procedures," March 10, 1966 (withdrawn 1972)

... I would dread being on the government side of the house trying to take a program through all its needed approval cycles before they can even let a contract. And God knows whether they get the system they wanted. Maybe their needs change in the meantime. You try to change something, and you're met with a group of congressional staffers who apparently are free to run rampant through the laboratories, saying "You are giving money away." So you end up not changing things that need to be changed because you're going to get into another approval cycle. I don't know where we developed the philosophy that people have to be prophets, but we have. That's imbedded in a lot of our procurement philosophy now. It doesn't permit change to happen when it needs to.

[STUDENT] ... [P]eople on the government side really don't understand the contracts they let, quite frequently. We say on our contracts "All provisions of **MIL-STD-490** (or -483) will apply" without having opened that document and realizing how generalized it is. We decide what data we want to have by citing every contract data requirements list (CDRL) item. As long as you have every number in your contract, you're safe. That's the forklift problem. Well, somebody has to understand this process and tailor it to the specific situation, and that is what is not happening.

MIL-STD-490—"Specification Practices," October 30, 1968

[OSBORNE] A plan is a living thing. If the circumstances change, the plans change. Don't do your planning just once a year, do it as it happens; maintaining currency is super important. But the government process doesn't really permit that to happen. They don't have enough people who, if you wish to have it happen, could do it anyhow.

[OETTINGER] Let me try to rephrase this. Suppose you express a need for a system delivery—say, **AEGIS**—years too early. You get turned down. Is it a bad idea because you wanted it too early? On the other hand, maybe the Secretary of the Air Force and the Secretary of Defense are right, maybe it is too early, and it is desirable to stretch out the **R&D**, or at least the development phase, in order to go further down the road before you cross the decision point. You have avoided having the wrong thing earlier, which may be a plus. What I hear you saying is that, in the government, the formalization of a lot of these processes makes it so that it is damn hard to have either a rational stretch-out or a forced march with an abrupt cutoff, no further changes, and delivery in 12 or 15 months. You imply a great deal, from the less constrained industrial side, how—between avoiding the mistake of committing too early to something that is going to be dumb in somebody's judgment, and the mistake of dragging out too long something that you bloody well need tomorrow—how that gets screwed up in the government. Could you draw now strictly on the industrial side? If you had your druthers, as General Manager, how would you most comfortably strike the balance between avoiding committing too soon to the wrong thing and dragging your feet too long on something even if it's not perfect? One of General Cushman's statements was that it is better to have something than nothing, and in some circumstances even if it's not perfect you want it tomorrow. I think you were starting to talk about that. Forget about the government for the moment; as a manager, a principal, how do you balance that?

AEGIS—Naval Air Defense System
R&D—Research and Development

[OSBORNE] Well, let's say this. You can't fight a war with things that are on the drawing board. You fight a war with things that are in your hand. You can't run a plant with things that you're planning to do sometime in the future. You run a plant with the things you have now. So you need to have the capability at any given point in time that's sufficient to meet at least your minimum needs. But that's a process that doesn't happen by itself. It takes a great deal of planning to be sure that you're probably postured as well as you can be at any given point in time.... I guess one of the things I feel is death, from the industry side, is to lock yourself in concrete by choosing a course that you refuse to change—even though there's a need to change.

For example, I started an **LSI** facility. It was a large-scale, integrated array facility that developed innovative circuits, and we had chosen a certain complement of equipment to go in there—we had budgeted for it and bought it. But another group of equipment came out that was far better, that would speed the process up, give us greater accuracies, better resolution in our lines, and the like. The Board was horrified when I went to them right after this stuff was delivered and put it on the block to sell it, to buy something else. But they went along, and we put in a facility that really did what we wanted it to do. In the near term it looked like a bad decision because we had spent more money in that period than we'd planned to spend. In the long term (after all, that's the thing we were aiming at), it made and saved a lot of money for us. But the government system now has gotten so complex in its needs analyses, specifications analyses, justification and quantification of programs—there are so many levels—that things do get locked in concrete; it's almost impossible to change them. As a consequence, we have systems which are less capable than they should be, and it takes longer to get them.

LSI—Large Scale Integration

... Now, government specifications theoretically try to map out that planning process. But they don't put any one person in control; the process runs through a whole series of bodies who are entirely different, who have their own ideas about things. I've prepared a lot of these presentations for, or in concert with, my government colleagues to take them through these steps. The name of the game is to get through the gate. And you're sometimes willing to sacrifice some of the more substantive things in order to get it through. And once you've got it through, for Christ's sake don't change it, because you'll have to start the whole thing all over again.

... There's an excellent piece by **Melvin Laird** pointing out that all Services are continuously having to lower their requirements for the people who are coming on board. So as our weapon systems and our command, control, and intelligence systems are becoming more complex, the capability of the people who are actually operating, maintaining, and repairing them is going just the other way. In turn that makes the systems even more complex, because now you have to build things into them to replace the intelligence you'd normally expect to find in the human being. That lengthens development time. Sure, things are getting more complex. We now have to put much more capability in the same size box. We are constrained in size, weight, and power, yet the functions to be performed are much more complex, so the equipment is

Melvin Laird—Secretary of Defense, January 1969–January 1973

more complex. Determining just how all this threads together is obviously more complex. Being more complex, it takes longer. Because we don't have people who are maintained at the needed proficiency, it takes a lot longer than it should.

Admittedly it's going to take a lot longer in any event, right from the beginning of the process. Engineering the system takes longer, intrinsically; it's more complex stuff. Manufacturing takes longer. Because it takes longer it costs more, but it takes much longer to engineer and manufacture, and costs a lot more, because we're not applying all the intelligence we could and should to the process. Finally we deliver the equipment to our customers—late, and at an exorbitant price. We hand it over to people who don't have the capability to operate, repair, maintain it, so in the end the intended use of the equipment is subverted. It's just not what we want. Somehow, despite all this, we just have to change.

[OETTINGER] Now how would you interpret your propositions, in terms of what you'd want to change?

[OSBORNE] The complexity of the system is not going to change. Indeed, it will get more complex. Since that's so, we have to look at how we can assess the needs of the system in a much different way, and with smarter people. The government, as I said, is less and less able to articulate those needs in the form of specifications. That is going to continue to be a problem. Those specifications are going to continue to be complex, even more complex than they are now. We have to come up with a means of obtaining the best product, and a mechanism to expedite changes when changes are needed. The procurement process, the testing process and the like, by their very nature, cause things to take longer and cost more money. And although I can understand theoretically why these things have been done the way they have—to keep out crooks and so forth—nonetheless it is a fact that things are taking much longer than we can afford to have them take. They're costing more than we can afford to have them cost; we've got to do something about that.

... The next thing that's important—especially in the LSI and VLSI type of circuit—is that once you have decided that a device will be used to do a specific something, it's very difficult and very expensive to change that later on, because now its function is embedded. For example, I once developed a PABX system—

VLSI—Very Large Scale Integration

Private Automatic Branch Exchange equipment. It was all solid state. The decision was that we would put it all into LSI circuitry. It was a beautiful system, with automatic wake-up, call-back, all sorts of cuing. It was the sexiest thing you ever saw—except that nobody would buy it because, when I told them how much it was going to cost and how big it would have to be, they simply didn't have that much money or room in the motel or hotel to fit it in. It was suggested that we take the features out. But you can't do that; they're embedded in the finished system. Therefore, it is super important, since you're going to be building things this way, to make sure you start off with the best evidence: what is it that I really want to do? What are the needs? It's important to spend enough time qualifying and quantifying these things to the point where you can say with reasonable accuracy, "That does represent what I want." But we just aren't doing as good a job of that as we need to. It's because we don't have the people to do it, or we have processes which make it impossible.

. . . Oh, I think it's going to have to be a joint effort. It's nice to sit back and say somebody else is going to generate all the needs and the complete architecture, and will then hand it to an industry guy and he's going to go out and design the stuff and crank it out of a factory. Logically, though, it's not going to work that way. It's got to be an iterative process with a real partnership between government and industry if it's going to work right. Of course that's frowned on these days. The government-industry complex somehow or other got to be a dirty word—I don't know why, but it did. Yet I think we're going to have to go back to a lot more of that kind of collaboration. The development of the whole semiconductor business wasn't done in the military; it was done on the commercial side. The fact that you can get all this stuff on chips now wasn't a consequence of government work, it was the competitive force in the commercial marketplace that caused it to happen. I think that, like it or not, there has to be a degree of partnership between industry and the government.

[OETTINGER] I wonder how much of the problem is an absolute, and how much of it is perception. A tire is one hell of a complicated thing to fabricate, but any bloody idiot can change a tire on a truck. By the time it gets to the end consumption point, it has to be operable. The internal complexity may be increased, but still you have to design the truck so that the bolts can be unscrewed and somebody can use any old wrench; and you have to think about whether it's desirable to require a specialized wrench, and so forth. Maybe some of the problems are not as much the diminishing capabilities of people, or the increasing complexities of systems, but the need for more attention to making sure things are operable by human beings. You may have to take five- or ten-year intervals between major changes so that things are engineered at a level where people at a particular time can use

them effectively, as they would a tire. Now, is that nonsense, or is there a germ of something sensible in it?

[STUDENT] It's not responsive to today's demands, but it's perfectly true. For instance, the Air Force has problems not only with internal complexity, as reflected by computer programs and designs, but with external complexity, as reflected in the interfaces of what you're building today with the other systems that are already in place or, worse, with those that are already being simultaneously developed without the communications view. This problem is going to exist until those systems are fielded and they somehow come together. For example, we wanted to build an automated TACC—this is one of our disasters—an automated tactical air control center, and it was pointed out to us that current technology will support multiprocessing—that is, several computers which can share jobs. That's fairly complicated. Well, one company said yes, our computers can do it, and we've got an operating system that works, and another company said we'll build the applications systems if you'll give us a specification of how the operating system performs. Another company said, well, uh, we're the system integrators, and if those computer programs work on that computer, then we can make the system work. But it didn't work, and you've got fingers pointing all over the place. Now was that all complexity, or poor management? It's very hard to distill lessons learned out of disasters. You can draw almost any conclusion you want, but I think complexity was certainly a factor.

]OSBORNE] Over in Minuteman, we had a problem with the cable systems. Invariably some farmer using a posthole digger would punch a hole in the cable; and gophers, it turned out, loved to eat lead; they'd eat holes in the stuff. So we developed a system to pinpoint where the leaks had occurred with great accuracy—within 50 feet. That saved the Air Force an enormous amount, having this handy little gadget on the link that would tell them right away there was a leak; all they needed to do was go out and dig a hole there and fix it. But then we had to pull that gadget out—it wasn't to Minuteman standards. As a consequence, the Minuteman system is operating without that device now. It just wasn't in the game plan. (3, 4–5, 6, 10, 11, 12, 13, 14–15, 17, 18–19, 19–20, 20–21, 22, 23)

4. **RICHARD D. DELAUER,** *Executive Vice President, TRW, Inc.*
"A Major Contractor's View of C³I" 1981, pp. 69–94)

Command is not a thing, it's not something you can go procure. At most it has the half-life of the individual commander, and that half-life is probably no more than three to four years, maybe only two years. Putting in the things that are needed to support his views on what the command function is may take a much longer period of time.

... Now, despite what some might think, this [the NORAD Command Operations Center] is a good program—precisely because they did keep changing the requirements, kept it flexible and kept throwing things out to make it happen. If instead they had kept to the original program lines, in Bob Everett's view they would still be working on it, and we still wouldn't have it in 1981. The heart of the recommendation of the Defense Science Board study on systems acquisition was that you ought to build command and control systems in an evolutionary fashion and get them in the user's hands very quickly. You find out what the commander wants, evolve the system, add to it, update it, bring it along; in the meantime you install a backbone system that really works, and we've been trying to do that. Finally after much blood, sweat, and tears we have gotten the Services to admit that command and control systems are different kinds of things from airplanes or guns. They're acquired in small numbers, generally they're one of a kind, and their operational characteristics are largely determined by the user in an evolutionary process. In many cases existing commercial equipment can emulate the function, and you ought to be flexible and be ready to take advantage of that in procurement. And remember that these systems are not just for use at major command headquarters, but are also deployed at small units down to the corps, even perhaps the division and company levels. They all ought to take a common approach; at the same time, such wide deployment and such a wide range of needs demands flexibility.

[OETTINGER] The inference is that if the commanders stayed around longer, or systems people were smarter, or contractors were better at producing things faster, as either a backbone or a completed system, this problem could be solved. Doesn't the real problem lie deeper? An operational guy is likely to state his requirements in terms of functions—he needs this, that or the other thing—if he's capable of articulating them at all. The technical guy at **ESD** is more likely to talk about capabilities—the gears, the technology.

ESD—Electronic Systems Division

[DELAUER] Not only that; he wants to put a fence around it so he can meet the budget.

[OETTINGER] Even given a greater amount of time, though, mightn't that kind of cultural gap be unbridgeable?

[DeLAUER] All those tendencies are going to continue, and the characteristics of the people involved aren't going to change very much....

[EVERETT] The last thing you want to do is give the communications capability to the President. Evolutionary development can be like what the African colonials used to call the "white man's madness"—big changes every time a new administrator came to the colonies. One would be an agricultural bug and say, "The boll weevils are eating up all the cotton plants by the roots. Pull out the cotton roots, that's how to solve that problem." So the natives would run out and pull up the cotton roots. The next guy would be a civil engineer and he would say, "We need roads. So forget that boll weevil nonsense and get on with road building." And they would go along with whatever the new thing was, because they didn't want to spend their time in jail. Similarly, in the command and control function, every incoming commander's background, environment, personality, whether he likes staff or hates staff, whether he's an authoritarian or not—his whole style, his whole being will dictate to one hell of an extent his and his staff's command information requirements. A lot of thought has been given to this, to identify basic informational requirements. As we get down to tactical situations we arrive at some constants—things that tend to happen over and over. But that only gives us maybe ten percent of the needs. There's still the other 90 percent that's going to change with every new "white man" who comes in....

Everett—Robert R. Everett, President of MITRE; visitor and participant in this discussion

[OETTINGER] I sense that there may be "pure gold" evolution and "fool's gold" evolution. Where is the distinction? The ideal evolutionary model, as I hear you, is a simple "backbone" kind of thing to which you can add on. But another model, not incompatible with a naive notion of evolution, says that you evolve a German PTT, a French PTT, some US military Service facilities, separately. They're all nicely evolved—until the day comes when you try to hook them together, totally or partially, and things come to a grinding halt. And somebody says, "Jeez, you know, if only we had planned ahead and thought the thing through up front, we wouldn't have had to come to a

PTT—postal, telephone, and telegraph agency; government-owned commercial communications system

grinding halt now and build interfaces which are larger than all the systems together." Somebody else says, "Well, we did it in an evolutionary way." Is that not what you mean when you say "evolutionary," or is there some qualification to that notion of evolution which makes it good? And if so, how do I tell "pure gold" evolution from "fool's gold" evolution?

[EVERETT] Now as it turns out, the German and French PTTs will work together; the French and Germans do talk to each other, and that's been true ever since the early days. Therefore, in the course of evolution, it's worked. But if they had never talked to each other and a time comes, at two o'clock in the morning, when they will need to talk together, rest assured that they won't be able to. This is the situation in our military. People say, "It's just absurd that the Army and the Navy can't talk to each other. We'll legislate it: Everybody shall buy the same radios; or, we'll make them all get together in one room and design the communications center." Those things don't work. The only way you're going to get them to work together is to make them work together, make them work joint exercises, and when they can't work together and the thing fails, you sneer at them and they have to go out and fix it. If you don't do that, they won't ever fix it.

... In Darwinian evolution you go out and keep doing things; the ones that fail, you throw away; the ones that work, you keep. I expect that you might be able to mend the telephone system by means of evolutionary function, but we don't have a few million years. So you need to assess the course of the evolution—try to make the things you try sensible, and fix the small difficulties. That is a tremendous engineering task, and it is what is normally thought of as systems engineering. The trouble comes when you say, "Look, the present telephone system is all analog; what you ought to do is throw it away and build a new one using digital technology. We'll set up a **SPO**, we'll write specs and get everybody going, and the **IOC** will be 1992."

SPO—System Program Office
IOC—initial operational capability

[DELAUER] And it's going to cost this number of dollars to four significant figures.

[EVERETT] Now you know that nobody would be able to talk to anybody in the United States 'til God knows when. We try that all the time in the military.

[OETTINGER] Here are two of you who are in full agreement on that score; why is the rest of the world so dumb?

[DELAUER] Everybody who's talked to me says, "Let's do away with C³I." So we do away with C³I—but you can't make it disappear, we're still going to have some resource allocation. One of the problems we have had with the C³I organization was that when we did focus it, and aggregate it to, at least, define what the needs were, the warfare groups—strategic, space, general purpose—didn't have enough capability in it, and since they're not looking for things to do, they went on their merry way without considering the command, control, and communications requirements. In MX that's still missing; we really haven't addressed that leftover problem yet. What I want to do is be sure that the weapons systems people, who are putting in all that money, consider the implications of the command, control, and communications requirements when they start thinking about the weapons system. (70, 78, 79, 80–81, 82, 83, 84, 85)

MX—latest generation of intercontinental ballistic missile

5. **JOHN H. CUSHMAN**, "C³I and the Commander: Responsibility and Accountability" (1981, pp. 95–118)

Management consultant; former Commandant, Command and General Staff College

[T]he specific process of adaptation generally takes place through constructive dialogue between the providers and the users of computer systems. We are largely in the field of information technology. Computers and information technology are not necessarily synonymous. Command and control amount to much more than computers, though they are frequently referred to as adapting to the computer. In the business world the providers are the developers, the generators of new ideas, the creators. They make computers or their components. They work in the universities, the software houses, the research institutions. They are thinking of new things to do. The users in this evolutionary process are out there in the banks and bakeries, the refineries and business institutions of our land and around the world. They are doing the world's work, and they need computers to survive . The providers give the users ideas, the users keep the providers from being impractical, and the ultimate measure of merit for the computer is its utility in the contest of advantage. Users' influence governs.

As a management consultant, I'm working right now on a study of how users are adapting to computers. Citibank is doing a very good job adapting

to the computer, and I just read a briefing given by a developer of computer systems in that banking organization. This was his approach: "First, study the users. Second, understand the interoffice relationships and what the users are actually doing. Third, design a tool that performs today's function. Fourth, make it usable." Of course you must provide for growth as you make it usable (because the user is going to want to make it better) and implement it, get it going and let it grow. (98)

6. **CHARLES W. SNODGRASS,** "Funding C³I" (1981, pp. 119–46)

Vice President, Electronic Data Systems Corp.; formet Assistant Secretary of the Air Force for Financial Management

I will confess that it is more difficult to articulate the need for a C³ system than for many other things, because many of the most important parts of the C³ system are intangible things that you can't "show and tell" to Congress. You can take congressmen to **Cheyenne Mountain** and show them the Command Operations Center and they will see a bunch of computers, but those computers look just like the ones they saw at the National Military Command Center and down at the Kennedy Space Shuttle facility. Whereas, although they are all IBM 3033s, the software in them is totally different. And the huge cost overruns, the failures and problems in Cheyenne Mountain, for example, were software failures, not hardware failures. And how do you explain to a congressman—how do you explain even to a General—how it operates, how much it costs, where it should go, how much it weighs? How do you explain what software is? You can't take it in to show him at a congressional hearing. On the other hand, if you are selling F–15 aircraft, you can take the congressman and give him a flight in an F–15, pull six Gs, go to 15,000 feet, go to **Mach–2**, and they come back and say, "Boy, where do I buy more of those?" The product the C³I people are selling is just more difficult to articulate.

Cheyenne Mountain—site of NORAD's underground command post near Colorado Springs, CO

Gs—units of force, each equal to the pull of gravity on a resting body

Mach–2—twice the speed of sound

... The final problem that C³ has is its unique dependence on the perspective of the commander who is using it. We change commanders in the military every two to three years, so what was a perfectly adequate C³ system for General X is totally inadequate for General Y.

... Fundamentally the problem was to make sure the right information got to the right person no matter who collected it, so most of the things we dealt with were interface problems of a kind that are unique to C³I. Air Force F–15s don't compete very much with Army Cobra helicopters. F–15s are engaged in aerial dogfights with **MIG–23s** or **MIG–25s**, and a Cobra can't go after a MIG–23 or vice versa—though we are starting to change this in the Air Force. The F–15 was built primarily as an air-to-air fighter, and it couldn't compete with the Cobra for close air support for an Army ground unit. A ship doesn't compete with an Army field kitchen. So it's mostly in C³ where you have this competition across the Services.

MIG–23s or MIG–25s—Soviet fighter aircraft

Furthermore, C³ has the most common technology. There is all the difference in the world between Huey helicopter technology and **SR–71** technology. But an IBM 3033 computer can do all sorts of things depending on where you apply it and what kind of software you put on it. I think that's why C³I has so many more fights. We see this in our corporation. The management information system is where most of the bureaucratic battles in private companies are fought—because, after all, how you put the management information system together determines where the profit centers are. The measures of internal investment, internal rate of return, all of that, can make a tremendous difference in your bonus, depending upon how you set up the management information system. The same analogy holds true in the C³ arena. If you let everybody have his own C³ that's one thing; if you concentrate it all on the flight deck of the aircraft carrier or in the National Military Command Center in the Pentagon, you have a different bureaucratic power relationship and some three-star generals are up while others are down, depending upon where you place it.

SR–71—US strategic reconnaissance aircraft

... So I don't think that lack of resources is the reason this country has not been able to build an effective command and control system. I think it's more the non-budgetary issues: fighting for turf, the separation of the military Services, the competition between the civilian and military sides of the Pentagon, and with the civilian agencies such as **NASA**.

NASA—National Aeronautics and Space Administration

... I guess my biggest concern about what's happening to the defense budget now is that it's possible to spend 225 billion dollars a year in very stupid ways and not really increase the US defense capability at all.

... I think that at some point in your course you should look at the **Brooks Act** and the Paperwork Reduction Act, which regulate how the government can buy computers. In essence, at least in my opinion, we buy computers in ways that make no sense. I wish I had more time to talk about it. We essentially buy computers on the basis of hardware cost when, in the current systems, hardware is about 20 per cent of the cost and software is about 80 per cent. Yet, for historic legislative reasons, we let that 20 per cent tail drive the 80 per cent dog. I think many of the failures you see in government command and control, communications, and computer acquisition are directly related to the Brooks Act. And I can assure you that in the private sector we do not procure computers that way.

Brooks Act—Federal Property and Administrative Services Act of 1949

As a matter of fact, the biggest problem I had when I was Assistant Secretary of the Air Force responsible for computers was trying to convince highly skilled and reputable private sector computer managers that the government did it that way. The reaction always was "My God, you must be kidding. You can't possibly do that."

My favorite story: when I asked a very senior industrial person whether he leased or bought his computers, he said he leased them, because they had just gotten a 3033 and it was already an obsolete machine, and they didn't want to be stuck with it. Yet we had just had absolute champagne parties and everything else a couple of months before because **SAC** had just gotten its first 3033. And I think many of the problems are traceable to that. (128–29, 131, 133, 135, 145)

SAC—Strategic Air Command

7. **DAVID C. RICHARDSON**, "The Uses of Intelligence" (1981, pp. 147–68)

Consultant, Defense Intelligence Review Panel, the Defense Science Board, and other panels

I must simply observe that the system we have now is so complex that many people who have neither understanding nor responsibility other than to chop on a program have in fact the authority to delay it, or send it back for further analysis nf the need. It is just about impossible to get any project through the system at this point. I'm reminded of the old gunnery instructions, back hefore World War II. A problem would occur, and new safety rules he written. There would he a terrible explosion and then a whole new hunch of safety rules, then something else would happen, and more safety rules, all justifiahle. But a point is reached where the constraints are so great that you just ought tn zip it up and forget about it. I think it's possible to aggregate a whole bunch nf regulations, procedures and so forth, each of which is understandable in the context of a particular problem that arises, and end up with an aggregate that is counterproductive. Each is good, within its limited sphere for its limited purpose, hut you add them all together and you end up with something that's just far too complex to manage. There is the point of diminishing returns.

... One of the things I've been maintaining here today is that, if we make good and proper use of intelligence, a great deal of the development and procurement process problems will he alleviated or disappear. I think, though, that in this entire process it is absolutely essential that we conceptualize our weapons—formulate their characteristics—much hetter than we have in the past, and I view intelligence as heing a principal factor in that effort.... The Soviet navy had the job of becoming a first-rate navy, able to contend not only with the US Navy but with the British, French, and Italian navies as well. And how did they do it? Well, they studied our Navy. They studied the US, British and French navies very carefully. They found the weaknesses in our naval weapons systems as they viewed them. They looked at the promise of technology and in particular electronic technology. And they came to the view that we were overly dependent upon radars, which are electronically very noisy, and on lots of communications activity. So they designed standoff weapons that could exploit, through their sensor systems and their terminal guidance systems, our great dependence on electronics. They developed some fairly simple, basic concepts. One such: sink the carriers.

... We have systems in development that started out with threat assessments. We have program managers in charge of hringing those systems along. In this management climate the predominant features that bear on the program manager's effectiveness, that describe whether or not he's promoted are, first, "Is it on schedule?" And second, "Is it within cost?" This makes him—no matter how good a guy he is, how knowledgeable he is—hostile to any new intelligence or any further resolution of heretofore

tentative intelligence. The last thing that a program manager wants to hear is that his system is not completely responsive. So he's not receptive to new enemy information, and that is an institutional ailment which I think has to be corrected. You can find all the right words in the SECDEF procurement directives that contradict what I have said, but the fact is he knows he might lose his weapon system; and second, something is better than nothing—they know that it's better to get something and then maybe fix it later than to jeopardize a whole system because of some substantial weakness that can be fixed at some later date. That's one of the program manager's very powerful and understandable reasons, but it's more costly. My point is that there needs to be a better way of getting into people's minds the changing nature of intelligence and an understanding of intelligence—so that hostility, be it in the Office of Management and Budget or in Congress, in the Office of the Secretary of Defense or in the Service itself, can be converted into understanding and support. Where things need updating, they should be updated. The sooner, the less expensive—the better from just about any point of view. Now that doesn't exist today. (150–51, 161)

8. **RICHARD H. ELLIS**, "Strategic Connectivity" (1982, pp. 1–10)

former Commander-in-Chief, SAC

But a lot has been done in the last few years. Studies have been completed on strategic connectivity. Probably the ground breaker was the one SAC ran between fall 1978 and early 1979. We had the best brains in the country there, from all the Services and from industry. We spelled out the vulnerability of military C³I, strategic connectivity, and we reached everybody in town except the President on that. That is the kind of effort that is required in the years ahead. We must keep tab on how well we're doing. We must run detailed books. We must do it from an operational, not a system point of view. The operator is the person who has to use it, and he's the person who makes the best judgment on its effectiveness. We must ensure that the equipment is standardized. Having 18 billion dollars in back of it would help too, but that's just words so far. What we're going to have to do in the **out-years** is see whether the Services put connectivity on a par with Service weapons programs in priority of effort and funding. Because it's real easy to put money into C³ this year and then see it disappear into purely Service-related programs later on. At this point I will settle for higher reliability of C³I. (8)

out-years—in the future

9. **HILLMAN DICKINSON,** "Planning for Defense-Wide Command and Control" (1982, pp. 11–55)

Director, Command, Control, and Communications Systems, JCS

A program objective memorandum (POM) comes in from each Service and each defense agency. It is submitted about May and is the important document that will eventually result in the President's budget, presented to Congress the following January. The POM covers five years, but the really important years are the two immediate years—that's real money that you're dickering for there.

[OETTINGER] I just want to interject; those of you who have not experienced the terror of the middle-level military or civilian manager talking about missing a POM cycle, I think, cannot appreciate the depth of what he is talking about right now.

[DICKINSON] Now, how does this work practically? Having gotten the POMs in and had our CINCs' review this summer, we look for example at the strategic connectivity issue. We had a set of items that we felt were absolutely vital to improve in the area of strategic connectivity. They were presented to the Joint Chiefs, each of whom is a Service chief. When their budget came back in, it reflected about 80 percent of the recommendations I had made. Now, that happened as a result of our seeing that budget and acting. The Joint Chiefs had a reputation for never being able to address these sorts of things, but in fact, in recognizing things of this importance for cross-Service use, I think the process works, and I've got to compliment all the chiefs on their responsiveness to the problems we saw in connectivity at that time.

It culminated **in October** with a presidential decision memorandum. The announcement was made on the second of October. It said, among other things, that C³ is even more important than the other pieces of the strategic improvement program, which included the MX and the **B–1**, the **advanced technology bomber** and so on. C³'s importance was recognized through this process. We were able to show, in fairly simplified diagram form, where the gaps in the system were likely to be as a function of various kinds of threats and scenarios. We were able to present the problem, and we were able to get action.

in October—October 2, 1981

B–1—US strategic bomber developed in mid-70s

advanced technology bomber—the B-2 ("Stealth") bomber

Another example. The Air Force is a good example of the budget crush, with those three big programs: the MX, and B–1, the advanced technology bomber. They were pretty well choked to manage those kinds of programs and come in on target. A number of other things came out of the budget in various places, in particular for cross-Service C³. From a decision made at the upper **OSD** level in the **DRB** for about a billion dollars of cross-Service funding, by the time the budgets came back in the Services were able to fund only about $175 million. Well, that's a tremendous gap in other essential improvements in theater and tactical C³. We went back with the most important of those gaps in a list of some 20 items as late as November, and again, about 80 percent of them were funded by the Services before the budget was finally produced. So that's the way the process has worked: a combination of pressures, of presentations to the chiefs and the opsdeps—their operational deputies—and recommendations to OSD and the chairman's own voice in some of the final councils. That's the practical role—what you have to do, when you don't control the money, to get other people to understand the problem. (25, 27)

OSD—Office of the Secretary of Defense
DRB—Defense Resources Board

10. **ROBERT T. MARSH**, "Air Force C³I Systems" (1982, pp. 95–114)

Commander, Air Force Systems Command (AFSC)

The users—the commander of the Strategic Air Command, or tactical force commanders—play an important role in defining their needs or requirements for future weapon systems based on the potential threat. But I think you know it's not as simple as that, because no field commander ever dreamed up the need for a ballistic missile, an atomic weapon or a laser. Instead the technologists brought them forward, and matured them to a point where, all of a sudden, they appeared as potential systems for the user to exploit. The user didn't express a need in those instances; rather, technology came forward and offered him a tool to perform his job better. So our new requirements and new systems evolve from both sides: a statement of need on the user's part, and technological opportunities that present themselves.

... The void, then, is in how we are to satisfy the command and control needs of unified commands. Now, I don't embrace what some others say: all you have to do is give them a big pot of money and a whole bunch of engineers and let them invent their own. That's nonsense. What you ought

to do—no matter whether it's the Air Force, Army or Navy—is have a good clear way for them to interact with a development agency, articulate their needs, iterate those needs back and forth and get them established, get the JCS' blessing, and then direct a lead Service to work with the unified commander and satisfy his needs.

That simple process doesn't exist today. Unfortunately, JCS doesn't have the authority to direct that it be done. Command and control responsibilities go back to the Constitution, to the role of the military departments, and the way they train and equip their forces. Besides, JCS doesn't have any equipment. So somehow you have to close that gap, and get the military departments to provide the equipment for the unified command. That's a fundamental problem with C³I. And I don't believe this nonsense that, "Well, those guys over there in those development white towers don't know what the hell we operators need, so the way to solve this problem is to let us operators build them." There's just no way. I've taken on General Cushman about that: "Do you mean you want SAC to go build a B-1 bomber, for example?" We have precious few scientific and engineering and acquisition skills in the Services today. We shouldn't dilute those further by setting up another development agency.

[OETTINGER] I'm impressed with the recurring evidence that while the problems are easily overcome to the extent that they're technical, they keep coming down to control of the money on anything that goes into an interservice mission. You indicated earlier that the Cushman proposition of money for the CINCs and so on doesn't appeal to you. But there is nothing in place that would provide the Joint Chiefs or OSD with authority to control the money that is in the Services. What might be a way of going at this problem, if you agree that it is a problem?

[MARSH] Well, I agree it's a problem, and I think it's fairly straightforward. I think all the secretary of defense has to do is recognize it—and there have been a couple of DSB studies that have recognized it, one as recent as three years ago. I think all he has to do is saddle up somebody in OSD and give him the clout to enforce interservice integration. They've tried to do that with the C³I position, but they've just never given it the authority and the responsibility to do it.

DSB—Defense Science Board

[OETTINGER] Do you mean Lieutenant General Dickinson's shop in the JCS office?

[MARSH] No, not in the JCS, I meant **USDR&E**, Don Latham's shop, earlier Dinneen's, the Assistant Secretary of Defense for C³I. I think organizationally it's easy to solve. The problem is simply to achieve high-level recognition of this need, and then recognize that you've got to establish an office under the Secretary of Defense that has the authority and responsibility to make sure that the needs of the unified and specified commands are met. They tell us everything else to do, why in the world do they resist with a difficult thing to do? I don't understand that. Historically the DSB has reported that we ought to form a DC³A, a defense command, control, and communications agency, hut I think people felt that we've got too much centralization already and that that one wouldn't sell, so they ended up doing nothing. They ended up doing nothing as a result of the **Buchsbaum** study. There were alternatives in that study. One was to establish the important focal point on the Joint Staff, and one was to establish an important position within USDR&E, and that's all it takes.

USDR&E—Under Secretary of Defense for Research and Engineering
Buchsbaum study—DSB task force on command and control which recommended giving C³ funds to operational commands. (The task force was headed by Dr. Buchsbaum of Bell Laboratories.)

[MCLAUGHLIN] We've gotten the impression from past speakers within the Services that there are competing priorities—people wanting a solution in terms of planes for the Air Force, tanks for the Army, and competition fur resources.

[MARSH] Yes. There will always be such priorities; I hope everyone will agree that we must have priorities. The Air Force is in desperate shape, in my judgment, for all kinds of things—war-fighting capability and the C³ that goes with it. We've put a lot of rubber on the ramp over the last decade in F–15s, F–16s, A–10s, F–111s, you name it. But none of them were sustainable. We didn't have the logistic support to go with them because we couldn't afford it. We didn't have the air-to-air missiles to go with our fighters, we couldn't afford them. We didn't have the bombs. We had planned more precision-guided munitions that we could have put into production than you could shake a stick at, but we couldn't afford them. Now, try telling a tactical commander who's got 72 airplanes sitting out on the ramp but hasn't any munitions to go with them, no spares at all to keep them flying, that what he really needs is C³. You know he won't go for it. It's a matter of priorities.

I think we're getting to the point now where we're ready tu address C³ in a serious way, and I think this administration recognizes it. But during the last

two years—the 1981 supplemental budget, the 1982 amendment and the basic appropriations themselves—we really got working on sustainability for the first time. We poured billions into spares and munitions; that was the first order of business and incidentally still has very high priority. We've got to sustain that spending out into, say, 1985 or 1986 before we'll get to where we can conduct 90 days' worth of operations. I think you'll find the Air Force saying, "Well, now that we've got that well underway, we're ready to invest in upgrading our C³." But yes, it is a matter of priorities, and C³ has suffered.

... [O]ur weapons system acquisition cycle is cumbersome and too damn long. I'd almost characterize it as bankrupt; the system's almost constipated in trying to get a job done nowadays. Endless review, checkpoints, the way we do things serially—complete this phase, stand down and chew on it, and then the next, then test, retest, and so on—that's terrible, and must be reversed.

[OETTINGER] You begin to see that if something persists that long it must be functional, it must do something for somebody, and the next target is to say it's the bureaucracy. But you know, in Pogo's words, "We have met the enemy and he is us," so it isn't altogether the bureaucracy. How and why did we get into this swamp in the first place? Among the reasons there were failures, there were some interesting things, there were procurement irregularities. Do you have any sense of where the perversions came from, and how, with whatever good or bad intentions, maybe porkbarreling, making sure things were adequately reviewed, whatever—your installations are so nicely gerrymandered the way NASA installations are, which is of political value but doesn't necessarily speed up the process? Could you look beyond the bureaucracy blanket and give us a sense of what original functions were served, what current purposes? Why does this persist? If we had a sense of that, maybe we could gain greater clarity about what one might do to change it, whether it means bowling somebody over, paying them off, opening their eyes, or whatever it takes. But the "bureaucracy," or "people are stupid" view seems too simplistic. It's been around too long and it's too deeply entrenched.

[MARSH] Well, back in the late 1950s and the early 1960s I think we, at least in the Air Force, did a pretty darn good job of acquiring systems. The **B-52** is a pretty damned good weapons system. The **C-141** is held up by many as the finest acquisition the Air Force ever did on cost and schedule, and it

B-52—US strategic bomber; mainstay of current bomber force
C-141—US strategic airlift aircraft

worked like gangbusters. I would say that the ballistic missile program was well managed; it spilled a few dollars, but the nation wanted it in the worst way. We brought it in in fine fashion. It worked as advertised. I think Minuteman is certainly good.

Now, about that time **Mr. McNamara** came in. There were, sitting around, examples of systems that didn't work as well as they should and, perhaps, systems that people didn't think we ought to have. "Why do you need this one?" or, "You've got too many on your platter." We started institutionalizing: front-end planning, sorting things and getting them well defined before you move, and once you move you go all the way. Well, we got the C-5 as a result of that, and the F-111. Great deliberation went into laying those programs out right, but as far as I'm concerned that started the cycle. Those programs didn't work out, and from then on we continually tried to Band-Aid the process. We said, "Well, it didn't work out, and we didn't know it until it got all the way down to the end. So we won't do that again. We'll put more checkpoints in this process, and to make sure our design is coming along as advertised, we'll build some prototypes, test them ... we're going to put really tight control on this process, detect our mistakes earlier."

Mr. McNamara—Robert C. McNamara, Secretary of Defense under Presidents Kennedy and Johnson

We took the risk-reduction approach to life, and I think it's grown from that. And nearly every new administration has put further checks on it, has refined the process. Instead of single production decision or development decisions we'll have three or four, we'll call them **DSARCs** and we'll even have a zero point before you start thinking about it. We'll say, "It's a good system to think about, and to study," and then when you finish your studies we'll have another one and say, "It's a good system to explore further with some hardware," and then we'll go through that "explore" door and determine if it's a good system to develop.

DSARCs—Defense System Acquisition Review Council (The acronym is often—as here—used to refer to the major decision points in the acquisition process.)

Now, believe me when I say a bureaucracy builds up around this process. You get secretariats, you get special cost estimating groups—they don't estimate costs, they check the Services' cost estimates—you get other offices that do nothing but develop the concept papers. I'm telling you, it gets well

entrenched. And nobody stands back and says, "But what's happening to the process?" It's an elegant process, and it looks good on charts: "Who in the world would develop anything and produce it without thinking about it first? We ought to do that." So it looks super, and it takes fifteen years, and by the time you get into the field the system's obsolete.

So I think we must go back to where we acknowledge and concur. Do you know that if you go out into a factory, every person you see costs the taxpayer a hundred thousand dollars in round numbers by the time you load him with his support and all? If you load him with overhead it's more than that. A hundred thousand dollars—count up ten of those folks, and it's a million dollars.

Now what happens if you slow down? We're spending, on the B–1, 30 million dollars a day. If we run a test and something goes bad on it, and somebody says, "Hey, hold everything, we want to go check on this, the landing gear's got a little shimmy in it and we're not going to approve your going into the next phase till you fix it," we're ringing up 30 million bucks on your tax register for every extra day, and that cost isn't going to go away. That's what's happening in these 15-year-long cycles. We're keeping the whole industry team together to do a job that can be done in half the time, or a third of the time. That's a fundamental problem with the process, in my opinion. People cite—and it makes good copy—how much you spent after you should have known better. And you're going to send some systems out into the field with big retrofit kits. But retrofit kits are cheap compared to keeping the weapon system in an idle mode for a year under contract.

But the question you were asking was a little different from that. There is the problem of how you cope with the acquisition cycle, now that the half-life of technology is down by an order of magnitude or more. That's tough one: how to keep our system technologically abreast.

Now, you might ask why you want to do that. If it's effective, why do you give a damn whether it's state-of-the-art or not? Well, usually it's in the logistics area. The guys out there are prima donnas. If they want to shut down a chip line, bang, they shut it down, and they're gone; and unless you had the foresight to stockpile a bunch of them (and then they may not have a shelf life, so that may not be a good idea anyway) you're sitting there with a major problem on you hands. Now that's a real problem. It happened to us on AWACS. Motorola just said, "We're not going to produce these chips any longer"—a real sophisticated chip that implemented our clutter rejection algorithm. And

AWACS—Airborne Warning and Control System

they stopped producing them. We finally got some outfit to do it, put a lot of money into them, and got them up to where they could handle it. But coping with the shortened half-life of technology, especially in the electronics area, is a hell of a problem. What we try to do is focus on "form, fit, and function." We put a bunch of little modular boxes in, and when this box gets obsoleted, throw it away and replace it with another box. The housing may be only half full, but it's got the new technology in it, and the rest of the system doesn't know you have replaced that box.

[OETTINGER] There's a chicken and egg thing here. One of the reasons some of the speakers last year from the industry side pointed out their desire to get out of the chip business is that again, with the delays in procurement and one thing or another, they can't afford to put their own money into it indefinitely to wait for the US government or a particular Service to make up its mind about a procurement. So we've created a monster that feeds on itself. Again, what's your sense of how one might get out of it?

[MARSH] Well, we're thinking about that on **VHSIC**. If we develop some of these really highly capable chips, the kind that are needed for real fast operation on, say, waveform analysis, that have fairly exclusive application to the military, we may have to set up a government-owned, contractor-operated plant. Or we may have to reach an arrangement with some manufacturer that we'll come in and buy one of his lines, and keep it manned up. This has been discussed before, and we've almost done it in certain instances. We've almost had to do it in the space business, where we need an element—a transistor, you name it—that's say, a hundred times more reliable than the run-of-the-mill version. We've almost decided we ought to produce these things ourselves in a government facility or contract, and I think that's the answer. If industry won't accommodate to us, we'll have to do it.

VHSIC—Very High Speed Integrated Circuit

Now, there's another solution: multi-year procurement. Rather than go to the manufacturer once a year and ask for seventeen items that he can produce in three days and then shut down for the rest of the year, if we get multi-year procurement through, we could order our foreseeable quantity for the next seven or eight years, let him produce them all at once, and then shut down. It's our crazy procurement system that keeps us in the annual ordering business, which isn't good for the military, obviously.

[STUDENT] I'm interested in the issue of multi-year procurement. We've contracted things like the B-1 bomber, and that's going to spread over

several years. Then you talk about the whole procurement system being built into the congressional cycle—I'm not clear on what the snag has been in allowing the B–1 procurement to be a multi-year system. I know it has been done at the state as well as the federal level. Multi-year procurement seems to make such great sense. Are you trying to press it as something that would be helpful, and even make financial sense?

[MARSH] We are, and we intend to do it on the third buy, starting with the eighth airplane. We're buying one airplane the first year, seven the next. Then we really come up to speed, and that's when we'll institute multi-year procurement. But what is the hang up? It's Congress mortgaging away the future. If Congress, or even the Defense Department says it's going to produce this airplane for the next four years, the people say, "Well, I'm not sure about that," and a two-year Congress has trouble. A new Congress will be coming in, and there's a whole defense program laid out to them, and they don't have any authority over it; they aren't going to be very happy. That's the root cause of the problem.

[STUDENT] But I'm curious about how they can make commitments for periods beyond their term—submarines, airplanes, all kinds of things require a much longer commitment than the annual one—not being able to transfer that into long-term programs that really make more sense.

[MARSH] I agree, it doesn't seem to make much sense; but those are different problems. When they buy the three-year airplane (that's the time it takes to build an airplane), they put all the money up front in that year, in other words they authorize and appropriate the full $25 million to buy this airplane that we won't see for three years.

[STUDENT] Except for the cost overrun.

[MARSH] Except for the cost overrun. But multi-year procurement is not as simple as it sounds, because it still tries to preserve the prerogatives of Congress. What it really does is authorize. It says, "We intend to procure four years' worth of airplanes," and we just sign the contract for 120 F–16s a year, for a total of 480, four-year multi-year procurement. The first year we put up more obligation authority, more money, and tell them to go out and buy. If you can save a lot of money buying landing gear in a big lot, you go out and buy 480 sets of landing gear—or canopies, if the guy can turn out canopies like that, go buy all of those. But you have to plan that out very carefully and determine the highest-payoff items that you want to buy in lot quantities. You buy those, and you take the savings that accumulate from them. But you still only

ask Congress for the money for those 120 airplanes. So you have to go back next year to get the 120—but if you don't pick up those next 120 airplanes it's going to cost the government some money, so you have some termination liability. So there's some leverage to continue a program once you start, because it's such a complex process. But you don't want to get everything on a multi-year basis, obviously, because you lose all your flexibility. You have to be selective. And on those programs that have high stability, you've got a consensus between the Department of Defense and Congress, and they're not controversial.

[STUDENT] But generally the chairmen of the committees that these programs are going through will have some longer-term understanding. They're generally in Congress longer than two or four or six years, and it would seem that working some kind of arrangement might make a good deal of practical sense.

[MARSH] It does. The military departments really pushed this multi-year process and got it through, and we save a lot of money. We estimate that on the F–16 we'll save about 10.5 percent, which on those 480 airplanes is, I think, something like 350 million dollars. (95, 98, 103, 104, 110, 111–13)

11. **RICHARD G. STILWELL,** "Policy and National Command" (1982, pp. 115–45)

Deputy Under Secretary of Defense for Policy

[N]othing is more frustrating to those of us in command of forces than the inordinate length of time a system takes to go from concept to mission capability. It just drives you up the wall. There are many reasons for it, but I submit that the basic reason is inadequate funding of the system to begin with, underestimating the costs, which drives you back to Congress a year later to say, "We missed our estimate by X million dollars and we need more money." You get in trouble with the top level too because they say, "The military doesn't know what it's doing." And so the system becomes suspect for not front-loading and getting really good estimates, not being realistic. I'll take my licks along with the rest. Moreover, there is an unfortunate tendency in the military to say, "That looks good, but it could be better. Just change this, this, and this." And you begin to get change orders, which cost money and slow the progress. And a number of people at the top level do change their minds, whether they want to admit it or not.

The most horrible example of all is the Patriot, the much-lauded new surface-to-air missile system. Phased array radars, multiple target engagement capability, effective from zero altitude up to a hundred thousand feet—it's great. It needs minimal maintenance, and can be manned by a small crew. It's tremendous, except that it was conceived in 1963 and we'll field it in 1983. At the time it was really pushing the state of art, but still we should have bettered that initial fielding date by years. It was delayed by problems of funding, change orders, differences over operational concepts, disputes as to the logistic support system it would need, whether to give it a nuclear capability or not, whether to give it an anti-tactical ballistic missile capability or not. (This is out of my field; we ought to send some of the Patriot project managers here to talk to you.)

So we develop this great concept—the Air Force and Navy have done better on new systems than the Army has on Patriot, by the way—and it goes through development, engineering, testing. We get the bright and rising star and put him in charge—"You field the system, it's your baby." But having put him in charge, there has been a terrible tendency to put a pyramid of review on top of him, to the point where he is almost suffocated. We could correct a lot of that.

[OETTINGER] Your sense is that the process itself is to blame?

[STILWELL] Yes. It takes two years to plan the program in enough detail to get justification from Congress to get money.

So where's the real problem? It may be more difficult in the Army than in the Navy and Air Force, because we have a far greater multiplicity of systems than the major weapons systems in the other two Services. But the problem is the lack of proper feedback and interface between the user and the developers, mainly on issues of functional utility. Once we've done the human engineering, we need to ask: "Is this the right way to do this thing is it what we really need?" (129)

12. **RICHARD D. DELAUER**, "The View from the Hot Seat" (1982, pp. 147–63)

Under Secretary of Defense for Research and Engineering

The first thing this new management did, just about the time I came into the building, was review the biggest weakness we had, which was the mismatch

between the planning system—it was called the Planning, Programming, and Budgeting System, which in the past has been a budgeting exercise, completely managed by the Office of the Secretary of Defense—and DSARC, the system that acquires equipment and services. They were never coupled together. This lack of coupling has always been a problem. Nobody can understand how you could run the budgeting system, the resource allocation system, without knowing where you were going to put the money. The new team integrated the two systems and reconstituted them as the Defense Resources Board, which serves as the allocation authority. As they restructured it, the board now included a mixture of people from the Office of the Secretary of Defense, which is the Defense Department staff, and the leadership of the uniformed Services. So for the first time in the resource allocation process, the Service secretaries sat at the table with the Secretary of Defense, the deputy secretary, and us under secretaries and assistant secretaries. This group then essentially provides management oversight of the resource allocation process. That was a fundamental change in the way we allocate the money.

The next structural change that was accomplished was to integrate the process. The policy side of the house would generate what we call defense guidance, a document the Secretary signs that says what we expect to do for the next five-year period. It has broad categories to show where resources ought to be applied, who ought to do them, and how they should be implemented over what period of time. The defense guidance is reviewed by the comptroller, who makes a first-cut allocation of resources for the Army, Navy (including the Marines) and Air Force, and the elements of the Defense Department: the Defense Communications Agency, the Defense Mapping Agency, the Nuclear Agency—all the agencies that cut across all the Services. Those recommendations are sent to the Services which publish their five-year plans in the form of POMs—program objective memoranda. In these documents they lay out for five years how they're going to meet the secretary's defense guidance: force structure, personnel, operational readiness, research and development. The POM document spells out funding for the five-year period, number of articles, development time, pay structure, building and housing. So in one document you've got all the resource allocation.

Now, it doesn't take any genius to figure out that, as submitted—Army, Navy, Air Force, OSD—put them all together and there really are mismatches. In the past, those mismatches were essentially reduced to a zero-error function by the staff of OSD. They resolved it, sent the material back to the Services, and said, "This is it." This time it wasn't done that way. Instead it was done in a series of reviews by the Defense Resources Board. But in order to be able to have it manageable, they had an interim process in

which it was looked at by Research and Engineering, which I run—by our PA&E (Program Analysis and Evaluation) staff, primarily people who look at the cost-effectiveness of different force structure mixes—and by the comptroller.

We integrated the three different program objective memoranda into one coherent document. We identified mismatches, underfunding, and programs that weren't funded in adequate amounts in each of the Services. Command, control, and communications was a perfect example of that. You can't have the Navy funding it at one level, the Air Force at another, and the Army not funding it at all, and expect them all to play together as a choir. We fixed that by an iterative process—not perfectly, not even semi-perfectly, but as a first cut.

And then, right in the midst of trying to do all this, the whole budget exercise of last spring got involved: the big fight in Congress over what the budget was going to be, whether it was going to be balanced or unbalanced, and the whole question of taxes. So we had to change our allocation levels up and down. But it served as a first model, and it came out reasonably well. We identified many things that could be better integrated, and we proceeded to prepare the budget that way, and that's the way the 1982 budget went in. Now we're doing the same thing for 1983. This goes on just like clockwork. We're doing a 1984 program objective memorandum pricing right now, and we're starting to get it for integration.

So that was one of the fundamental changes in the planning structure of the Defense Department. It's the right way to go, everybody's always wanted to do it this way. I think we can do a better job of integrating.

... Then we took a look at the acquisition process itself. All the management studies of the past had great recommendations about the instability of programs, how they were underfunded initially and therefore always had a bow wave out in front, so that everybody always gets accused of having overruns when really they were underestimated by design, and never could catch up. Buy-rates were made uneconomical in order to stay within the budgetary limitations. Other recommendations from the past included a certain amount of decentralization of program management, reduction in documentation—all the things that any decent manager would look at and say, "These are the things we ought to do." We looked at all the recommended improvements to our acquisition process and ended up with what were loosely called the 32 Carlucci initiatives. Now we're in the process of trying to implement the initiatives, and we've had some reasonable success.

The problem is, everything moves at the speed of a glacier there; you take one step forward and three steps back, then you do four steps, and after a week's gone by you've made a step. I'm in the process of trying to institute a program management reporting system which will tell me how much money we've spent, how far along we are on the program, the dollars and the content, and the real estimate to complete. We worked the hell out of it and sent it up for review—and the reviewers came back with, "Why can't you use this document, and why can't you use that document." So we're back to square zero, and I've got to go back tomorrow night and start working it all over again, because for every guy who says yes, there are three guys who say no. That's the kind of situation we face.

... The real problem is that the great white hope of the early 1970s, congressional reform, has turned out to be a disaster. There's no strong leadership in Congress, a jillion committees all with big staffs, and the staffs have all the leverage, since they do all the work that the members vote on. I go up there to the—oh, let's take the House Armed Services Committee, which is one of the authorization committees. They tell us what things we can have. The hearings are held before the full committee, some 32 members, and if six show up, you're lucky. But always the committee's two or three staff guys are there—very bright, very hard-working, they're good guys. They don't always agree. Tony Battista came out of the Navy lab structure. Tom Cooper is a Ph.D. engineer out of Berkeley, a teacher at the Naval Postgraduate School, now on the staff. He's a bright guy, knows the business, knows the technical aspects. But they've got to explain program after program. They have a special subcommittee for the space-based laser. The chairman sits there and doesn't do anything, and these two guys do all the talking: "Why are you doing this? Why are you doing that?" We had 90 million dollars in for space-based lasers: a tracking experiment, some other things, all in high-powered five-megawatt chemical lasers. They cut all the money out except for the pointing and tracking, and they inserted their own line item to do millimeter wave laser work. It makes you wonder about who has the responsibility to get the job done.

That's the problem right now. There's not enough strong leadership, so it's wide open to whoever can get to the staff, or to a member who will take an interest. I look back and wish to hell that we had it like they used to have it, when a guy like **Carl Vinson** would say, "Okay, gentlemen, this is what the Defense Department's going to look like for the next three years," and he'd tell it not just to the members of his committee, but to the Defense Department people out in front, and that's how it'd be. You'd work out a deal with Carl Vinson and you had a deal, and you could run

Carl Vinson—former Chairman, House Armed Services Committee

Senator Stevens—Senator Ted C. Stevens of Alaska

the place that way. But today you really can't run it. It's a day-to-day operation. I mean, they were fighting on the floor of the Senate and in the Senate Appropriations Committee, I was in continuous contact with Senator Stevens, the chairman of the Defense Appropriations Subcommittee of the Senate Appropriations Committee. Ted worked his heart out to get a reasonable bill through the Senate. He and I ended up negotiating over the telephone. He says, "Will you take this?" "No, I don't want to." "If you don't take that, you're going to lose the whole bit." "I'll take it." And he'd go and get the votes. And, boy, that's a hell of a way to run a railroad. We both end up reacting to the politics of the moment. It sure raises he- with the orderly process of planning. That's a lot different than it used to be. (147–48, 149, 151)

13. **JAMES W. STANSBERRY,** "Cost-Effective Rearmament" (1984, pp. 49–61)

former Commander, Air Force Electronic Systems Division

[W]here we have failed, in terms of maintenance, has to do with our not buying adequate spares. When the defense budget wasn't quite as rosy as it is now, we bought airplanes and took our chances on spares. The reasoning was, "Let's get the airplanes while we have a chance. We'll buy spares for them later." I think it was a deliberate strategy: once we've got airplanes, Congress is certainly going to let us buy spares. We did go through a period where we were very "under-spared" on some of these aircraft but the situation has improved.

... American arms are the best in the world, but they cost too much. They truly do cost too much. And that's a problem of very large dimensions. Why do they cost so much? American arms are built, for the most part, by companies that don't have to compete the same way a commercial company has to. They have little motivation to modernize. In fact, our defense procurement system has in it strong disincentives toward substantial modernization. For example, in the Nixon administration, the Air Force program was to replace our 30-year-old B–52 bombers. Everyone reasoned, "We've got airplanes flying that are older than their pilots. Sooner or later, they're going to wear out and kill a bunch of people. We can't depend on them, they're too expensive to operate and maintain. Let's go build a B–1." Congress says, "Good idea," and you issue requests for proposals, and Rockwell wins.

Somebody at Rockwell determines that to build a B–1 bomber and do it right, they have to modernize and build new facilities. Some corporate official calculates that they'll need $100 million in new capital goods to do an efficient job. And so they proceed with this large capital spending program. Nixon says build the B–1. And then Mr. Carter comes in and cancels the B–1. Now this corporate official is sitting there wondering how to explain to his boss what he is going to do with a $100 million worth of new machinery. And then the next administration comes along and says, "We're going to build a B–1." Now this executive has been burned once and he's skeptical. His response is, "OK, we'll build a B–1 for you. Instead of machinery, though, I think I'll hire a lot of people and hand-build a B–1 because it's easier to lay them off than to get rid of capital equipment."

That's obviously an extreme example but it is pretty close to the truth. The lack of stability in the defense business makes it basically very high risk. If you're in the business and you capture a chunk of it, you have to worry a lot about any major investment in new equipment. It takes about three years to order and install a lot of modern machinery. Once you get it installed, we have accounting rules that say you can't amortize it in anything less than seven or eight years. And over on the commercial side, companies are turning things over in two or three years. This is a disincentive to plant modernization and capital goods acquisition. Now if you don't invest, don't modernize, you remain notably unproductive. Maybe you're productive compared to the private sector of 15 years ago, but you are certainly not so productive as the private sector today. The answer is increased stability in defense spending.

I think it is scandalous that defense should be a partisan issue. If we get in trouble, nobody is going to check as to whether or not you're a Democrat or Republican before they shoot you. We're all in it together. Why should defense enter the area of partisan politics? Now some say, "Well, really it doesn't become a partisan issue, except when you get down to details." Details such as where we should base an MX missile. Should we put it on a track? Should we hide it in the ground? And then you get into the very peculiar phenomenon of experienced, even brilliant, legislators voting on something they know nothing about. And splitting that vote along party lines, whether it's right or wrong. You certainly might vote on what level of spending your country can afford in the defense area and how it will be financed. But why would you vote on something like MX-basing? We have things going on today in this annual Congressional look at our programs that boggle the mind. I believe the Secretary of the Navy just commented that Congress, in looking at more than 300 line items submitted as the Navy's

RDT&E budget, changed more than 200. Are our elected representatives that bright in science and engineering? Obviously not.

RDT&E—research, development, test and evaluation.

... I think part of the answer is stability of our programs. Although not everyone would agree with my number, that if we were to do things efficiently and well and at reasonable production rates, we would knock 20 to 30 percent off the price of most of the products we field. I actually think it would be about 40 percent, but I publicly say 20 to 30 percent. You know, we're the guys who built one F–111 a month. Twelve a year. Why? Because they were issued to us by people who had a vested interest in seeing to it that the Air Force got F–111s. Let me tell you something else about the acquisition business because I could just preach multi-year all day long. I was once asked, what are the three most important things you would do to address problems in the development and acquisition process. I answered, "Multi-year, multi-year, multi-year." It's the single most important thing we can do and multi-year budgets make more sense even than multi-year contracts....

[STUDENT] I'd like to follow up on that answer to the question of why the Services go off and do what they want to do. The answer seems simple to me. It's the whole structure of the federal budget, the way money is allocated, who is responsible in the end for the execution of a project. If it's someone down in the bowels of an organization, a project manager somewhere, who is responsible for the way money is spent on a particular project, you can damn well bet that the decisions made on that project are going to be the project manager's decisions.

Now a good example is the logistics question, the fact that decisions are made in favor of airplanes instead of logistics support. Well, a project manager who is in a job for two or three years and has to make a decision how to spend a million dollars, whether he should field a weapons system or whether he should buy logistic support that is going to start paying off ten years from now, that guy would be stupid to make the logistics support decision. He would be a fool, because his performance is going to be measured on those three years he is in that job, not what's going to happen ten years from now.

[MCLAUGHLIN] ... I want to come back to something we discussed briefly at lunch, and that is the shifting balance of the muscle and nervous system. It seems to me that an awful lot of the present body of procurement law and

regulations was designed for procuring tanks or trucks or planes. Do you see a difference in procuring a nervous system as opposed to procuring muscle? Does the system work as well, better, or worse?

[STANSBERRY] Well, first off, most of your regulations pertain to off-the-shelf beans and bullets, and one of the problems we have is taking a regulation that was designed for buying things off-the-shelf and trying to apply it to the system. Secondly, I think buying electronics is a lot easier even though the systems and the laws are, as you say, sort of pointed towards airplanes and tanks. The reason is, you look at the firms we deal with, most of them have a very heavy commercial flavor and a very heavy commercial R&D program, whereas in the airplane business, the industry sort of followed the Services for a while—we'd invent things and they'd put them to commercial use—the electronics business is sort of turned around. They're out there innovating and inventing and we're putting their products to military use. (51–52, 53, 56, 60)

14. **STUART E. BRANCH**, "C³I and Crisis Management" (1984, pp. 87–102)

Deputy Assistant Secretary of State for Communications and member, National Communications System and US Communications Security Board, NSC

Now if you build a separate communications capability in addition to what is out there, are you building one that you're going to be able to guarantee for the long term? Will it work when you need it? My experience to date has been that if you want a system that's going to respond in emergency situations, it ought to be the same system you're using to meet daily operational needs. Or it ought to be built on, or integrated with, the same system used in a day-to-day operation. The hardware to meet an expanded crisis requirement is a carbon copy of what is in place today. Thus, the logistics chain is the same for that segment of the network intended to meet stress situations as it is for that which is meeting the day-to-day need. Your training is no different, nor your assignments, nor your support. What happens in a stress situation when you move a technician from a regional center into a stress post, if when he gets there he finds out he doesn't know that equipment? He doesn't have the tools, training, or the test equipment. What do you do with the cadre of people you trained on that equipment? Do you expect them to maintain it all? Where do the multiple skills you expect these people to possess come from? Where do you recruit, train and retain those kinds of skills in this environment, competing with the private sector? In my judgment the two systems need to be fully integrated. (96)

15. **RICHARD G. STILWELL**, "Structure and Mechanisms for Command and Control" (1985, pp. 33–65)

Chairman, Department of Defense Security Review Commission

[W]e are beginning to change the way the Defense Review Board does its business, and to focus increasingly on mission areas. Instead of dealing as we have in the past with intelligence here, and command and communication here, and forces here, and so forth, we started something last year that I think was reasonably successful. We began by looking at deep interdiction as an entity. In one special book we put together sensors, airborne platforms for the sensors, communications, fusion, and weapons systems so that we look at, as an entity, what you would need to provide a commander on the ground: the capability to detect targets, acquire targets, make the decisions on targets, and engage targets out to various ranges beyond the line of contact, for various amounts of investment. I believe that's a good way; at least an old soldier feels that's the way one ought to look at the programming business in terms of output—accretions, additions to capabilities. (61)

16. **DONALD C. LATHAM**, "A View from Inside OSD" (1985, pp. 103–23)

Assistant Secretary of Defense, C³I

To give you some idea, the total C³ request in **FY86** adds up to $22.1 billion, of which strategic is around five billion, theater tactical a little under four and COMSEC (communications security) about one billion. The C³ total was $18.5 billion in FY85, so our total FY86 C³ request is 19.5 percent higher than FY85, which includes inflation of about 3.5 percent.

FY86—fiscal year which began October 1, 1985 and ended September 30, 1986

[OETTINGER] That does not include the intelligence portions that have recently been put under you, does it?

[LATHAM] No. It does not include any intelligence.

These are the figures we have requested. Now how well have we done? C³I has fared better than the defense budget as a whole over the last five years. If you compare the annual increase in C³ funding against those of defense over the past several years (we've gotten 17.9%, 12.4%, then 13.5%), you can see that every year C³ has received several percent more than what defense as a whole has received. Now that C³ is in at a 19.5 percent request for FY86, if you take inflation out at around 3.8 to 4 percent, C³ is requesting at 15.5 percent real growth, and defense is at 5.9 percent real growth. If we get cut to three percent overall on defense (which is probably where we'll end up—if not worse), I'm hoping that I could come back next year and tell you that instead of getting 19.5 percent I received 14 percent, or something like that. Generally C³ has been able to prevail and get much better numbers than defense as a whole. But that also tells you that we've really, really been putting the money to it. And if you look back just a few years, C³ was nowhere near this size. In fact, C³ back in the late 1970s was way under $10 billion. So, we have grown enormously, and we're putting big bucks against the area; it has the priority, and it has the momentum. (112)

17. **CLARENCE E. MCKNIGHT, JR.**, "C³I Systems at the Joint Level" (1986, pp. 1–30)

Director, Command, Control, and Communications Systems, JCS

Only a relatively small part of your equipment should be military equipment, long cycle. Most of the stuff should be off-the-shelf; when you train people how to use the latest technology, you teach them technical expertise, which overflows into the national education systems. That training and that education give you the greatest ability to do crisis management, giving you in turn a profile of peacetime readiness, which is then reflected in the public state of mind. And it is just that simple. When I was on the tactical side of the world, struggling along with 40-year old equipment and trying to look very professional, that was really tough.

So we should be using what our industrial base is surging toward in order to project confidence among the great American public that we know what we're doing. This has a better spinoff than a lot of other things that are related to weapon systems. That's why I think procurement of C³ systems/equipment should be different. However, we shouldn't limit ourselves to just "off-the-shelf" procurement being pursued uniquely. Procurement in

general should be different. C³ equipment should be purchased in a different mode from the way we buy just pure weapon systems, although the two processes should be closely related. I do not believe that you need to have a lot of dedicated military equipment that ends up in motor pools around the world and is not used, because it quickly decays and it's very, very expensive. (8, 13)

18. **LIONEL OLMER, Esq.**, "Intelligence and the American Business Community" (1986, pp. 59–71)

Member, Paul, Weiss, Rifkind, Wharton & Garrison, an international law firm; former Under Secretary for International Trade, Department of Commerce

I would argue that defense procurement has recently been harmful to the process of industrial competitiveness. Not helpful. On the one hand it has spoiled a lot of suppliers, and on the other hand it has masked what I believe is a chronic condition, a chronic illness, in the American industrial base. If one is taking a political, partisan point of view, one can say the value of US exports from 1979 to 1983 in the manufacturing sector grew by eight percent. That's not great, but it is growth. The troublesome part of that is that nearly half of that growth has come from defense procurement. When you wash that out, the growth has been nonexistent. Nonexistent, in a two-and-a-half trillion dollar economy, over a period of some five years. (65)

19. **B.R. INMAN**, "Technological Innovation and the Cost of Change" (1986, pp. 151–68)

President and Chief Executive Officer, Microelectronics and Computer Technology Corporation

If you look carefully at the period 1946 to 1960, Department of Defense (DoD) investment and research was the pacing element in creating new technologies in a broader way. They were moved through for commercialization in four to five years, because that was the length of the defense procurement cycle. Then we launched off to create a perfect procurement process, and we ended up with a procurement process that takes 12 to 13 years, and we don't get that flow-through for commercialization. So the significant competitive advantage to the U.S. which came from Defense-funded research up to the early 1960s does not exist today, by virtue of our own internal constraints.

I was somewhat optimistic three years ago that Defense would once again play a leading role in addressing manufacturing technologies, which is an area that colleges of business administration don't seem to want to join with colleges of engineering to address. What's happened? Under **Gramm-Rudman** those programs are the first casualties. Almost all of the Air Force's funding for the integrated computer-aided manufacturing (ICAM) technology program is being reduced. So Defense, which could indeed play a role—I've heard some people out at **Berkeley** saying, only half in jest, that DoD is really the US **MITI**—isn't doing so because of our own arbitrary internal constraints.

Gramm-Rudman—1985 Gramm-Rudman-Hollings Deficit Reduction Bill

Berkeley—University of California at Berkeley

MITI—Japan's Ministry for International Trade and Industry

... I'd institute a six-year legislated ceiling for the Defense procurement cycle. Accept some mistakes, and put in an accountability process; if someone's ship goes aground, if there's a major cost overrun in a program, that's the end of his career. Accountability for performance. We do it in **black box programs** all the time, in those kinds of time frames. It isn't asking for the impossible, it's just asking for a standard of performance. But it's also forcing an approach to design wherein the ship, the aircraft, the personnel carrier is designed to last 30 years. You plan from the beginning to replace the avionics, the electronics, the areas where technology is moving fast, every six to eight years. You use a modular design to force a focus on interoperability and on minimizing the cost of change. That approach will be fought tooth and nail by those who are in the procurement process because it gets at a large number of jobs and procedures that have been in place for a long time.

black box programs—classified programs

Am I recommending it purely to make Defense procurement a lot better? I think it would have that result, but that's not my primary objective. My primary objective is an early commercial flow-through of the technologies that come from that Defense investment. Another reaction I see often is, "Let's shift 20 percent of the federal research investment from defense research to civilian research." Well, Norm Hackerman taught me some years ago when he was president of Rice that there is no such thing as military science or civilian science. There are scientific disciplines that you push, and it's how you choose to apply it later that shapes its use. I can't fight the structure.

Maybe the NSF is one area where you could shift 20 percent of all that funding and hope to get a broader focus on the things that will flow on to good use. I'm very skeptical of that. I think you would be much more likely to get it from the six-year procurement cycle, accepting that there would indeed be some mistakes made in looking for efficiency and speed rather than perfection. (154, 159–60)

NSF—National Science Foundation

4

C³I and Organizational Structure

The connection between C³I and the organization of the Department of Defense (DoD) can be traced to critics who saw theater and operational commanders being cut out of the decision loop in C³I acquisition. The debate about who should control the budget strings—for C³I as well as other elements of defense—triggered Congressional concerns about the quality of military planning, of military performance—especially in interservice operations—and of military advice to civilian leaders. In 1986, those concerns led to the passage of the Goldwater-Nichols Department of Defense Reorganization Act.

Reorganization tends to be viewed in two ways: as change for the sake of change or as necessary evolution. According to the first view, drawing little boxes and diagrams and shuffling people around is an exercise that wastes time, effort, and money; and accomplishes nothing. "It's the people filling the positions," say the opponents of reorganization, "who make things work or fail to work. Personalities are far more important than structures; the right people will make any structure viable."

Those who favor reorganization believe that structures must be adapted to changes in environment or goals. "Only unreasoning fear, laziness, or inertia," they argue, "will resist progressive, well-considered change. An organization cannot assume it will always have people capable of overcoming structural obstacles; it should always be open to better ways of doing business and to adjusting structures to recognize and institutionalize those better ways."

Frequently other issues determine which side of the argument a given player will take. Opponents of reorganization are often people who see it as a threat to their own power or the power wielded by individuals or groups they value. Similarly, advocates of organizational change are likely to be those who see the change enlarging their own power bases or those of their allies. This is not to say that all men and women are power hungry, only that objectivity may be more apparent than real in discussions about reorganization.

In the private sector, corporate gain or loss is often perceived to offer an unbiased criterion for determining whether or not a restructuring is necessary. If profits are down, it's time to reorganize; if they're up, it's not. Of course, there's always room to argue that an improved structure could raise already good profits or that a change will aggravate losses.

In government, unfortunately, the gain or loss yardstick isn't applicable. The balance sheet of the Department of Defense would have on one side the hundreds of billions of dollars expended; on the other, the words "national security." Is that an acceptable balance, or does it reflect a need to reorganize?

The nation's primary national security goal is deterrence of nuclear war. Does the fact that no such war has occurred indicate that DoD is doing its job well, or that the threat has been overstated? When things go wrong in a time of crisis—e.g. the bombing of the Marine barracks in Lebanon or the communications problems in Grenada—is it time to reorganize DoD or time to realize that things get screwed up in war? Does not being prepared for a minor crisis—e.g., not having minesweepers for use in the Persian Gulf—mean the nation would lose a major war? Or does it simply mean attention is focused—as it should be—on bigger issues?

Warnings about the inadequacies of theater C³I helped draw the attention of House and Senate staffers to the issue of DoD organization. Many argued that those inadequacies were directly attributable to a power imbalance, with the Services—the Navy, the Army, and Air Force—having all the power, and the specified and unified commands having all the responsibility.

For example, the Services would go though the procurement process for new systems without inputs from the specified and unified commanders whose forces would be employing those systems. As a result, field commanders might find that the "latest" communications equipment had left them unable to talk to subordinate or allied units, or that a new weapons system was incompatible with those already on hand.

Even more serious were the Services' holds on component forces. Though such forces were designated to fight under the theater commander, they had to rely on their parent Services for supplies, equipment, pay, promotions, and just about everything else—a relationship sure to encourage divided loyalties.

Finally, many argued that interservice collusion, a reaction to the bloody interservice squabbles of the late 1940s, diminished the

value of military advice provided by the Joint Chiefs of Staff (JCS), that such advice was often determined by a "lowest common denominator" process focused on the Services' interests rather than the interests of the nation.

Those opposed to major changes argued that putting the right people in important jobs—a strong and aggressive JCS Chairman, for example—would solve most problems in the existing system. Others expressed concern about allowing theater commanders to be distracted by procurement issues or exchanging Service specialization for "jointness."

The extracts in this chapter show the twists and turns in the path that led to the Goldwater-Nichols Act. Moving from General Odom's reflections on the need for some kind of general staff—which imply more than they say about interservice rivalry—to the stinging criticisms voiced by General Cushman, through comments like those of Admiral Richardson and General Marsh, which reflect an uncertainty about whether more or less centralization is needed, to Dr. Barrett's retrospective view of the Act's evolution and his concerns about the Services' efforts to evade compliance, one is tempted to attribute an almost serendipitous quality to the deliberations that have taken place. However, a comment Dr. Barrett made in his 1985 presentation offers a healthy counterbalance to such temptations:

> . . . [E]ven if a divine presence could give us a perfect organization today, it wouldn't be perfect a year from now because changing circumstances—weapons systems development and those sorts of things—would blur those boundaries and you'd have to redefine them. That means Service roles and missions need constant examination and redefinition.*

*Archie D. Barrett, "Politics and the Military—The Climate for Reform," *Seminar on Command, Control, Communications, and Intelligence*, Spring 1985 (Cambridge, MA: Harvard University Program on Information Resources Policy, 1986), p. 69.

Extracts

1. WILLIAM ODOM, "C³I and Telecommunications at the Policy Level" (1980, pp. 1–23)

Military Assistant to the President's Assistant for National Security Affairs

I am making a pitch for some kind of national military staff surviving and protecting the President. Otherwise he is going to go off and probably be taken into refuge in one of the commanders' staffs. So I wonder if the National Security Act of 1947 is adequate any longer. I wonder if it is adequate for deterrence in the 1980s and '90s. I wonder if we must not have some kind of military staff which stands above the military Services, which is not a prisoner of those Services and has some sort of survivability billeting or a system of command centers that will allow it to support the President in a variety of situations.

. . . I understand civilian control to mean control of the military establishment by elected officials. Is that fair? Now that's a very important point. Does it mean civil servants with GS numbers? GS–18s? You see, I am not sure that the OSD staff is any more responsible to the electorate, or is any less a political danger, than a uniformed national command staff. There is enormous confusion on that point, and most discussions like this—you hear it every day in the Pentagon—justify redundancy, layers of staff, extra people looking at papers they don't understand, in the name of civilian control. The discussion won't go very far if you get that red herring mixed in.

GS—general schedule, a pay and ranking system for Civil Service workers

OSD—Office of the Secretary of Defense

One other point. An interesting dynamic happens around the Executive Office of the President: if a staff feels responsible to the President (which I think a National Military Command Staff would do), I think you would find it being very much more responsive to political considerations than the Joint Chiefs will be. There is a great tendency to take the President's side. I know that from where I sit. I take his side on issues that I really have trouble with

personally. But I can work up a lot of enthusiasm just because of the atmosphere.

... You can do analysis for the purposes of enlightenment, for a parochial advocacy, or to achieve bureaucratic paralysis. My argument would be that in ordinary peacetime, under non-stress conditions, the second and third games get played with a great deal of vigor. But when the system is under stress from an external opponent, and the we/they syndrome is felt very strongly, I think the second and third games will be repressed, relatively speaking, and the incentives for getting it right and analysis for enlightenment go up. I quite agree that the national command staff, not under stress, left to look after the distribution of budgets, will become as corrupt and involved in games two and three as any other bureaucratic institution in the world. But if you put competitive units together, trying to put forth the most impressive operations plan for the President, under stress, I don't think the competitive mode is going to generate a better outcome. I think under stress I would rather have a well-structured timely bias than a group of biases with which I have to puzzle over when or how to choose. (15, 16, 21–22)

2. **B.R. INMAN**, "Managing Intelligence for Effective Use" (1980, pp. 141–61)

Director, National Security Agency and Chief, Central Security Service

I became a Vice Director of the Defense Intelligence Agency, a troubled agency, unstable, with rapid turnover of leaders, a perfect example of how not to create a government agency. The organization had been created in 1961 by establishing billets and then filling them by permitting the Services to send the agency the 60 percent of their people they wanted to get rid of, while holding on to the 40 percent they wanted to have. This made for a group of people who had no great reason to be innovative. They were just sufficiently accomplished so that they were at too high an achievement level to be fired. (143)

3. **JOHN H. CUSHMAN**, "C³I and the Commander: Responsibility and Accountability" (1981, pp. 95–118)

Lieutenant General, US Army (ret.); Management consultant

The problem today, as it was in the days of Pearl Harbor is elementary. It lies simply in the institutional failure to assign proper responsibility and accountability to major operational commanders.

... I have said that the adaptation that's successful in the business world takes place in the environment of the user. And that brings me to my point about the military adaptation. The military C^2 adaptation must therefore take place in the user's environment too. The key point, though, is that the user is NOT the military Service. The users are the fighting formations of the military Service under **unified** or **allied** command. That's an extraordinarily important distinction. The user is the major, the operational commander. And the institutional anomaly, the institutional block that's caused the deficiencies I listed in my indictment at the start of this talk, is that the way the Services are organized disregards this.

unified—a command which involves more than one US Service

allied—a command involving the military forces of more than one nation

When I say that the Services are the providers, not the users, and that the users are the fighting formations of the Services under unified or allied command, I'm not just giving you some idea that I have. I'm actually quoting the law to you. That's the statute that's been in effect since 1958. In the 1958 Department of Defense Reorganization Act, the only responsibility the Services retain is that of providing. The act set up the idea of combatant command, either unified or specified. It didn't set up the idea of allied command, but it implied that. But, notwithstanding the law, many of the practices have remained much as before. The command and control system requirements have been generated primarily by the Services, who still think of themselves as the users.

Now then, you can do that quite possibly with a tank. The Service can be a user of a fighter aircraft or even a destroyer, as long as you don't get too much into the communications that link them with the other allied fighter aircraft and destroyers. Those do pretty much the same task; in all they have the same air speed, ground speed, and weaponry, whether they're under Service or **Joint** command. But that's not so with command and control systems. Because, in NATO, the electrons of Germany's air force—the Luftwaffe—mingle with those of the US Army, the British **RAF**, and all the rest of them. If you need to figure out anything—for example, identification of friend and foe so you don't shoot down

joint—command composed of assigned or attached elements of two or more Services

RAF—Royal Air Force

your own aircraft with an air defense missile—you have to look at the user's way of operating and deal with the procedures of the user in the field, because the right procedure is going to simplify the electronics problem and the right electronics are going to permit different procedures. You have to have trial and error out there where the users are, just as you have to at Citibank or J.C. Penny or TRW.

... A good example is this. The Marines have developed, and in due time will field, a system for controlling artillery fire and tactical air, called MIFASS. The Army for some time has had a system for calculating the direction of artillery fire—TACFIRE. They will not work together if the present trend of development continues. If we ever have to fight Marines alongside Army artillery, the Marines will not be able to participate and use TACFIRE, and the Army won't be able to use MIFASS. That's an example of what I am talking about.

... Because a Service doesn't think about the fact that it will have to fight with some other Service. They think about fighting all by themselves. They figure that if another Service fights with them it will have to use their methods.

... Here's what the Secretary of Defense can do. He can call in his major operational commanders and have them meet as a group.... [H]e'd tell these men that they are responsible. He wouldn't have to do it quite the way General Patton did, but they would get the message, because that's the way they've been brought up. He'd look them in the eye and say, "I want you gentlemen to understand that you are responsible for the command and control systems of your commands—top to bottom—for their readiness for war, and for conditions short of war." He might say, "I have just read the Pearl Harbor investigation again, and I see that that responsibility was not very clearly assigned by the political magistrates of the United States in December 1941, and I don't want any misunderstandings. You are responsible for the systems' working condition in war and in conditions short of war.... I expect you to exercise your command and control system top to bottom—exercise it." ... Then he'd say that somehow he is going to create, at the seat of government in Washington, and stateside in the United States, institutions for multi-service concept and procedures development, for technical support of multi-service activity, for battle simulation of multi-service operations, for requirements generation that looks at the problem as a multi-service problem for configuration management, so that you're not going to have systems in one area of operation that can't get on target. Institutions are going to have to be responsive to these commanders' future systems needs. And now he expects his commanders to create institutions for the

same purposes in their commands, because that is what is needed—enduring institutions.... And then he says, "I want to make very clear to the Service chiefs that they are only the providers, they are not the users of systems." You know, that's bitter medicine, because they really don't believe it. Then he's going to say (my fantasy only goes on a little while longer), "I'm not fooling around about this. I mean what I say. I'm giving you the responsibility. I know what that means to you, and I expect you to take these responsibilities very seriously, because you're in command and this kind of responsibility goes with command. Readiness of your own command and control system, the full web, goes with command—inseparably. And I intend to support you in it. But I also intend to visit your commands. In fact, I intend to audit your commands, have inspections made and see how well you're meeting this responsibility. And then, in a couple of months, I will call you in again—one at a time—and you will give me a personal report about what you have done and what you intend to do. And I will listen to that report and I will take the appropriate action if I'm not satisfied."

Service chiefs—the Commanders-in-Chief of the Air Force and Army and the Chief of Naval Operations

I think that's a very sober charge to these gentlemen, and if he means business it'll be very profoundly motivating. It'll call for a rather substantial change in outlook—by everybody. That's what's required. Finally, the Secretary of Defense vigorously concerns himself with rearranging the bureaucracy at the seat of government so that the influence of the major operational commanders comes to bear as they move to meet their responsibilities, and can be accommodated. That's no simple matter. It might take several blowings of the trumpet to get the attention of the bureaucracy, and convince them that he really means it when he says that. It'll eventually happen.

... One of the institutions which will no doubt throw fear and trembling into the hearts of the personnel chiefs of the Services is to have some way of managing the selection of officers for Joint Staff or Joint command, and managing their development. The Joint Service schools, which are purely educational institutions now and are not developing doctrine, have very little responsibility for doctrinal development and thought; those Joint schools have to be developed. These are the sorts of institutions that the Secretary of Defense would busy himself in creating.

... When you finally figure out responsibility, the question is who gets relieved if it goes wrong? Unfortunately, the Department of Defense is not well organized, you can thank the government for that. I was a brigade

commander in the 101st Airborne Division in Vietnam in 1968—and I say to you that if I had conducted an operation in the manner of the Iran rescue mission I would have expected to be relieved. But you look around in the Department of Defense to find someone to relieve, and it's hard to find. That's one of the problems. Responsibility is not fixed, nor is accountability. The **Pearl Harbor investigators** had a very difficult time trying to find out who was responsible. In the seat of government, hardly anybody could be fixed as responsible; the institutions were not there for that. As it ended up, the two cummanders in the field, **Short and Kimmel**, were relieved and retired in disgrace. And that is very illuminating—but that principle has to be established, and guarded against the man un horseback, the great General Staff, and all that.

Pearl Harbor investigators—See *the report of the Cnmmittee on the Investigation of the Pearl Harbor Attack*, Investigation of the Pearl Harbor Attack *(79th Congress, 1946).*

Short and Kimmel—the two principle military leaders in Hawaii on December 7, 1941

These are very key issues. The federal nature of our federal guvernment—the checks and halances within the executive hranch itself, and certainly within the Pentagon—has got to be maintained. (96, 102–03, 106–08, 110, 113)

4. **DAVID C. RICHARDSON**, "The Uses of Intelligence" (1981, pp. 147–68)

Consultant, Defense Intelligence Review Panel, the Defense Science Board, and other panels

The planning structure within the Navy, the Air Force, and the Army these days is pretty much a mirror image of the structure within the Office of the Secretary of Defense itself. An enormous amount of time and energy is spent hy the higher-ranking military people working with their OSD counterparts. The nature of the current development process is so time-absorbing for our top people that they have very little time to think within the context of their Services. They seem to be caught up in a mechanism that just eats up their time, their energies, their human resources, and that is part of the problem.

. . . I have not seen very many good new things come out of Washington. The practical ideas largely come out of the fleet—I think my Air Force and Army colleagues would make similar remarks. Organizational structural changes are needed to reflect this.

. . . The fleet has a structure that's supportive of training and keeping up individual systems. What we call "type commanders" are responsible for all the ships or aircraft types. The Commander of Surface Forces, Pacific Fleet, is responsible for keeping the surface types of ships in good shape. The Carrier Air Force, Pacific Fleet, is responsible for the aircraft carriers, the aircraft, training, maintenance, people, everything that goes into that. The numbered fleet commander is responsible for blending the aircraft carriers, cruisers, and submarines and working them together as a coherent group. The commander in chief of the fleet is the boss of both kinds of people—the type commanders and the fleet commanders. That works out quite well in getting the most out of what we've got in the operating forces. I think that same sort of arrangement needs to be set up in Washington. I think the fleet voice in Washington has to be much stronger. In World War II we had the COMINCH, the Commander in Chief, in Washington, who was also Chief of Naval Operations. He spoke for both. I don't support the present National Security Act—that is, I don't think it's wise. I think a very significant part of our problems has come from the structure that we have, and I think it should be modified. (153)

5. **HILLMAN DICKINSON**, "Planning For Defense-Wide Command and Control" (1982, pp. 11–55)

Director, Command, Control, and Communications Systems, Joint Chiefs of Staff (JCS)

I am one of the directors of the Joint Staff. The chairman is General David Jones and, of course, the JCS are composed, as a committee, of the four Service chiefs of the Army, Navy, Air Force, and Marine Corps, the highest-ranking members and chiefs of each of their Services. This group of directorates supports the Joint Staff, and we also support the chairman as an individual in some roles that can be separated from supporting the chiefs as a body. They are the principal military advisers to the Secretary of Defense, the National Security Council, the President and the Congress. And a presidential decision involving a military force flows from the White House down through the secretary and deputy secretary of defense, the only people in the OSD who are in the line of command, and then through the Joint Chiefs and on to the **unified and specified commanders** in the field. That's the organization that was created in the 1947 National Security Act, as modified in 1958.

unified and specified commanders—refers here to all operational commanders

From that stem a great many of the problems we have in C³ systems, because C³ system development was certainly not provided for in any reasonable way in that act, in my opinion. I think eventually we will have to face that, or else we're going to begin to work around it more and more.... [C]learly the role of the Services as the independent developers, essentially, of all the material is part of that problem....

Change could happen, I suppose, on the basis of personality, but you ought to try to institutionalize it so that it is more difficult to change it for just personality reasons. Now, if the enemy threat changes, you have to change. You've got to react.

We are there to represent the interests of the highest two echelons of the command structure, particularly. One reason we were created was that it was apparent (you'll find it stated in the Defense Science Board report, and so on) that those two top echelons—the national command authority itself, the President's and JCS chairman's echelon, and the next echelon down, the unified commanders in Europe and the Pacific, and SAC and NORAD and so on, but particularly the unified commanders—the ones overseas, in Europe and the Pacific, for example—were under-represented and were disadvantaged users of the whole system. It's hard to understand how the President could become a disadvantaged user, but he really was. His presidential airborne command post was removed from the Air Force budget time after time because the programmers in the Air Force were more interested in fighter squads. We are now a counter-balancing force there, but even so, the requirements for the upper-level command and control systems of Europe, the Pacific, Korea, and so on have a very tough time in the budgeting and programming process within an individual Service—those who are worrying about Army things, or Air Force things, and properly so because that's the way they were set up within the national security organization. (15–17, 19)

We—directorate for Command, Control, and Communications Systems, JCS

SAC—Strategic Air Command

NORAD—North American Air Defense Command

6. **GERALD P. DINNEEN**, "C³ Priorities" (1982, pp. 77–93)

Corporate Vice President, Honeywell, Inc.; former Assistant Secretary of Defense for C³I

What Dave is recommending really isn't that big a change, which is why I think there is a chance of doing it. He's saying strengthen the role of the chairman, give him a deputy who will act for him. (Right now whenever the chairman's away one of the Service chiefs sits in.) Limit the Service staff involvement in the Joint process. Now when the chief of staff of the Army wants to do something he gets his staff to work up all the papers. Well, you know you're not going to get Joint advice that way, so you limit that. And he wants to broaden the training and experience and rewards of this Joint Staff. (90)

Dave—General David Jones, Chairman, JCS, 1978-82

7. **ROBERT T. MARSH**, "Air Force C³I Systems" (1982, pp. 95–114)

Commander, Air Force Systems Command (AFSC)

. . . I think all he [Secretary of Defense] has to do is saddle up somebody in OSD and give him the clout to enforce **interservice integration**. They've tried to do that with **the C³I position**, but they've just never given it the authority and the responsibility to do it.

interservice integration—here refers to interoperability of communications equipment "owned" by different Services

the C³I position—Assistant Secretary of Defense for C³I

[OETTINGER] Interoperability has been around for so long that one wonders whether it's not being killed with kindness. Everybody is so much for it, and asking for such total interconnectivity, that people throw up their hands at the cost and complexity—particularly Congress and the appropriations committees. So nothing happens—which may be a sophisticated way of reaching the end result desired in the first place, in keeping with Service autonomy. (103, 105)

8. **RICHARD G. STILWELL**, "Policy and National Command" (1982, pp. 115–45)

Deputy Under Secretary of Defense for Policy

The Secretary of Defense does not have a military staff as such. Most of the broad decisions made at his level have to be translated into specific

instructions which are not subject to misinterpretation, and which are properly formatted, explicated and elaborated to ensure that the decision takes cognizance of all the derivative and peripheral things that are set in train by it. The **National Military Command Center**, the communications nexus, is geared to do all of this. So it's both implicit and explicit that the way these decisions get translated to the field is through the Joint Chiefs of Staff. In 1972 the chairman's role increased, in recognition of the realities of the world situation—the growing importance of what and who is in the channel of communication, the Soviet Union's development of a capability for devastating attack on the United States, and the understanding that we were in an area where crisis can come up very suddenly. It was determined that, for time-sensitive operations—an emergency action message involving a nuclear explosion or something; a one-shot, limited situation—the chairman would act for the chiefs. . . .

National Military Command Center—command post located in the Pentagon

Over the years, the Secretary of Defense has acquired considerable power. There has been a decrease in the overall responsibilities and prestige of the Service secretaries, at least until very recently. It has been clarified that the unified and specified commanders are the ones who are going to fight our nation's wars, and that they're really the key to our response in the last analysis. And the chiefs' advisory role, in all instances, demands all of their expertise.

How have the chiefs done in performing their several missions? In strategic direction, the results have been mixed. We haven't had that many wars, of course. They were not significant players in the Korean conflict, for a number of reasons. They weren't capable of taking on MacArthur. They did not encourage him, though they supported him, in the most brilliant turning operation in modern history. They were not able to check him before he launched off on what was probably one of the greatest tactical disasters in our history: an uncoordinated, ill-conceived march to the Yalu. They were unable to constrain him in the actions that led to his relief. Thereafter we were, as you know, in a holding action in Korea in which the military strategy was secondary to termination of hostilities on conditions acceptable to us.

In the Vietnam conflict, the chiefs made a strong pitch in 1965 and were rebuffed. Thereafter they were pretty much relegated to support the recommendations of the field commanders, **Westmoreland followed by Abrams**.

Westmoreland followed by Abrams—Gen. William C. Westmoreland and Gen. Creighton W. Abrams, Military Assistance Command, Vietnam (MACV) commanders; the primary American commanders during the Vietnam Conflict

As to the development of strategic plans—well, we had no strategic planning in either Korea or Vietnam. In my parochial view, they have done better in this area, though there is a whole menu of plans which need to be better tested, validated, and so forth to make sure they are politically realistic, that their assumptions are correct, and the like.

In the matter of advice, again they have shown us very mixed performance. When the chiefs can sit down with the President eyeball to eyeball, they come across pretty well. Their written responses to queries for recommendations are sometimes less than persuasive, by the nature of a system that attempts to seek a consensus on many issues.

Where the chiefs are primarily faulted is in their role in programming and budgeting, and that area is the genesis of some of the suggestions for reform. There are two schools of thought. One says that you can't ask a Service chief, as the number one military professional in his department, to fight hard for the resources that he and all his like-minded subordinates consider absolutely essential for modernization, sustenance, or readiness, and then expect him to put on his other hat as part of a corporate body which looks at the total available defense resources, and to participate in a process which arrives at a different recommendation as to how the shares should be allocated.

The other group, to which I am a party, says, "Why the hell can't they?" We have all kinds of comparable experience in the corporate world, where chief operating officers of vertical divisions of corporations are also members of the board of directors, look at the large problem from a wide perspective and say, "Okay, I'll have to take my lumps with my guys when I get back, but you're right; there may be a better, more cost-effective way to do it."

One important item sometimes gets eclipsed. The 1958 amendment to the National Security Act, recognizing the pull and tear involved in how a chief divides his time, upgraded his vice-chief to four-star rank, so that the vice-chiefs could run the Services and the Service chiefs could be freed to spend the bulk of their time on Joint matters, because Joint matters are most important. The name of the game is to produce the most effective multi-service organization that can apply violence in the most efficient way, or combine most effectively with forces of other nations. We can't be sure how well that has succeeded, because it hasn't been put to the test yet.

... In July 1965, to go back to the real turning point in what then appeared to be a minor sequence of events, two of the chiefs said, "We're not for

massive intervention in Vietnam unless you mobilize the country, call up the reserves, and deal with this problem, if it is internationally significant, in a way that marshals the power of the United States." That outspoken view was not accepted. It was not a unanimous view. It would have been my view. Maybe those two guys should have tried to bring a couple more over to their side, or should have resigned right there to dramatize the point they were making, but they didn't. And from there we went on to gradualism, incrementalism, the whole works.

I do think that different points of view, whether they are the President's, the Secretary of Defense's, or Congress', are at least as important in the whole decision-making framework as unanimity—perhaps even more so. From time to time the chiefs have worried about "split papers," as we call them, recommendations going forward underscoring, "This is three to two," or "This is four to one," "There's one dissenter, two dissenters"—they worried that that could be used against them to whipsaw their positions. From time to time that has driven them to strive for unanimity, but at the cost of substance in many instances. And the chiefs are properly criticized for that.

... Jones is saying, "We need a more efficient system. The Joint Staff should do the creative thinking, the basic analyses, the answers to the tough problems. Then, when they've done their best, the chiefs should look at it, rather than have it emerge as a watered-down consensus to begin with. Next, we need better people on the Joint Staff, and they've got to be working for me. We need the cream of the crop. And to do that, the chairman ought to have a certain latitude in promotion, in getting the right guys and ensuring a somewhat longer tenure."

Those are Dave Jones' views. Some of them have been voiced many times. He suggests that there be a deputy chairman, a new four-star, assigned to ensure continuity when the chairman is out in the field, in more direct and continuing contact with the field commanders, the unified and specified commanders, than is now possible. Now the Chief of Staff of the Army, General Meyer, has come up with a more sweeping suggestion. In essence he's saying, "Okay, Jones, as far as you've gone, but you haven't gone far enough. What you really should do is take the Service chiefs of staff completely out of the JCS ring. Let them concentrated exclusively on administering, motivating, equipping, training, supporting their individual Services, and create a body of military advisors, a council chaired by the chairman, which would deal with all the Joint matters in resource allocation, and would advise the Secretary of Defense and the President on military posture. There's your strategic direction; there's the advice; no change, of course, in the chain of command as such."

Now, of course Jones and Meyer are significantly modifying the channel of communication. They are making the chairman the key guy in strategic direction of the armed Services, rather than the chiefs. My own view is this: clearly, for the small, time-urgent crisis, the chairman has to act quickly, because you can't get the whole corporate body together. But if you're fighting a war of any size, you had better be able to bring to bear the total competence and expertise that's available. . . .

Now, what are the problems with Meyer's solution? One comes immediately to mind: you then begin to really develop two power centers, two foci of advice. Certainly this is true from the standpoint of Congress, because in the budgetary process the Service chiefs are defending their programs in ways which could be in disagreement with the advice coming from the council of military advisors.

. . . They [the council of military advisors] would be four-star generals who somehow would be able to put together all their skills, all that they've learned in 30-plus years, divest Service motivations—and become total purple-suiters. Those gentlemen would never return to their Service—they wouldn't be wanted. They would be in the twilight of their careers. . . . But it isn't a foregone conclusion that a sailor, a pilot, and a soldier of this rank would agree with any more alacrity than is the case now.

. . . Well, everybody's had a crack at this. . . . All that is part of the decision-making matrix. It isn't easy when you stop and think about the parameters that have been put out. Congress does not want a single general staff, that's point one. Point two, the possibility of the Joint Staff becoming the Secretary of Defense's staff is probably not in the cards, though something approaching the parliamentary system would be welcome to many of us. The staff changes color dramatically in the office of the Secretary of Defense every time a new President is elected; all the senior people go and you don't have the continuity. So there's an area where greater efficiency and continuity in institutions could be developed. The great thing about the parliamentary system is that you just change the minister; everything else stays the same.

. . . I would underscore one thing: the unified commanders really command only the infrastructure. They fight with whatever forces are allocated, but their priceless assets institutionally are their mechanisms for exercising command and control and their intelligence framework. Their interrelationships with the countries in this area are their other key assets. What we haven't done yet, but we're gradually inching toward, is to do for them what we

have long since done for the national intelligence program: fence it off, free it from Service proclivity so theater intelligence capabilities don't have to compete with Service priorities.

We've begun to give money directly to the CINCs for experimentation, for innovations in command and control. Eventually we hope to fence off more funds for those commanders. Each area's going to be different; in contrast to strategic activity, there isn't all that much commonality. (117, 119–20, 121, 125–26)

CINCs—Commanders-in-Chief; here refers to the CINCs of the unified and specified commands

9. **JAMES W. STANSBERRY**, "Cost-Effective Rearmament" (1984, pp. 49–61)

former Commander, Air Force Electronic Systems Division

And by the way, in terms of Joint programs, which we're sort of addressing, I once was quoted accurately as saying, "compared to herpes, Joint programs are a lot of fun." They're very, very difficult to execute and administer. And I won't go into too much detail on that but let me tell you how it works. It works two or three ways. Number one, one Service invents something that another Service looks at and says, "Hey, that'll fill the bill." That's what happened with the F-4. The Navy developed the F-4 and the Air Force went and bought it. That's what happened with a little slick radio I'll tell you something about. It's called Have Quick. The Soviets have a jammer that they used in the desert war, and it got to the point where Israeli pilots couldn't talk to their own tower because the Soviet jammers were doing such a good job....

F-4—fighter aircraft

Anyway, what happens ... the guys in the jammer van listen. They find out what frequency the pilots are talking on, they tune their jammer to that frequency and send up a lot of energy, and now the pilots can't talk. So, we invented a frequency-hopping radio. It hops all over a certain band. And now they can't jam it. That was invented by the Air Force, purchased by the Army, purchased by the Navy, and the Marine Corps will also use it. Another way it works goes like this. We had all three Services spending money on a radar for ground targets. A moving-target indicator. The Army had a program that'd put a little radar up and it would peek across the edge

of the battlefield and say, "Aha? Ten klicks away is a tank, somebody shoot it!" I don't know what the Navy had, but they had something. The Air Force had a program called Pave Mover, where we had a big radar in a big airplane that could look way across, maybe a couple of hundred miles deep, across the FEBA, and spot not only movers, you know, heavy metal, tanks, but also stationary targets through the use of synthetic aperture techniques. OSD said, "Hold it guys, you both are doing essentially the same thing. You're trying to put a radar in an airplane and look across the battlefield. There should be one program." And they dictated it. It's my program now, it's called Joint STARS. And given 20 minutes, I might remember what STARS stands for. We've had a lot of trouble getting started on the program because rarely do you find that the two Services have identical needs. You know, the Army guys would run around and say, "Hey! We just want a little radar, a nice little airplane, go about ten klicks deep, and you guys are going to run off and invent a great big radar for a great big airplane and we won't be able to afford it." Because the money still comes out of the Service budgets, see? OSD doesn't print the money; anything they parcel out they first take out of Service budgets. It's off, it's launched, it's running. We'll probably release the request for proposals on that this week. That's one way—the second classic way—a Joint program comes out. (54)

FEBA—Forward Edge of Battle Area
Joint STARS—Joint Surveillance and Target Attack Radar System

10. SAMUEL P. HUNTINGTON, "Centralization of Authority in Defense Organizations" (1985, pp. 1-15)

Director, Center for International Affairs, Harvard University; former Coordinator of Security Planning, National Security Council

There's been monumental indifference to reorganization of the Department of Defense on the administration's part and, at times, rather articulate hostility coming from the Secretary of Defense and people around him. One can understand the indifference, since the Secretary of Defense can legitimately feel he has other priorities, including the military budget, weapons systems issues, and other things ranking considerably higher than tinkering with the way his office and associated offices work. There is also an argument articulated by Fred Ikle, Under Secretary of Defense for Policy, that organization isn't terribly important after all; that with the right people, any organizational structure can function. Consequently, Ikle believes it is almost a waste of time to tinker with organization. If he is right, however, then clearly an

awful lot of people—important people, busy people, powerful people—have been concerned with inconsequential issues, and have, in effect, been wasting their time.

The behavior of top national security decision makers indicates that organization is important. That is clear from the memoirs of people who have been National Security Advisors and Secretaries of State. For example, the first thing that Henry Kissinger or Zbigniew Brzezinski did on Inauguration Day when they were National Security Advisors or that Alexander Haig did when he was Secretary of State, was to stick a piece of paper under the newly sworn in President's nose, and ask him to sign a presidential directive setting up or defining the national security policy-making structure for his administration. When Kissinger and Brzezinski got their papers signed, they were very happy, but Cyrus Vance was terribly unhappy when Brzezinski's paper was signed, and Haig was furious because the President didn't sign his piece of paper. Presumably, that indicates that these people must think that organization is of some importance. And, of course, if it is unimportant, certainly during the past several months, John F. Lehman, Jr., Secretary of the Navy, has been charging about denouncing proposed changes in the defense system for no good reason.

If one looks at the history of organization and decision making, one can see that the decision-making process—whether the authority to make decisions rests with an individual or with a committee; whether entities are set up to report in one way or another; whether an organization is structured in one way or another, or whether or not there's autonomy given to a particular organization or part of it—makes a lot of difference.

One very interesting study done two years ago for the Director of Net Assessment in the Pentagon, Andrew W. Marshall, relates the differences in development of naval aviation during the 1920–30s among the major naval powers to precisely the differences in their organizations. In the U.S., a group of Congressmen and civilian leaders became convinced of the importance of naval aviation early on. They convinced Congress to create, against the wishes of the most important admirals in the Navy, a Bureau of Aviation, which, by legislation, had to be headed by an aviator and was given a very distinct position in the Naval hierarchy. In Great Britain, on the other hand, naval aviation was folded into the RAF (Royal Air Force). Obviously, an officer in the RAF didn't particularly want to go on detached duty to try to learn how to fly off an aircraft carrier; an RAF officer's future was elsewhere. In the Royal Navy, meanwhile, there really wasn't any interest or any incentive to learn anything about aviation. The Japanese came along later and eventually created a bureau of aviation near the end of the 1920s,

but considerably after we did. The study argues that the significant differences which existed in the development of carrier aviation between the United States on the one hand, and Great Britain and Japan on the other, can be at least partly accounted for by this difference in organization....

As I'm sure you all know, a wide variety of concerns have been raised in the past few years about US defense organization, and since I summarized those in my article, I won't attempt to elaborate on them here. I think it's important to note that those deficiencies, or alleged deficiencies, that have been debated in public recently are ones that have figured in almost every significant study of the Defense Department, official or unofficial, since the 1950s. They were precisely the deficiencies that led President Eisenhower to attempt a major reorganization of the department in 1958, and to succeed in getting a modest reorganization that people, nonetheless, thought had cured some of the major problems. In fact, as report after report during the 1960s and 1970s made clear, the same problems continued, and the Department of Defense has changed very little in terms of basic organizational structure since the early 1960s.

my article—"Defense Organization and Military Strategy," The Public Interest, Spring 1984, pp. 20-47

In effect, the organization of the Department of Defense has gone through two phases: one beginning at the end of World War II and extending through the early McNamara years, when there was a tendency toward increasing centralization on the civilian side, and relatively little change on the military side—albeit some change. This was followed by a period from the early 1960s to the early 1980s, when there was relatively little change anywhere in terms of organizational structure and relationships.

We are now moving into a third phase where there very probably will be some significant changes. But unlike the first phase when the changes were mostly on the civilian side and strengthened the authority of the Secretary, the focus of these changes will be, to a much greater extent, on the military side. There is a desire to strengthen the authority of the central military institutions in the Department of Defense, most particularly the powers of those members perceived as being divorced in some way or another from the Services—the Chairman and the unified and specified commanders.

A further factor that plays into all of this and that obviously is a highly debatable one, is the difficulty the U.S. has had in conducting successful military operations. After all, with one exception—the triviality of which only underlines the point, we haven't won a war since 1945. We have also suffered a

variety of miscarriages using military force in more limited ways, including the ***Pueblo*** incident, Son Tay, the ***Mayaguez***, the Iranian hostages, and Beirut. Consequently, the perception of our ability to utilize our military force, as a result of the accumulation of these incidents, is at a rather low ebb. Our successful conquest of **Grenada** hasn't changed that, since more questions—in many respects very real questions—have been raised concerning our effectiveness in that operation: the way it was planned (recognizing it was planned under very short deadlines), and the way the command arrangements were structured on the island. The whole conduct of the Grenada operation has simply reinforced the picture that our command relationships are not set up to employ military force effectively.

Pueblo incident—USS Pueblo, *an intelligence-gathering ship, was seized by North Koreans in January 1968. The ship's 82 surviving crew members were released 11 months later.*

Son Tay—abortive attempt to rescue POWs during Vietnam conflict. The rescuers found the prison site abandoned.

Mayaguez—In 1975, communist forces from Cambodia seized the US-flag freighter Mayaguez. *A small force of Marines was sent to recapture the ship and its crew. The captives had already been freed and put on another ship, but the operation cost the lives of a number of Marines.*

Iranian hostages—In November 1979 militant Iranians invaded the US Embassy in Tehran, taking 66 hostages. A failed rescue mission cost 7 lives. The hostages were released in January 1981.

Beirut—1983 truck-bombing of US Marine barracks in Beirut; 246 killed

Grenada—1983 invasion of Grenada marred by communications foul-ups, poor intelligence

At the same time that the Grenada operation was underway, similar questions were being raised about the Beirut tragedy. One of the most peculiar, frightening things was the problem of pinning down responsibility for what happened. In the end, the President said it was really his responsibility, which meant that it was no one's responsibility, and that, in fact, is an extraordinary conclusion. It was obviously reinforced by the fact that a Marine detachment was at the Beirut airport, the commander of which had to report up through this very complicated chain of command to the Sixth Fleet and then to European Command (EUCOM) headquarters, to General Bernard W. Rogers, SACEUR. Yet quite clearly, the extent to which the European Command and others were directly involved and concerned with what happened on the ground in Beirut was rather limited.

You may remember that after the incident, General P.X. Kelley, the Commandant of the Marine Corps, was sent to survey the situation. He came back and reported that what happened there really wasn't his worry. He said, "I am chartered by law to organize, train, and equip the US Marine

Corps. We hand forces over to the operational command for its use." So, in effect he's saying, "Well, General Rogers, it's really your fault, yours and your supporting commanders."

The fact of the matter is that the European Command had very little control over the Marines in Beirut. In many other situations, certainly in World War II, or certainly in Korea, and I would suspect in Vietnam, if gross negligence on somebody's part had been apparent concerning the proper security precautions during an incident, somebody would have been summarily relieved of command. And yet, that didn't happen. General Rogers and his deputy at EUCOM don't have the authority to relieve anybody of command. That is part of the problem with which we are dealing.

I don't want to continue in detail about the various perceived deficiencies, though they tend, as you know, to focus on the role of the JCS. The focus is on the difficulty the JCS have in performing an effective planning role, the weakness of the Chairman, the problems faced in resource allocation and weapons acquisition, the problems in the operations of planning, programming, and budgeting systems. They also focus on the chain of command in terms of the problems to which I just referred: the effort to maintain the distinction, so close to President Eisenhower's heart, between the operational command belonging to the unified and specified commanders and the administrative command belonging to the Services. As General Kelley said, the Services are the trainers and the providers of military forces, but not the users of military forces....

Just about a year ago, we had a very interesting conference here at the Center for International Affairs for which we prepared papers on the evolution of defense establishments since World War II in six countries including the U.S. The other five countries were the Soviet Union, the Federal Republic of Germany (West Germany), the United Kingdom, Israel, and Canada. ... Despite all the differences in these cases, since World War II the trend has been towards increasing centralization. The continental powers in particular have highly centralized armed forces, but even with the insular powers, there is a very well-defined series of progressions toward greater centralization....

If one begins with an assumption of separate land and sea Service departments each having its own minister and chief of staff, then the next step is to create an air ministry with a minister and a chief of staff. Then, because there are three Services, a chiefs of staff committee is created, as the British did in 1924, and as we did in 1942, to discuss and to deal with issues of

common concern to all military Services. At some point, the next step—I guess this would be step three—a defense minister is created, not a ministry, but a minister, who is a political coordinator. Well, he always ends up having an impossible task, of course, so at some point there is not only a minister of defense, but also a chairman of the chiefs of staff committee. Then, in order to support the minister of defense and make his life somewhat more bearable, a defense ministry evolves, which supports the minister of defense, and the Service ministers get removed from the cabinet. And then, in the next step, one finds a situation wherein the chairman of the chiefs of staff committee acquires greater power over the other chiefs of staff, and replaces in fact, in name, or both, the chiefs of staff as the principal military advisor to the government.

Meanwhile, another step has usually already taken place: the gradual centralization of control over support services. New central bodies are created to handle the civilian personnel, logistics, and administration. Then, and this is a most important step, the chairman of the chiefs of staff committee is converted into chief of the defense staff, and he gets control over the central interservice staff working for the chiefs of staff, which then becomes his staff, not the committee's staff. Immediately following that step, the Service ministers are abolished, then the Service chiefs of staff are abolished. Neither the U.S. nor the U.K. have reached this point yet, although the U.K.'s latest reorganization brings them very close to it. Ultimately, a central staff is organized purely on functional lines. By looking at these steps of gradual centralization, one can see that we are about halfway through the series, while the British are coming to the end of it.

... One of the things that came through most strikingly in this comparative analysis was the weakness of the US central military organization. It was the weakest of the six countries, and I'm sure this would be true compared to other countries that have significant armed forces as well.

... But the problem doesn't reside in the fact of decentralization as such, it resides in the nature of the decentralization. As I indicated in my article, the basic problem is what I label "servicism." In the absence of a stronger central military institution, the power basically resides with the Services. And that has all sorts of consequences such as the way decisions are made, the way programs are developed or which programs are developed or not developed, and the way military operations are carried out, as well as the fact that if there is a military operation of any size, no matter how small, all four Services have to be cut into it in one way or another, as was the case in Grenada.

I think it is wrong to refer to the problem in the US defense establishment as interservice competition or rivalry, because that's only part of it. If competition or rivalry exists among the Services—as it did in the '40s and the '50s, which at times got rather vicious—there's a way to deal with that. Any economist would predict how it would be handled in an oligopolistic situation: the parties get together and collaborate. As a result, the problem is not just interservice rivalry now as much as it is the apparent solution to that rivalry: interservice collusion. Both of these are manifestations of this servicism phenomenon that permeates the US defense establishment.

... Now, you can contrast the period since the early 1960s with what went on during the 1940s and 1950s when there was vicious interservice rivalry. A top general of the Army Air Force was describing the Marine Corps as a "bitched-up little Army talking Navy lingo" and Air Force and Army people were saying, "What do we need the Navy for? There's no one for it to fight." And, of course, in 1947 there weren't many enemies around for the Navy to fight. Navy people were responding in turn, and there were battles over the introduction of the so-called supercarriers.

We had never experienced such interservice disagreement before. Now suddenly they had obviously different interests. They have since learned to cooperate or collude and to divvy things up, each Service chief counting on the others to back him up in turn after he backs them up. This period of collusion or cooperation has replaced the earlier one of intense, vicious, bureaucratic battling, and one can argue about which is better or which is worse. As I indicated, they are both manifestations of a more deeply rooted problem in the sense that the power does lie with the Services, and until a counterbalance is created to the Services' power, there's either going to be intense rivalry or the friendly I'll-scratch-your-back, you-scratch-mine type of collusion.

Well, let me make a few comments on the proposals for changing these perceived deficiencies. As I mentioned, over the past few decades, a variety of studies have been made of the Department of Defense's organization, virtually all of which have argued to a greater or lesser degree for centralization. The Nichols Bill that was passed by Congress made some modest changes in the organization.

That bill essentially provided for five things. First, it gave the Chairman of the JCS statutory authorization to be the spokesman for the CINCs, for the unified and specified commands. While this provision was not necessary in order for him to carry out that role, it gave legislative blessing to the idea.

Second, it gave the Chairman control of the JCS schedule in terms of bringing potentially important things before the JCS, although he already—as far as I can gather—had played a substantial role in determining the JCS schedule. Third, it provided, by legislation, that the Chairman should select the officers of the JCS on nomination of the Services. This is one of those provisions that I think could be rather significant, if an aggressive Chairman wanted to use it and assert a power that hadn't been asserted before. However, it's unlikely that a Chairman would be terribly assertive with his power. I'll come back to this point in just a moment. Fourth, it extended the possible tour of JCS service for officers to four years. And fifth, it told the Secretary of Defense to make sure that the JCS would function as an independent staff, a rather vague declaration. It's not entirely clear what, if any, meaning that will have in practice.

This bill, I think, is more notable for what it didn't do. It didn't give the Chairman the power to manage the Joint Staff, and that was what many people expected. And it didn't say that he could, on his own, provide independent advice to the President, the Secretary of Defense, and to the National Security Council, instead of simply reporting the views of the Joint Chiefs. It didn't make him the principal military advisor to the President or the Secretary of Defense. It didn't give him a deputy, which is something many people had recommended. It didn't put him in the chain of command.

The chain of command down from the Secretary of Defense is not specified by law. But going back many years to Secretary McNamara, the chain of command has run from the President to the Secretary of Defense, then through the JCS to the unified and specified commanders. Many people argued that the Chairman should replace the JCS. The bill didn't—as some people argued it should and as a bill previously passed in the House had provided—place the Chairman on the National Security Council (NSC) as a formal statutory member. That's a bad idea. And it didn't give the chairman control over the promotions of people on the Joint Staff. That's a good idea.

... It's hard to distinguish what is cause and what is effect. But it is alleged that the Services, by and large, tend to send their better officers, not to the Joint Staff, but to their own staff. Not that they send only poor officers to the Joint Staff, that clearly isn't the case, but they tend to give preference, as one would expect, to their own staffs.

... General Rogers, who technically is the ultimate commanding officer, had no control over the situation [in Beirut], couldn't remove anyone, didn't have the authority to do so. That is a very bad way to divide responsibility.

And if, as I suggest in my article, you're going to have a unified command, then the unified commander ought to be able to move people around, fire them, relieve them, and so forth. Now he doesn't have that authority.

... There are some people who would go further and say that the Chairman really ought to prepare the military program of the government, and that he should submit each year to the President and the Secretary of Defense a fiscally constrained military program, which in effect would be the defense program. I don't feel strongly one way or another on that; I think that would probably be a useful thing for him to do. But I'm very sure that no Secretary of Defense is going to want to allow himself to be in the position where he has the Chairman's recommendation and nothing else. He is going to want to come up with his own, and he inevitably will turn to mission under secretaries or personnel like that, to work as his staff and provide him with advice. Given the importance of civilian control in our system, it is very, very important that he have that sort capability.

... There are certain places whence opposition to reorganization and centralization of authority has come. In the past it generally came from three sources: first, from liberal groups and leaders who were afraid of a Prussian general staff and militarism; second, from congressional groups who saw greater concentration of power in the Executive Branch as limiting their ability to gain entree into it and to influence what was going on (Congress always wants to decentralize the executive); third, from the Navy and the Marine Corps.

The striking thing about the situation now, it seems to me, is that the opposition to reorganization and greater centralization from the first two opponents that I mentioned—from the liberals and from Congress—has greatly weakened. Basically, the people in Congress and, you know, the more liberal groups and newspapers, are supporting the same reforms we are recommending in this task force. And so now the only really strong opposition comes from the Navy and Marine Corps, the traditional centers of opposition.

... Change, particularly in our system of government, occurs very, very slowly.

David Jones told a story that illustrates that. He used to sit with his British counterpart, Admiral Sir Terence Lewin, their Chief of Defence Staff, at NATO meetings and elsewhere, and they would compare notes. This was back in 1981. They would discuss how they wanted to change their defense

or military structures, and Jones and Lewin had the same ideas about strengthening their central defense organization in order to get control over the Services and have a more rational and effective planning system. And David Jones said Lewin went back, wrote up his plan in a memorandum and sent it to the Prime Minister. He got it back two weeks later with "Approved, Margaret Thatcher," written on it. It was implemented immediately.

And David Jones said, "I went back, wrote an article and published it three years ago, and today it is still being debated." (1–2, 2–7, 8, 9, 13–14, 15)

11. **RICHARD G. STILWELL,** "Structure and Mechanisms for Command and Control" (1985, pp. 33–65)

Chairman, DoD Security Review Commission

The Joint Chiefs of Staff (JCS) are not in the direct chain of command, but, as we'll discuss a little later, they are in the channel of communication with a very important function of strategic direction, because orders go through them. And we'll talk briefly about the interface between the channel of communications and strategic direction.

The military departments are responsible for raising, training, equipping, and supporting the forces. They're not in the operational chain....

Now, you can say, if they're [the JCS] not in the chain of command, but just in the channel of communications, then how do they provide "strategic direction"? Well, what that really means is that when the President makes a decision, it's obviously a very broad decision in which he's saying he approves such and such a recommendation. That has to be translated by somebody—some competent military body—into a full-fledged instruction for the people in the field. Sometimes that requires concurrent compensating or supporting action by many elements of the armed forces, because if you say to one organization, "Go do this," you may need to bring to bear more assets. Moreover, if that commander is going to carry out that action, he may need help; there are people on his flanks who may have to do something also.

There are a host of things that are the province of the military that have got to be done either by the National Military Command Center itself, or by the very competent Joint Staff. These are very basic functions: They make

recommendations on force structure, unified command plans, doctrine, education, and other matters.

Now, one thing not included in those JCS functions ... is any charge to the Joint Chiefs to advise the Secretary of Defense, or the President, on how the budget should be divided, or how resources should be allocated among the Services. Although many times the Chiefs are castigated for that failing, that's not written into their charter.

Frequently they are also castigated for tabling in the Joint Strategic Planning Document (which is at the apex of the planning cycle of the Department of Defense) mission requirements that exceed, by quite a margin, what is likely to be available in the way of resources for defense. Now, I maintain that they shouldn't be castigated for that. I maintain that it is explicit in the charter that the military advisors have a cardinal responsibility to inform the civilian leadership of this nation, through the Congress, of what would really be required to defend our territory, our people, and our value system, with prudent risk, if we were attacked. Recognizing that they're not going to get those resources in steady state, the JCS is at least keeping that mark on the wall so that if we got into a period of increased tension, if we were attacked, those stipulated requirements would become the blueprint against which additional resources would be applied to equip and flesh out the armed forces for defense. If they didn't do that, if we did all our planning on the basis of the resources we thought might be available, we would soon lose that mark on the wall showing what was required, and we would have no real basis for the immediate commitment and utilization of additional resources—be they manpower, equipment, or anything else—in the instance of aggression. Those are the functions of the Joint Chiefs of Staff, and I believe they are discharging them quite well.

The other area for which the Chiefs are castigated is on the timeliness or the precision of advice to the President, the NSC, and the Secretary of Defense in times of crisis, or in meeting unexpected situations. That's a fair criticism. In the past, they have not done all that well in telling their superiors what they wanted to hear in many instances, such as on arms control. But there again, it was very hard for the Chiefs to modify their views, to take full account of political realities, because that's really not their job. They're supposed to come at things from a military perspective. They have done, in my view, far better under **General Vessey's leadership** than they did under Dave Jones, Vessey's predecessor. I have been extremely pleased by the ability of the Chiefs to coalesce and to present a united front on

General Vessey's leadership—General John W. Vessey, Jr., USA, Chairman, JCS at the time of this presentation

most current issues. I believe that a lot of that has to do with the exemplary leadership of that fine Chairman, Jack Vessey.

... I don't believe in making the Chairman the sole military advisor to the President. That's fine for some minor crisis, but for a major crisis you need the expertise represented by all five Chiefs. ... But I would give the Chairman more control over the Joint Staff. We have just created for General Vessey, by the way, an analytical capability so that he can have more of an independent backup for the deliberations of the Defense Resources Board during the programmatic and budget review process. An organization called SPRAA, Strategic Plans Research and Analysis Agency, now has the capability of analyzing the data of the several Services on cross-cutting, cross-mission areas, and there are many of those. The two-star who heads SPRAA also prepares the Chairman for his role on the Defense Review Board (DRB).

The Chairman is, in my view, the individual who is most listened to on a contentious issue by the Deputy Secretary of Defense. And the Chairman's view usually prevails. The Chairman's view is mainly in support of what's in the Service Program Objective Memorandum (POM), and mainly in opposition to any of the advocates on the Office of the Secretary of Defense (OSD) staff who wants to change the POM. But on certain issues, he will disagree with what's in the POM and recommend a modification, particularly when it's something that can be translated into an output and related to mission accomplishment. So, in short, it's important to make the Chairman the spokesman for the unified and specified commands, because as we'll see in a moment, while I believe that it is an area in which we have done a lot, we've got to do a lot more to give visibility and influence to the unified and specified commanders. They are the guys on whom the whole responsibility rests in time of crisis and war.

We should also give the Chairman a little more control over the work of the Joint Staff; give him tacit authority to reject candidates for the Joint Staff, in the interests of getting the best possible quality. Additionally, we should support him analytically so that he can carry the battles of the unified and specified commanders against the other members of the Defense Resources Board when there is a major issue on resource allocation....

In terms of command and control, it's important to understand the structure of the unified and specified commands. All of those commands have Service components. For example, in Europe, under the joint headquarters

commanded by **General Rogers**, there is an Army component, a very minor Navy component, and an Air Force component. They report back to their parent Services for everything except operations. Their Services then determine, in the last analysis, how many troops and what type of equipment they'll have, and the rate at which they get that equipment. So, you have a certain duality there; the whole resource development process is done on a departmental basis as opposed to a Joint basis. And that's the way it's defined in the Congress. It takes a bit of doing to ensure that the Joint and the Service things are properly intermeshed. And that's really where most of our problems lie.

General Rogers—General Bernard W. Rogers, USA, Supreme Allied Commander, Europe and Commander-in-Chief, US European Command

... I believe the current JCS system, consistent with the mandate of Congress (which we haven't changed), along with more authority for the Chairman, as we discussed, is the way to go. And we have moved a little closer to that, I think, over time. But you've got to remember that any organization, and how good or how bad it is, is a function of the personalities you put in it. I don't want a structure that puts too much authority in one man's hand, because if you get a loser, a guy who doesn't measure up, it's pretty hard to get rid of him. We've operated on consensus pretty much in the past, and reasonably effectively.

... [T]he traditional roles and missions of the Service are to provide the forces, equip the forces, and so on. The CINCs have largely gotten their input for requirements from their major Service commands: Army, Navy, Air Force, whatever. You have the fortunate situation, I think, in the Air Force, where the specified commanders have a much better link to their Service in the Joint hat, because they're also **MACOM** commander in the unilateral hat, than the others do.

MACOM—(also "majcom") major command

Also, the defense in the Congress is by the Service, and by the Service program. But we have increasingly found with the new Congress, with more attention being given by the Congress to the last budget, with sharper questions being asked, that a lot of the questions are ones that the Service representatives cannot answer as well. They can answer from a programmatic and technical standpoint everything about System A, B, C, or D, but they can't answer as well as the operational commander why you need that system, and what it will do for you if you have it. In other words, they can answer the

what and the how of the system at the Service level, but it takes the operational commander to tell the why for it. So it's been evolutionary. We've always done our business that way. We've always had the theater commanders lamenting the fact that they had very little influence on the cross-cutting issues.

The other thing that's happening is that more and more programs are being initiated for weapons systems that involve more than one Service; particularly in this whole command, control, and communications area where the **black box** that the Air Force needs is essentially what Marine Air and Naval Air need: **IFF**, tactical fusion, so on and so forth. So, we learn slowly in a democracy, Dr. Oettinger. There's more attention, though not enough, being paid to the complexities of coalition warfare. We've done quite a bit on that. (33, 38, 40, 40–41, 44, 60, 61)

black box—electronic component

IFF—Identification Friend or Foe; computerized system for identifying aircraft

12. **ARCHIE D. BARRETT**, "Politics and the Military: The Climate for Reform" (1985, pp. 67–86)

Staff member, House Armed Services Committee; former Military Staff Assistant to the Executive Secretary of the Defense Organization Study; author, Reappraising Defense Organization *(1983)*

The characteristics of the Services must be taken into consideration when looking at reform of the way the Department of Defense is organized. Like all organizations, the Services want to protect their significant interests and to exert influence. That's any organization's reason for being. The Services are no different in that respect, but they are stronger organizations than most.

Services, like other organizations, vie for autonomy. They want to protect their budgets and expand them, for example. They want to protect and nurture their personnel, to control all aspects of a Service career to keep their personnel imbued with the essence of their own organization.

This essence is the distinctive mode of warfare each Service represents. The Air Force has considered itself historically the organization that fights and wins wars by sending men in airplanes to accomplish long-range strategic bombing and tactical air operations. The Army, through organized units, prosecutes land warfare. The Navy, through large capital ships, maintains

control of the sea. That's the essence. The Army has other responsibilities, such as air defense, but that is not the essence of its role.

Pursuant to its essence, each Service has a purpose that can be called its objective or mission. It is the preparation for that Service's distinctive style of warfare. For example, the Navy's mission is to prepare naval forces for the effective prosecution of war at sea.

These purposes require large capabilities. How much is enough? From the perspective of the Services, there is never enough. Why is this so? Because their missions are so broad. They operate in conditions of uncertainty with respect to their enemy, the threat he poses, and his intentions. No one can know for certain how many ships will be enough to ensure that the Navy can accomplish its mission. Because there are four Services grappling with broad missions in conditions of uncertainty and, at the same time, operating in an environment of scarce resources, there is built-in conflict between the Services. This conflict will always exist, no matter how you organize the Department of Defense.

Another aspect of this discussion is the tendency to identify Service interests with national interests, because it is difficult to translate national objectives or national interests into operational terms. For example, deterrence. What does it take to deter the Soviet Union? Who can say? Because national objectives are difficult to "operationalize," one finds the opposite tendency. The Services evolve an agreement in terms of operational weapons, and agree that deterrence requires a triad of land- and sea-based missiles and strategic bombers. The triad becomes not only a Service interest, not only an Air Force interest in missiles and bombers, but a national interest. That is, in the Air Force's view the triad becomes a national interest and a national objective. Moreover, it's a short logical step from that reasoning to the conclusion that the Service's well-being itself is in the national interest. After all, if the Air Force or the Navy is providing deterrence, then that Service itself is of instrumental value to the nation. To paraphrase **Charlie Wilson**, what's good for the Air Force, or the Navy, is good for the country. Now let me talk about two characteristics of the Department of Defense as a whole. I've already mentioned one, conflict. There's always conflict in the Department, as in any organization.

Charlie Wilson—Charles E. Wilson, 1890-1961, automobile executive and Secretary of Defense during the Eisenhower Administration; noted for saying, "What's good for the country is good for General Motors, and what's good for General Motors is good for the country."

There is also coordination. If you examine **Max Weber**'s model, he didn't recognize conflict. His idea was that if a task was too large for one or two individuals, you should divide it up into separate sub-tasks or functions. If it's a very large task you subdivide those functions into more functions and you achieve a hierarchical organization. From Weber one gets the idea that moving boxes around on an organizational chart leads to solutions for structural problems. If we could just get the boxes right, we could improve the organization's efficiency. The problem with that idea is that Weber assumed everybody in the organization was cooperating. If everyone did cooperate for the larger good of the organization, maybe Weber's model would be completely valid.

Max Weber—German sociologist and economist, 1864-1920

In fact, once you set out functions, you encounter conflict as each of those organizations or sub-organizations demonstrates some of the characteristics I mentioned earlier. They want to influence, they want to protect their domain, roles, and missions. They have an essential nature that they developed internally. They seek independence, they seek a budget of their own, and they want to maintain the morale of their members to cement their loyalty. So, there's a valid perspective of the Pentagon as a large organization in which the sub-elements conflict.

Yet I don't want to slight the cooperative aspect. As members of the overall Department of Defense, the constituent organizations respond to, or can be made to respond to, the national interest as well as the interest of the Army and the Air Force and the Navy. Although contradictory, conflict and cooperation are going on at the same time. So if you're studying organization, you have to consider both aspects.

Now, if all this is going on at the same time, the trick for higher managers, or for people attempting to organize a defense establishment, is to do three things. First, they must ensure that all important interests are mobilized. By mobilized I mean that every interest is represented by an organization. For example, Department of Defense critics today claim that the Joint interest is too weak and not organized. Yet it's a legitimate interest that should be considered when the civilian leadership makes decisions about resource allocation. Joint military organizations will employ US forces in any war. On the other hand, the interests of the Services are considered by critics to be too strong, relatively. So you want the organization to ensure that all valid interests are mobilized. Second, high-level officials should ensure that those interests are adequately represented in decision-making bodies. Finally, the decision-making bodies must be structured to resolve conflicts, so that ultimately cooperation emerges from conflict resolution.

... [E]ven if a divine presence could give us a perfect organization today, it wouldn't be perfect a year from now because changing circumstances—weapons systems developments and those sorts of things—would blur those boundaries and you'd have to redefine them. That means that Service roles and missions need constant reexamination and redefinition. Yet we haven't done that, formally at least, since the 1940s.

... [W]ith regard to the Department of Defense, a Secretary who knows his business will reserve 10 to 15 percent of his time to detach himself from the issues of the day—to get above his organization, figuratively, and look down on it—and attempt to perceive what is or has happened organizationally. He will continually reshape the organization because there will always be some interests that are stronger than others, growing and tending to coopt. As I recall, **Simon** dwells on this: It's a dynamic thing. The higher-level manager has to spend time shaping and reshaping his organization so that it funnels to him the perspective of the various interests as he makes decisions. In a way I think this is what the reform movement is trying to set up in the Department of Defense.

Simon—Herbert A. Simon, The New Science of Management Decision, *revised ed. (Englewood Cliffs, NJ: Prentice Hall, 1977), pp. 126-31*

... Superimposed over the Services is a very strong Secretary of Defense. Successive secretaries in the 1940s and 1950s continued to go to Congress to complain about how weak they were. So in 1958 Congress said, you have overall "authority, direction, and control" of the department. In the report Congress said, in effect, we can't think of any stronger words. If anybody can think of a stronger formulation, we'll take it. We're telling you, Mr. Secretary, that you've got the whole ballgame. So we have a very strong Secretary of Defense, according to the law.

... [J]uxtaposed opposite the Services who are supposed to recruit, train, and support the armed forces, what I termed "maintain"—is the employment side of the organization. It is composed of the Joint Chiefs of Staff and the unified and specified commands. This is the Joint part of the Department of Defense. If you read the introductory policy statement to the National Security Act, you will find the elements of this organization set out in one paragraph—separate Services but an integrated land, sea, and air team when the United States goes to war. The unified and specified commands are created to fight—to employ forces.

... In fact, by Pentagon directive, as I'm sure you know, the chain of command extends from the President to the Secretary of Defense through the

Joint Chiefs of Staff committee to the unified and specified commanders. "Through" means that the JCS cannot issue an order, cannot command, on its own. It issues orders in the name of the Secretary or the President.

The Joint Chiefs of Staff are supposed to provide military advice from a Joint perspective. That is, on the Service side, each chief attends to single-Service concerns and interests but, in theory at least, when the chiefs go over to the Joint side and act as members of the Joint Chiefs of Staff they are supposed to put on a Joint or unified hat. They are supposed to assist in the exercise of command. That's the reason the chain of command goes through the JCS. They're supposed to develop integrated strategic, logistic, and contingency war plans. And they're supposed to ensure that the plans integrate the contributions of the Services and the unified and specified commanders.

Also on the Joint side of the organization are component commands that report to the unified and specified commanders. As things have worked out, the unified and specified commanders only have operational command—a much more limited concept than full command. Although you cannot prove it by researching the law, I think that Congress, in giving operational command to the unified and specified commanders, meant that they should have a great deal more authority....

Just as the members of the Air Forces in Europe focus on their individual Service, the members of the Joint Staff, which was created to assist the Joint Chiefs of Staff, as officers assigned by the Services know that they are going back to their Services. When I was in the Air Force we talked about bringing an officer in and "blue-ing" him before he went to the Joint Staff to become "purple." And by that we meant sending him to the Air War College, bringing him to the Air Staff, and then letting him be assigned to the Joint Staff. But even if these things didn't happen to indoctrinate officers, the procedures under which the Joint Staff works, which have been woven by the Joint Chiefs of Staff, are such that any Service has a veto over almost any word or phrase of any document that might originate in the Joint Staff. So it is very difficult for the Joint Staff to be a dynamic institution and to act as a true Joint institution. It serves, I think, more as an executive secretariat, putting the views of the Services together in some palatable form that all four can agree to and then pushing the agreed position up to the Joint Chiefs of Staff.

The Joint Chiefs of Staff is dominated by Service interests and it's difficult for the chiefs to put aside the Service hat. The JCS is criticized because its military advice is inadequate, often sidestepping critical issues. I might

comment here that the present Joint Chiefs of Staff under General Vessey is reputed, and I think probably rightly so, to operate just about as well as the system can work, principally because of Vessey's leadership and the chiefs of staff we have. But even now I would maintain that the Joint Chiefs of Staff cannot, and does not, address some of the most critical defense issues. It is very difficult for the Joint Chiefs of Staff even to look at issues such as resource allocation, roles and missions, the unified command plan—how the world is divided up into unified and specified commands—or the cross-Service missions the Air Force is supposed to provide for the Army, such as airlift, sealift, and close air support. The Chiefs don't even want to open the unified command book because it becomes a bloodletting when they do. . . .

[By law] the Chairman became spokesman for the CINCs on operational requirements, but not their supervisor as the House proposed. The word "supervisor" did not survive the conference. On the timeliness issue, the Chairman became "responsible for determining when issues will be decided," once again a relatively minor provision. Probably most significant is the provision regarding the Joint Staff officers. The Services will now nominate Joint Staff officers, and the Chairman, through the mechanism of a Joint Staff personnel process, will choose them. So Joint Staff officers now will work for the Chairman, and not for the Services. They will know they weren't just sent to the Joint Staff by the Navy or the Air Force or the Army, rather they were chosen by the Chairman. I hope that provision straightens out the loyalty issue somewhat. There is also a provision that changes the limitation on the length of a Joint Staff assignment from three years to four years. As a further spur to continuity, Joint Staff officers can also be reassigned to the Joint Staff after only two years now, rather than three. Finally, there is this oversight hook that I talked about earlier, requiring the Secretary of Defense to ensure that promotion and retention and career opportunities are protected for Joint Staff officers.

By law—HR 3718, Joint Chiefs of Staff Reorganization Act of 1983 (the Nichols Bill), was passed by the House on October 17, 1983 but was stalled in the Senate. Some of its provisions were subsequently incorporated into the House version of the FY 1985 DoD Authorization Bill.

. . . We know that if a certain portion of Joint officers must be promoted, and that portion must be comparable statistically to the Service promotion rates, the Services are going to place officers in Joint positions that they want to promote. They will not want to be caught in the position of having to promote officers they would not otherwise promote. So we're after the assignment process; not the output, but the input.

... Why has the Senate been the stumbling block? The Senate Armed Services Committee contains Senators who are proponents of the opposing views on the JCS issue. Several have strong lasting ties to the Navy and are persuaded that those who want to maintain the status quo are correct. I believe the divisions extend to the Senate staff also. (67–68, 69, 70, 72, 81–82, 83)

13. **DONALD C. LATHAM, "A View From Inside OSD" (1985, pp. 103–23)**

Assistant Secretary of Defense, C³I

I think that all the stuff I've read about the reorganization is way off base, giving the Chairman more of this and more of that. That is not the problem. Grenada is one beautiful case in point; Vietnam is another, probably much more so because we were there so long. In my judgment we didn't have the political courage within the military, when we look back at Vietnam, to put together the right command structure because of the politics, the tugging, and so on. We didn't really apply the unified command theory that we had at our grasp in order to make the thing work. If you look at Vietnam and the command structures of the Air Force and the Navy and the Army, it was a nightmare. We had some things that were being commanded from **CINC PAC**, some things from MACV (Military Assistance Command, Vietnam) in terms of air support, and North Vietnam air support was commanded by two or three different guys. So, the Chairman could have had all the things in the world provided in this bill or any other, and it wouldn't have changed that situation unless he had the courage to go make it happen and fight down the politics of each of the individual Services.

CINC PAC—Commander-in-Chief of the Pacific Command (PACOM)

And if you carry through and think about the illogic of some of the things that have been proposed, like moving personnel with experience to the Joint Staff, it becomes absurd. For example, take a mid-career officer who has had experience in flying helicopters around in the Navy, and assign him to the Joint Staff for the rest of his life, and he will wear the so-called purple suit, he will forget everything he ever knew about allegiance to the Navy and all of that and become a nuclear war planner in the Joint Staff. And he never goes back to operations again, and for the rest of his career until he dies, he's in the Joint Staff arena. That's one of the proposals. I think it's crazy.

The Chairman's got all the power he needs. He really does. They say he doesn't have any staff. That's nonsense; he's got that huge staff supporting him. It's just a matter of using the Joint Staff and having the political courage to make the hard decisions, so you don't bring everything down to the lowest common denominator, which is what happens down in the "Tank" almost every single day.

... The Joint Staff is limited, theoretically, by law, to some 400 people. Yet thousands of guys are supporting the JCS down there. And the Chairman has agencies all over the place to support him. So, we've got this incredible swollen bureaucracy, number one.

Number two, everything has some sort of a resource implication or perk implication, so the simplest things take years to get through the system. Required operational capabilities (ROCs) that are sent in by the CINCs to make improvements, presumably to their C^3 in the forces, have sat in the Joint Staff arena trying to get through the wickets they have to go through to get "validated" for two years. Yet we know that ROC is an obvious need; everybody agrees to it, and so on. But we must "validate" it. Until it's "validated" we can't put any money against it. As a result, things slip for years. One of the biggest reasons we haven't fixed a lot of things in my area is that we can't get the JCS to validate ROCs so we can allocate funds to them. And we have, I think, twelve ROCs outstanding for PACOM today, and **Admiral Crowe** is beside himself. I hope he becomes Chairman; then I can go down to him and say, okay, Mr. Admiral, you fix the damn process, because it's the most bureaucratic situation you've ever seen. And so the first thing is to go down there and, frankly, kick some rear ends and take names—in fact, I'd get rid of about every other person.

Admiral Crowe—Admiral William J. Crowe, CINC PAC at the time of this presentation; later Chairman, JCS

You know how big the **JC^3S** is? The JC^3S does not include, under **General McKnight**, anything to do with electronic warfare; so, he really has a limited C^3 responsibility, and has no I. Yet he has over 200 people on his staff. I have all of C^3I, and I had, until this reorganization, 87 people. It's incredible. If you tell me to do it with 40 people, I'll do it with 40, but I'll tell you, we could probably get rid of an awful lot of

JC^3S—Joint Command, Control, and Communications Systems, Organization of the Joint Chiefs of Staff

General McKnight—Lt. Gen. Clarence E. McKnight, Jr., Director, JC^3S at the time of this presentation

action officers out of the service and staffs and business would get done much faster. (122–23)

14. **ROBERT T. HERRES**, "A CINC's View of Defense Organization" (1985, pp. 125–45)

Commander-in-Chief, US Space Command, Aerospace Defense Command, North American Aerospace Defense Command and Commander, Air Force Space Command

As Commander-in-Chief of Aerospace Defense Command, I am responsible through the JCS to the Secretary of Defense for the operational employment of forces associated with the strategic aerospace defense mission. Within that role and in that chain of command, I do not have resource management responsibility. I have nothing to do with research and development, or with training, equipping, organizing, and administering the forces that I would employ. However, as the commander of Air Force Space Command, a component of Aerospace Defense Command, I am responsible to the Secretary of the Air Force, through the Chief of Staff of the Air Force, and thence to the Secretary of Defense, to train, equip, organize, and administer the resources and forces, the people, the money, the equipment, and so forth, that are used by Aerospace Defense Command to carry out appropriate aspects of the mission. I use my situation as an example. I have two completely distinct and separate chains of command. Thousands of people in the Pentagon and in Washington don't understand this. Even some people pontificating on how the JCS ought to be reorganized don't understand that important distinction.

The military departments do not have operational missions. The military departments have responsibility to train, equip, organize, and administer forces and resources that are provided to the unified and specified commanders for employment. Title 10 of the US Code specifies that employment of US armed forces shall be conducted under direction of the commanders of unified and specified commands. There are nine: six unified and three specified commands. The only difference between a unified and a specified command is that the forces in a specified command are predominantly from one Service, and hence there is only one Service component. Strategic Air Command, Military Airlift Command, and Aerospace Defense Command are the three specified commands, because their forces are all predominantly in the Air Force. This doesn't mean we don't have any Army or Navy people; it just means that almost all of our people are Air Force, and there is no standing Navy or Army component. There may be augmentees during crises or when certain operations plans are implemented, but the only standing component comes from one Service.

... A unified commander—well, it's not that clean, it depends on which unified command—but General Rogers, for example, has to look almost equally to all three Service departments for support. He has three separate components, and has to depend on his component commanders to provide resources—Army, Navy, and Air Force resources—from CINC **USAFE**, from CINC **USNAVEUR** who has split headquarters in Naples and London, and from CINC **USAREUR** at Heidelberg. They're almost equally balanced. He must depend on those three four-stars to work through their departments to get resources so they'll be able to provide him with the forces. Each of them is dual-hatted also, because they have subordinate command responsibilities within that Joint unified and specified chain of command.

USAFE—US Air Forces, Europe
USNAVEUR—US Naval Forces, Europe
USAREUR—US Army, Europe

... Let me emphasize that the departmental commands are linked to the Joint unified and specified command structure, the nine unified and specified CINCs, because many of these departmental commands are component commands with people dual hatted as component commanders of these unified and specified commands. Remember the example of the US forces in Europe? There's an Army component, a Navy component, and an Air Force component. There are department commands within this operational chain of command....

Now, I'm commander of Air Force Space Command, a US component of ADCOM, which is a component of a binational command I haven't told you much about, the North American Aerospace Defense Command (NORAD). With that hat on I am also responsible to the Canadian government, through the Chief of Defense Staff in Ottawa, then through the Ministry of Defense, and then to the Prime Minister of Canada.

... Wouldn't it be simpler, cheaper, and more straightforward if you just organized around the missions and combined military departments in unified commands so that we don't have this duality? The reason is that people in this country have never wanted a strong military, we have wanted to fragment military authority. After World War II the Congress and the people, through the 1947 National Security Act, and then the Amendments in 1958, made certain we had a good, manageable, unified structure, while leaving just enough fragmentation in the system to ensure political control over the military establishment. That way we could never have a military establishment that would be too strong. If that's your ground rule, I challenge you to find an improvement to this system that amounts to anything more than a tweak here and there. Some may be major tweaks, but the basic structure,

the duality of responsibility, up to the level of political leadership, is built into this system. This system even has some political leadership in the Service departments, and very tight political leadership control here in the JCS. The JCS Chairmen are appointed for two-year terms, and they can leave in a hurry. JCS terms don't have to be renewed. The Chairman must be confirmed by the Congress every two years, as well as nominated by the President.

In other words, there are a lot of checks and balances in this system. You could improve it here and there, but it is essential to unify the diversity of resources necessary to carry out military missions: naval resources, air resources, and land-based resources. The system combines the best of resource management, which is what this departmental chain of command is all about. Resource management—training, equipping, organizing, and administering—is done by types of systems: naval, air, and land. But we employ them jointly because we no longer live in a world in which you can employ them separately. Hence the unified commands. We try to weave them together. I submit to you that the system works a lot better than it gets credit for. And with every generation of people that comes along (a generation being about a four-year turnover of senior leadership), the system works better.

I think things could be done to make it better still, but I'm not sure that the recommendations being bandied about now are that great. The **CSIS study** I think is good. It's been criticized, but I think the study as a whole has made some fairly decent suggestions for tweaking the system without doing very much violence. We could probably live with it. The worst that could happen with the CSIS study would be to do it piecemeal, pick and choose. Those recommendations, in my view, hang together, and if we're not going to do them all, we shouldn't do any of them. Whatever's done should be comprehensive. (125–26, 133, 136–37)

CSIS study—Toward a More Effective Defense: The Final Report of the CSIS Defense Organization Project (Washington, D.C.: The Center for Strategic and International Studies, Georgetown University, February 1985)

15. **B.R. INMAN**, "Technological Innovation and the Cost of Change" (1986, pp. 151–68)

President and Chief Executive Officer of Microelectronics and Computer Technology Corporation

I have a worry about the onrush to reorganize and change things. I don't have any particular problems with a vice chairman who sits in the chain of

command and who channels the messages, and the rest of it. The concern I have is what I perceive to be a thrust to put the unified and specified commanders into the systems acquisition process, and even some significant movement of the Joint Chiefs into that process. In my long years of service in the Department of Defense, I came to realize that while we can't do much about the vicissitudes of external hostilities, there is a cyclical process in the availability of funds that we can predict. A period of growth is always followed by a period of cutbacks. When you're in growth it doesn't really matter all that much how you organize; you just hope you do it efficiently. When you go into a period of drawdowns, the fight for resources becomes absolutely all-consuming. I lived through some of those periods and I watched the Service chiefs, even in their JCS roles, come to view the number-one priority in their lives as protecting the resources.

If you bring the unified and specified commanders and the Joint Chiefs into that acquisition process, who's going to be paying attention to operations? Who's going to keep an undiluted focus on combat readiness? That's the only real worry I have about the reorganization. For the rest of it you can sort of redraw the boxes as you like. But somebody's got to mind the store, and you need to draw those boxes in such a way that the commanders' attention cannot be diluted by getting pulled off into different priorities. (167)

16. **JAMES R. LOCHER, III.** *Senior staff member, Subcommittee on Projection Force and Regional Defense, Senate Armed Services Committee*
"Defense Reorganization: A View from the Senate" (1987, pp. 147–71)

Last October 1st the Department of Defense entered a new era. Many people in the Department have not recognized it, but when the President signed the Goldwater-Nichols Department of Defense Reorganization Act into law, he set the way for a revitalization of the US military establishment and the military profession itself. The Department of Defense fought the legislation at every step, so effective implementation is not assured. In the end, the Department rendered itself irrelevant to the process. The Congress, retired military officers, and people from the defense academic community were the ones who were involved and decided what was going to happen in terms of defense reorganization. There are some concerns about the implementation, and I'll talk a little bit about that as we go along.

While I say that the Department of Defense fought the reorganization at every step, we need to distinguish between the institution itself and

individuals. While we were preparing our study on defense reorganization, and while we were actually going through the legislative process, we probably interviewed five or six hundred people in the Department of Defense in Washington and in the field. Our experience was that among the military officers, about 80 or 85 percent fully supported what we were doing. They could not speak out publicly on that, but privately they were prepared to tell us what their concerns were about defense organization, and their thoughts on what needed to be done. But they could not speak out publicly, which made the battle somewhat more difficult because we could not use these people while trying to convince members of Congress that changes needed to be made.

our study—US Congress, Senate, Committee on Armed Services, Defense Organization: The Need for Change, 99th Congress, 1st session, Oct. 16, 1985 (Washington, D.C.: GPO, 1985)

... [T]he kinds of people we were talking to ranged from the level of Army major up to four-star officers. I should say that field-grade officers were prepared to be much more forceful. As you went up, the percentage who were supporting us began to diminish, because more senior people were in much more difficult positions. If it were known that they were speaking out in favor of something which the most senior people in the Department, both civilian and military, were very much opposed to, they could be put in a very awkward situation. But privately they were very supportive, including a number of people at four-star rank. There were a few people like General Rogers who were very supportive both privately and publicly.

One of the things that I'd like to impress upon you, because it was miscast by a lot of people, is the nature of this battle. To introduce that issue, I'd like to read a quotation from a message to Congress from President Eisenhower in 1958 when he proposed the reorganization ideas at that time. He said, "Separate ground, sea, and air warfare has gone forever. If ever again we should be involved in war, we will fight it in all elements with all Services as one, single, concentrated effort. Peacetime, preparatory, and organizational activity must conform to this fact. Strategic and tactical planning must be completely unified, combat forces organized into unified commands, each equipped with the most efficient weapons systems that science can develop, singly led and prepared to fight as one, regardless of Service."

While Eisenhower said that in 1958, when we began this move towards reorganization of the Department of Defense, all of the things that he had talked about had not fully come about. Many of his attempts to force changes on the Department of Defense while he was President had been frustrated, primarily by the Services. The key point in this regard is that the

battle lines were not the Department of Defense *vs.* the Congress, civilians *vs.* the military, or warriors *vs.* bureaucrats. The battle lines were essentially drawn between those who sought a truly unified defense effort *vs.* those who would cling to traditional Service prerogatives. This is a very important point. Many of the issues were not debated on that basis, but that was the underlying argument.

... In general, I ought to say that almost all of the problems still remain unresolved. We have enacted some legislation, but the legislation has not taken effect. I'm not certain that it will be fully implemented. But I will talk about some of the things that we're still concerned about and that will need to be addressed in the future.

... What were the fundamental problems that we saw in the Department of Defense? In doing this study, we identified 34 problems, some of those in the Department of Defense, some of them on Capitol Hill. I tried to bring those down to 10 problems that I'd like to talk a little bit about [*See* Figure 1]. Then we will discuss what we've actually done in the legislation.

Figure 1—**Fundamental Problems**

1. Imbalance between service and joint interests
2. Inadequate joint military advice
3. Inadequate quality of joint duty military personnel
4. Imbalance between the responsibilities and command authority of unified combatant commanders
5. Confused and cumbersome operational chains of command
6. Ineffective strategic planning
7. Inadequate supervision and control of defense agencies and DoD field activities (e.g., Defense Logistics Agency and Defense Contract Audit Agency)
8. Confusion concerning the roles of the secretaries of the military departments
9. Unnecessary duplication in the top management headquarters of the departments
10. Congressional micromanagement of DoD

Source: James R. Locher, III

The first was the imbalance between Service and Joint interest in the Department of Defense. The Services absolutely dominated the Department of Defense. First of all, the Chairman of the Joint Chiefs of Staff was kept very weak. Each Service, essentially, had an effective veto over what was going to happen in the Joint Chiefs of Staff. The unified commands in the field were not really unified commands. They were confederations of single-Service forces. The unified commander himself was kept very weak, and he had powerful and independent Service components underneath him. So we continued to be dominated by a focus on Service interests with relatively scarce support for Joint needs in the Department of Defense.

The second major problem is related to the first; it was inadequate Joint military advice. We had a system of marriage agreements, truces, watered-down advice. The Joint Chiefs of Staff had a tendency to provide advice to which all members could agree. When you get down to reaching a consensus on each and every issue, you are coming up with the lowest common denominator.

In talking about Joint military advice, I think it's useful to think about the three types of advice. One was the informal advice: the President or the Secretary of Defense asking the Chairman or all of the members of the JCS to come in and provide advice on a particular issue. The informal advice normally got high marks. The Secretary of Defense, the President, or the National Security Advisor to the President felt that the informal advice was pretty good.

The second kind of advice was the formal advice that was worked through the Joint Chiefs of Staff system. That advice got very low marks. It was almost never used and did not play much of a role in Department of Defense decision making.

The third kind of advice was the advice not given, and that was the whole range of issues that the Joint Chiefs of Staff did not want to take on: the unified command plan, Service roles and missions. Anything that was going to touch on important Service interests they would attempt to stay out of. The strategy that the members of the Joint Chiefs of Staff put together was fiscally unconstrained because they couldn't deal with the tough choices. The Secretary of Defense didn't need a fiscally unconstrained strategy. He needed a fiscally constrained strategy so he could start making those trade-offs between Service capabilities, or missions, or whatever.

... The third fundamental problem our study identified was the inadequate quality of Joint duty military personnel. The basic problem in the Department of Defense is people generally do not want to be assigned to Joint duty. They know they're being pressured or monitored for loyalty by their Services while they're there. They're not prepared either by educatinn or experience to be there, and they serve a relatively short period of time. The whole idea is, if you get stuck with going to Joint duty assignment, get in, keep your head low, get your ticket punched, and get out before you ruin your career.... [A]s I mentioned, many of these Joint officer provisions dn not go into effect for two years. You're not actually seeing tbe effect of the law itself, but you're seeing people's anticipation of what the law is going to require. Traditionally, the Navy has not sent its line officers to Joint colleges, and they have filled far fewer than their share of Joint duty positions. Their technique would be to offer somebody who was not qualified. The organization would not accept him, and then the Navy would just leave the billet open. We are now seeing the Navy move smartly to fill the positions in Joint duty that are assigned to the Navy, including flag rank positions.

We are seeing much more interest by people in all Services, probably less so in the Navy given the orientation in the past, in having Joint duty assignments. In the law we did not go into the education area because the idea of the Congress trying to structure professional military education was something that we thought we ought to stay away from. The Chairman of the Joint Chiefs of Staff has set up a Senior Military Schools Review Board headed by **General Dougherty**, that is looking at what we need to do in terms of education. We did not define what Joint military education was. The Department of Defense may identify it as only the three colleges of the National Defense University or they may include the Defense Intelligence College. There's more work that needs to be done on that issue, and we think we have some leverage on the Department to get them to move out forcefully.

General Dougherty—General Russell E. Dougherty, USAF (Ret.)

... One of the things that we've done is establish some promotion policy objectives. These are not quotas. The law does not say this must be done. We have just said to the Secretary of Defense, "You shall ensure that qualifications of officers who are assigned to Joint duty are such that these kinds of promotion rates will result. If you don't meet these promotion rates, you write to us and tell us why you haven't and what corrective actions you're going to take."

The officers who are selected for the Joint specialty must be promoted at a rate not less than the rate for the Service Headquarters Staffs, which is the

highest promotion rate in the Department of Defense. People who serve on the Joint Staff must have the same promotion rate, not less than that for the Service Headquarters Staffs. Other officers assigned to Joint duty may not be promoted at a rate less than the Service-wide rate. It is hard to believe, but in the Navy, officers assigned to our most important military staff, the Joint Staff, are promoted at a rate less than the Service-wide rate, and the same thing for the Marine Corps....

[OETTINGER] You certainly wouldn't want 100 percent of all officers to be Joint officers, because the Services do perform an important function, to be specialists in their brand of war fighting, and if that didn't exist we'd have to invent it. It's like the academic battle over departmentalization and specialization. If you didn't have it, everybody would be a superficial dilettante. You'd say, "Let's get rid of all of these superficial generalists and let's have somebody who knows something." Then you get somebody who knows something, but he knows an amazing amount of detail in a very limited area. Then you say, "How do you put them together?" The military has an absence of such people ... you lose the advantage of specialists who can orchestrate the thing. You've got all these violin players, you've got all the percussionists and so on. Who is the orchestra leader? You don't need everybody to be capable of doing that, but you need some.

[LOCHER] As a matter of fact, if you think about Joint duty, you're really only talking about 3 to 5 or 6 percent of all officer positions being in Joint duty assignments. Even if you have a three-to-one base—you've got to be developing two other guys for every guy who's in a Joint position—we're not talking about more than half the military establishment in terms of its officer corps. You're still talking about a relatively small portion. But our problem has been that the system has been designed to prepare people for single-Service needs, and it has been designed to reward them for doing things that are important to their Service, not to prepare this small cadre of people who have to be able to understand more than just their own Service. We have not been able to do it in the field because the Services have remained fairly independent under the CINCs.

... As Eisenhower said, "Peacetime preparatory and organizational activity must recognize the fact that we have to be unified." We're not doing that. When they were preparing for Grenada, each Service did its own planning and had its own planning sessions without inviting anybody else, and then they expected to go down there and have an effective unified operation.

With the Iranian rescue mission, the same approach occurred. A long period of time was taken to prepare for the Iranian mission, but each Service went

off and did its own thing. They went to separate locations. There was no single commander. They weren't used to working with each other, and they were going to arrive in the desert in the middle of the night in Iran and expect the whole operation to work.

... You essentially divided Vietnam into five air wars. The Army, the Navy, and the Marine Corps each fought its own air war. The Air Force had two air wars, because SAC was being run from Omaha out of Thailand and Guam, and then the Tactical Air Force in Vietnam did its own thing as well.

We've made the Chairman of the Joint Chiefs of Staff responsible for development of Joint doctrine. He does not need to coordinate with the other chiefs. He'll hear their advice, but in the end, he's the one who's going to make the decision. There's always been a big problem with Marine air. Marine air arrives in the theater 40 or 45 days before the rest of the Marine Amphibious Force. But the Marine Corps had refused to allow those air assets to be assigned to the theater commander. That's all been changed now. JCS Publication No. 2, *Unified Action Armed Forces*, has broken the Marine Corps' back on that issue, and said that those assets belong to the theater commander and he shall determine how they'll be used.

We have a long way to go in Joint doctrine. We essentially have very little Joint doctrine, so when a Grenada happens, and Service forces have to operate together, there are going to be tremendous problems. There are always going to be problems. In war, you're not going to eliminate them, but we're giving ourselves some major disadvantages now.

... The CINC has now been given the authority to prepare the forces assigned to him for their missions. He will also be given a budget controlling Joint exercises. We believe that if we start with the people who are the CINCs and their immediate staffs, and they understand how all of this will need to fit together, they will prepare the forces below them for whatever Joint interactions are going to be necessary with more Joint exercises and by making certain that the people who are below them are responsive to their direction.

... One of the problems we have now is that we're getting CINCs who have never stepped outside of their Service. Their first Joint assignment is when they become a CINC, or they had nine months just prior to becoming a CINC. A very limited time. Officers are just going straight up the Service channel; the next thing you know, they're running a Joint organization with no prior exposure whatsoever. So we've said, "You had to have the Joint

specialty, and you had to have one Joint duty assignment of three years in length as a general or flag officer." We want these officers to be prepared for these responsibilities. A Service chief has to have had significant Joint experience, and he has to have one Joint duty assignment of three years as a general or flag officer.

... The JCS Chairman will review all promotion board reports where Joint duty officers were considered. The Secretary of Defense will establish some procedures for monitoring these officers' careers to make certain that at no time during their career is somebody coming along and trying to penalize them for what they did during a Joint duty assignment. Then we have established some congressional reports and oversight. The Secretary of Defense has to report when he doesn't meet some of these policy objectives.

The Joint Staff and the CINC staffs are made much more independent in the legislation, so they don't have to go to the Services. The Services can't watch every move that they're making. We've created some countervailing pressures to this. The Chairman and the CINCs can suspend any officer assigned to their command or to their Joint staff from duty, and recommend their reassignment. The CINCs will evaluate their subordinate commanders. That means that CINCPAC has an Air Force four-star CINCPACAF who reports to him, and CINCPAC will evaluate CINCPACAF's performance and that evaluation will go into the Air Force officer's personnel record.

... It's to give him the authority he needs to meld those forces together into an integrated fighting team. He does not have that now. One of the areas where the CINCs don't have any authority is in the field of logistics. To think that you're going to take these combatant forces without any logistics input and go off and fight is pretty silly, too. One of the key examples that we use is from my visit with Admiral Crowe in the Pacific. He had one of his Service component commanders who wanted to put his war reserve materials in location Y, and Admiral Crowe said to him, "Location Y doesn't support our war plans, we need it over here in location X." The Service component commander said, "Logistics is not a matter for consideration by the CINC." The Army—in this case it was the Army—said, "It would put its war reserve materials where it damn well pleases them to put them."

Essentially what happened is that the CINC would be assigned forces from four Services, all assuming a different war, trained and equipped differently, with different logistics policies, with no integration of logistics capability in peacetime, and then they would be forced to conduct an operation like Grenada, and it was just too much separateness to overcome.

... The next point is one that we've touched on already to a great extent, and that's the imbalance between the responsibilities and command authority of the unified combatant commanders. Even though we created some unified commands during World War II and then we formally created them in 1947 and 1948, they never have been unified. They've been unified only in name. They've essentially been confederations of single-Service forces. The commander has been very weak, not really even able to prepare his forces. To hold him accountable for the ability of his forces to carry out their missions was inappropriate given his limited authority.... The role of the Secretary of Defense in the chain of command was very confused. The role of the Chairman of the Joint Chiefs of Staff and the other members of the Joint Chiefs of Staff was confused, and the unified commanders in the field had very little authority with respect to the chain of command below them. The CINCs were required to go through all of the Service layers. So when General Bernie Rogers had that Marine battalion ashore in Lebanon, if he wanted to have tight control of that situation and to shorten that chain of command, he could not do so. He was required to go down through all those levels, and there were about five or six levels between himself and that battalion commander. It was a situation in which we had a lot of confusion, and we could not streamline the chain of command as appropriate to the situation.

Ineffective strategic planning. Strategic planning is really neglected in the Department of Defense. Everybody's chasing resources. The whole system in the Pentagon is dominated by programming and budgeting.

... In the Goldwater-Nichols Act coming out of the Senate side, we eliminated two-thirds of the recurring reports that the Congress required from the Department of Defense.... The problems of reforming the Congress are enormous. In defense reorganization, one of the things that the Senate Armed Services Committee attempted to do, within the committee's jurisdiction, was to reduce the burdens that we were placing on the Department of Defense.

The first effort that we made was to assess all 558 reports that are required on a recurring basis from the Pentagon or the President by either our committee, the Appropriations Committee, or in the national defense field. Two-thirds of those have been eliminated. That removes a big burden from the Department of Defense. We have made it much tougher for reports to be required of the Department of Defense. We've cut down on the questions for the record. We attempted to reduce the number of our hearings. But the really big changes we can't make on our own. Either it involves changes to Senate rules, or we have to get the House Armed Services Committee to

cooperate with us, or the Appropriations Committees. We're trying to do a two-year defense budget, which we have required the Department of Defense to submit. That requirement originated with the Senate Armed Services Committee. There are just enormous problems with a two-year budget. Whether we're going to be successful or not is hard to predict, but there's almost no interest outside of our committee. But there are some enormous problems in terms of congressional micromanagement.

... If you look at the study that the committee printed, you'll see recommendations that are much more forceful, such as abolish the Joint Chiefs of Staff and replace them with a group of wise men to be known as the Joint Military Advisory Council. It was our view that if we offered recommendations which were exactly where we wanted to come out, we would be compromising from there, and we'd come out with something less. We decided to offer more forceful proposals as a starting point.

The idea of a Joint Military Advisory Council had been offered by people in the past. General Bradley and a number of other people had proposed this idea. So it had enough credibility and was something that we could select to let the members of the Joint Chiefs of Staff know how serious we were on this issue, how disappointed we were in their performance, and how drastic the measures were that we had in mind. Essentially that provision came to be a "bullet trap" in that the members of the Joint Chiefs of Staff and much of the Department of Defense spent most of their ammunition firing at this idea of a Joint Military Advisory Council. Our real objective was strengthening the JCS Chairman. We thought that was something that was do-able. You could debate the merits of this Joint Military Advisory Council, but in our view, we couldn't start off by saying, "We want to make the Chairman the principal military adviser and give him a Vice Chairman," because then we would have been forced to compromise from that. We held onto this idea of a Joint Military Advisory Council—and it was just a staff recommendation—but when we put out the study, when the staff testified in front of the committee, when we received all of the media attention, the department spent a lot of its energy fighting off that idea.

There were certain things that we were not able to achieve in the legislation, and these are some of the unresolved issues I'll turn to later. But for the most part, we were able to achieve what we had in mind in terms of organizational changes. Part of that came about because, as you know, the House had started this reorganization work first, but they had focused solely on the Joint Chiefs of Staff. The Senate had decided it had to be a much broader reorganization effort. But the House got some momentum going. Then the Senate built on that to do our broader legislation. When our legislation was

voted out of the Senate 95 to nothing, it gave the House a real shot in the arm, and then the House could look at going further. We ended up compromising in the conference with the House Armed Services Committee. There are a few things that did not get done, but for the most part we're fairly satisfied with what we were able to work out. All of this was very carefully considered. You're talking about three or four years' worth of work.

Let me go straight to the fundamental purposes of the Act, and how we hope to achieve some of them.

One of the fundamental purposes was to improve the quality and enhance the role of professional military advice. What ended up happening was that Secretaries of Defense knew when they were getting mush from the JCS. They ended up often going to civilians to get military advice. They were civilians who often were not qualified to provide that advice, but a Secretary of Defense had nowhere else to turn. We had the view that military expertise must be more effectively applied to the very complex defense issues that we were facing. What did we end up doing? We made the Chairman of the Joint Chiefs of Staff the principal military adviser to the President, the National Security Council, and the Secretary of Defense. What did that mean? It essentially meant that the other members of the Joint Chiefs of Staff became advisers to the Chairman, and he was the decision maker in terms of the advice that would be offered to higher civilian authority.

There are certain instances in which the other members of the Joint Chiefs of Staff can take their views to the Secretary of Defense, the President, or the National Security Council, or any of those groups could ask them for their corporate views or their individual views. Or if they disagreed with the Chairman, then we gave them the right to present their views. But the normal process is that the Chairman is the principal military adviser. All the former duties that were assigned to the corporate JCS are now assigned to the Chairman. He manages the Joint Staff. He decides under what procedures they'll do their work.

We sought to strengthen civilian control of the military. We didn't see any major problems here, but we did have these problems in terms of the role of the Secretary of Defense in the chain of command, and the authority of the Service secretaries over their departments. We felt there were some useful clarifications that could be made, particularly in the area of intelligence in the military departments. Many people in the military departments said intelligence is an operational matter and, therefore, the Service secretaries had no business being involved. So there were activities that were actually done in the military departments in the intelligence field that were not brought to

the attention of the secretaries of the military departments. Some of these things, particularly in the Army, have backfired here recently. So we sought to strengthen civilian control, not that we had any real concerns, but that's something that Congress is going to be very careful about in doing its work.

Strengthen the authority of Joint military officers. The one thing the law does is provide for a fundamental shift of power and influence from Service officials and organizations to Joint officials and organizations. The Chairman has been made more powerful. We've created a Vice Chairman of the Joint Chiefs of Staff to assist him, who's the second-ranking military officer, and the CINCs have been made much more powerful. They now have the kind of authority they need to carry out their responsibilities.

... Enhancing the effectiveness of military operations goes back to this command and personnel authority that we have given to the CINCs. They now have all of the authority they need to prepare all of the forces in their command for assigned missions.

... [T]here are two actions that have been taken in terms of strengthening central direction, but also decentralizing. The central direction part of what we've done is try to get much better strategic planning. We've required that the strategy document prepared by the Chairman must be fiscally constrained. We've required that he prioritize the operational requirements of the CINCs, and that he look at what the Services are doing with their budgets and compare them to these other yardsticks that he's been required to develop. We tried to get more attention on strategic planning in the Department.

In terms of decentralization, a lot of the authority that had been held in the military department headquarters has now been pushed out into the field to the CINCs.

We've clarified the operational chain of command in terms of the Secretary of Defense. We made certain that everybody understands that neither the Chairman nor the other members of the Joint Chiefs of Staff are in the operational chain of command, and we've given the CINC the authority within his command to specify his chain of command. So when we go back to that Lebanon situation, if General Bernie Rogers decided, "I want that battalion commander reporting to me, and that's the only way I can get the kind of operational control I need," he could do so.... The chain of command runs from the President, to the Secretary of Defense, to the unified and specified combatant commanders in the field. Neither the Chairman nor the other

members of the JCS are in the operational chain of command. It does not flow through them. We have given the President and the Secretary of Defense the authority to use the Chairman to help them carry out their command functions, and there's a couple of ways he can do so. He can transmit orders that they give as he does now. He can also be used to oversee the implementation of their command instructions.

... We've attempted to reduce and streamline the defense bureaucracy. We felt that the headquarters organizations had become too large. The span of control of senior defense officials was just enormous. The Secretary of Defense has 42 people reporting directly to him. The Service chiefs had between 34 and 48 officials who reported directly to them. There was too much duplication in the military headquarters staff. We've tried some consolidation there. We have actually forced people out of these headquarters organizations in an effort to streamline them.

... We've attempted to provide for continued study and management attention to these defense reorganization issues. One of the key points is that our understanding of defense organization is very, very poor. Our thinking about these issues was retarded because the people who wanted to defend the status quo were extremely powerful, and they were able to blunt almost any initiative to think about these ideas.

What kind of a general staff did we need, or people for Joint duty? What should the Office of the Secretary of Defense look like? What kinds of responsibilities do they have? What authorities should the unified commanders in the field have? All of these kinds of thoughts have really been studied very little in the United States. When we did this work, we were breaking new ground in many areas. We have attempted to continue to require that these issues get some attention in the future.

... There are a couple of issues that I'd like to talk about. There are three things that are holdovers from defense reorganization that have not been adequately addressed so far. The most important of those, in my view, is the Office of the Secretary of Defense. Those of you who have read some of the things I've written and some things that Professor Sam Huntington has written on this subject know that we have the view that there is a need for very strong mission orientation in the Office of the Secretary of Defense. Currently, the Office is organized on almost an exclusively functional basis. When I say functional, I mean manpower, installations, logistics, and research and development. That came about in 1953 when OSD was expanded with six additional Assistant Secretaries of Defense and a Director of Defense Research and Engineering. It was decided to have the Office of

the Secretary of Defense mirror-image the Services, so that the Secretary of Defense could control the functional activities of the Services.

It's important that the Secretary of Defense be able to do that to a certain extent. But his real role is to be an integrator of Service capabilities to carry out the major missions of the Department of Defense, none of which can be done by any Service on its own. If you look at the organization that supports him, it's designed for functional integration—we can do manpower planning department-wide—but not for what we call mission integration.

... The second area that was left undone was on the defense agencies. They have received such limited attention over the last 30 years that there was not much information and analysis to work with. What we really needed was a rigorous re-examination of the defense agencies. Were they doing what was appropriate? Had they gathered too many activities that could be better done by the Services? Could they be structored better? There is a set of reports coming in on that issue as well. The defense agencies are Joint organizations. They play important roles, but they have been relatively neglected in terms of management attention.

The third issue is the Congress. What do we do about congressional review and oversight of national defense? The Congress has been working harder and harder and accomplishing less and less. We thought that one solution might be a two-year defense budget which could reduce the demands of the Congress on the Department of Defense. We're trying to implement a two-year budget this year—that's what I've been working on the past couple of days, the authorization request for fiscal years 1988 and 1989. It's very difficult to do the second year, primarily because decisions that you would make for the second year depend upon information you do not now have. They're dependent opon things like test results on R&D progress. Just in the few months since the budget has been submitted, there have been so many fact-of-life changes to FY88 that spilled over to FY89 that it is very difficult to think about how we're going to do a comprehensive two-year defense budget. Our current thinking is that we will approve fiscal year 1988, the current budget year, in its entirety, and in 1989 we will try to approve those programs that are stable and noncontroversial. We're going to be building the two-year budget from the bottom up. It won't he a complete effort.

... We have very serious problems in terms of nilitary strategy or national security strategy. It is very poorly developed. We just don't have a tradition of strategy making. We don't put our attention there. We've got a long way to go in terms of preparing our thoughts in that regard. Related to that is the fact that we do not have a direct link between our budget and our strategy.

We push a lot of paper and give a lot of lip service to what strategy work we do have, and then we build a defense budget from the bottom up, focusing on what the Services want. The Senate Armed Services Committee has been questioning the witnesses this year to tell us what the mission deficiencies are, based upon our strategy, and then how the authorization request relates to those deficiencies. They absolutely cannot do it. (147–48, 150, 152, 154, 155–56, 157, 158, 160, 161–62, 163–64, 166, 167, 169–70)

17. **ARCHIE D. BARRETT,** "Defense Reorganization: A View from the House" (1987, pp. 173–94)

Staff member, House Armed Services Committee; former Military Staff Assistant to the Executive Secretary of the Defense Organization Study; author, Reappraising Defense Organization *(1983)*

There's absolutely no question that the committee [House Armed Services Committee] and the Congress have the authority and the right to get into anything they want to in the Department of Defense, to the degree of specificity that they want to. The Constitution has one sentence about the President and the military. It says he's the Commander in Chief, and that's all. There are some historians who would point out that that was included so that there would be no question that the President has control of the militia of the several states, not as a grand idea about generalship in war. Nevertheless, I'm not disputing that "Commander in Chief" is a much broader concept today than it was then. The point is that the Constitution, with respect to Congress and the military, goes on, and on, and on—sentence after sentence—about what the Congress' power is: "The Congress shall have the power to declare war, and make rules concerning captures on land and water, raise and support armies, provide and maintain a navy, and make rules for the government, and regulations of the land and naval forces. To provide for calling forth the militia to execute the laws of the union, suppress insurrections and repel invasions. To provide for organizing armies, and disciplining the militia." Plus, of course, Congress authorizes and appropriates the resources of the Defense Department.

The distinction that must be made is that when you discuss congressional micromanagement or congressional meddling, you need, particularly if you are in the military, to understand that you're talking about a normative subject—what is prudential—and not a legal subject. I think people frequently misunderstand that. I often caution audiences to make the distinction between what they think Congress ought to do and what Congress legally can do. . . .

Military departments are the input side. They organize, train, and prepare forces for war.

The output side is the war-fighting side, the Joint commands—unified and specified—the organizations that Eisenhower was talking about. The input will be separate. The output will be integrated. Combinations of forces from four Services will be prepared to fight and they will fight wars if necessary. The commands I'm talking about are the European Command, the Pacific Command. Commands like that are unified. The specified commands are those such as the Strategic Air Command (SAC), the North American Aerospace Defense Command, and the Military Airlift Command (MAC).

Each of the unified commands has components that were established as a result of the National Security Act law, but not required by it. In Europe we have the US Air Forces, Europe; the US Army, Europe; and the US Navy, Europe. They come under the unified commander, and they're supposed to fight as one force under that unified commander. But, in fact, on a day-to-day basis they're Air Force commands, Army commands, and Navy commands. In effect, they're little armies, air forces, and navies. They have their own support, they fly their own training missions in the Air Force and run their own exercises in the Army.

... The organizational arrangements lend themselves, in other words, to allowing the Services to dominate more than, I think, an objective reading of the law would support. Let's just take a look at the unified and specified commanders. They come from the Services. They go back to the Services. Their promotions hinge on the Services. It was very difficult, for example, to get the unified commanders to testify on the reorganization legislation, because the Services were very much opposed to the legislation. Despite the fact that the legislation would benefit these commanders, most wanted no part of going on record with regard to these controversial issues.

Yet we found their command prerogatives were very, very limited. If you think about what a unified commander, or a military commander, must deal with, and what authority he should have, and if I asked you to put them down on a piece of paper, I think you would be surprised when you compared your piece of paper with the reality of the unified commanders' authority. The commanders had very limited authority over the selection or the firing of their subordinates. They had no court martial authority over their subordinates. They had very little authority to reorganize their subordinate commands, the component commands I mentioned earlier. They had very limited authority over the chain of command, and rearranging the chain of command below them. By law they were prohibited from exercising

authority over the support chain that came from the Services. They were severely limited in the area of administration. They were limited in the area of training. They had no budgetary resources, and, as you know, budget equals clout in the Pentagon. And, even in time of war, if you read their governing directives carefully, you wonder whether they would really have had complete authority over how to employ forces under them in order to win. They were very, very weak. Yet these are the commanders the United States would depend upon for its survival if there were a war.

Component commanders, under the unified commanders, on the other hand, had vast authority. They had all of the things that the unified commander didn't have. When I said the CINCs were limited, I meant they were limited because the component commanders had these things. General Jones, when he came before the Investigations Subcommittee, said that when he was a component commander in Europe, the head of US Air Forces, Europe, he got everything from the Air Force—his airplanes, his people, their promotions, their pay. Everything came through the US Air Force channel. On a day-to-day basis he did all of his training based upon Air Force directives. He said that his attention was not so much to the CINC above him as to the Air Force—90 percent of the time. The Services dominated the unified commands.

... The JCS was uniformly perceived as not being a factor in resource allocation decisions, which perhaps in peacetime are the most fundamental of all military issues.

The Joint Staff ... under the Joint Chiefs of Staff is criticized because it's a cipher for the Services; it's sort of a secretariat for the Services. The staff people come from the Services, and go back to the Services. The procedures that have been laid down by the Joint Chiefs of Staff cause any staff paper to go to four or five levels before it gets to the Joint Chiefs of Staff. If any Service at any level objects to the Joint Staff paper, it goes to the next level. In effect each Service has veto power in developing the content of any advice rendered.

Military advice is a major shortcoming of the JCS. I have some quotations ... to indicate that this is an opinion held by many, many people.... This is by Kissinger who says:

> The inevitable and natural concern of the Service chiefs—with their competitive and often mutually exclusive mandates—is the future of their Services which depends upon their share of the budget. Their incentive is more to enhance the weapons they have under their exclusive control than to plan overall defense policy.

Zbigniew Brzezinski: a similar type of quotation. I present both of these ... because one of these quoted served a Republican President; the other, a Democratic President.

> My own experience in the White House, working closely with President Carter, was that our military establishment has become, over time, increasingly unresponsive either to the pressing threats to our national security or to effective presidential direction.

Former Secretary of Defense Brown:

> Recommendations from the JCS during four years were almost without exception either not useful or the reverse of being helpful. That is, worse than nothing.

Former Secretary of Defense Schlesinger:

> The proffered advice is generally irrelevant, normally unread, and most always disregarded. The ultimate result is that decisions regarding the level of expenditures and the design of forces are made by civilians outside the military structure.

... Other criticisms of the system involve military planning, the chain of command, and military operations. In some cases every Service wants a piece of the action whether the prospective operation justifies it or not. I think the attempted Iranian hostage rescue probably shows that, although the Holloway Commission exonerated the military on that score. I don't think much of that Commission's report. Ask yourself, "Would the rescue effort have been carried out as it was if there hadn't been a JCS, with each Service equally represented, planning the operation?" I think the answer is no. Former Secretary of Defense James Schlesinger sums up his criticism as follows:

> The existing situation does impede planning, for each Service quite naturally wishes a piece of the action in any crisis—and the existing structure assures that all somehow will be fitted in, even if a Service provides less than optimal forces for dealing with a particular crisis.

... Grenada ... was obviously a successful operation. But there have been any number of criticisms. Communications. I don't want to get into whether the communications gear was right or not. The point is that there had not been sufficient Joint training and Joint exercises so that the Air Force and the Army could work together. In another case, Army helicopters wanted to land on Navy carriers; they had wounded aboard. The press has criticized the Navy for not letting them land. The Navy did exactly the right thing. It's a very dangerous operation, particularly at night. The Army pilot could have not only killed the people in the helicopter, but also done a lot of damage to the ship. The point is that Army helicopter pilots were not qualified to land on Navy ships. There had not been Joint exercises and Joint training so that

that could take place. Another example, naval gunfire was never able to come to the support of the Army; certainly not in the first stages. The problem is a lack of Joint training and preparation so that our forces can fight a war as an integrated team of land, sea, and air forces. All of these things point that out.

... The Services dominate not just the input side, but also the output side. They dominate the Joint Chiefs of Staff, the Joint Staff, the component commands; they have significant influence over the unified commands. As a result, decisions that are made in the Department of Defense have been made on the basis of conflicts between the Services and the civilians in the Office of the Secretary of Defense.

The subcommittee found other criticisms of DoD organization. For years there have been criticisms of the military department headquarters. There's a Secretary in each headquarters, with around 250 to 300 people serving him in the Army and the Air Force; 800 in the Navy. On the military headquarters staffs, there are 10 times that number in the Army and the Air Force, roughly 3,000; in the Navy, 2,500. Each one of those staffs will have something like a research and development office. There is a research and development office, for example, in the uniformed Navy headquarters, and a research and development office in the Navy secretariat. In the Office of the Secretary of Defense there is also a research and development office. Many sages have said, "You don't need three management headquarters staffs with the same function. You can get along with two. One should be cut out." There have been a lot of recommendations for consolidating these offices.

The subcommittee was also concerned when it looked at the defense agencies. The defense agencies are in a way analogous to the Services in that they're maintaining, or input, organizations. The subcommittee was concerned that the agencies were not sufficiently responsive to the output organizations which many of them would have to serve in wartime. For example, the Defense Intelligence Agency, the Defense Communications Agency, the Defense Mapping Agency, and the Defense Logistics Agency would be responsible for direct wartime support. Are they ready enough? Do they participate in Joint exercises? Are they sufficiently responsive to the unified and specified commands? Those are the sorts of questions that have been asked. The subcommittee did not think they have been sufficiently responsive to the employment side.

With respect to personnel policies, the subcommittee found that the Joint side suffered. I mentioned that the Joint Staff is more a cipher or secretarial

for the Services. The officers who work there go back to their Services. There were many indications that they weren't well trained in Joint matters before they went to the Joint side. They had very little, if any, experience in staff work, much less Joint Staff work, before they went to the Joint side. The experience level on the Joint side stayed low because they never came back. If a Joint officer took a position that was contrary to his Service, he was very likely to be penalized in his career in terms of promotions, and his career assignments would be as bad as his promotion prospects. (174, 176, 177, 178, 179, 180, 181–82)

5

Intelligence—The Eyes of C³I

The term "intelligence," meaning knowledge about a potential opponent's plans, capabilities, and weaknesses, has currency in the business and sports worlds as well as in national security. It can also be applied to simple games such as poker.

In all of these contexts, from national security to poker, players range from the naive to the very sophisticated. The former lack both knowledge of the rules of play and "card sense." The latter know all the rules and usually have a strong feeling—based partly on intuition and experience, partly on careful observation—for the cards in the hands of each player.

One goal of intelligence in each of these contexts is knowledge of the "cards" held by other players—their capabilities. Often more valuable—and more difficult to ascertain—are their intentions, their plans for using those capabilities. Some attempts to ascertain the capabilities and intentions of other players are considered legitimate: experienced poker players have systems to keep track of cards played; businessmen follow their rivals' advertising, sales figures, and other publicly available data; coaches scout rival teams; and governments collect data about other nations from open sources.

Sometimes players sidestep the rules in the interest of "fair play," "industrial security," or "national sovereignty"—or "the status quo," "unfair competition," "political repression," and so on. The terms change according to context and the vantage point of the individual choosing the term, just as using "traitor" or "patriot" to describe Benedict Arnold or Nathan Hale would depend on one's position relative to the Atlantic Ocean. In sports or poker, such an evasion of the rules would be called "cheating"; in business, it might be labeled "industrial espionage"; in national security circles, it's called "spying." Again, the moral tenor of the terminology chosen is relative.

Complete knowledge of other players' hands, were it attainable, would deprive the game—any game—of its sporting aspect. That loss would be most objectionable in the more sporting contexts, such as a "friendly game among friends," athletic or otherwise. When the

stake is national security, the quest for perfect knowledge of the opponent is easier to justify; a government trains and uses spies to protect the interests of its citizens.

Regardless of context, intelligence is a game of tradeoffs. In poker, some experienced players focus their attention on card order, others on betting patterns, still others on the mannerisms of the other players. Each approach—each system—has its own advantages and disadvantages. The most successful player may be the one with the most eclectic strategy, the one who recognizes and plays the tradeoffs.

The extracts in this chapter are concerned with intelligence tradeoffs in the context of national security, specifically the national security of the United States. Sometimes the tradeoffs involve matters of propriety: Should a constitutionally-based government run an intelligence program which, in the interests of secrecy, operates outside normal boundaries? Or should intelligence, like other government activities, be subject to the restraints of oversight and accountability? How should a democracy draw the line between individual rights and the security of its citizens? Should the need for objectivity outweigh the practical requirement for regular communication between the intelligence professionals and decision makers? Is the political neutrality of intelligence products more important than the mutual trust of producers and consumers?

In other cases, intelligence issues are matters of priority: Should emphasis be on collection or analysis of intelligence? On timeliness or accuracy? On more collection or better flow to decision makers? On providing for every potential information need, or avoiding information overdose? On protecting sources, or getting information to everyone who needs it?

Should scarce assets be expended on hardware or on people? On improving technical means of collection and analysis, or on expanding human means? On launching satellites or training linguists? On long or short term needs?

Should the goal of analysis be consensus or a thorough picture of competing views? Should its approach be geographic or functional? Should it be directed by a generalist who can draw all the details into a coherent picture or a specialist who might be less likely to sacrifice the accuracy of details for the sake of coherence?

Should intelligence operations be geared toward war-fighting or peacetime needs? Strategic warning or tactical operations? Details about the most likely enemy, or a broader picture of all potential foes?

Should fusion centers, where intelligence is correlated and analyzed, be centralized or kept close to the battle? Should "covert action" be run by an intelligence organization or by the military?

The parallels between the various contexts for intelligence gathering ultimately break down at the boundary between games and reality. Making the wrong choices among the tradeoffs in a poker game will cost a player a few hands or maybe some money; in the realm of national security, the cost could be national survival. Thus, where the alternatives are survival and sportsmanship, the former will probably take precedence. Still, when sportsmanship and playing by the rules constitute significant elements in a nation's *raison d'etre*, giving survival precedence may be the surest way to lose everything important.

Extracts

1. WILLIAM ODOM, "C³I and Telecommunications at the Policy Level" (1980, pp. 1–23)

Military Assistant to the President's Assistant for National Security Affairs

People sit out at the CIA—they never come to Washington, and they never come to talk to us, and I don't think they go anyplace else in the world. They read all the cables and they write nice essays and papers that are distributed around the government and nobody reads them. So they really cut themselves out of the action. You talk about finished intelligence, putting all this stuff together, filtering it out; true, you do need that process. And in some respects it works. It works reasonably well in the CIA's current intelligence system. The Joint Chairman, briefing every day, gets a pretty good rundown. And then occasionally you get some rather sharp, useful, analytical and more long-term pieces; but most of the stuff that comes up through this process is junk, and has some built-in biases that just can't be overcome. That's a general comment; it's not always that way.

... If you had read the NIEs in 1977 and 1978 about Soviet capabilities, goals, and intentions, you would have thought they were complete news to the policymakers, because almost all the secretaries were behaving and talking as if that weren't the case at all. In other words, there is a tremendous gap between what was produced and blessed as national intelligence and what the people who were making the policy were willing to accept as intelligence, between what's reported as intelligence reality and conventional wisdom.

NIEs—National Intelligence Estimates

Notice that I said it starts right down at the battalion level. You never trusted the S2 anyway; he is sort of a third-rate officer you want to get out of the way. Then it becomes sort of a second-rate operation and the S3 operator just assumes what the enemy is doing, or he gets it out of the newspaper, or he makes it

S2—Intelligence staff
S3—Operations staff

up. There is, even at the national level, a tendency to get one's intelligence from the newspapers or from one's best friends or some current intelligence, and to operate off the cuff. I think there is a corrective effect eventually, and I think we have already had a swing back. But in the year 1978, during the budget cycle, that gap was pretty wide. (20-21)

2. **RAYMOND TATE**, "Worldwide C³I and Telecommunications" (1980, pp. 25–47)

former Deputy Assistant Secretary of the Navy and Deputy Director, National Security Agency

The BETA program is an R&D program going on now in which the Army and the Navy are developing a data processing system to quickly turn around intelligence information and provide it to tactical commanders in as near real time as possible. If you are trying to bypass bureaucracy, a lot of it is found in this series of links too, so you are trying to get the information to tactical units in as automatic a form as possible. A very large **ADP** is being built, hopefully compatible with the existing set of sensors and the existing command structures modeled after the command structure in Europe. So we try to put intelligence at the strategic levels in as near real time as possible, and in time, with systems like this, we will have parallel intelligence as quickly as possible going throughout the command, all the way down to units.

ADP—Automatic Data Processing

[STUDENT] As part of that, have they done anything more with the idea of using state-of-the-art computer technology to get down to the S2 at battalion-brigade levels?

[TATE] Yes, they are working hard on it. It is primarily a military rather than a technology problem—there has not been any agreement to my knowledge, even in the Air Force and the Army, on exactly what that S2 needs to know. Once you establish that, the technologies can put in simple filters to ensure that he is not inundated with data unless it is what he wants to be told. That is going to take time. We are making progress, but views naturally clash, depending on your vantage point and preferences. The Commander of the Sixth Fleet, for instance, is a good friend of mine. In the Pentagon he had one view; as the Commander of the Sixth Fleet he has another view, and his view now is that he is being inundated. His predecessor made a big case, with some justification, that he was never told enough. So you have both extremes, and a pendulum effect.

[OETTINGER] If I may take issue, Ray. I don't think the problem is solvable, in the sense of finding one level between what is inundation and what is too little. I stress that because you were talking before about give-and-take between personalities. If it were only personalities you might have some selection scheme which would put compatible people together. But underlying that is the fact that you can't win statically. At one extreme you feed everything to somebody and he can't possibly assimilate it all, so you start putting in fixed filtering; but on what basis do you do that? At the other extreme, if you have some information which has been carefully interpreted and worked over, you get the reaction "Oh, those guys at CIA—it's all worthless stuff; it may be elegant, but it's ten weeks after the fact and who needs it?" So while the technical components are an important element in all this, at the heart of the matter is the intellectual problem of figuring out how to live with the tension between overload at one extreme and the wrong kind of filter hy the wrong sort of people with excessive delays at the other extreme. I've witnessed at first hand a number of players falling on their swords, or appearing to, over that same issue. It's very, very complex. These are not just questions of personalities, hut theories of warfare: how do you do that? Some commanders, as you point out, want to know everything. There are others who simply want to know what they need to do.

[TATE] The raw product coming in from all those sensors, technical data of all sorts, is analyzed by engineers, mathematicians, telemetry experts and others. NSA does the technical analysis; the results are passed to the DIA or the CIA, depending on their nature. As for intelligence analysis, that's supposedly done hy the DIA or CIA from all sources.

NSA—National Security Agency
DIA—Defense Intelligence Agency

... Intelligence has hecome so technical that it takes real specialists to do many facets of it. NSA has the largest collection of mathematicians under one organizational roof in this country, and for very good reasons. Breaking codes, judging weapons systems, and all the technical judgments involved in analysis, are a lifetime career in themselves. Many of the people there are ahsolute experts on the Soviets. Some of the people, particularly those who came in the latter part of World War II, were schoolteachers and whatnot—there was a large influx of math teachers, many of them women, many of them still there. Some are well beyond retirement, hut they have worked these Soviet activities for 20 to 25 years, they think like them. And that's the hest kind of analyst to have. Because it is difficult to "mirror-image" a potential opponent like an Oriental, or a Soviet—who in my view has tendencies similar to Oriental. You need longevity to think in that way, to

imagine, if such-and-such a thing happens, what your opponent's reaction would be.

So, then, intelligence is seldom the whole story. It's a web, a sequence of events, pieces in a puzzle that is seldom or never completely put together. Postulations have to be run. Those technical people have an essential mission, not just in doing their technical job, but also in judging the implications. But then I think the implications ought to be scrutinized at the national level, not by someone who has spent his whole life looking at the Ninth Regiment or the rocket force.

... Do you know that the **'73 war** was an intelligence failure? I was sitting in a colleague's office on the afternoon in which the White House Situation Room was put on a **SIGINT** alert, and it went over to **the big maze** and was not believed. That came out in congressional testimony later. But each time the system is "pinged" it seems to upgrade the operation and make it a little more sensitive. I don't know what the answer is; but it is give and take. I believe in give and take, but I would also like to see less bureaucracy.... (35–36, 44, 45)

'73 war—Yom Kippur War
SIGINT—Signal Intelligence
the big maze—Pentagon

3. **ROBERT ROSENBERG**, "The Influence of Policy Making on C³I" (1980, pp. 49–65)

Policy Assistant to the President for National Security Affairs, National Security Council staff

If I don't know where the empty silos are in the Soviet Union from whence the missiles came, I could expend an unnecessarily large percentage of my force and my deterrent at random ... [P]art of the need to look at the endurance of these functions is that after these nuclear exchanges (God forbid they ever happen), we must make sure we don't find ourselves in a position where an aggressor still has a secure reserve force of such magnitude that he can hold our governmental system hostage because he has blinded us—decapitated our ability to conduct military operations and run a civil entity called government.

The problem in intelligence is that it grew up under the philosophy: we are a peacetime operation; when the bell goes off we have a long leave. Very little

of our national intelligence is survivable. And there are different perceptions of what's important and what's not. The Director of Central Intelligence, under Executive Order 12036, is the head of the US intelligence community. He is responsible for the national intelligence budget; he is responsible for developing programs against the set of requirements levied on him by the National Security Council Policy Review Committee, which acts as a consumer union to set the priority for what we need. And the perception is that military operations support is, by and large, not as important as peacetime intelligence functions. (63)

4. **LEE PASCHALL**, "C³I and the National Military Command System" (1980, pp. 67–86)

Consultant; former Director, Defense Communications Agency and Manager, National Communications System

There's a lot of intelligence information, and it's gathered from various sources. One of the basic tenets of intelligence collection is that you must protect your sources, otherwise you'll lose them. Very few people must know about the source. So intelligence over the years has grown up in compartmented ways. That mindset says, "We need to protect everything about intelligence," and if you're not a member of the community and you don't have all the compartmented clearances, it's hard to get it all together. But some intelligence collection is in near-real time, and it's getting precise enough so that it can be given to a battlefield commander and he can make use of it. So what you want to be able to do is be sure that somehow the intelligence useful to the operator, the commander and the staff officers, gets disseminated to them—not in a weekly or daily intelligence broadcast or message whose source has been sanitized, but directly from the source—and still somehow protect where it came from. It's an engineering problem, I think, and an attitudinal problem more than anything else.

. . . [Another] problem: information needs, or information overdose. . . . It's very hard to define. The typical staff officer, when asked what he wants in the data base often responds: "Everything, because I don't know what the Chairman of the Joint Chiefs of Staff is going to ask me next." I can cite you one instance. . . . The White House asked about the possibility of putting some troops at a certain place in a hurry. There was a Marine landing craft in the Mediterranean on an exercise schedule. The Marines were scheduled to go over the side on landing, into the landing boats and then ashore, to practice an amphibious landing. The first question that occurred to the staff officer was, "Have the Marines gone over the side of the landing craft

yet?" And, you know, who knows? Well, what good is that computer? Things like that, said in a moment of tension, leave impressions on people; so the net result is that, when somebody asks what you want in your computer, the almost inevitable answer is "everything"—and real time. That obviously will not work.

So defining what you want and deciding on timeliness, and when to update, and all those kinds of things is very difficult indeed—and if you're not careful how you do it, you end up with much more than you need. Then the decision maker gets a bad case of indigestion called information overdose. When that happens to him he's confronted with so much information that he can't figure out which is important to decide. I think we saw some of that on the part of the Nuclear Regulatory Commission when they were trying to decide what to do about **Three Mile Island**, and ended up deciding the best thing to do was prepare a press release, which is focusing entirely on the wrong problem. That can happen to you.

Three Mile Island—site of nuclear power plant accident near Harrisburg, PA, in March 1979

So command and control systems and management systems both have the same kinds of characteristics. You have to find some way to control that information, or display it in such a way that the important elements emerge, so that what is important is driven to the attention of the decision maker. (82, 83–84)

5. **WILLIAM E. COLBY**, "The Developing Perspective of Intelligence" (1980, pp. 115–39)

Counsel, Reed & Priest; former Director of Central Intelligence

Most people think of intelligence as a spy service. I think most of the public thinks that way; a lot of responsible people even think that way: that the function of intelligence is to have a spy steal a secret and get it to the general so the general wins the battle.

Well, that really was what intelligence was all about until the Americans got serious about working on the subject. We began to get serious right after Pearl Harbor, when we discovered that it really wasn't for lack of information that we were surprised there. It was the fact that though we had

information in the Army, the Navy, and the State Department, we hadn't brought it together—centralized it—in the sense we've since come to develop. We started at that period to reach out for a new concept of intelligence. **General Donovan**, who set up our wartime intelligence agency, was a World War I hero, and he did indeed run a service that sent spies and guerrillas around the world. But he also added a new dimension to intelligence by reaching out here in America to find people who knew something about the distant parts of the world. He went to the colleges and universities, the businesses and industries that exchanged products and raw materials and the cultural, anthropological, and geographic societies. He developed a core of experts and scholars to work on intelligence, to study these matters and come out with the best possible evaluation of them, and this was a change in some of the concepts of intelligence.

General Donovan—Maj. Gen. William J. Donovan, USA, 1883-1959

When Donovan disbanded the wartime agency at the end of the war, in compliance with our unbroken tradition of organizing spy services for wars and disbanding them afterwards, he gave a little ceremony. And the ceremony was very indicative, in that in his speech of praise for the people who had worked for him, he singled out first the scholars he had assembled in Washington for the unique contribution they had made to the President's and Joint Chiefs of Staff's understanding of some of the complex factors that were at work around the world.

We've continued along those lines since then. When we organized our intelligence service for the Cold War in 1947, we continued to put scholarship at the core of modern American intelligence. As a result you'll probably find about as many doctors and masters of all kinds of arts and sciences on the CIA staff as on the faculty of this university, and they are doing more or less the same thing: looking for the facts, gathering them together.

... The President, Congress, the press, opinion leaders, the public all thought: if you are going to have intelligence, spies, it has to be all secret. Therefore it can't be under the normal relationships of our government structure. Leave it to the President; it's just the President's business, nobody else's. Well, the fact was that it was too big and too obvious to fit within that old concept. . . Finally we had to resolve the disparity between the reality and the theory. Partly it came about because the old consensus involved a contradiction with the constitutional definition of the responsibilities and accountabilities of government. Intelligence was a category that had just been passed over to the President—"You do it"—without any of the normal

controls, without any rules being set up. My generation had to make up the rules as we went along, and we made a few mistakes in the process—not very many, I think, but a few, no question about it, because of that concept of a spy service at the edge of the President's desk that was nobody else's business. Congressmen and senators said they didn't want to know about it. They would just appropriate the money blindly and say—"Go in and do what is useful." Sooner or later that contradiction had to be resolved. Either we're going to have the constitutional system without exception, or we're going to have an exception to it, not just an understood exception, but one that is admitted in some fashion.

Well, we had those two problems: the organization's inherent size and activity because of its changed nature from an old spy service, and the inherent contradiction with the constitutional norms; and we had to resolve them in some fashion. Now we did that in the most clamorous fashion possible, waving our arms, and everybody got histrionic and denounced each other and we caused ourselves a lot of harm around the world in the process. We created the image that the CIA was under every bed and responsible for every volcano in the world. We also created the image that Americans really aren't serious about serious things and can't be trusted to be dealt with on a secret basis. Foreigners who had previously shared sensitive information with us would no longer do it, or they wouldn't work for us—they didn't dare.

Now, however, I think we've gone through that period, and the pendulum has swung back to seeking a sensible middle position. Now Congress is looking at a new, reasonable kind of charter—it's a novelty in the intelligence world, a charter enacted by Congress. It will have in it some procedures and strictures, some guidelines saying what intelligence will do and what it won't do. It will set up procedures for different people who have to be consulted and take responsibility, another novel concept since the old idea was that nobody was responsible for intelligence. The President could deny it, the spy could be disowned, and you couldn't prove it to the contrary; that was the old theory: plausible denial. But now two congressional committees are seriously involved in responsibility under the separation of powers, knowing and keeping the secrets and exerting Congress' full constitutional role.

Bringing the whole concept of intelligence under this constitutional system is, as I say, a very great novelty in the world, and one that many people still don't believe. Some of my former associates don't really believe it; some would like to go back to the good old days. But I don't think that's feasible. Others would like to have intelligence's hands tied, conduct it as a totally

open thing. The American Civil Liberties Union came out with a resolution a few years ago which they've kind of forgotten recently. It said that we shouldn't collect anything secretly around the world, shouldn't have any secrets—which I think is a little absurd.

Well, the pendulum, as I say, is swinging to a center position, and the new charter is a reasonable solution of some of the contradictions. We are going to admit that we conduct intelligence activities, and we're going to conduct them under our constitutional system. We think we can do it. We think we can be just as effective, or even more effective, because we have a new concept of intelligence.... In the revolution in intelligence brought about by the concepts of scholarship and technology, the third factor is the concept of constitutionality....

Do we expect our intelligence system to be a crystal ball giving us an absolute prediction of what's going to happen in the future? No. In the first place it's probably not possible, because the number of variations and variables gets beyond you. Secondly you wouldn't want it if you had it, you don't want to be condemned to go through the experience the crystal ball predicts for you. The purpose of intelligence is to help you act so that you can have a better rather than a worse future. And if you act intelligently, and cause a change in that future, then of course the prediction turns out to be wrong—for the right reason, and you've really capitalized on what intelligence is all about.

Now how do you do this? We've had various attempts in various directions. We've tried to organize the pipe-smoking, tweed-jacketed professor with his yellow pad and his good judgment. We've tried to have a group of generalists sit around and try to make wise assessments about what the world's about. Over the years, however, some of those assessments have become progressively less useful to the harried and busy people they were supposed to be helping, and increasingly the harried and busy people stopped reading them. On the other hand we have had some great ideas, such as enormous new automatic estimating systems where you put all the factors into a computer, develop the model, wiggle the factors a little bit, see how the result changes and that gives you an absolute prediction. But it's garbage in-garbage out; you've got a certain amount of garbage on both ends, and so that isn't the answer.

But then what do we have to do? After the Iranian revolution began the President wrote to **Secretary Vance**, **Dr. Brzezinski**, and **Admiral Turner** and said, "We have really got to do a better job on our political intelligence. You've got to give us better warnings on these kinds of

Secretary Vance—Cyrus R. Vance, Secretary of State under President Carter

explosions." Now, was that a collection problem? If we had just had a spy next to the Ayatollah Khomeini would that have changed the circumstances and made us more able to act? No. The Ayatollah Khomeini made it crystal clear what he wanted to happen in Iran. The factors that led to the explosion were all out in the open: the political difficulties, the weaknesses of some of the Shah's structures, the absence of a political base, the destabilizing effect of the massive changes that are taking place in Iranian society. The problem wasn't a matter of collecting some fact that said there's going to be a revolution in February, 1979. If you'd gotten a report that said that, you probably wouldn't have believed it anyway. I mean, nobody can produce that as the result of a report. You've got a much more complex job of assessing all the forces that impact on the problem and coming out with a resolution.

Dr. Brzezinski—Zbigniew Brzezinski, National Security Advisor to President Carter

Admiral Turner—Stansfield Turner, Director of Central Intelligence under President Carter

Ayatollah Khomeini—spiritual and political leader of the revolution that ousted the Shah of Iran in 1979

Now, we've had some successful estimates. *The Pentagon Papers* contain assessments of the likelihood that the North Vietnamese would give up, that the war would be taken care of by more military forces. They said both prospects seemed very unlikely—and those assessments turned out pretty good in retrospect. They weren't used, perhaps because the President didn't want to use them, because the Secretary of Defense thought we could put some more force into Vietnam and have an effect—just achieve numerical preponderance and everything would be all right. We didn't have the institutions to do some of the non-military things that for many years, maybe, should have been done—even things we knew should be done and were called for. But we did have the institutions to do the military action, and that was the easy thing, so we went ahead and did that—it was a case of "When in frustration don't just stand there, do something!"

So we've had both good ones and bad ones. I think we're going to be grappling with new methods of estimating, new methods of putting together these factors. I'll give you a gross oversimplification as an example. There has been a great deal of R&D trying to come up with better ways of estimating probabilities, and they still aren't very satisfactory. Some of the methods are useful in a way, at least for tracking the estimating ability of certain people. For a number of years we made different analysts write their estimates of the likelihood that war would break out in the Middle East. It was interesting to compare their attitudes—some would say 10 percent, some 50 percent, sometimes it would go up, sometimes down—and you'd try to establish why, and so there was a disciplinary effect. It didn't help you

particularly with the estimate as such, since you were still basing it on the individual's judgment. It did help impart and enforce discipline on the process. Looking back at our estimates on Iran—I haven't read them, because they're classified and I haven't been reading classified ones—I'm sure you'll find some language in those of the last two or three years saying, "There are political problems under the Shah, but probably he will continue to be in power." That word "probably" tends to make you think, "Well, I guess I can forget that. There's some wild chance that he might fall, but the intelligence people have come up with a judgment that he's going to stay in there." So you forget about it.

Now suppose you go a step further and put the "probably" in numbers: 90 percent, 95 percent. You say, yes, there's a 10 percent chance that the Shah will fall, but that doesn't make much impression on you either. But then suppose your discipline calls for you to put next to each of these results a big multiplication sign. That is, you have to assign a factor for the importance of that development if it occurs, and you must multiply the probability factor by that importance factor. Well, if you were looking at Iran three years ago, I think you would say, "Well, if the Shah were thrown out, boy, that would be a real mess. That would be very, very important." So, doing the multiplication, you'd really have a flag that says, "Hey, you'd better pay attention to this. This is something you really have to spend some time and effort thinking about, and act to avoid it happening."

I'm saying this to relate the job of intelligence to what I think this class is really all about: how do you make decisions? And not only how do you collect information, and analyze it so that you get pretty good judgments about what may happen, but how do you communicate that information? It doesn't do any good to have the best report in the world lying on the President's desk if the ideas aren't in his head.

You have to put those ideas into his head. How do you do that? I think this is part of the experiment you're working on. I think you've got to try new methods. We've tried various experiments; some worked and some didn't, some were liked and some were not. But part of the challenge that's before us is to develop these new techniques. Collection, in this information age and with the way we use and disclose substantive information, is really not much of a problem. Most of the major facts are pretty well known these days—a lot of tactical facts aren't, but the fundamental facts that drive world affairs are pretty well known, if you think about them: the demographics, the economics, the social backgrounds, the cultural factors. But I think a lot remains to be done to improve our management of the analytical process, our discipline of it, to shake out what I call the "mindset problem"

that will afflict any organization you set up. That is, the inertia that means if they have gone through the alternatives 50 times and 49 times it came out in direction A, then the 50th time it's almost certain that that group is going to think it will come out in direction A again.

... You see, one of the problems of analysis is the relationship among those who collect information, those who analyze it and the policymakers who decide on it. The old idea was to hermetically seal each of the three areas so that they did not influence each other—so that the collectors are not just feeding the policymaker what he wants to hear, and the analyst isn't warping his judgments to be pleasant to whoever's in the White House at the moment, and isn't overwhelmed by the collector's enthusiasm for some particular item, but can be objective and independent. But quite frankly these theories are all wrong. What gives you real value is the degree to which you can put all those people together, so that you can begin to work on the problems the policymaker sees, instead of just reporting things that sound important to you that he really couldn't care less about. That doesn't mean that you should only report what he wants. Sometimes you have to report to him what he ought to know, things he doesn't know he needs: some new development he doesn't know anything about, for instance. But you do have to get communication among the collector, the analyst, and the decision maker extremely well hooked up, so that they can relate to each other and be of maximum utility to each other.

... But the fact is, we are still protecting those sources [of information about new Soviet missile designs]—the specific technology and exactly where we're learning various things—and yet we're producing the designs and technical factors of Soviet missiles. You can do it. It takes a little ingenuity; I'm not saying it's easy. And, yes, there are a few things you couldn't do it with, where there absolutely could be no other source, so producing it would reveal it. Even so, however, you may be able to put it into a general statement, not really indicate it precisely, and circulate it that way.

Now, if your intelligence officer feels the responsibility to get a certain message over to the people who need to know it, who in this country needs to know about a new Soviet missile? The President, the Secretary of Defense, the military. Is that enough? Not by a long shot. The congressional committees absolutely have to know it if they're going to do their job right. Opinion, the media, the public need to know about that startling new weapon system.

When the Soviets began to build a big boat in one of their yards, we saw the keel being laid, and we had a big argument in the intelligence committee as

to whether it was an aireraft carrier or not. We watched it grow, and finally, sure enough, there it was. We followed it for about three or four years, we followed it when it was launched and on its trials, and all the rest. When that carrier sailed through the Bosporus, it didn't have the impact on America that **Sputnlk** had had; it didn't suddenly frighten us to that extent, because we had circulated, not only in the official community but in public, in *Aviation Week*, designs of what that aireraft carrier was probably going to look like. The fact that that information had been prevalent contributed to our thinking process.

Sputnik—artificial earth satellite launched by the USSR on 4 October 1957

[OETTINGER] If I hear you correctly, you're saying there really is no incompatibility between source protection and wide availability of the information. Do you believe the paranoia is waning about extending source protection to make information unavailable, not just to the public, but to some segments of the intelligence community or military?

[COLBY] It's definitely waning, partly as a fact of life. One of the most dangerous things right now is that, if you train your intelligence officers to write reports which include reference to the sources, when they're leaked they leak the sources too. That's the worst of all worlds. If we could at least train them to write reports which summarize the situation and try not to reveal sources, then when the material goes out, even if it's sensitive it wouldn't contain the source references.

[OETTINGER] I'd have a problem with that, not perhaps if I were a member of the public, but if I were in a staff or line position. Without the sources, I'm robbed of the audit trail that enables me to make an independent judgment of the credibility of the material.

[COLBY] That's why I say you have to develop confidence in the source of the report. In other words, the intelligence officer cannot duck by saying, "I just got the report, I don't know whether it's any good or not." Either he makes a judgment that it is good enough to put out, or he throws it away.

... In a very good book, *Strategic Intelligence and World Policy* (1949), Sherman Kent wrote that you can organize analysis geographically, or by discipline, functionally; and he said we ought to organize it geographically. He said that all the economists, political scientists, social scientists, and military experts who work on East Asia should be interrelated in an East Asian

Analytical Center, and we'd get somebody to speak for an estimate of East Asia. But we organized the intelligence community exactly the opposite way. We put the economists in one bureau, political scientists in another, physical scientists in another, and the military experts in another, in the best academic tradition, because that's the way you organize universities. The result, I think, has been a great mistake, because you don't know who speaks for East Asia. I had a problem about China shortly after I got into my job, and I called in the people who knew something about it from the different offices. About ten people came into the room, and I was the only central point for them. I said, "This is ridiculous. I don't have time to integrate all these different elements of the problem. Get some other system so that somebody else does the integrating and then he helps me."

[STUDENT] At the State Department they have the opposite problem. The real clout is at the desk where they have integrated information for each country. You say, "Give me the man on China," and the head of the China desk will come in and give you the China perspective. But what you lose is the functional perspective on how the economic problem in China is relating to the rest of East Asia or other concerns. Don't you need a multiple approach?

[COLBY] Yes. The problem is that, when we made an estimate on say, Bulgaria, we'd make a political estimate and then tack on a military estimate and then maybe an economic estimate. But they'd be annexes to the basic paper. The three groups would never sit down and analyze it together.

[STUDENT] So you're saying that the process should be reversed—have the generalist make the analysis and then have the economists, the military guys—

[COLBY] Contribute to it through the machine. Yes, you need both cuts of the problem. But I think the dominant one ought to be geographic. . . . There is a thesis that you ought to organize it one way for five years and then the other way for the next five years to shake everybody up. There's some value to that.

. . . [W]e are moving into a world which is much more open, just due to technology. We can look at a Soviet factory and see how much power and what kind of coolants and materials go into it, and what kind of freight cars are there—on a steady basis.

. . The thing that we're concerned about is their [the Soviets'] ability to pick up microwave communications. We know for certain that they do it; all

those gadgets on the roof aren't just for decoration, and it just so happens that they chose as their new embassy site one of the highest points in Washington. How we let them get away with it I'll never know.... But then, you see, if you absorb masses of this stuff, and then put key words into the computer, you can drag out by phone number or some criterion everything that comes out of a given office. That's the danger: that they will build up coverage of specific economic events, of matters that they can use for blackmail or exploitation. That's why the pressure's on for some solution to this problem, in the Washington area anyway, and the same problems occur in various other areas. I think just the unbearably large volume of American communications may solve it, since I doubt even a big Soviet computer could keep up with it....

[STUDENT] How do you set up a system so that the people down the line know what are the concerns of the people further up the line at each level?

[COLBY] I'll give you the theoretical answer and the real answer. The theoretical answer is that there's a system of requirements, very carefully considered by the President and his staff, as to what they want to know about the world. Obviously the President doesn't really have time to figure out what he wants to know about the world. He's counting on somebody telling him what he needs to know about the world, so he's not going to pay any attention to that. Therefore a staff develops those requirements; and the staff, like most staffs, wants to make sure that it's never found wanting, so it covers everything in the requirements. That's a natural reaction. The requirements look like a list of everything in the world, and therefore they're useless to the collectors, who never read them because they express the obvious in great detail—so much detail that it bores you to tears when you read it and you know you're not getting anywhere. The only function it has is that sometimes the reports are indexed to the requirement numbers to prove what a good job you did in responding to the requirements.

Now, the real answer is twofold. One is osmosis, which works either well or poorly, depending on the situation. I think it's working better at the Director-President level now than it did when I was there, because the Director sees the President, I think, about once a week, and that's a good thing. He sits down and talks with him about intelligence. He probably gets a lot of hints as to what the President's concerned about in that meeting, and he can get things across formally. When I was there, President Nixon was preoccupied with the Watergate problem and didn't have the time. Moreover, Henry Kissinger was in the circuit, and I wasn't about to indicate that I was trying to get around Henry, because I would have lost my head the next day. I don't object to that; he was right for the position; he was trusted

and did a good job. I saw President Ford a lot more than I did Kissinger, but in meetings. But osmosis does work through regular meetings of leadership and filters down through the regular command structore.

The other side of the real pietore is the intelligence offieer's responsibility not to just sit there and say, "Well, golly, the Russians are coming over the hills, but it isn't here in the requirements so I guess I won't report it." He's responsible for being out there and reporting things that look like they ought to be reported and, if he's worth his salt, he's got his eye fixed out ahead and sees things that are threatening, and dangeroos, and problems, and he reports them. If he gets a phobia about something that torns out to be absolutely boring to Washington, and Washington doesn't want any part of it, why, they can tell him, "Cool it, forget it." (115–16, 117–18, 118–20, 123, 124–25, 128–29, 131, 133, 137–38)

6. **B.R. INMAN, "Managing Intelligence for Effeetive Use" (1980, pp. 141–61)**

Director, NSA and Chief, Central Security Service

[STUDENT] Would you comment on the CIA's reluctance to share details with Congress (whereas NSA and some of the other offices are not so reticent) because if there's a mistake they have people to lose, while NSA has machines?

[INMAN] I believe if the CIA were to tell Congress it was prepared to fully share all details except the identities of the individuals, they'd probably reach a bargain pretty quickly. The question of how forthcoming you intend to be in a dialogue is fundamental. One has to sort out between covert operations and clandestine intelligence collection. In clandestine intelligence collection you are providing information as a service; the identity of the source is rarely at issue unless there is some question about the validity of the data, and I believe that's a very rare occurrence. In covert operations, on the other hand, you are dealing with plans for activity supporting either foreign relations or quasi-military operations. You could view that as something classified by the separation of powers in the Constitution. But in any case I don't believe the real issue is identity of the source. It's a larger reloctance to share information on sources and nethods. I find the same thing in the conduct of my own business. I direct all the signals intelligence operation of the US government, except that conducted in direct support of clandestine operations. The theory is that there is greater hazard to those homan lives if someone from NSA is watching surveillance communications, that there's

somehow a danger of a leak if there's sharing. The question is, are you getting the most competent examination and support for the clandestine operations without sharing? So what you're really dealing with is a basic reluctance to deal with Congress and with the other intelligence organizations and parts of the government. In all such questions you get exactly the same issue—that you're dealing with the lives of people as opposed to machines.

... You have a Director of Central Intelligence with a series of staffs and a charge to do some performance evaluation and resource allocation. You have a Secretary of Defense responsible for a substantial portion of the actual execution of intelligence operations, since he has responsibility for all the reconnaissance satellites, all the signals intelligence in another structure, and the analytical areas of various departments and defense intelligence agencies. You have the Intelligence Oversight Board at the White House that only looks, in this kind of structure, at abuses. You have the Office of Management and Budget which recommends to the President how much investment he should make in intelligence. For some years you had a separate body, the President's Foreign Intelligence Advisory Board, that did not so much screen budget levels or volume of outflow as select specific target areas of interest and examine them in great detail, and gave the President individual, independent judgments on either the utility of the activity or the appropriateness of the level. To some degree that involved the investment issue—were you doing enough fast enough. Certainly, in my experience, a major impetus for the step forward in satellite reconnaissance came from the urgings of the President's Foreign Intelligence Advisory Board; it went at a much faster pace than it would have gone otherwise. The Board was early in recognizing the need to do more with economic intelligence; that was about its last action before the Board was disestablished as part of the overall review process in 1977. I believe it has left a void; this is an area where we have the institutional checks and balances for looking for abuses, but we don't have the checks and balances to foresee effectively the needs of the government over the next decade or two. We don't have independent judgments whether a sufficient percentage of the resources are going into a given area to assure that, in the competition against the number of aircraft or tanks being bought, there is a flow of tactical intelligence. Or that at the national level there is sufficient investment in a data base, in linguists, in coverage of third-world economic targets. My view is that there is a void in doing that effectively.

... I am in favor of competition in the area of analysis. In the area of collection, I believe, the problem is entirely different. You want to be able to focus your collection, so you want it to be pretty closely coordinated, not competitive, and you spread as much as you can to cover it. But in most

instances you are dealing with bits and pieces of information, and your judgment about what those bits and pieces mean is shaped by the assumptions you bring to the problem. You very rarely get the hard copy document that tells you precisely what's going on or what they intend to do in the future. So competition in the sense of rigorously going back and examining the assumptions as well as the pieces of information will give you a better product. The best-quality intelligence the U.S. has is its military intelligence, precisely because of the focus of effort, including CIA and Service examination, that goes into it. When you move to political intelligence items the Services and DIA don't take part. There's no real in-depth analysis of the political sector, so the only competition you really have at work is between CIA and I&R. And in the economic area there is no competition. There is a small, very competent effort at CIA. But I believe the country would benefit by quickly creating another separate, competitive economic intelligence analysis body.

I&R—Bureau of Intelligence and Research, Department of State

... In the speed versus accuracy issue it depends how the information will be used. If it is for tactical support of military operations, speed takes precedence; accuracy follows very closely behind. But from living out at the user's end, I can tell you I very quickly ceased worrying about who the information came from. It was "Could we get it fast?" and "Was it accurate?" in that order. The only area that comes close to having the same condition, it seems to me, is support for conduct of foreign relations, in the specific question of negotiations. If you can obtain the other guy's bottom bargaining position, or what his instructions are as that position is revised, there is immediate tactical utility, and you don't need a lot of analytical effort to examine and massage it. But if you can't move it very rapidly from the point of recognition it is likely to be obsolete. So you hope it's accurate; it will have impacted on your own strategy, but the key is speed.

Those are the only instances in which I can make a case for speed. For the others the emphasis is indeed on accuracy. But accuracy is very hard to judge. Because, again, you're dealing with bits and pieces of information. I became very frustrated on this topic. Looking at the question of support for weapons systems, the more I delved into it the more I found that everybody was allowed to go and get their own contractor to build their favorite weapons system; and one of the early things that would occur is that the contractor would give them a threat analysis which supported precisely the design of the weapons system they wanted to build. We intended to stop all that, so that nobody could issue threat assessments for use on naval weapons systems but the Director of Naval Intelligence. We got a directive signed,

but then it was difficult getting the talent to do it, or getting analysts who were willing to go out on a limb for what they believed. I finally pressed to try to structure it—put down the facts, then the postulations you make based on those facts, and the choice of what we think are the best ones, with a range of options. I even explored whether or not I could get them printed in different color ink so it would be clear which were the facts and which were the postulations, but that was too hard; the technology is not yet here to let you do that rapidly.

You really do need to be able to sort that out for people, because the vast bulk of what you're providing is not hard fact. And the assumptions need to be apparent to the reader. Let me skirt around an example, a classified interagency paper slant estimate which is now in progress. It examines some Soviet activity in a specific military sphere and finds it unimpressive, and the conclusion says its likely to stay that way for a long period of time. The body of evidence, when examined, consists of reports of the activity's difficulties, which one would anticipate being sent rapidly, plus interviews with defectors and refugees, all of whom left disgruntled. Consider what sort of estimate you would get if you were to go to any part of the current US military establishment, tap a series of messages dealing with casualty reports for equipment, and interview a series of people who had left the military disgruntled, and were to take that as your only base of evidence in making judgments about the likely readiness of a given capability in the next ten years! In one of our own weapon systems developments it would be interpreted as normal difficulties in the path of an otherwise on-schedule, on-time, on-budget task.

The principal worry I have at this point has to do with the adequacy of our intelligence effort in providing our government a broad range of information, both in depth and in time-sensitive reports, on a great range of potential problem areas all over the world. We are probably better in our capability against the Soviets now than we have ever been, in responding to the need to verify treaties and a whole range of things. But we also have reduced our manpower on much of the rest of the world to the lowest levels since at least the 1950s.

And the great worry I have about this question of balance is, "How does one bring about an effective planning process that examines targets, not just systems?" I don't have any problem with examining systems, but I want them examined in light of the targets one needs to cover. I want to focus not just on the current problems, but on the perceived problems most likely to be faced by the country over the next decade or two. And I want the structure to have at least an equal voice in voting on the adequacy of existing

application of resources—in my view that just does not occur in the current structure. The current structure is designed to sustain the status quo. Cuts were applied across the government to bring manpower levels down—you know, everybody take their fair share to pay for new collection means, to pay for new processing systems. So we lack a counterbalance for target examination, and we lack a data base on the areas of the world which were overlooked in the 1960s when we were focused totally on Southeast Asia—there wasn't a lot of worry about countries in Central America, the Caribbean, Latin America, Africa. I believe the odds are very high that in this decade we will face a lot of challenges in those areas.

... In my earlier experience with the Navy's Human Intelligence Collection Agency, the problem was what we were permitted to target with. Human intelligence is governed by both the DIA and CIA. DIA first had to agree on the division of effort across what all the military human intelligence efforts were doing, and then the CIA had the veto. DIA was not permitted to move into any areas CIA considered as its primary—so, for example, DIA was not to collect against economic or political targets, only military ones. Admittedly, that is where you would expect the basic competence to lie. But to do clandestine **HUMINT** collection requires elaborate cover staff, elaborate support structure, and the only agency really good at that is the CIA. I would make some rather radical changes on the human side. I would be inclined to consolidate the clandestine HUMINT collection efforts under the CIA's auspices. I would also separate out the covert action. So I succeed, in that brief description, in making both the military and the CIA angry. But I think over the long term the focus would turn toward information collection, as opposed to going in and conducting clandestine operations (which turn out to be more fun).... You recognize that I'm talking now, not as the Director of the National Security Agency, but as an observer with years of watching—... I put priority on human collection because I believe it is likely to be of greater utility to the government. You want to make sure that you keep effort focused on doing that, and I would leave that as a central core role of the CIA. And rather than have it be just a civilian effort I would give the military veto power. I would probably end up putting the covert operations under the Department of Defense. DoD has a support structure, and does have to support a great deal of it anyway. The HUMINT effort would need to be a mix of civilian and military; it probably would need to be a separate small agency—keep it small, and don't give it any incentive to go do things to be lively.

HUMINT—Human Intelligence; data collected by or from human sources

... I would say on balance the US intelligence community is functioning reasonably well. The dialogue that has sustained it for 25 years continues

reasonably good. The reductions have gone beyond the safe level, in my view, for dealing with all the problems that are likely to face this country in the 1980s. We need somehow, as a government, to be able to do viable long-range planning—not just for intelligence—but particularly to enable the intelligence community to focus on projected problem areas and shift focused attention ahead of the problems, rather than after they arise. In crisis response we are probably doing the best work across the spectrum at this time—it has worked effectively once the crisis was past; we've been able to focus on it and flow information about it, but there are limits. It's too late to establish viable agent nets when the crisis is underway.

But overriding all this, there is going to be the need to preserve secrecy—about how you access the information, what you are particularly interested in, how it's being used—and that's always going to be a barrier for public discussion. We must find new vehicles to put the era of the 1960s and early 1970s behind us in the relationship between the intelligence community and the academic world, as quickly as the process will allow without creating a new fear of suppression or intrusion on academic freedom. It is going to be necessary, if that is effective, to find ways in which classified research can be undertaken, however unpalatable that may be to some segments. The decades ahead are going to be so troubled that we're going to have to find ways around these barriers. We need to rebuild the information base. We need to bring some resurgence in the availability and quality of linguists. Finally, from the government side, there clearly needs to be a better effort to try to make information accessible as the "fertilizer" to keep that relationship going. (148–49, 153, 155–56, 156–57, 159, 161)

7. **LIONEL OLMER**, "Watchdogging Intelligence" (1980, pp. 163–83)

Director, International Programs, Motorola, Inc.; former Acting Executive Secretary, President's Foreign Intelligence Advisory Board

The President's Foreign Intelligence Advisory Board (PFIAB), as you know, was created by President Eisenhower in 1956 and abolished by President Carter in early 1977. I care about that institution, because I was convinced during my service in the White House (and the past three years have reinforced my conviction) that any President needs an institutionalized source of advice on foreign intelligence which is independent of the bureaucracy and which is provided to him by men and women of broad experience in whom he has confidence and who enjoy a public reputation for judgment and probity.... Please bear in mind during the discussion that although the term "oversight" was used when the Board was created in

1956, its meaning was substantially different from what the word came to mean beginning in 1974. As originally applied to the PFIAB, it signified watching over the intelligence process to assure the adequacy and effectiveness of intelligence. It did not include matters dealing with the propriety and legality of intelligence. Maybe it should have. But such was not the case, and none of the members with whom I served ever felt they had a mandate in that area.

A Board has value to the President who appoints it and to whom it must exclusively report. It also has value to the entire intelligence community. And finally, to a lesser, but nonetheless important extent, it can be of value to the public at large. As regards the President, it is my feeling that however essential good intelligence is, and however from time to time it may determine whether or not given activities should be undertaken, the entire subject must not occupy a substantial part of any President's time and attention. There are simply too many things of crucial importance to the country for the Chief Executive to ponder at any length substantive budgetary or administrative intelligence issues. Thus, say, during the 10 percent of the time he spends on intelligence matters, the President is often likely to receive a distilled "least-common-denominator" presentation of alternatives, frequently representing the self-perceived best interest of the agency presenting them, and sometimes bereft of an indefinable quality—perhaps somewhat like what a Supreme Court Justice said about pornography: it is something you know when you see it—the quality of sound judgment.

I think PFIAB over the years demonstrated its capacity for sound judgment on innumerable occasions. I will suggest four areas. First, economic intelligence, which indeed was first given life as a direct consequence of PFIAB activity. Second, accelerated construction of satellites for intelligence purposes, which would have lagged for years without the strong push it received from the Board. Third, a presidentially directed, government-wide program to deal with Soviet electronic surveillance in the United States, a subject which was virtually taboo for discussion even within the intelligence community until the Board brought it to the President's attention. And fourth, the now notorious "A team-B team" experiment in competitive analysis, which was officially resisted in every part of the intelligence community until the Board convinced the President of its merits.

... The value of the PFIAB to the intelligence community itself might be likened to a doctor's prescription for unpleasant-tasting medicine; the patient doesn't have to like it to know that it is supposed to do him some good. Many times people in the intelligence community expressed to me their view of the utility of the Board, either with respect to a specific issue then being

deliberated or in the abstract, as in "It's good to know there is a group of wise men with full access to all the data and with direct access to the President. That's one way of keeping the bureaucrats on their toes." I would add that the Board's existence by its very nature gave some within the community hope that contentious issues, which to their minds had been papered over, would be fully aired and examined by a Board immune from agency mindsets or jurisdictional disputes....

[OETTINGER] [R]egardless of personalities (the interesting thing about the PFIAB is that it survived administrations of both parties and very different characters for a period of time), and under any President with any kind of staff structure, can dissent or evaluation be institutionalized within the bureaucracy as effectively as within a board of the PFIAB's quasi-public character that is not on the government payroll? Does it make sense not just to have a clean break between what's inside government and what is private sector, but to have (and this is only one example; there have been others, some of which also have been dismantled by the Carter Administration) diffuse boundaries where it isn't quite clear whether a given activity is government or private sector?

[OLMER] There were instances that to me, and I think to the President, proved the Board's utility, when the President would be confronted by several alternatives. Under Kissinger's national security system, option B was generally the one that he wanted and selected, and things were organized to make option B the most attractive. But in any event alternatives were clearly presented. It still left the President sometimes not feeling satisfied—in fact, it left Kissinger feeling unsatisfied. There were periods when he would say, "The papers submitted to me don't really present alternatives. They present a single choice and don't develop the opportunities for other kinds of decisions, and their impact, and their long-range implications." It's entirely another matter to bring someone in from the outside without any of the trappings of bureaucracy. They really don't look on it from the point of view of the State Department, which has a constituency, or the Defense Department. The NSC staff is supposed to be capable of truly objective reasoning and presentation, but it just doesn't work that way.... Not all things should be thought of as suitable for the kind of purpose the PFIAB served. But the big ones, and some less big, ought to be referred to a body which tends to be oblivious to the deep-seated rivalries and bitter arguments that prevail even on the substantive divisions....

NSC—National Security Council

[STUDENT] You talked about the value and necessity of an oversight board, a board that can examine intelligence to assure accuracy and efficiency of foreign intelligence, which is an admirable goal. But in my own experience and knowledge of the PFIAB and the items you mentioned, that was not what the Board did. That didn't appear to be its function. I have some knowledge of two of the four items you mentioned. They originated with small groups or individuals in the bowels of bureaucracy who wished someone would pay attention to their topics—such as economic analysis—and the PFIAB seemed to pick up random (I have not seen evidence of any systematic search), sexy issues which caught the attention of these very intelligent, very wise, but very busy individuals who didn't have a great deal of time to devote to foreign intelligence, which is an ongoing flo of tremendous complexity. It did not in fact appear to exercise the kind of oversight you were talking about. Instead it became another channel to the highest level for people pushing pet projects. The U.S. benefited by the fact that somebody did pick up these pet projects; but an equa' number, if not more projects, which would also be beneficial if someone picked them up, did not catch the attention of the PFIAB. My point is that while in the abstract an outside board that can exercise this kind of oversight would seem essential, without the baggage of the bureaucracy—which includes knowledge and background—no such board can function in that way. I don't mean that an institutionalized dispute panel and a wild-eyed guess examiner is not useful—but that's not an intelligence oversight board.

[OLMER] I think the PFIAB added a dimension which is simply not available from within the bureaucracy. Sophistication and perceived lack of self-interest are, without any elaboration, the two things I think the outside board was and would be capable of contributing. (163–65, 166–67, 168, 170)

8. **CHARLES W. SNODGRASS**, "Funding C³I" (1981, pp. 119–46)

Vice President, Electronic Data Systems Corp.; former Assistant Secretary of the Air Force for Financial Management

I might say that another witness, Secretary of the Air Force **Mark**, has often told Congress that he thought that the intelligence capability of this country had been strengthened, not weakened, because of the increased congressional involvement in the intelligence budget. He mentioned a couple of things. He said that we

Mark—Hans Mark, Secretary of the Air Force under President Carter

had helped break down many of the barriers that I've been talking about: interservice barriers, security barriers, technological barriers, that sort of thing. He also said he thought that the great difference between the American system and the Soviet system was that we are much more flexible and responsive to changes in technology, in military strategy, whatever—because, after all, they've had the same head of the Soviet Navy for twenty-five years. Now, if that commander makes right choices, that can be a very powerful plus, but with technology changing so quickly it's more and more unlikely that the same kind of technological imperative will last for long periods of time. Secretary Mark thinks that the give-and-take between Congress and the military makes them sharpen their intellectual arguments, makes them examine their assumptions.

... I believe that the most overlooked issue is production, and that we're collecting far more intelligence than we know how to assimilate, to make into usable information for decision makers. And that the really significant marginal returns will come from buying more analysts, giving them authority, if they're an Iranian specialist, to go off and learn to speak Farsi, to go live for two years in Iran—and then, when all this marvelous technical collection stuff collects intelligence, we will have analysts who will be able to tell us what the raw data mean. (139, 144)

9. **DAVID C. RICHARDSON**, "The Uses of Intelligence" (1981, pp. 147–68)

Consultant, Defense Intelligence Review Panel, the Defense Science Board, and other panels

I mentioned earlier that we need a new kind of intelligence that links the operator and the intelligence community, and I liken that to a net assessment process. The problem I'm talking about is our Naval conventional forces in the context of Soviet capabilities. A way to make that net assessment is to study the systems the Soviets have fielded, and seek out their weaknesses.... That net assessment tells me I've got some things to do. It tells me, first of all, that if my developments and my new weapons are not keeping me at least abreast, or hopefully ahead, I'd better be looking at my strategy. When I start looking at my strategy, and start sizing forces calculated to achieve certain strategies, I find myself thrown back again into an assessment process. I may be led to the view that I can successfully do a smaller job. Or else I need new forces, or new approaches. Out of that kind

of process I can see how to make judgments about what I can do now—what I need to do to improve my position, and what sort of constraints weigh on me until I'm able to get there. I don't see any other good way to get there, I haven't been able to think of any other good way to do it. We simply cannot continue to blithely accept worldwide ocean commitments—and we certainly have one in the Northern Indian Ocean that's in that category—without regard to our capabilities to sustain ourselves there in combat action.

... My first real exposure to intelligence, as I said, was in the Gulf of Tonkin, and it was courtesy of my Operations Officer, Captain Robert Hunt. Bob Hunt was a very smart fellow and he said something that's been fundamental to my thinking since: if you want to screw up the other fellnw, find out how he functions and focus on his weaknesses. Our job was interdiction in North Vietnam. I made Bob targeting officer, reasoning that if we could select our targets more wisely we could double or triple our effectiveness. Bob pored over photography, studied it full time. I turned his Ops Officer job over tn the Assistant Ops Officer and Bob did the targeting. Pretty soon he developed a general concept for targeting which focused our resources against targets where we really accomplished something more significant than by previous, less systematic approaches.

To give you just one example: it seemed apparent that when striking a rail line if, instead of hitting tbe big bridge in the middle of a tuwn where they could cross with boats and do other things, you hit four or five smaller rail structures between towns, they would be forced to send work crews out and fix the outer unes before they could get to the inner ones, so that it touk them much longer to get back in commission. There was little or no antiaircraft power out there, so your costs were lighter, the threat was lower. That made a lut more sense than hitting a big bridge in town. We were working against three modes of transportation: rail, highways, and barges on waterways. We produced the system, and the Juint Chiefs sent out a study group that louked at the targeting we were doing, and they were very complimentary about it. I converted what had been a photo distribution group in Subic Bay into an analysis group, and had two individuals, an intelligence ufficer and an operator, working together in cunstant interaction, so that all the operators and all the intelligence officers could come in and work with them, and afterward go back and each contribute in greater understanding. My point is that, in this instance, we developed an office that bridged the gap between intelligence and operations. And it seemed to facilitate communications. It made this particular system a good system, the best we could conceive of. (155, 157)

10. **CHARLES ROSE**, "Congress and C³I" (1981, pp. 169–91)

Member, US House of Representatives; Chairman, Policy Group on Information and Computers

I would like to address what I consider one of the major problems concerning our defense establishment and our intelligence community: the need for good analysis. All too often the policymaker and defense planner alike would like to hear the tune played back the way they have composed it—like editorial writers who send out reporters to make their editorials come true. Unfortunately the world doesn't always work that way. There is a need for considerable improvement in the academic rigor of studies, analyses and estimates in the intelligence and defense communities. This is not to say that a lot of good work doesn't get done, but all too often there is a tendency for school solutions to appear with directed endings. The more we continue to have school solutions, the more we feel free to pick and choose the evidence that supports a particular case, the longer we will continue to pay the price and make mistakes, which means we will keep making major landmark decisions for defense planning and policy formulation in a cavalier manner.

... During the last fifteen years we've had unprecedented growth in technical systems. The decision was made in the early 1970s that the price of those technical collection systems would be paid in people. You may think I'm kidding, but believe me it was a conscious decision. A number of people in the intelligence community have told me the same thing. As a result of that decision we find ourselves in poor shape as we try to assess the Third World, analyze the Persian Gulf, predict trends in Central America. We find ourselves with few linguists in languages which we felt a few years ago were insignificant and unimportant, but which today are highly critical.

... We've also seen some evidence that the intelligence community is playing a little game with us—coming in and requesting one of those elements [people or hardware] in their budgets knowing full well that they have omitted the other one. For example, they come in asking for hardware but no people, and they say, "Well you know, my God, Congress will add the people" or they come in asking for people and no hardware—whichever one they forget to ask for, good old Congress in its patriotic wisdom will add it—and that way they don't get caught inflating the budget.

... Consider the Iranian hostage rescue mission. I'm sure some of you have read the unclassified version of the after-action report by the five generals on the mission; the top secret version which I have had access to is not really much different. In it they discussed a couple of problems that tell me we

haven't learned the lessons of the past very well. One of those problems was excessive secrecy, too much compartmentation. Another was fragmented lines of command and control. I had occasion recently to scan a fine book entitled *First Line of Defense: The Navy Since 1945* by Paul Ryan, published by the Hoover Institution at Stanford. It discusses the Bay of Pigs operation and the role the Navy played or did not play in it ... The key operating factors in the Bay of Pigs and the Iranian hostage rescue mission were similar. Individuals who ought to have had access to information did not. Planning took place in isolation and clearly was hampered by the poor command and control setup.

... In many cases of past "failures" it has been found that information was largely available, but either hadn't been analyzed or hadn't been placed in proper context. This is partly the fault of intelligence, but is shared equally, and sometimes to a greater degree, by the policy community. Certainly it is true in the case of the fall of the Shah of Iran. Our examination of intelligence performance in Iran prior to November 1978 found that the intelligence problem was partly due to the collection elements' failure to ask the proper questions. This so-called failure, however, was orchestrated by the policy community, which had forbidden the intelligence community to go out and collect data on dissident groups within Iran, lest our intelligence activities offend the Shah.

I'm concerned that we don't put ourselves in that kind of position again, and I think there is great danger that we could do so, especially in some areas of the world where we are awfully cozy with our allies. We may have a tendency to overlook things going on within a country which could be inimical to our relations with that country, perhaps not today, but five or ten years in the future.... I think what would cure that problem best would be finding some way (I don't have the solution) to depoliticize our whole intelligence operation. Time and time again our national intelligence estimates seem to have been rewritten because the policymakers didn't like the bottom line. Maybe dividing up the chores the way you suggested [Oettinger—separating covert and intelligence operations] could have somewhat the same effect. Now that Mr. Casey is an actual member of the President's cabinet, one must seriously question how much the policy of the White House drives analytical conclusions. And, analysts and collection to the contrary notwithstanding, how often do those conclusions wind up being a justification for a policy that was made somewhere else? These are exactly the kinds of matters our Committee looks into.

... [T]here is a need, not only to insure good competitive analysis, but to maintain the objectivity of the intelligence process and keep it as

depoliticized as possible in a highly strung town like Washington. This is not an easy issue to come to grips with. We're far better off structuring our estimate products with footnotes and diverse opinions, rather than trying to develop consensus judgments on issues. You may have read in the newspaper a couple of weeks ago about some problems with a recent estimate on terrorism. This issue is still in the limelight. I'm reluctant to comment on it too much, except to note that the more the administration dillydallies in attempting to come to a consensus judgment on such issues, the more it will open itself up to accusations of politicizing intelligence judgments. The less it is tinkered with, the better off it is. In the final analysis a better intelligence product will be produced. If you've got five different analysts' opinions that you can't somehow meld into one, don't fudge it, don't hide the bottom line. Show that there is a diversity of opinion, a genuine attempt is being made to come up with the answer. There may be more than one answer. (174, 175–76, 177, 178–79, 185)

11. **B.R. INMAN**, "Issues in Intelligence" (1981, pp. 193–214) *Deputy Director of Central Intelligence*

In the period immediately after World War II, when the current national security structure was formed, an attitude prevailed, in addressing the question of information needs, that we should endeavor to obtain any information we might ever need to support any form of government activity. It was the World War II experience that, in trying to deal with everything from long-term strategic policy formulation to day-by-day engagement in conflict, you needed an incredible array of intelligence on any given target or topic, or set of targets or topics, if you were to be effective in either the planning and decision-making process or, much more importantly, the execution.

That general philosophy led to the creation of a number of organizations and agencies. It led to a substantial investment in people, in systems and in a general approach of making available a very detailed data base—essentially a classified Encyclopedia Britannica: all you might ever need to know about any given topic. In my perception, less attention was given during that phase to the timely flow of that information—whether for indications and warning purposes, crisis monitoring or execution. The Korean War then provided a major shot-in-the-arm investment toward the goal of supplying any information which might be needed. So you had, at the national level, a number of intelligence agencies cooperatively working together to develop a very large and expensive data base. Those were the days before computers were

available, so the data was essentially hard copy publications, slow to produce, very difficult to maintain, and heavily manpower-intensive.

When the national mood began to shift with, during, because of (you may choose the preposition) the Vietnam conflict, a very sharp shift occurred in attitudes about the question of information need, at least as it applied to intelligence. And by 1969 the mold was very firmly established: "What can we do without?" was the prevailing view. To meet the pressing detailed needs of Vietnam, assets were dropped that had been involved in maintaining in-depth data bases against a large number of geographic targets of relatively low current foreign policy or military operations need. The people were diverted to work in depth on Vietnamese problems. Thus, when the new "What can we do without?" view took hold in 1969 and we began reducing assets—people in large measure—there was no return to maintenance of that earlier expansive data base. Rather, there was a move simply to remove people from the inventory. And so the general health of that data base began to deteriorate at the end of the 1960s. It got a stimulus in the late '60s and early '70s, when new technology being developed, partly for the space race, offered new ways to access information which had previously not been available at all. But its general decline really began to impact on the US intelligence capability and ability to deal with information needs in the early '70s, with the decision to trade off manpower to buy advanced technical capability.

Let me digress, to deal with a myth. The popular literature holds that we gave up human intelligence collection assets to buy technical collection capability. I stress: that's a myth. We really gave up manpower-intensive technical collectors; and we did not buy the manpower to process the huge volumes of different additional information which were made accessible by a whole range of technical sensors. If you scan the notes of last year's talk you will know that I picked up much of my interest in the information flow part of this information-need/information-flow equation through watching the government's difficulty in dealing with crises, beginning with the capture of the *Pueblo* and the impact that slowness in the flow of available information had in restricting the government's options in trying to respond to that crisis. We made very little progress, at least through the first half of the '70s, in dealing with that problem. We had lots of studies and a fair amount of investment in command and control systems that—from this critic's vantage point—too often were focused on ownership questions rather than on the degree to which the systems would accelerate the movement of information to a whole range of people who might be able to make effective use of it. We really did not get any change in the general attitude toward dealing with information-need/information-flow until the end of the 1970s. Now, I believe, we have again crossed a major obstacle: the attitude is

moving toward "What do you need to know," not "What can you do without," and there is a growing awareness that much more has to be done than has been done to date in facilitating information flow.

... So I would set forth the principle that one needs to look at geographical targets, and that this country needs a given level of information on all parts of the world with which we have to interact—at least a level of detail sufficient to understand the key factors in all the countries with which we have to deal. To understand their degree of internal stability, to understand at least to some extent the economic forces at work, and to have at least a passing understanding of their military capabilities. And, increasingly, to understand what those capabilities may mean to us if they include equipment of friendly origin—US, British, French, German, Italian—as well as equipment that comes from the Soviet bloc. Iran is a case in point. It suddenly moved from being a fast friend to a holder of hostages, and we contemplated the prospect of military activity in the rescue effort a year ago today. And the equipment we had to try to deal with, to collect information on, for direct operation support, was US equipment, with which US collection systems had never been designed to deal.

In a functional sense, meanwhile, one has to pay more attention to political and economic intelligence issues. At the same time a substantial level of effort, at least for the more advanced countries, must be focused on scientific and technical intelligence matters, watching for signs of instability, paying additional attention to internal security, in countries that have the potential for becoming targets of the Soviets and their proxies, or where our own specific national, economic or military interests may be directly at stake.

... It is a fact of life that a great deal of the world is not as open to us as it was 20 years ago. For a variety of reasons a lot of countries, including newly emerged countries, feel no need to have a close relationship with the US or to make information easily available to us about their own internal activity. It is therefore a hard fact of life that for a good deal of information, particularly to really understand the internal security equation, clandestine human collection must be contemplated. We can no longer get away with focusing clandestine human collection solely on the communist countries.

... When you are making great leaps forward in technology, and you are maintaining a stable or slightly reduced analytical work force, a decision to acquire additional technical capabilities to give you huge volumes of information, and not to make the processing investment that will offer the opportunity of greater productivity, is a very foolhardy approach to the problem—but it's taken us a decade to really understand that and to begin to turn it

around. That will get a great deal of additional attention, I believe, in the early part of the decade ahead.

In the field of analysis there is a manpower part, driven by simply the need to deal with volumes of information. But there is a much greater need for quality and, as elements of that quality, for people to understand in substantial depth the targets they are examining. You cannot take an individual, however well educated, put him on a new target and give him bits and pieces of information, and expect that he will give you insightful, in-depth understanding of what those fragments mean in a very short time. The track record of the decade is that the analytical elements, in fact, were not drawn down as much as the collection side—notwithstanding some public mythology that might lead you to believe otherwise.

But the problem, I believe, is that we did not expand our analytical work force at the same time that the volume of data was being vastly expanded, and we suffered significantly from the public attitude toward getting the quality of input to that analytical effort that we had been able to draw in an earlier decade. There is a perceptible impact to that. We also failed to buy the technical kinds of things that would have improved the productivity of the analyst and lessened some of that impact. And again, as you draw down your investment, incentives which produce quality unfortunately tend to be among the earliest casualties. One gives up the extra incentives to maintain in-depth language proficiency in a variety of languages, one gives up the sabbaticals that let someone get a totally fresh outlook on the problems. One gives up, not necessarily by choice, the relationships and the dialogue with other organizations, other institutions, which may not have access to the same depths of classified information, but that have different insights and attitudes about the same kinds of targets you're examining, that might have helped you to understand what those bits and pieces mean.

... Retaining objectivity is probably the greatest prize for analysts in the intelligence process, probably also in other fields. But when you leave people in the same area for a long time without any break, without any incentive to go elsewhere, without any encouragement to continue to be promoted by broadening themselves, you run a very high risk that they will become enamored of answers for the topics they're dealing with, that they will select those bits and pieces of information which support their predetermined theory, and that they will be far less likely to give credence at all to bits and pieces of information which would challenge that or send them off in an entirely different direction.

... An interesting feature in watching this process over the last decade is that Congress by itself, substantially ahead of the Executive Branch, reached

the decision that we needed to start investing more in our intelligence capabilities. Had the leadership not been in the same party as the President, I think we would have seen greater impetus to do more, and more quickly, but they found themselves in the very difficult position that it was not politic to add to the budget of the President of their own party when he was unwilling to have them do so.

... My views on this area [compartmentalization] are largely shaped by my experience in the Seventh Fleet in supporting combat operations in Southeast Asia, and when there was a substantial fear on a couple of occasions that I was going to have to support combat operations in Northeast Asia. That pressure does wondrous things in cutting through the ownership syndrome. You very quickly get down to basic essentials: your ability to get information fast, and hopefully accurately. The most important thing is that it's fast. If it isn't accurate, very often you'll drop the source, you won't want it any more.

The second thing that happens, though, after you turn it on, is that you get drowned in information that is of peripheral interest. When you have a crisis, in particular, everybody is suddenly willing to turn on what they know, even down to a fairly compartmented level. And people at the receiving end never have the time at that point to sort through the huge volume of data which, in a crisis, suddenly becomes available—unlike the peacetime situation, when usually you complain that there isn't enough available to keep you going. I have a strong belief that most of the imagery data can be totally decompartmented; it has no need to be compartmented, because there is very little that a target country can do, without great expense, to deprive you of the value of the intelligence you have derived, even if it knows about it. In fact, if you can cause that country to spend a lot of money on camouflage, cover, and deception instead of on a new weapons system, that may not be a bad tradeoff, because once the enemy starts moving, that cover and deception isn't going to be a great deal of value to him.

On other matters the potential for loss of access is much greater. And there you're forced to a different approach: to take information out of compartments entirely, sanitize it at the very first point of access, and to flow it by the fastest available communications into the hands of those who can potentially use it for tactical purposes.

... A lot of people were eager to throw out anything that might be a constraint in order to get started in doing more counterintelligence, and I guess I, having watched the damage to the intelligence community the last time around, would rather have a clear understanding this time of exactly what it

is we are trying to get at before we lurch off in all directions. That is not necessarily the popular view. (193–95, 196, 197–98, 200, 203, 210)

12. **WILLIAM G. MILLER**, "Foreign Affairs, Diplomacy, and Intelligence" (1982, pp. 165–81)

Associate Dean and Professor of International Politics, Fletcher School of Law and Diplomacy, Tufts University

So both the House and the Senate were launched on investigations as well as an inquiry. It was a two-headed approach, carried out by two houses with very different styles and temperaments. As you know, the House committee broke apart due to leaks. The Senate committee managed to hang together, and its efforts over two years led to a change in procedures, passage of a number of governing statutes for intelligence, and creation of an oversight system. But lying behind this whole sequence of events, really, was the desire by the legislature to have intelligence information as a tool to use in its work. There was a belief, reinforced by the outcome of the inquiries and the hearings, that intelligence was useful to sound policy.

... The agencies, after a period of reluctance, decided that they would cooperate. Two successive White Houses—Nixon and Ford—decided that they too would cooperate, after initial reluctance. The most difficult task, of course, fell on people like **Colby**, who had to deal with two cultures—his own hermetically sealed world and the people who operated within it, and the open public world of public affairs and the legislature. I think the country owes him a tremendous debt for the difficult task he undertook. Many of his colleagues, unfortunately, looked on him as a traitor to his profession, betraying trust of a kind, and felt that he should not have cooperated in the ways he did. There were others, the majority of them in the agencies, who felt the opposite. His view at any rate was that he was obliged by the terms of the Constitution to cooperate, and he did.

Colby—William E. Colby, Director of Central Intelligence under Presidents Nixon and Ford

That was also true of officers like **Admiral Inman**, who's just resigned—in my view one of the finest intelligence people I've ever come across. He was then in charge of naval intelligence, and

Admiral Inman—B.R. Inman, former Director, NSA, Chief, Central Security Service and Deputy Director of Central Intelligence

he couldn't have been more helpful and forthcoming right from the outset. Indeed that was true of almost everyone in the agencies.

... For the first time there was an awareness of the struggle between rival intelligence services, outside one's own bureaucratic establishment (although the internal struggle often seems just as intense). Over a period of years those in both the legislative and executive branches with responsibility were being tutored in every aspect of intelligence for the first time in our government's history, were asking and being told and learning and categorizing what the American intelligence system was and what its purposes were. And for the first time the intelligence agencies were asking the same questions of themselves, and thinking about where they fitted in the government that they were a part of, and being asked to serve.

... The new legal framework was established as follows: intelligence is a joint responsibility, like every other aspect of public policy, of the legislative and executive branches. Whatever the United States does in this area is a joint responsibility in accord with regular processes, and consequently both branches must have full knowledge and full responsibility. The only statute that's been passed thus far requires the intelligence agencies to supply the oversight committees with all information fully and currently without exception. There are no exceptions in any category of intelligence matters....

The process now in effect is that the record of every single intelligence activity is made available to the oversight committees, which then must vote funding for all the activities after reviewing them. One benefit of this process of legislative review has been that it has required the highest levels of the executive branch to review proposed intelligence activities with a degree of detail they had never done before. And there have been more evaluations of usefulness of certain kinds of activities across the board than had ever been the case before—technological collection, covert counterintelligence and, of course, simple collection of information.

... Consensus is natural to the intelligence bureaucracy, but consensus may not be as accurate or useful as particular opinion. One of the problems of national estimates is that it is difficult to present sharpened opinion in them. The art form says that there is a conclusion, an evaluation—an estimate; the various points of view that contribute to it logically support that conclusion. That has been, and remains, the problem inherent in bringing to bear for the leadership other points of view that might be helpful.

... We have had a series of national leaders who have come to their positions without any acquaintance with the intelligence resources at their command, and only after several years of mistakes and ignorance has the awareness emerged that mistakes might have been avoided if they had better information which was, in fact, available. Perhaps that is a phenomenon characteristic of a large superstate, a complicated society—but the resources that are there are not being made use of, except by those who are acquainted with the organism in the first place. Proper use of intelligence is a habit, an intellectual discipline; it does not come naturally. Intelligence can also be very misleading if its limitations are not understood. The uses of intelligence are ultimately one of the most sophisticated tools of leadership. A very real question, very relevant to any discussion of the quality of leadership, is how intelligently a leader can use the sophisticated material intelligence provides.

... In the intelligence world I think it is now, perhaps for the first time, very important that there should be a permanent long-term director. It should not be a political appointment, but rather a career appointment. There also might be some value in having an intelligence top leadership that is free of political change, that is there because they know the world, or know vital intelligence processes and procedures. In order to obtain the best from the narrow world of intelligence, which must present facts in a way that is fully appreciative of the facts' pedigree, you need people who are relatively detached from policy. We ought to seek such people out—that ought to be a value. But we have not had apolitical continuity in the top echelons of any of our major national security departments. That's a loss, but I think more and more people are coming to understand that.

... The standard now adopted by our country as a whole is that covert action will only be used when no other means will do, and when it is in the vital interest of the United States to do so.... The crucial point is how you define "vital." There are continuing efforts to lessen the standard to "necessary" rather than "vital," moving the possible swings of policy from left to right from margins of 5 to 10 percent to 20 percent. But you're still in the same ballpark in either case....

[OETTINGER] But what about the effect of our oscillations, as in the Watergate revelations, where after a period of years what was classified becomes declassified under a shifting definition of freedom of information and becomes widely available? What is the chilling effect of that? It seems to me any observer of the ways confidentiality is maintained, or not, in the US intelligence community would have to take into account not just the current situation, but our democratic gyrations.

[MILLER] The American intelligence system, as Colby likes to point out, is different from anyone else's. It has the limitations of extraordinary democratic institutions. It's necessary for other countries which don't follow quite the same ways to understand what the differences and changes have been; but Colby says on balance it's still very workable for this country. (167–68, 169, 170, 171–72, 176, 178)

13. DAVID MCMANIS, "Warning as a Peacekeeping Mechanism" (1984, pp. 21–34)

National Intelligence Officer for Warning and Director, National Warning Staff

Another difficulty is inherent in analysis. You go into a problem trying to discover truth. You work your way through it, collecting all the evidence, and you put forward a brilliant exposition. Now having gone through all that pain and soul-searching, you have become so wedded to your viewpoint that you will never question it, never go back and ask yourself what is wrong with it. I think we have all been there. It is a very hard failing to avoid. Even though we warn our analysts that this is going to happen, and not to let it happen, it happens time and time again, and I am not sure we will ever totally overcome it.

Even worse is when you go in with your mind already made up, and collect evidence to suit your particular hypothesis. That is very damaging.

. . . We have become, technologically, an extremely competent collection mechanism. Our intelligence resources today are phenomenal. I can't go into them, but I can tell you they are phenomenal. If you read *Aviation Week* you get some appreciation for them, and you have to think of what the Soviet Union thinks about them.

They are really good, not only because they are so sophisticated, so much like vacuum cleaners, but because they are varied. They give us lots of different ways of getting at our problems. They are not complete, certainly, and no intelligence analyst would say, "Collect less for me." But we are doing so much. And our problem has become one of having literally more data than we can possibly convert into knowledge. We have to work on that part of the equation, and I think that is where we can work toward avoiding surprise. Again, the more pieces of that jigsaw puzzle we have, the better off we will be in divining the picture.

Most of our post-mortems have shown us that the information has usually been there. It has not necessarily been pulled together or synthesized properly. Often it is not recognized. (Often, too, the decision maker didn't want to hear that particular message on that day, and so ignored it.) But the information is usually in the data.

So there is a tremendous challenge—not just in the intelligence community, but to the entire information community—to try to exploit what we have. We are spending millions and millions of dollars each year collecting information. There is also the whole world of open source material, which we are not close to exploiting fully. Putting those two together makes your problem worse, but it makes the opportunities even greater. The challenge is to somehow convert the bits of data into knowledge bases without having thousands of trained monkeys sitting at their CRTs entering the data and trying to recognize and identify it.

... It's very important that there be a dialogue between intelligence analysts and the policy decision maker. That's not an easy thing to establish or sustain. It tends to be confined to specialists; for example, actual intelligence officers who will deal at senior echelons. Very few of us, if any, have direct access to the President. But we do have fairly direct access to **Richard Beal** and the rest of the national security officers and Security Council staff who are much more cognizant of the current policy considerations.

Until his death in 1984, Dr. Beal was Special Assistant to the President for National Security Affairs and Senior Director for Crisis Management Systems and Planning.

Now, they are very careful because of the risk of having policy drive intelligence. As a community, we have to guard against that. It really is rather easy at times to put forth a good analytic judgment which, by changing just a couple of words, can be brought a little closer to current administration policy. We try very carefully to avoid that.

... I don't think the investment in either the human or analytic side is nearly adequate, not by a long shot. It gets my technical collection friends up in arms to think about putting up one less satellite, but I almost would do that. I really think we have to start investing elsewhere. Part of the technological aspect is that we have to start trying to build the knowledge base: getting the information in usable form, getting it to our analysts, and really working on training analysts. We have had a very significant turnover in the analytic corps in the last ten years. They are a much younger set than we've had in

the past, and they haven't lived through as many serious situations as many of us have. That may be good or bad, but they do have fewer preconceptions. (24–25, 27, 30)

14. LEO CHERNE, "Television News and the National Interest" (1984, pp. 35–48)

Executive Director, Research Institute of America

Because it is the particular purpose of this seminar to examine the critical links between communications, command, control, and intelligence, let me advance my reasons for resisting a larger infusion of classified information and judgment into the public discourse.

1. The security of sources and methods must be inviolate. It is essential to recognize that what to laymen may seem to be information which in no way reveals sources or methods can to an intelligence professional be dangerously revealing.

2. The perception of the intelligence community as a source of apolitical objective information and findings must not be sacrificed for an assumed immediate gain in public understanding or support. We must recognize that substantial segments of the public do not entirely believe this to be the case at present. This makes it all the more vital that no change occur that increases that public disbelief or cynicism.

3. The credibility of intelligence content is one of its most important attributes. Painstaking efforts have been made during recent years to rebuild an effective intelligence capability and restore public confidence in its work. That effort is very far from complete.

4. The intelligence community is not and should not be part of the public debate. The more serious and least considered effect of any weakening of this principle is the deleterious effect it would have on the analysts and others among the staffs of the intelligence community who not only highly prize their objectivity but are frequently exhorted to improve the quality of their analysis and estimates.

5. Intelligence must not be trivialized if it is to retain its credibility. Secrets are the intelligence community's "crown jewels." Their value must not be impaired by enlarging the supply. There is a Gresham's Law in intelligence as in all other valuable and limited properties.

6. The need for wider understanding remains. There is an urgent need, if our foreign policies are to succeed, for public and congressional support of those policies. It is clear that there will be occasions and subjects in which no persuasive presentation of vital foreign policies can be made without resort to declassified intelligence material. But the painful fact remains

that other than a limited and carefully considered use of such sanitized evidence risks a kickback injurious to the intelligence community. The obstacles that exist and have the effect of eroding understanding and support of certain of our foreign policies remain. And for some of our foreign policies, the absence of public support is often quite warranted.

7. This national syndrome of detachment and disbelief, which so seriously impedes our efforts to strengthen our national security, must be the object of continuing corrective steps. If these are to be effective, the nature of the problem must be accurately understood if the remedies, difficult at best, are in fact to have a useful relationship to the problem. An unwise and inappropriate use of intelligence may not have just a tangential relationship to the problem; it may, in fact, further complicate it. In this connection, one intelligence fact must be emphasized. In sanitizing intelligence information to protect sources and methods, the sanitizers will, in most instances, be compelled to remove the very core of what makes the particular information persuasive. Much of what would be made available would still have to be taken on faith.

8. The anatomy of ignorance, misunderstanding, and disbelief must be understood in greater depth. The obstacles—and they are very real—are, I suggest, a sum total of the following factors:

a. The collapse of what for a period of time was a bipartisan consensus on foreign policy.

b. The increasing partisan use and politicization of foreign policy issues in the Congress.

c. The certainty that these pressures will be increased and made more shrill during the months of the national election campaign.

d. Probably most fundamental, this same problem has bedeviled Presidents of the United States during the last fifty years in virtually every instance in which US military participation overseas existed or was suggested. It's w rth recalling that only Pearl Harbor ended the long debate about US intervention in World War II. And this was in spite of the historic contribution to bipartisan support by Senator Arthur Vandenberg prior to December 1941.

e. Understanding and support of our foreign policy is so difficult to attain that a concluding element must be added—the lingering effects of Watergate and the misperceived and exaggerated role of the intelligence community during those events, the details of which were belabored by two congressional investigation committees in the House and Senate.

. . . I said that condensation of complex or copious material runs a high risk of loss of information, loss of vital information—that's high risk. It's not inevitable. You and I know the kinds of materials that provide the briefings the President receives. They are prepared with great care, but of necessity,

they are very limited by time and space. You and I have a sense of the volume of material from which it's drawn. There are any one of several stages at which the information can be distorted, not for reasons of intention and certainly not for theater. Here I'm not talking about the theatrical impulse. The interjection of human judgments multiplies the chances of vital information loss and that of course increases the chance that the outcome may be deficient.

[OETTINGER] OK, but I would like to leave with the class this unsolvable dilemma of the balances to be struck. The alternative is drowning in unassimilated data and the key problem is where to strike that balance. Anybody who believes that there is some kind of easy fix is either a knave or a fool. It's an incredibly difficult balance to strike between the risks, as Leo points out, of those multiple stages of condensation and the equally horrendous *prima facie* possibility nf drowning in all the stuff that's available at any instant in time about any subject. (38–39, 47)

15. **JAMES W. STANSBERRY**, "Cost-Effective Rearmament" (1984, pp. 49–61) — *former Commander, Air Force Electronic Systems Division*

The Soviets have a jammer that they used in the desert war, and it got to the point where Israeli pilots couldn't talk to their own tower because the Soviet jammers were doing such a good joh. By the way, the designation of the jammer—I think this is hilarious—is classified. For some reason, we figured out and don't want the Soviets to know the designation of their own equipment. How about that for bureaucracy?

... In our own intelligence community—and by that I mean not just the Air Force, but also Army, Navy, DIA, the guys who like to pretend nobody knows they're in Washington—I think we have gone so far in protecting the information that we limit its usefulness to the operational forces.

[STUDENT] What do you mean by that?

[STANSBERRY] Let's say the intelligence guys have got a great sensor, and they collect all this data and say what do we do with it? Well, let's take it and put it in our own little vault, and nobody goes into the vault except the intelligence guy and he's got to have a badge and clearance and all that. And now we're going to massage the information and process it and display it in

different ways to each other, and then someday we'll even go give it to a guy who has to fight on the ground, maybe, and tell him there's the enemy. We've worked very hard on gathering information, but we haven't worked very hard on the problem of making the information available to those who need it. That becomes a particularly difficult problem with respect to divulging the information to our allies. If you don't work that problem, here's what happens. Let's say the balloon goes up and there's going to be some kind of a ground war in Europe, and now the intelligence guys quickly say, hey, it's time to go show the shooters what we've got. And the shooters say wait a minute, I never saw anything like that before. Who are you, anyway? Why should I believe this information? I'm a busy guy, there's a tank coming through. Now that is an institutional problem, one that we're at work on. It's a difficult problem, and it goes back to that protection of information syndrome.

[OETTINGER] It's the green door problem that we've mentioned in some of the past seminar proceedings. And it's the compartmentation problem that Admiral Inman mentions. The interesting thing is that the higher up you go in the professional ranks, the more agreement you find with what General Stansberry has said. Inman is quite eloquent on the notion that if you do your intelligence job properly, there's no reason you shouldn't make it available to the folks in whose name it's being gathered. It's kind of a middle level bureaucratic thing, the worry that if you give it away you've got no special reason for existing anymore ...

[STANSBERRY] And the fear I would have is that we manage to protect that source and that information totally from our friends, but our enemies may have had it for a long time. (54, 58–59)

16. **ROBERT A. ROSENBERG**, "Strategic Defense: A Challenge for C³I" (1984, pp. 63–86)

Vice Commander-in-Chief, North American Aerospace Defense Command and Assistant Vice Commander, US Air Force Space Command

How do we get warning to the National Command Authority in that short time and how does it all add up to deterrence? Well, if the Soviets believe we have a credible warning system—they will be persuaded that there is no such thing as a surprise attack, and that 8 to 15 minutes is, in fact, enough time for the President to make a retaliatory decision.

I'm going to show you the systems we use to do that, but I'll start by saying that we do it 500 times a year. Every time there is a missile or space launch anywhere in the world, be it one of our own, Soviet, French or whoever, **NORAD** makes an assessment as to whether North America is under attack. It sounds silly to say that we do it even for our own launches, but, you see, the missile warning system doesn't know that that's a space shuttle taking off from Cape Kennedy. There are **Yankee submarines** sitting off the coast, and it just might be a missile coming up out of the water from a Soviet submarine.

NORAD—North American Aerospace Defense Command

Yankee submarine—class of Soviet submarines capable of carrying nuclear missiles

The point is, we don't just do paper exercises, we actually use these systems on an average of 500 times a year.

... We use that catalog of 5200 space objects to keep very precise track of where our critical national security assets are flying in space. When we see a Soviet anti-satellite (ASAT) launched, our computers calculate whether or not it is going to intercept one of our satellites. The booster the Soviets use to launch their ASAT is also used to launch several different kinds of satellites. So when it first lifts off the pad, and we see it on our satellite early warning system, we can't say that's an ASAT, because we don't know yet. They launch four different kinds of satellites off that same SL-11 booster. When we identify it as an ASAT, we provide advisory notices to certain critical US satellite owner/operators who can take action to defend themselves. (77, 81)

17. **LINCOLN FAURER**, "The Role of Intelligence Within C³I" (1985, pp. 17–32)

former Director, NSA and Chief, Central Security Service

So, what is the intelligence mission for the NSA? The Secretary of Defense is directed to serve the President as our government's executive agent for three missions: the provision of signals intelligence, the provision of communications security, and the provision of computer security across our government structure. Those are in addition to the hat he wears as the Secretary of Defense. As the Director of NSA, I am charged to manage that executive

agency responsibility for him. The NSA is responsible for collecting, processing, and disseminating signals intelligence (SIGINT) and the information attendant to that.

... While I am attempting principally to obtain SIGINT for others, I also am trying to protect our own signals, our communications, from exploitation by the other side. A reasonable extrapolation of this, which occurred within the last several months, was the assignment of a similar responsibility for computer security.

Underlying virtually all I will say, and essential for your understanding, is SIGINT fragility. Success in gathering signals intelligence requires an advantage over the other side. The other side must not know exactly how we gather intelligence or the extent to which we are able to exploit it. Stories that have come out about the World War II Enigma machines and the exploitation of Japanese communications illustrate this. Our success had to be a carefully protected secret in both instances to have survived the war and to have left us with that advantage over both enemies. Any disclosure or hints of capability could have provoked relatively easy changes by the other side, which would have denied us an enormous advantage.

The world has not changed that much since World War II, and our present advantages must be protected. They can be destroyed very easily by media references to intelligence successes. I regret that we see these as often as we do. That we listen is not secret. Anyone can imagine that "to listen" is our mission. What is important is that our successes be protected. I have made a point of asking senior people in the news media, managing editors and higher, to spend a few hours with us at the agency and to allow me to sensitize them to the problem of SIGINT fragility. Often I encounter a belief on their part that the United States is so capable that we must be able to divine what any target country is saying, doing, and transmitting. The media uses that image of our omnipotence as an excuse for being able to talk freely about success. But that image is ridiculous. We can't possibly do everything.

... Earlier, I mentioned the capabilities of the Services in the context of SIGINT consolidation. Each Service has cryptologic elements: In the Army, Navy, Air Force, and to a far lesser extent in the Marine Corps, there is a command for which the principal responsibility is cryptologic intelligence. In the Army's case, it's an even broader definition than that, but it includes cryptologic intelligence. In addition to having cryptologic elements, each Service has organic assets, or specific cryptologic collection capabilities—actually, collection, processing, and analysis capabilities. While the

technical tasking arrangements are good, the division of effort is imperfect. There is still room for improvement in administrating the collection and processing, in analyzing, and in disseminating the intelligence.

... The national intelligence apparatus is designed to gather intelligence for all of the government. It may have an application to the Commerce Department, the State Department, or the Defense Department. That is what I refer to as national, and that is the bulk of our program. As we gather intelligence under that national hat, it may have some application to the conduct of battle.

Over the last five to ten years there has been a dramatic increase in the applicability of nationally-derived intelligence to tactical commanders. That's because there's been an enormous time compression between the instant of collection and product usability. It used to be weeks, weeks gradually became days, and now it is seconds, minutes, and hours between the instant of obtaining intelligence and a usable product. Time compression alone has made national intelligence usable in a fast-moving, tactical situation.

I'm concentrating on SIGINT because that's my job. I acknowledge that there are other intelligence disciplines which also are considerably valuable in moving data to the tactical commander, which come into the C³I equation, and which must be handled when solving problems associated with moving data. There is imagery (IMINT), there is human-derived intelligence (HUMINT), and each has advantages as well as limitations. HUMINT has a problem in timeliness. It's often difficult to move that human-acquired intelligence quickly back through the structure and out to a tactical commander. Imagery does not have a timeliness problem, but it has a volume problem. What is moved makes a great deal of difference in one's communications load. What is important is that the data be combined, and that we recognize the absolute necessity of interaction among all intelligence derived from the various disciplines. That is the crux of the C³I problem.

How does all the derived intelligence flow together so that all is complementary, and then how is that combined answer moved to the appropriate decision maker? That process is being improved through applied automation and enhanced communication. The integration of automation and communication into tactical intelligence systems will ensure timely and meaningful exchange of the data. And I heartily endorse that occurrence. The issue becomes *where*, because it becomes a problem if extremely large amounts of data are generated that can saturate the decision maker. We're talking about all the SIGINT in a battlefield situation and the imagery that might pertain to

it or the human source of intelligence coming from the reconnaissance element.

Colonel Beckwith, in writing about his experience in *Delta Force* (his book recounting the Iranian hostage crisis), makes much of the saturation problem. I don't think his is a perfect example, because it mostly discusses the saturation occurring prior to going in on the operation, but Beckwith addresses the problem of assembling all the pertinent intelligence, then having to sift through it to create a necessary picture.

Col. Charlie A. Beckwith, USA (Ret.) and Donald Knox, Delta Force (New York: Harcourt, Brace, Jovanovich, 1983)

The **Long Commission Report** is an example from a slightly different direction. When they looked at the disaster of blown-up Marine barracks in Beirut, they strongly recommended that there be a fusion center to tailor and focus all source intelligence in support of military command. They argued that, stretched across the intelligence community, there had been quite a bit of potentially pertinent information prior to that terrorist attack, but it hadn't come together because there hadn't been a forced fusion of all pertinent intelligence.

Long Commission Report—Department of Defense, Commission on Beirut International Airport Terrorist Act, October 23, 1983, Admiral Robert L. Long, USN (Ret.), Chairman, Report of December 20, 1983.

What is this fusion we're talking about? There are a lot of definitions of fusion. Simply stated, it's the integration of multiple sources of intelligence. The real issue is not wasting time arguing about what fusion is, because it can mean different things to different people. The real issue is where the fusion should take place, and that, in my opinion, is the far more difficult question.

There are a number of automated fusion systems being developed or designed. Industry has a dozen or more potential systems that will digest intelligence information and present easy-to-use displays for commanders' decisions. Many voices in the Services are asking industry to provide them with specific attacks on fusion. The various attempts at automated fusion systems are designed to provide battle information, or to censor data from multiple sources and combine that data. They're trying to provide near real-time enemy ground situation, display it, and make target nominations that a commander may choose to pursue. They're trying to aid in assessing the enemy's situation and capabilities, and to

assist a commander in using his organic sensors and jammers so he can manage them against that changing enemy target. And, these systems attempt to give him the insight to coordinate with higher echelons those sensors he needs assistance from away from the battle.

Let me talk for a moment about SIGINT support to the military commander. A conflict exists between the desire of that commander to control his own assets, and maximum SIGINT support. Every commander will tell you he feels far more confident going into battle with control over both what will fight and what will support him. On the other hand, he currently does not have, and is unlikely to acquire (because of cost limitations) the intelligence wherewithal to fight that battle alone. The assets just can't be made available.

[STUDENT] Excuse me. Are there any of these fusion systems in the field now?

[FAURER] Yes, we have a system in Europe called LOCE (Limited Operational Capability, Europe). It is a prototype system, an evolution of a system called BETA (Battlefield Exploitation and Target Acquisition System) that first saw the light of day in the late '70s. There are two systems somewhere between prototype and initial operating capability status called ASAS (All Source Analysis System) and ENSCE (Enemy Situation Correlation Element), which are Army and Air Force systems, respectively. So, yes, there are systems in existence. In addition, there are a number of usable systems that various contractors suggest be purchased.

[STUDENT] Is there interoperability among the systems—the Services' systems? Is that necessary?

[FAURER] Interoperability isn't as necessary among fusion devices. What is necessary is the assurance that intelligence can be entered into the fusion system easily and promptly. I'll touch on that in a moment, but all the intelligence one would like to handle within that fusion process doesn't lend itself equally to digital handling and digital display. Technical parametric data is very easily handled; it's quantitative and can go into that display without much trouble, if one is dealing with radars and so forth. But if human-analyzed information is to be handled, it's much more difficult to enter and judge properly.

It's also difficult to enter data that raises the security level. There can be all kinds of problems with accessibility, working with the allies, and so on. If

those fusion devices are to function in areas where not everyone is cleared for compartmented intelligence, then there is a problem inserting compartmented intelligence into the fusion system. Leaving it out does the fusion process great harm, but putting it in causes that SIGINT fragility problem.

[STUDENT] In the European theater, how important is NATO to interoperability and compatibility?

[FAURER] It's terribly important. We haven't solved the C³I-related problems that I'm talking about with respect to our own forces. When you compound the problems by trying to solve them so that we remain interoperable with allies, you have a solution that lies well ahead of us.

[STUDENT] Are these fusion devices basically a computer with an associated network?

[FAURER] Yes.

[STUDENT] I'm not quite sure I understand the location of the fusion. It seems to me that before the fusion devices came about, who should get what information was clearly established. How does the technology change that organization?

[FAURER] If there were no fusion devices, the basic problem of where the fusion should take place would still exist. Don't mix the issue of hardware with the philosophic issue of where the digestion, correlation, and coordination should take place. It is the latter problem that is the crux of the issue.

[STUDENT] So, it's not really a new problem.

[FAURER] It is not a new problem, but it is accentuated by automation in the fusion process because it places a very disciplined demand on communications to move volumes of data. Before, all of the right intelligence may or may not have reached the right decision node, even though the problem of where the decision nodes were and to what intelligence they were entitled had been considered. Once carefully structured automation devices are available, there's a clearly defined tug on the intelligence system demanding that there be a communications flow to move data to certain nodal points. There is a clear trade-off between letting all the intelligence be assembled at one

place, well out of theater where processing assets are optimally employed, and letting intelligence be processed out in front. If all intelligence is to flow from wherever it's collected, and it all returns from the theater, is processed and analyzed, and is sent back out in tailored bullets to the levels of command that have bespoken a certain need, there can be a dynamic dialogue. One can tailor answers to needs. That is one measure of how to do it, and it will have a certain communications demand.

The communications demand of moving everything collected back to a central processing and analysis capability, and then sending data back in tailored form to the multiple users, must be measured. Conversely, doing everything forward could be optimized. The various collection capabilities could channel their immediate take into the theater to be processed, analyzed, and turned around there for the decision maker. If that's the method, there's obviously going to be a big tail of support people, computers, and capability forward, but communications will only need to cover a relatively short distance.

As I say, which is the best answer is not intuitive. I lean toward the centralization, intuitively, but I am not a proponent of either if one excludes the other. There should be more attention to accepting the sacrifice of the commander who wishes to control everything. But if one follows that route, one had better carefully measure the communications requirements to make sure that they are affordable.

... My use of the term "finished intelligence," of course, was designed to try to calm your concerns about an excessive delay at fusion centers—be they automated in their assistance, or the fusion accomplished by people. An example in the case of hostilities is this: You have the same worry that a front-line commander has, not just about the forces in front of him, but about the type of reinforcement actions that may be happening in the second echelon. He has the capability to call upon a system to do something for him concerning those second echelons that will pertain directly to the battle in front of him, if he has some knowledge of it.

Now, there are certain things that simply must take place as forces move up. You need not wait until there is a bridge down and troops are pouring across it to suspect strongly that there is a river crossing intended, and the distances are such that those forces will pertain to the battle in 18 hours. As those kinds of early indicators come in, one would like to see them seized upon: a potential river crossing identified, the correct tasking information sent out, and an air strike laid on that could strike four hours later at the height of

their movement. With this example, I'm suggesting that fusion is essential if you're to bring together the bits and pieces that will permit action to result. A commander need not worry that the collating of bits and pieces is occurring somewhere behind him. They need to be provided to him directly so he can decide whether or not he cares about that river crossing. He has got other problems: He may want to call for air support, which may not be the first thing to do, or he may want to send an enveloping tank column out. I don't want to intrude on his decision. I want to provide him with the intelligence as rapidly as I can; I do not want him to sit there with an intelligence staff and sort through a saturation of intelligence that will force him to arrive at his own conclusions. I believe one can tailor the intelligence provided to meet the demands a commander has expressed.

... What are some of the problems with the system? Well, I alluded to the fact that when computers work outside special channels, the information that can be input is influenced. One way or another, you have to face up to that problem. If that computer remains outside, there must be a method to feed the computer the sanitized information. And, with sanitization, which may be essential, there is at least some delay imparted into the introduction of that intelligence to the computer system.

I said that narrative descriptions reduced to quantified data often lose their essence. Intelligence that has been produced to describe something is difficult to quantify and put in so that it will balance properly against the more mechanistic and technical data going in. At least at this time, machines don't make associations well. That's something that still lies in the future when we become more proficient at artificial intelligence.

Moreover, weighting is absolutely essential to analysis. All pieces of intelligence simply do not have the same value. We'd like fusion assistance—that use of automation—to make it more likely to find the right answer. So, we must be capable of facing that weighting problem. It leaves a problem of how to introduce information into that device in such a manner that weighting is not ignored, and that everything doesn't come out weighted the same.

It's difficult to verify information once it's entered into the computer. Some control over the ability to manipulate is lost, and it's difficult to maintain a data base and perform quality control at the same time. This is particularly true in fast-breaking situations—crises or war fighting. One can move data quickly, but maintaining a consistent data base and running quality control may be more than one can handle.

What are some of the ways to improve this? Well, the process can be reversed, and can be selective in collection and processing so that the input is constrained by some responsible analytical decision process. It doesn't have to be performed by humans, but it has to be an achievable, responsible analytic process. One can tailor the reporting at the collection end for substance, format, and timeliness. That also can be done, to some extent, with computers as opposed to people. With properly programmed software, different characteristics of an event may be converted to a set of common features and values if one can properly forecast what sort of intelligence is to be assimilated. However that is done—and I hope it's some solace to you—analysts are still essential to the process. There's no question about that. Analysts have to assess the significance of an event; they've got to update the battlefield picture because they're dealing with both red and blue data, and irrelevant data must be discarded. And the information has to be weighted. All of those things can be done to some extent by machines, but not sufficiently, and not with an adequate degrees of perfection.

I told you that there were two concepts of how to manage that information and make it useful. You may have direct delivery from the source in SIGINT channels, where the tactical commander correlates the data and produces his own intelligence. That puts a pretty good-size tail there, allowing him to do that. Or, you can have an all-source intelligence center that tailors the intelligence to different user categories.

There are advantages to both the direct delivery and the intermediate nodes. I emphasize intermediate nodes because one must not think only of choosing between the proliferation of decision nodal points attendant to each tactical commander on the one hand, and one central processing pie-in-the-sky on the other. There certainly may be some redundancy, but the nodal points should remain back out of theater or be responsible for segments of the theater. That's still something different from having them with each tactical decision level. Those intermediate nodes, or that sort of centralized processing, surely provide more economy of resources. One is better able to monitor the overall success of the system, and one is better able to know the disposition of enemy and friendly forces. I don't think either complete centralization or complete redundancy is the sole answer. I believe there is a middle ground.

... Unfortunately all three of us, private industry, the tactical commander, and the NSA, bring a particular bias to the debate. I first contend we all must sit down and work very hard together, but I concede that each of us has a significant bias. Private industry is obviously after a profit. It wants to sell something marketable and attractive, that sounds like it will do

absolutely everything. The operational user or the tactical commander has an insatiable appetite for information. The tactical commander would provide a list of what is needed to conduct battle. This list would become so long, it would not be possible to provide a commander with that amount of intelligence. It's very difficult to get back to talking about essentials.

We at NSA have a security bias. We're more interested in protecting—or we appear in many instances to be more interested in protecting—the security of our intelligence than we are in providing intelligence. That probably is an excessive allegation, but it certainly appears that way. We simply recognize those biases and recognize the need for all of us to talk, particularly to industry. We're trying to be as aggressive in marketing our concepts as we can justify. I have the total NSA responsibility to interact with the military customer, to be the bridge between those military customers and the rest of the agency, and to be the catalyst within the agency for provoking problem-solving ideas.

... You can't exercise without giving away something. We work very hard at studying Soviet exercises. They work very hard at studying our exercises. We constantly ask ourselves, "Are they going to fight the way they exercise, or are we being deceived?"

They undoubtedly will ask themselves the same question. But the bottom line is, you can't go out and perform on Sunday if you haven't practiced all week. You can toss in a few little wrinkles, but you really must have practiced what you're going to fight, and so you give away a little, but that's necessary.... Unfortunately, our exercises are not that sophisticated. To my knowledge, we have not spent much time trying to forecast capability attrition in a sophisticated way, or imposed upon ourselves the most likely attrition that will occur in wartime. We happened upon a certain amount of realism by our very inability to operate simultaneously in peacetime and wartime.

So when we exercise, we quickly clog our communications and make it difficult to move data. We find ourselves artificially constrained from having all the information we're trying to pass, so that in a somewhat obscure fashion, we can say we've imposed some realism on ourselves, but not intentionally. We have not thought this constrained situation through and imposed it in a methodic way. That is something yet to be done, and the need for far more realistic exercising than we now do requires a carefully orchestrated capability attrition. You're right in suggesting that there will be a dramatic difference between that intelligence available to us in real war

from that available to us in peacetime, but it isn't all in one direction, I would hasten to add.

... A very often voiced criticism of the CIA, for example, and by spillover sometimes the DCI, who is both head of the CIA and head of the intelligence community, is that the CIA is overly policy-attentive. Allegedly, the CIA tends to produce national intelligence designed to complement the policy makers' desires. Over the years when I have operated in the national scene that has occasionally been a justified criticism, not as often as it is made, but occasionally. It is not a valid criticism over the past four years, despite its having been made often about Mr. Casey and the current CIA.

DCI—Director of Central Intelligence

You see, even the most well-intentioned of the intelligence community, as they prepare estimates or advise the policy maker, must have an eye on the policy maker's interests. That is, not what conclusions he ought to reach, but in what he ought to be interested, or in what he is interested. As an estimate is put together, it is essential that certain aspects not be overlooked in regard to a problem that the policy maker clearly needs to confront. In doing that, one occasionally provides the policy maker with exactly the kind of information he wants, because he's made up his mind in advance about what he wants the answer to be. And just as often that does not happen. When it does, the screams go up about playing into the hands of policy makers. I simply have not seen it happen. I believe the community has operated during the last four years with considerable integrity.

Pertinent to this question is the role that the DCI plays. You will find advocates of a DCI who is isolated from the administration; you will find those who would say, "Let's have a professional agency, an employee as the head of the agency, and let's not bring in a political appointee each time the administration changes."

That would probably guarantee you maximum objectivity on the part of the DCI, but it would give you a DCI who might not have the ear of the President and the administration, and, therefore, would be disadvantaged in helping the policy makers because he wouldn't be a part of that policy in the first place. I think the best of all worlds is to have a political appointee, if that's how you would refer to a Mr. Casey, who does have the ear of the President and who is thoroughly aware of the administration's deliberations and policy development, yet who also has the intellectual integrity to stay aloof from pandering and oversees a community that he demands put together

intelligence pertinent to the issues at hand without trying to color it. I don't know how many people like that there are around.

... I could wax eloquent or attempt to be eloquent for an hour or two on the subject of leaks, which I consider abhorrent. I listened to a very edifying TV clip a year and a half or so ago, using a corporate broadcasting service that staged a forum. Typical of these forums, a moderator was named, people were invited in from both sides of the issue, and a discussion ensued—a very effective means to discuss an issue. I watched one that discussed intelligence and leaks, or classified information and leaks. It had prominent newsmen like Dan Rather and others arguing the media side, and it had a few government officials present and past—James Schlesinger and others—on the government side.

Over the course of that discussion, there were some terribly pointed questions asked, and a couple remained rather clearly in my mind. One was that the media has almost unanimously suggested that it is government's burden to protect classified information, and it is media's obligation to the public to obtain it by any means possible. That includes specific statements by some of those media people sitting there on camera, saying that if they were in the Secretary of Defense's office for a legitimate purpose and saw an opportunity to take a top secret document off his desk, they would take it and use it. I have trouble understanding that. Dan Rather himself said, that if provided with clearly classified information—stamped classified—and if it pertained to a story he felt needed telling, he would use it. He would feel uninhibited about using it. I don't understand that. (17–18, 19, 20–22, 23, 24–26, 27, 28–30)

18. **RICHARD G. STILWELL,** "Structure and Mechanisms for Command and Control" (1985, pp. 33–65)

Chairman, DoD Security Review Commission

I think it was fine to put the Marines **in there** to begin with, to assist in the evacuation of the PLO. When it was a question of redeploying for the new type of mission they had, I think that one should have questioned whether it was the right contingent to put in there.

in there—Beirut, Lebanon

For example, a Marine battalion landing team, or even a regimental landing team, does not have the structured intelligence mechanisms that the Army has to handle all the functions of intelligence, such as intelligence preparation of the battlefield, the counterintelligence responsibilities, the estimates function, and the collection management. They weren't there. That's my view of the mistake. Actually, by the time we decided how to re-rig that intelligence structure, we were ready to pull out. So, as far as I'm concerned the less we say about Lebanon and the whole thing—the terrible loss of precious lives—the better.

As to procedures—we still have more to do in the armed Services. We're doing quite a bit, of course, with terrorism rife as it is. And we also need to work on the basic ABCs of passive protection against contingent terrorist attack, which involves not only physical protection, but also the interface with the local authorities. And I might add that that was another deficiency, in my view, shared by the entire intelligence community: The interface with the Lebanese intelligence community, as well as with some of the other nations in the area, was poor. That's an area in which our people on the ground are not all that expert.

... Now, what is the function of intelligence? The basic function of intelligence is to support; to provide the requisite support for timely, sound decisions of all sorts, both in and out of conflict. And from a purely military standpoint, it's to ensure the flow of facts, analysis, and estimates to optimize the effectiveness of our armed forces....

All of those national and foreign intelligence programs support the Executive Branch throughout, and they support the President in all three of his hats. Their functions are manifold. Much of the work—the collection, analytical, processing, and dissemination efforts of our national intelligence community—is targeted on indications and warning. They provide a tremendous amount of support in the fields of science and technology, so that we may have the best possible information on what the enemy is doing in the development of new systems, which is important, of course, for countermeasures and everything else. They also put an enormous amount of effort into the verification area, which has application to arms control or arms reduction support. They're paying increasing attention to narcotics, terrorism, international finance and economics.

One of the things the national programs don't have primary responsibility for is the development of intelligence that has unique application to war fighting. And, therefore, you have outside the national foreign intelligence program, the capabilities of the several Services, which we call "tactical intelligence and related activities." These represent the military assets that

have unique application to the military instrument itself, for example, the reconnaissance aircraft, the **SR–71s, TR–1s,** and the **RECCE birds** of the tactical Air Force, the **P–3s** of the Navy; the major intelligence centers of the unified and specified commands; the tactical units of the Army, principally, and to a limited degree of the Navy and the Air Force; certain satellites under our Defense Reconnaissance Support Program that are uniquely designed for warning purposes—and the list goes on. It's quite a lot. Now, that's a separate program, and those are unique military assets whose priority of collection is determined solely by the Department of Defense. The priorities of collection for the national systems are determined by the Director of Central Intelligence, although they can be changed on Secretary of Defense recommendations.

SR–71s, TR–1s, RECCE birds, P–3s—reconnaissance aircraft

... You always do a little better in times of affluence, as opposed to belt tightening. But the requirements continue to soar out of proportion to resources. We are getting to the point where there has to be a very rigorous establishment of priorities throughout the intelligence community, throughout the Executive Branch, making a clear distinction between what's nice to have and what's essential. And I think the only way you're going to get it is simply to stop delivering reports to a lot of the customers, and then wait for a month to see if they even notice they're not getting any. And you probably will get very little reaction.

There has to be a better interface between the policy maker and the intelligence community, which again underscores a point with regard to this prioritization: we have improved our collection capability somewhat out of proportion to our ability to analyze, process, and disseminate finished products. We collect with big buckets, as General Faurer may have indicated to you.

... We have done all too little planning on this matter of transition from peace to war in the intelligence community, particularly with respect to those national systems. The national systems do not belong to the theater commander; they may be allocated to him, depending upon what the priorities are back here. He cannot count on that totally. But regardless, there needs to be much more attention given to planning today for the new utilization of those national systems in support of **CINC PAC, EUCOM, or the others**. It is very hard, a tough business that we have done very little about up to this stage of the game. (50–51, 62–63)

CINC PAC, EUCOM, or the others—refers to the commanders-in-chief of the Pacific Command, the European Command, and other operational commands—most assigned specific geographic areas of responsibility

19. **ROBERT T. HERRES**, "A CINC's View of Defense Organization" (1985, pp. 125–45)

Commander-in-Chief, US Space Command, Aerospace Defense Command, North American Aerospace Defense Command, and Commander, Air Force Space Command

Intelligence information and tasking come together to help the commander decide what he's going to do. Sometimes what you're going to do with the forces gets so complicated that you don't have time to analyze very quickly and describe what you want to do and build plans and get them in the field. So good military people plan ahead.

All planning is a sort of what-if game. Let's pretend that the Soviets attack Iran. They come across the border and take over Iran. What are we going to do about that? What do you think the President will want us to do? That's part of the what-if scenario. Suppose the President says, "Don't let them take Teheran. Hold the Soviets outside of Teheran. Prevent that from happening." So we pretend that's something we might get tasked to do. And you think through all the things associated with being able to carry out that tasking. How many forces do you have to put there? You do a lot of what-if on the intelligence side: What do you think the Soviets are really going to do? How many tanks are there going to be? How many airplanes are there going to be? And so forth. You put all that together, and you put those plans on the shelf. While you're doing that you build up expertise in your plans shop about what it takes to get your thoughts organized in advance, so that when the Soviets come across the border it's not chaos, running around trying to figure out who you're going to send where to do what.

Plans, even though you may never use them, help organize your thinking in advance. They develop options that you may not formalize in terms of structured operations plans, but that you have available for the commander to consider when contingencies occur.

Then you get tasking and decide what you're going to tell the forces. The forces engage the enemy. Intelligence reports on what the enemy does and how they react before and after engagement. You have tactical sensors that do that, and of course the other intelligence sources. You have field reports that come from the troops out there involved in the engagement process. Fighter pilots come back and say, "I just shot down five airplanes," and we say, "We don't believe that. You probably only shot down three, but we'll mark you up for four and split the difference." Then you try to track how many airplanes they have left. You need to know what the enemy's force status is. You also need to know what your own force status is. That's very

important and often overlooked as a key part of the command and control process. Sometimes it's harder than collecting intelligence on the enemy. It's frustrating when you can't find out the conditions of your own forces. There are a lot of reasons for that which I won't go into.

But force status reporting is a dynamic process, because if you engage, you take losses, you redispose your forces, and that creates change all the time. And of course intelligence is dynamic. Mission and tasking is originally static, but as things go on you start running out of operations plans. So you send a guy down the hall to the planners and say, "Hey, take a look at this option, see what it would take to implement that and come back to me with a quick plan—I need it in two hours." This goes on at the Pentagon all the time, believe me. Even for things that you never hear about, things that never happened but that somebody thinks might occur. So plans and options are a dynamic process, too, because there's a little inner circle here: What if I want to do X? I don't know a better way to describe that piece of the process. This is what command and control is all about, these dynamic little circles spinning around. (140)

20. **ROBERT HILTON**, "Roles of the Joint Chiefs of Staff in Crisis Management" (1985, pp. 147–78)

Consultant, specializing in national and international security affairs and political risk analysis; former Vice Director for Operations, Joint Chiefs of Staff

Another thing I would like to mention is that some of our best sources in learning of an event are in the news media. CNN has become one of our prime sources; it's monitored in the Command Center all the time. There are also tickers in the National Military Command Center for Reuters, UPI, and AP. Many times a first indication of something is from a reporter on the spot, a stringer. For example, the first pictures we had of the barracks in Beirut being blown up were from CNN. We first learned of Sadat's assassination from a stringer for CBS, I believe, who was on the scene and got to a telephone and got a call back before they could even get it back through the embassy circuits. I guess he had a handful of change in his pocket and used the local telephone, wasn't worried about security or things like that.

... There's a system called something like "worldwide indicators." There are about 800 indicators that the intelligence community monitors, including things like the movement of refugees, the requisitioning of food, the use of trucks for something other than the harvest—traditionally the military trucks

go out and help with the harvest. That was one of the indications that contributed to the ex post facto analysis of the invasion of Czechoslovakia. The grain harvest suffered greatly in that period because they diverted the trucks. They did it under the screen of an exercise; that was the way it was assessed. These indicators are briefed, I think, every day, to the Chairman of the JCS, and the DCI makes his reports to the President.

I remember when the North Koreans in December of 1981 went into the biggest exercise they'd ever done at that time. In 1982 they had an even bigger one. We were watching those indicators and assessing whether they were, in fact, just exercising. In 1981 we didn't pay as much attention to it as we did in 1982, because in 1982 General Vessey was the Chairman. General Vessey had been the UN Commander in Korea. He was much more sensitive to Korea than we were, and the point he made, I remember, was that even though it was correct to assess those as indicators for an exercise, each one was also a preparation for war. Now in these cases the war didn't happen. But if they're going to go to wa they're going to go through all of those steps. Some day it may not be an exercise, and if you keep watching it as an exercise, you may be caught.

So you always have to be looking at the possibility that you are describing a process of going to war. And you look for other indications that it's an exercise: Have they requisitioned the civilian economy? That was what DIA used as a deciding factor in the Korean thing—they requisitioned a lot of things, but not everything. The DIA thought that if they were really going to war they would not just have taken 20%, they would have taken 80% of civilian transportation.

[STUDENT] Do we have any corporate body with enough experience to keep up with that on a year-to-year or crisis-to-crisis basis?

[HILTON] Computers are our corporate body, I think. There is also a national warning officer who is dual-hatted between CIA and DIA. One of last year's speakers, Dave McManis, was the National Intelligence Officer for Warning.

At one time it was Linc Faurer, when he was a two-star and double-hatted as a Deputy Director of CIA. The warning center was put in the Pentagon and it's still there. So, you have this warning technology, but it's only as good as the people who are on watch. (167, 169–70)

21. **LIONEL OLMER, ESQ.**, "Intelligence and the American Business Community" (1986, pp. 59-71)

Member, Paul, Weiss, Rifkind, Wharton & Garrison, an international law firm; former Under Secretary for International Trade, Department of Commerce

While that initial period, from 1961, had truly been marked by a sense of confidence in the intelligence system, the later 1960s were different. In 1968 I went to Vietnam and was put in charge of a reconnaissance organization that was providing what we called "early warning" to Navy and Air Force pilots flying over Hanoi.

We did a number of different things, one of which was to alert them to surface-to-air missiles (SAMs) launched in their direction. It was a very complicated affair, technically speaking, in terms of both the equipment and the training that were required. We felt we worked very hard at it, and we were occasionally quite proud of what we were able to achieve. I can remember being utterly deflated when I talked to a fighter pilot who said, "Oh yeah, I turn that box off. I don't listen to what you say." I said, "Why?" He said, "What good is it to know from you that a missile has been launched in our direction? What the hell do you think is happening over Hanoi when we fly there? Missiles are everywhere!" We were just a distraction.

It reminds me of the joke about the lost hot air balloonists. They come down over a university campus and yell down to some fellow walking along the path, "Where are we?" He looks up and he looks down, and he scratches his beard and he says, "You're in a balloon." One of them gets very angry and says, "You're an economist!" His friend says, "How did you know that?" "Because he's exactly correct and of no help whatsoever!" We were not economists, but we were exactly correct and of no help whatsoever.

That was an instructive part of my career as an intelligence officer, to discover that it isn't enough merely to be accurate and sometimes it's not even enough to be timely. There are several other characteristics that have to go along with accuracy and timeliness, the most important of which is relevance. In this increasingly complicated world in which we live, it's harder and harder to be relevant, because in order to be relevant you really have to know what it's like to be a fighter pilot in the midst of a combat situation. An intelligence specialist providing support to a group of foreign policy negotiators or economic negotiators has got to be more than just an academic. You've really got to be part of the process. There's no other alternative.

... When I came back into government in 1981 with the Reagan Administration, I believed that the government could do more to support its economic interests. That is, the intelligence community could, in an open way, support certain business activities of American companies by seeing to the production of a greater volume of unclassified information and to the analysis, not of a particular competitive endeavor on a micro level, but of significant trends, such as Japan's drive to technological preeminence, or the less developed country (LDC) debt situation, or the analysis of why the ASEAN nations consistently produced higher rates of productivity growth than the Western European nations and the United States.

ASEAN—Association of Southeast Asian Nations

I did encourage this kind of effort in the intelligence system, and because of my lineage, I think that I was given a more receptive audience than would ordinarily have been the case. I have to say that the economic analysis produced by the intelligence community, at least in the period of 1982 to 1985, was simply superb. I read almost all of it, and I could not fault it, except for its volume, which was awesome. But when you start to rely on staff to tell you what's most important to know, it means you'd better have some good people who understand what is relevant to you, not only to your interests, but to the things on which you are required to vote in, say, a policy development gathering of other senior officials.

My areas of interest were divided into three parts. One was the support to trade policy. The second was in the nature of gaining a better understanding of the competitiveness of foreign manufacturers and producers of technology, relative to US competence in equivalent or similar areas. The third area, which we haven't talked about at all, is the subject of technology transfer.

On the one hand, we must learn more about the competence of the Soviets in areas where we're attempting to control the transfer of technology, because it's not relevant to restrain the flow of technology to areas in which the Soviets have already got a demonstrable capability—and it's harmful to companies that might otherwise create jobs and pay more taxes through legitimate trade with the USSR. On the other hand, we need to know better where the gaps are in our system of export controls. We need to understand more about the areas in which diversion of technology does occur so as to be more able to stop it.... We also have to try to build a consensus in the community by pointing to areas where the Soviets have developed a strong capacity simply because of their access to Western sources of products and technology. (60, 62)

22. **HAROLD DANIELS**, "The Role of the National Security Agency in Command, Control, and Communications" (1986, pp. 73–102)

Deputy Director for Information Security, NSA; former Assistant Deputy Director for Communications Security

Now, what's the threat? The major threat is that anything that goes out into the ether can be intercepted if you have the proper equipment to do it. There was a time when people thought that was a major job. It turns out that if you go down to the local Radio Shack and you're really interested in collecting someone else's data, you can build yourself a system to do that for less than $2,000. If you look at the roof of the Soviet Embassy on Sixteenth Street in Washington, you'll see that those antennae certainly aren't all for TV....

It's not only the Soviets who pose this threat; it's anyone who wants to invest in, or who already has, this capacity. The threat is a real thing, and it's not understood well by all. I can't get into too much detail. Let me just say that it's not a hard job for someone to find out about what you're doing when you're communicating out through the ether. It's not well understood by industry, and only, I would say, in the last five or six years has it really been understood within government—and even if understood, in some cases, not acted upon.

There are three important components to any decision involving information security: value, vulnerability, and threat. When one considers protecting information, one first looks at the value of it, then what the vulnerability is, and then what the threat is. If you have any combination of those parts, you'll probably want to do something to protect that information while it traverses the telephone system or whatever takes it out into the ether. The value is your own determination. You have to decide that. If you value your information, chances are, someone else will value it. What vulnerabilities do you have? Well, if you're on a piece of wire between this room and that room over there, and you have some sort of protection around the enclave, chances are the vulnerability may be very small. If you're talking to the West Coast, that information leaves this building, goes perhaps on a cable to some microwave point, goes across the country partly by microwave, partly over satellite, and then goes back down again. Then that information, while it's out there on microwave or on the satellite, is vulnerable.

If you decide you have highly valuable information that you've determined to be somewhat vulnerable, then you have to say all right, now what's the

real threat? If you're going to invest in protecting this, you've got to have some idea that somebody else has (a) the desire, and (b) the capability to take advantage of your vulnerabilities. That decision involves information that you, as an individual, cannot always have. It's my job, along with some of our other intelligence agencies, to help the government make that decision as to what that threat is. Under **NSDD 145** we've also been asked to advise the private sector. We do that in such a way that we're able to explain to them what possible threats there might be to their particular communications.

NSDD—National Security Decision Directive; NSDD 145 was signed by President Reagan in September 1984.

Take the computer world, for example. There is a perfectly legal way that an adversary, let's take the Soviets for example, can get into a US data base containing a lot of technology simply by subscribing to a public system. For example, they can come in through Vienna into Dialog, which is a service offered by Lockheed, and get into the National Technical Information Service (NTIS) where the US files on a number of projects and information and weapons systems are held. This is a clearly legal method for someone to get into that. Anyone is capable of buying into that system and getting that information. (74–75)

23. **MARK LOWENTHAL**, "The Quest for 'Good' Intelligence" (1986, pp. 103–20)

Acting Director, Office of Strategic Forces Analysis, Bureau of Intelligence and Research, Department of State

The rank order for the Executive, I would say, is policy support, management issues, and then propriety. The most important is policy support, and by that I mean, there's a positive question that the consumers ask, and there's a negative question. The positive question is, "Where did intelligence help? We got out of this really well. Did intelligence help, or did we just sort of do this brilliantly on our own, again?" Then there's the question you don't want to be asked, and that is, "Where did intelligence fail?"

One of the great overused terms in American intelligence is "failure." I have argued in an article for the Air Force Academy that we haven't had that many genuine intelligence failures. We've had screwups, and bad calls, and most of these so-called "failures" usually happen for policy reasons rather than intelligence reasons.

Pearl Harbor is an intelligence failure. It's very hard to argue your way around that. When you lose half your fleet at the outset of the war something really has gone wrong. The Middle East War in 1973 was a gross intelligence failure for the Israelis. The other cases that I've looked at, though—South Korea in 1950, Cyprus, Portugal, Tet, Iran—all probably were less failures of intelligence than areas where policy had sort nf prejudiced the outcome. But when something goes wrong there is a certain amount of head hunting, and the issue is where intelligence failed.

The management issues are the second rank of issues for the Executive. These are the average simple things like how much money, and how many people, and are they getting their work in on time. That's the typical sort of thing that you worry about in management.

The propriety question is less of a concern in the Executive Branch. There are people whose job it is to make sure that operations are proper: that we're not doping people with LSD anymore without their knowledge, and that we're not attempting to assassinate heads of state.

In Congress, I would say the order for those same three things is probably propriety, policy support, and management. Congress worries least about management issues. Their main preoccupation is with propriety because, quite frankly, that's how they got into this business. . . .

Their second issue is policy support. But here they're basically coming at it in a more negative respect, because the view of intelligence in Congress is largely part of the necessarily adversarial oversight function. The two branches aren't supposed to get along. It's built into the Constitution. . . . When you're in Congress your first rank order problem is the Executive Branch. They're your main day-to-day problem. Then there's everybody else in the world, or every other domestic lobby.

Both branches are policy makers, but there's a large difference between the two. The Executive has a policy to sell, a policy to support. If there was a new treaty overnight, a new arms treaty, an Administration spokesman wouldn't come before the Foreign Relations Committee and say, "Hey, it was late. I was tired. I had jet lag. It's not a great treaty. It's a good treaty." He would say that treaty was truth, justice, freedom, and national security. Congress would then say, "Could we get another point of view on this? I mean, you negotiated the treaty, what else are you going to tell us?" So, the Executive's always selling policy.

Congress is reviewing policy; it doesn't really have a policy of its own to sell. It may have alternative policies to propose, but largely as thwarts to the Executive policy. In the Executive, policy makers hope that intelligence is going to come in and say that this is the thing to do, and this supports what you're going to do. In Congress the response is, "I'll bet they cooked that up to sell something." There's a tremendous dose of skepticism about the intelligence they're getting; they assume that it's self-serving at a certain level.

If you are a producer you find this very annoying. You like to believe every morning that you're being honest and intellectually objective, which I think I probably am most days! There are times when the numbers haven't come out the way we wanted them or things like that. In the Library of Congress, they sort of legislate or mandate objectivity in the Congressional Research Service (CRS). There's a very rigorous reviewing procedure. In the Bureau of Intelligence and Research (INR) and the CIA you have to do it more on your own. My analysts and I like to assume that we're being objective. But some in Congress assume that intelligence is being shaped to support policy. When you produce the odd number of guerrillas that you've captured in the boonies in Honduras, Congress says, "Oh, come on, guys. Where did you recruit these? This is the 'Central Casting Guerrilla Department.'" Congress approaches lots of issues like this. You collect AK–47s and they want to know, "Well, didn't you just buy those from Egypt?" Congress naturally assumes that intelligence is just part of the salesmanship.

The two branches diverge functionally on the issue of production. Only the Executive is the producer of intelligence. The Congress isn't. It hasn't the facility. It just doesn't exist in that area.

The conclusion out of all this is that the two branches approach the intelligence issue very differently; their relationship to intelligence is different; their need for intelligence is different; their knowledge of intelligence is different; and their concerns over intelligence will differ. Beyond this agreement that what we want is good intelligence, the value of intelligence lies in the eyes of the beholder. That's also true in the Executive, at a different level, where you get this argument about what constitutes good intelligence. I'll come back to that.

Having sort of laid that as a groundwork, how do you assess intelligence? I have two different paradigms; one is the ideal, and one is the bureaucratic. The ideal was derived from the late **Sherman Kent** who was both an academician, a scholar, and a producer of

Sherman Kent—former Director, Office of National Estimates, CIA, author Strategic Intelligence for American World Policy, 1949.

intelligence; he said, "If an intelligence analyst had three wishes in life, they would be to know everything, to be listened to and believed, and to influence policy for the good."

The second model is your more customary bureaucratic model, which in intelligence, I think, boils down into accuracy, timeliness, and cost effectiveness. Let's go through the first model—the ideal—knowing everything.

In the Executive, I think most policy makers know that the ideal is not reasonable for either the producers or the consumers. No one can know everything, nor can every organization know everything. In fact, to save time, they basically only want to be told what they need to know. I have a lot of technicians who work for me. They do, in a technical sense, what regional analysts do. You want to tell the boss everything. You don't want just to tell him why there's a trade war with Japan; you want to go back to the Meiji Restoration so he can sort of imbue himself in Nipponese culture. I often tell my analysts you can just explain the miracles without telling the lives of all the saints. This is very difficult for analysts. It's very hard to discipline yourself to do that.

Policy makers realize that there's a great amount of competition for their time. Therefore, they will leave it to the analyst basically to tell them what they need to know, and perhaps toss in a couple of the odd tidbits that will also be interesting or fun. The mistake, I think, that consumers make in the Executive is that they probably believe that everything else is being covered and waiting to be tapped. If Botswana were to go up tomorrow night, most likely we could indeed suddenly find someone who has been covering Botswana for 40 years and tell him, "This is your moment in the sun. Let's do Botswana!" But every so often that's just not true. It wasn't true in Iran. It wasn't true in Portugal in 1974. You do find that you have to make management choices. For example, we drew a lot of people out of the Soviet area in the CIA during Vietnam, and really consumed a lot of time. It was an ongoing concern. It was a war. Then when Vietnam wound down, we found that we had lots of other regions that no longer were being covered where we were tremendously weak. In the Middle East, I think we've always been very weak; we've relied for about two decades on the British. Well, the British pulled out and it's been very hard to replace them. This assumption of "Don't worry about it—if it happens someone will cover it," prevails among producers and consumers in the Executive, and it's not always true.

With Congress, the likelihood of knowing everything is probably an even more limited phenomenon. Congress just can't take in intelligence in the

same doses or in the same frequency that the Executive is taking it in. There's much more divergent competition for the time and attention of a Congressman, I think, than there is for the average Assistant Secretary of whatever. The Congressman and the Senator have day-to-day preoccupations that really eat up a lot of time. That's part of the system. It means that they can't devote the same sort of time and attention to knowing everything.

As for the second of Kent's wishes—to be listened to and to be believed—in the Executive, getting listened to means competing with all your fellow analysts. For example, in I&R there are 11 production offices in addition to mine. Each day we're all producing papers that we feel are what the Secretary really wants to read tonight. There are some 18 bureaus in the building where the same competition is going on. That's some 300 levels of competition to write that one memo that the Secretary's going to read in the evening, or those two memos, or those three memos. This is very difficult. It's the job of certain people, the Assistant Secretaries at one level, and then the Executive Secretary at another, to filter and make choices of what the Secretary really needs to read, and what do you do with the other papers. Do you send them to Assistant Secretaries? Under Secretaries? Publish them? My office does a biweekly magazine. Some memos that haven't gone to the Secretary will appear as lead stories. If we're smart, we'll make the decision that it's interesting but it's a little too technical for the Secretary. So there's one problem with being listened to in the Executive.

The other problem is what you do when intelligence runs counter to policy, and it happens. Policy makers can always reject intelligence out of hand. A classic case is President Johnson in 1965. His Director of Central Intelligence (DCI), John McCone told him, "You want to win in Vietnam? You've got to put in 300,000 troops; you've got to go to war; you've got to destroy the North; and then you'll win." Well, that was not what Johnson wanted to hear in 1965 on a continuing basis from his DCI. He wanted to hear, "Don't worry, the Viet Cong is small, and if you throw in a couple of advisors and a couple of ground forces on the bases, everything will be fine."

At first Johnson cut McCone out, and then he just sacked him. From Johnson's point of view that made good sense, because he wasn't hearing what he wanted to be told. In retrospect, obviously, it was a mistake. McCone was right and Johnson was wrong. But there's nothing you can do about the policy maker ignoring you. You can't grab him by the lapels and speak to him the way Americans speak to foreigners, which is to say it louder and slower. That doesn't work. You can't do that. So that's the other problem.

Congress, again, is more selective. They have two major motives in listening to intelligence. What you're telling them had better be directly related to a key policy issue. You cannot often tell them, "Well, this is interesting and a sleeper and you ought to worry about this." There are very few members of Congress who have the luxury of saying, "That could be a problem in 15 years, so I'm really going to worry about that." First of all, there's a chance they won't be there in 15 years. Their sense of the immediate future, I would say, is anywhere from two to six years, maybe eight years. You'd better be able to relate what you're telling them directly to something that's going on right then in their lives in terms of legislation or important public events. They want to make sure the sleeper problem is covered because they don't want to be surprised by it, but it's very hard to devote any time, attention, or resources to it—which is also true in the Executive, but more of a problem, I think, in the Congress.

Congress also has an even greater ability than the Executive to reject intelligence they don't like, because they're first passing it through the filter of asking, "Is this intelligence self-serving?" When they get intelligence they don't like, some may be inclined to say the answer is yes.

On influencing policy for the good: In the Executive, the first question you have to ask yourself is, "What is the good? Is it in the policy makers' outcome or is it in the intelligence analysts' outcome?" Intelligence analysts, like everyone else in the world, develop a certain clientism. They know their subject really well. All these other people at the top are transient phenomena. The Secretary of State will be gone in four to five years, and the Assistant Secretary will probably be gone in two years. Nixon was right about that; the permanent bureaucracy really thinks that way. They can outlast anybody; they're not going anywhere. They're very happy in their jobs. Therefore, you do end up with the policy makers, the guys who are currently responsible—which I would say is from the Deputy Assistant Secretary level on up, where political appointments tend to begin, although at the deputy level you'd get a mix of some career and some political—usually holding two different views of what is the good in policy....

The second thing is, how do you know what the good is? I think most intelligence producers have enough sense at least to question whether or not they're right, even if they hold private views, and think, "I know better than they how to fix it."

In Congress, well, what Congress wants is good, and what the Executive wants is bad if they disagree. That's a very simple phenomenon. That's why they're two separate branches of government. Again Congressmen are back

in the situation of tending to accept that which fulfills their policy goals and rejecting that which fulfills the Executive policy goals that they oppose.

So that's the ideal model, according to Kent's three wishes, for both branches. The ideal might be nice. I don't think any intelligence producer assumes it can ever be achieved. I'm not sure the ideal in the end would lead to any meeting of the minds on what is good intelligence.

Let's go to the bureaucratic paradigm of accuracy, timeliness, and cost effectiveness. Obviously, accuracy is essential. You want to avoid the surprise phenomenon. You want to have accurate intelligence. Most of my customers tend to appreciate the necessary limits of what we can achieve in terms of accurate predictions. In politics it's very hard predicting on the average afternoon what Khaddafi's going to do. It's probably not something you want to do for long if you're keeping a batting average. My analysts cover a lot of technical matters with the Soviet weapons systems, worrying about range and throw weight and number of RVs (reentry vehicles) and size of the blast and so on. Technical intelligence can be more precise than political intelligence, so we can get what we feel is pretty close and pretty accurate, although even here there will be a wide divergence of opinion on some issues.

I think there is some tolerance among the producers for the finite limits of intelligence. I'm not sure that the consumers in the Executive always appreciate the need for "maybes" and "perhapses" and "it appears thats,"—sort of what someone called "writing in the suhjunctive." Most intelligence analysts are smart enough, or have been burnt enough times, that they don't want to state flatly, "At 9:05 tomorrow morning they're going to do X." Unless you've got the world's best intelligence that tells you that, most producers aren't going to write that. They write, "Well, it appears they're going to do X, then again they may do Y, or Z, or possibly go back to A." Sometimes it's necessary and sometimes it's simply **CYA**. I don't think, though, when it's necessary, that consumers always understand why. So we have a divergence between the producer and the consumer where, if the consumer does not appreciate the need for this hedged analysis and cries "failure" whenever he gets hurnt, then you end up with very timorous producers.

CYA—cover your ass

Also, there's a learning curve. During the period when we had sick old men running the Soviet Union, we really got very complacent in predicting Soviet policy issues. I never understood people who say, "Well, we want

them to have a dynamic leader." Why? I don't! I think we were in much better shape when they had sick old men. Gorbachev is a whole new ball game. We're coming up to speed on him. You get burnt enough times, you become a little more cautious.

In Congress, among the three issues of accuracy, timeliness, and cost effectiveness, accuracy is probably the key factor in terms of assessing intelligence. But it's probably applied with less understanding for the limits, for the 'maybe,' for the need to hedge the analysis; therefore, the notion of accuracy is applied more rigorously and perhaps less reasonably, I think. The average member of Congress is not exposed to a lot of what we call intelligence. They don't *all* see the *National Intelligence Daily* (NID) every day. They certainly don't see the *President's Daily Briefing* (PDB), or the Secretary's morning summary. The members of the Intelligence Committee will see the NID, but you're talking about 17 on one side and 15 on the other. So not even 10 percent of the whole is being exposed to intelligence on anything close to a regular basis. The Foreign Relations Committee members will get to see more, but even then it's selective. You don't bring up cartloads of stuff on the People's Republic of China (PRC) nuclear test program. You give them the stuff that you think they'll need.

... The issue of timeliness is obviously essential for the Executive. There's no sense telling anyone on December 8th that you're going to have your fleet attacked when it's been attacked on December 7th. There's a wonderful story about Talleyrand having dinner in Paris in July of 1821 when news came that Napoleon had died at St. Helena in May. His companion said, "What an event!" Talleyrand said, "No, Madame, now it is only news." You don't want to be in a situation of producing intelligence that's only news, and especially old news. The thing that you have to convince consumers of is the time it takes to produce good intelligence, or to work up a good briefing, unless it's something that's already been done. If there is a need for a briefing in an area where our intelligence is less firm, it takes a certain amount of time before we can whip that presentation into shape. That's one problem.

Then there's the problem of, again, getting the attention of the consumers. Pinning down an Assistant Secretary is difficult. Similarly, when the ambassadors for the arms control talks are in Washington, they get briefed regularly. But there are some days when the 9 o'clock briefing goes to 10 and some days the 10 o'clock briefing gets postponed to tomorrow. That's just a fact of life. If it's something really urgent you can always get to the consumer. There are ways that you can wave flags and push the right buttons. But you also don't want to cry wolf too often.

... [M]oving on to the timeliness issue in the other branch, the Congress, I think that unless you've been in the intelligence production process or unless you've had a lot of exposure to it as an overseer, there's less appreciation for how hard it is to coordinate policy, and how hard it is to coordinate intelligence in the Executive Branch. Lots of people have axes to grind. Every intelligence producer has his own benighted view of the world. The intelligence production process is no better than the clearance process, which is abysmal. You've got to get everyone to sign on, and you end up with lots of lowest common denominator paragraphs, or you end up with papers that read like first-year German translations of Nietzsche, where all the verbs are in the wrong places and all the adjectives are in the wrong places, and yet it's in English. (NIEs, stylistically, are some of the most unrewarding reading you can do in your entire given life). So timeliness is important to the Congress; as I said, though, I think they're less aware of the problems involved.

Cost is the next way of measuring the value of intelligence. For the Executive, it's not so much a question of cost effectiveness as it is of resource allocation. You're always playing with fewer resources than you need, and you've got this intense competition within the budget as a whole, and within the intelligence budget, for resources. I never have understood the arguments that the CIA hypes the Soviet threat to improve the defense budget. It doesn't make any sense to me bureaucratically. The CIA has no institutional interest in a higher defense budget except for collection systems. If more money's going to defense, less money's going to CIA, and that's a fact of life.

... To go back to the question of competition in the budget; there are two levels of competition in the intelligence budget. One is between and among technical collectors, and these things are really expensive. Most of the intelligence budget goes to two commodities, collectors and computers. The bottom of the NSA installation, the subbasements, is reportedly one very large computer. It's very expensive stuff.

Then you get the competition between the technical collectors and the analysts. What if you collect all the information and no one can analyze it? And we do collect more information than you can easily go through in a given day. Every morning when my analysts take "the take," they've got a stack of cables a foot high. A lot of it is absolutely inconsequential stuff. Then there are the interesting items. Winnowing that out in the half an hour that I give my staff in the morning, before I go to my director's meeting, is a very hard task. The trouble is that it's always easier to get money for collectors. This is true in both the Executive and Congress. You can always sell

gadgets to Congress and the Executive. We have a lot of belief in technology in this country. People are always easier to cut, or easier not to buy. It seems less threatening. Obviously you reach a certain point where that's not true; if you don't have enough analysts, and you have too much incoming information, then you have a big problem.

Congress, I think, suffers in that they have a less reliable means for creating a standard. They have more difficulty judging where to make these choices within the intelligence budget. What's interesting is, we've had instances where the Congress has questioned the choices the intelligence community made and tried to increase the money. For example, in one of the annual reports of the House Intelligence Committee, I think it was around 1983, possibly 1984, the committee said that OMB's (Office of Management and Budget) decisions on which collectors to buy were wholly divorced from any intelligence requirements. They were just a bunch of green eyeshade people going over the intelligence budget and making bad resource choices, just deciding this is expensive, this is cheap, buy this. Congress actually reversed a lot of OMB decisions. So if you've got a group of informed members and an informed staff, congressional review can actually work to the benefit of the intelligence community. But I think, on a day-to-day basis, it's probably harder for them to do. Congress nevertheless really has been very interested in resource management.

Having said all that, let me add one other feature to the bureaucratic paradigm, and that's quality control. Who performs quality control? In the Executive, I would say the consumers are largely performing quality control, but usually through negative feedback. Usually you only hear from your customers when they feel they haven't been served well. You don't get a lot of complimentary notes going back and forth, although it happens. There's also the President's Foreign Intelligence Advisory Board, PFIAB, which serves as an overseer. The trouble with PFIAB is that it's somewhat irregular and unsystematic. It's a group of high-powered people who've had interesting jobs in industry, government, or the private sector, who then get paid per diem to sit on this board and assess the effectiveness or the utility of intelligence. But it's done somewhat irregularly, making it difficult in terms of quality control for the Executive.

In Congress the quality control is being performed by the intelligence committees. The first issue the committees have to face is what their standards are for good intelligence. As I've said, I think that their sense of what constitutes good intelligence is different from that of the Executive. Yet, in many respects, I think the committees are much better situated to do postmortems, at least intellectually, if not in terms of access. Postmortem is

not something that we do an awful lot of in the Executive Branch, for a reason that I'll come back to. We've had the committees now for 10 years, and they've been very helpful in trying to promote good intelligence. For example, the House Intelligence Committee's Report on Iran was a very useful study, not only of why we didn't know that the Shah was on his last legs, but also the entire intelligence production process. They went through the NIE process and said that it is not a very sound intellectual procedure, and that the NIEs are not worth fighting for because they're not influencing policy makers.

Let me draw some conclusions then and throw the rest of the time over into discussion disagreement, or whatever. I think both branches tend to judge intelligence largely through a negative reference, especially during so-called failures. I think it's easier to assess when things have apparently gone wrong than to figure out when things are going right. When you're getting intelligence right it's just basically not news. It's when you've left people in the lurch or surprised them that they come and tell you. Every so often you will hear that your product was very useful.

Between the branches, intelligence is treated politically. In part I would say, "Why not?" Everything else is. Why should intelligence be exempt?

And in part it's the nature of the system we have, especially in foreign policy. We have a wonderful myth in this country that foreign policy is bipartisan. Politics stops at the water's edge. In reality we have always had partisan debates over foreign policy, and I would argue that with 2.5 exceptions, every political campaign since 1948 has had a major foreign policy input. The trouble is that intelligence has now become part of this debate, for a number of reasons. One was the effect of the investigations which left people with the attitude that these agencies can do some really nasty or inept things if they're not controlled; and they did, in fact, do some things that were illegal as assessed by both branches.

The second, I think, was that we politicized the position of the DCI. Until 15 DCIs did not change with every administration. There was usually an overlap of about a year, because this was seen as a nonpolitical position. Eventually a President will want his own DCI, but they [were] not changed automatically. We're now in a situation where a new President appoints a new DCI....

Finally, the partisanship issue in foreign policy has obviously affected the way in which intelligence is treated between the branches. As I mentioned earlier, the Executive tends to resist making assessments and postmortems. There are two reasons.

First, the consumers resist it because they don't have the time. They've solved whatever that crisis is or they've stopped worrying about whatever that crisis is, and they're on to the next one. "Let's just keep moving." It's a very now-oriented environment. The consumers don't have time for it.

Second, the producers don't want report cards. Adults are no different from children in that respect; they don't want to be assessed on a continuing basis. There's always that element of chance that you didn't get the grade you wanted or felt you deserved. So the producers tend to resist it.

Congress, I think, is more interested in doing postmortems, and I think that they're better suited to it. Congress has actually at times said, "Hey, that was good." One example that stands out in my mind is during the Mariel boat lift. Les Aspin (D-WI), who at that time was Chairman of the Oversight Subcommittee, issued a report saying, "Intelligence was really good on this. They predicted that Castro would do this, and they predicted the numbers of people we would have to deal with, and the policy makers had every reason to be prepared."

Congress has tried to foster more postmortems, and I think they've been fairly successful. The Iran one stands out in my mind as a good one. There was one on Grenada that was less successful. I think Congress is well suited to do this as long as they're not simply grinding their axes because they also disagree with the Administration's policy.

But I think Congress can do this, and has done it well, which leads us to the question that I started with: What constitutes good intelligence? The more I thought about this, the more I felt like Justice Potter Stewart in his comment about pornography: "I can't define it, but I know it when I see it." I think to a certain extent that's what good intelligence is. I sat through a briefing recently that didn't tell me anything I hadn't really known before, except it was a bit more concrete. But I walked out saying that was really a good analytical job. They pulled together lots of disparate pieces. They made a couple of leaps in the dark of their own that worked. They pulled together all sorts of interesting knowledge. That was really good intelligence! But I can't prescribe how to do it. If I could prescribe how to do it, I wouldn't make my own mistakes.

There are two paradoxes in intelligence. One is that intelligence often serves best on the areas that are little known. For example, the PDRY, South Yemen. Little regular attention is paid to South Yemen. But, when a civil war erupted, we were able to get people up to speed very fast. Also, there you're dealing with consumers who know that they don't know anything

about South Yemen. There's no reason to pay tremendous amounts of policy-making time to South Yemen until it blows up and the Yemeni Cabinet starts shooting each other.

In contrast, when it comes to US-Soviet relations, everyone assumes he knows what's going on. We've been living with this problem for 41 years, and everyone assumes, "Oh, yeah, I can do US-Soviet analysis. You're not telling me anything I didn't know before." This becomes heightened during a crisis. I think the major thing that goes wrong during a crisis between the producers and the consumers is that the consumers tend to act as their own analysts. Their attitude is, "Give me raw cable traffic. I can make up my own mind." Terrible, terrible thing to do, and it happens.

So there is this paradox that we probably do better on the rare, odd event than on the general long-running event. In ongoing situations, you also tend to get trapped by your own analysis after a while. There is a certain timidity about predicting major changes in assessments because this raises the question, "Well if you were wrong then, why are you right now?" Then when the assessment gets changed again, people keep asking, "When are you going to give me a number that was the right number?" The answer is, "Never." It's very hard to explain that to a consumer.

The other paradox is that Congress may in many respects be in a better position than the Executive to make improvements in intelligence, because they're not involved on a day-to-day basis; they can sort of step away and take the long view. The question is, will the Executive really allow that? My sense is, on a regular basis, probably not. It's going to take some major gaffe. The CIA is a direct result of Pearl Harbor. That's why we have the CIA. It's not because some genius came up with the idea in 1947. It's because we lost a fleet once. That's the kind of event it takes to make a massive improvement in intelligence. But as I've said, Congress may be better suited to do it.

... One of the things that has always bothered me as an analyst, and something that I've tried to avoid doing now as a producer, is focusing on how much money the Soviet Union is putting on defense. I don't think you can calculate it. I'm never sure. Should we be doing dollars to rubles, or rubles to dollars? (I once suggested we find neutral currency; we'll convert everything to Polish zlotys and see if we can come up with a better number.) I'm not sure what it tells you. If I were convinced you could get a good GNP number for the Soviet Union, which you can't, and if I were convinced that you could then translate what percentage of their resources they put into

defense, it might be interesting. The only useful commodity that you come up with in terms of analysis is, well, what have they produced? They've got 1,398 ballistic missiles. That's an interesting number. That's real. Now you get into the issue of how many refires, and how many spares, but numbers won't necessarily tell you that. Not numbers of dollars, or numbers of rubles.

I have always found this to be a very bizarre discussion, yet it always happens. Ted Turner said, "Money is how people keep score." Well, Congress and the Executive both do that with the defense budget of the Soviet Union, or they compare their budget with our budget. We're buying apples and they're buying oranges, or we're buying beefsteak and they're buying potatoes. Yet everyone is saying they're spending different amounts of money. Of course they're spending different amounts of money.

I think one of the big mistakes you can make as an intelligence analyst, and this is apparent even before you become a producer, is mirror imaging—assuming that everyone is making decisions for the same reasons. You make all these wonderfully, facile intellectual comments like, "They're all just people. They're all just like us." Nobody's like us. I don't even know what "just like us" is on the average afternoon, but you get that kind of discussion....

... Being held responsible for keeping surprises down to zero would be unreasonable. A certain number of surprises will get through. It just happens. I think the standard to which we tend to be held, of keeping people informed on a regular basis on things we feel they need to know, is feasible. If they're missing something, they'll let us know. We tend to hear from the consumer when he feels that he's not getting what he needs.

... Analyzing the wisdom of buying more **D-5s** as opposed to **MXs** or **Midgetmen** is just not a function to which I'm entitled. I can analyze Soviet forces all day, and I can lay out the implications for the United States. I can say, for example, if the Soviets are making the following buys in the next 10 years, and I have a pretty good sense that they are, these are the *kinds* of forces the United States would need to hold them at risk. That's not the same as then saying, "Therefore, buy the D-5 and not the MX." That's something that all the intelligence agencies have to keep out of.

D-5s—Navy's Trident missile
MXs—10 warhead replacement for the Minuteman missile
Midgetmen—low-yield, precision follow-on to Minuteman

What happens in defense is that each of the Services has kept its own intelligence staff—a very small one, but a separate one. There you probably are getting more of the recommendations such as, "Well, this is what we think the Russians are going to buy at sea, therefore, we should buy this missile, not that missile, or this surface ship or that surface ship." In the larger sense of the community, we don't do that and we can't do that. . . .

[STUDENT] I want to ask one question about oversight, given your background, particularly the oversight of all kinds of intelligence operations. It seems to be increasingly impossible for the United States to have both Congressional oversight in its present state, chiefly for covert operations, and covert collection activities that remain covert.

[LOWENTHAL] I don't think that's true. I think the action of the oversight mechanism has worked very well. To go back to one of your points about perception, one of the other great myths in American political life is that Congress leaks like a sieve. Ninety percent, 95 percent of all leaks come from the Executive Branch. Of course, leaks are like murder mysteries. The first thing you ask in a murder mystery is, "Cui bono?" Who benefits? Leaks are like that, and most of the time it's someone in the Executive who's benefiting. The record of the Intelligence Committees has been absolutely admirable on this business of keeping operations that were supposed to be secret, secret.

What's interesting is institutionally, if you read the rules of the two committees, there are very severe penalties for leaks, such as getting thrown off the committee, and being censured on the floor, which is something that no member wants to see happen. It's worse than death. (104–08, 109, 110–12, 113, 119, 120)

24. **RICHARD J. LEVINE**, "Electronic Publishing for Business Intelligence" (1986, pp. 121–34)

Editorial Director, Data Base Publishing, Dow Jones & Company

Over the years . . . News/Retrieval has grown into a very broad-based electronic information service, aimed not just at the stockbroker but at the businessperson, regardless of the industry in which he or she is working. It combines news with data, analysis, and transactional capabilities, including brokerage services, electronic mail, and services that allow you to make

airline reservations and actually buy and sell retail goods. It's delivered not only to dedicated terminals, but also to personal computers and communicating terminals over packet-switching networks.

... Eighty-six percent of the middle managers need or have an interest in information about their own company, 64 percent want information about their customers, and 54 percent want information about their competitors. Among top executives, 96 percent were interested in information about their own company, 50 percent about their customers, and 44 percent about their competitors. Those findings are really confirmed in the usage patterns and statistics that we are seeing.

... I recall a conversation several years ago with a space salesman for a business magazine. We had just started to offer a data base that contained earnings estimates on thousands of companies; I frankly thought it was of greatest value to investors. But to my surprise he said, "That thing is just making my life wondrously easier and it's contributing to my salary." I said, "What are you talking about?" He said, "Look, what I'm selling is corporate advertising to companies. I check this data base, and if the stock analysts believe that the earnings are about to soar, I go in and I tell the executives of the company that they're hot right now on the street and they might as well ride that wave. They ought to buy advertising and get out their corporate message in my publication." Likewise, if the Wall Street analysts are turning bearish on the company, he turned that to his advantage too. He'd say, "Look, you're in trouble. These guys are going against you. They think your earnings are going to plummet. You're stock price is going to hell if you don't act now. You need corporate advertising."

... The uses to which this kind of information are being put are many and varied. The same is true of some of the transactional services that I mentioned. Through a gateway arrangement with Dun & Bradstreet's Official Airline Guide (OAG) subsidiary, we provide not only schedules and fare information for hundreds of airlines around the world, but we also enable you to make reservations from your terminal. OAG allows you to rationalize the often anachronistic pricing arrangements within the airline industry, and, as a result, to control travel costs. When you go in and say, "I want Flight 273 on this carrier," it lists the various ways you can make that flight, from the lowest price to the highest price. The variations on that same flight can be enormous. In a disinflationary environment, this capability becomes an important tool for cost control.

... Our research indicates that the questions that the executives ask aren't very precise. As they get passed down the chain they get fuzzier and fuzzier.

The real reason for the search is unclear, and the real interest of the originator of the search is unclear, and as a result, the maximum effectiveness of these systems isn't evident. And they're spending considerable amounts of money to get this information. It is much better where the end user does the retrieval himself or herself.

... [W]e were positioning ourselves as an important source of major national and international news event. That's all happened within the last year or two. I ask myself, "But why, when people are getting live television coverage of that?" I think one reason is simply that television sets are not as accessible in corporate offices as terminals.

There is also a desire, which we want to learn more about through focus group research, to supplement the information that is being distributed on television with something that's not print but goes beyond the ephemeral nature of television.

... You can start to see the future in this article that I brought along. It appeared in the *Boston Globe* on October 16, 1983, when we were a lot smaller than we are today. The headline read, "Shultz Has Fun With Computer," and it was written by Bill Beecher, who's the diplomatic correspondent for the *Globe*. It said: "At the end of the interview, as the reporter was putting away his tape recorder, Secretary of State Shultz asked if the reporter had a personal computer on his desk, 'as I do.'" Turned out each had the same brand. "You know what I do with mine?" Shultz asked. "I subscribe to the *Dow Jones World News Service*. From time to time I scroll over reports from one part of the world or another, and then I phone the appropriate official to ask what he makes of this development or that." Obviously, in many cases he would be asking questions on late-breaking developments they had not even heard of yet. "'It drives them wild!,' he said with impish glee."

... One of the consequences in terms of organizational structure within a corporation is that people who have access to these services and know how to use them can bypass formal channels. The Shultz anecdote is a perfect example. He's not waiting for formal reporting channels. He's bypassing them. You read about this process from time to time in the computer magazines. An article last year on personal computing among the top executives in a number of Fortune 500 companies revealed that they were often reaching down into the bureaucracy with very specific questions. With the use of internal and external data bases, they were

article—Henry Fersko-Weiss, "Personal Computing at the Top," Personal Computing, *March 1985, p. 68*

accessing information that they'd never had before. They were able to exercise much greater firsthand, direct control over operations, in some cases leaping past three or four levels of managers, by going through the data bases themselves and taking their questions straight to the originating manager. In the more traditional process of passing information through the hierarchy, that stuff gets reduced to a page or so. The higher you go in a corporation in a sense, maybe the broader the range of the information you get, but also the shallower the information, because it tends to be filtered as it rises. These systems allow that senior level management to retain tremendous control over access to very detailed information.

... The point in doing it [putting each day's *Journal* into the News/Retrieval computer] is that no one's coming in just to search that day's *Journal*, but they are coming in to search the historical files with the knowledge that the search is encyclopedic as of the moment they make it. It encompasses all known knowledge, or at least all knowledge known to Dow Jones. What we are offering is the protection that the search covers not only the historical information, but also all our information right up to that point. (122, 123, 124–25, 127, 128–29, 133)

25. **JOHN GRIMES**, "Information Technology and Multinational Corporations" (1986, pp. 135–49)

Director, National Security Telecommunications and Director, Defense Programs (C³), NSC

While the government has had to address this issue for many years, and has done things to protect information—particularly critical military information—industry has not yet accepted interception as a threat to corporate planning, other than those companies that are in high technology arenas. Some of the high tech firms have been required by law, or by contract, to protect certain information. Access to computer data bases and systems has become a major issue. Unauthorized access by the Soviets to high technology data bases in the universities, through various associations and exchanges, etc., will probably be the most highly debated information issue over the next five years. Technology can fix the problem, I think, to a point. You can't entirely stop it, we know that; but in the main we can fix it. Yet, when you apply certain security techniques, then you deny other people access to that information, whether for economic or technical reasons. It's going to be a major debate in Congress and in the Executive; General Stilwell is involved with it, and also Congressman Ed Brooks (D-TX, Chairman, Government Operations Committee). It will pose a constitutional question eventually.

[STUDENT] There were two news items in regard to that this week. One is that NSA's offer of endorsement to industry's standardization of cryptographic equipment for the private sector makes it more secure to have industrial communications, but some also say it makes information in society more available to NSA. The other item is that DoD supposedly wants to go into disinformation on weapons or contract information in a big way, putting spurious data into the system so as to confuse potential information gatherers. Actually, those techniques, to deny an enemy information and to overload him with false data, seem to come at the problem from two different ends. Considering the nature of American society, overload might be the more promising of the two, but difficult to carry out, I suppose.

[GRIMES] Well, the government has made no actual claim of disinformation, even though accusations to that effect have been made in the media. I can tell you, from where I sit, that there has been no conscious decision or policy to do that. I can't say the thought doesn't reside in people's minds. Actually, I think we're already engaging in overload because anybody trying to sort out the information we publish has a major task ahead of him. But if somebody wants to spook the system, to get at corporate planning, stock market information, or bank records, they can; you've got to look at the various threats. There are hackers out there who have been put into jail and are back now as consultants to industry and to individuals. Security is a real issue in information systems. All I'm saying, as a closing remark, is that it will he the major debate in government; we can fix most of it with technology, but I'm not sure we want to do that because we might end up denying information to people who do need it. It's a national issue that we have before us, and it won't be resolved in an hour's discussion. (149)

26. **B.R. INMAN**, "Technological Innovation and the Cost of Change" (1986, pp. 151–68)

President and Chief Executive Officer, Microelectronics and Computer Technology Corporation

[W]hat has surprised me more than anything else about the performance of industry as compared to government in this broad area we're discussing—the ability to gather knowledge or intelligence on the outside world and then integrate it into a decision-making process—is how poorly that is done. I had always held the view, from my 31 years of government service, that industry must be far more effective, far more efficient than government. I'm sure that there are many cases where that is true, but I haven't been exposed to a large number of them in the past four years. (152)

27. **GREGORY D. FOSTER**, "The National Defense University's Command and Control Program" (1987, pp. 1–22)

Senior Fellow, Institute of National Strategic Studies, National Defense University (NDU); former Director, NDU Command and Control Research Program

When I was a consultant several years back, I worked on a study for the intelligence community staff. We did an input/output analysis in which we attempted to assess the productivity of the various elements of the intelligence community, relative to established intelligence requirements. We quickly learned that day-to-day intelligence collection and analysis deals with the real world, with real-time things. Annual intelligence requirements—once upon a time called Key Intelligence Questions; they're called something else now—lag well behind the dynamics of the real-world intelligence process. In fact, they have very little impact on actual collection and analysis.... I agree that there is a critical need for intelligence-command feedback. The difficulty is creating an environment in which such feedback works effectively because, typically, at the risk of overgeneralizing, policymakers don't know how to ask the right questions. (3)

28. **ROBERT L. DEGROSS**, "Teaching Intelligence" (1987, pp. 41–59)

Provost, Defense Intelligence College

The demands on an intelligence person are to understand the political system that he works with and the need for information, to collect information, to analyze that information, to get some sort of product which is readable by a decision maker, and then to disseminate that information.... The intelligence cycle is the collection, production, and dissemination of information.

... Military attaches are collectors of military information. They are legal representatives of this country in foreign countries who are there to collect information. This is a recognized diplomatic activity.

[OETTINGER] ... Let's take for granted that for purposes of this discussion we're not dealing with covert operations, but with the analytical information acquisition. Is that what your intention was?

[DEGROSS] In fact, one of the great disagreements within the community—I guess those people who are intelligence professionals—is whether covert action is actually part of intelligence. There are those people who say that covert actions are implementation of policy decisions and, therefore, while they are done sometimes by intelligence agencies, they in fact are not part of the intelligence process.

... [W]e're desperately concemed about the status of languages, primarily Third World. The government cannot and should not maintain enough resources to provide everyone with language capability, and yet we know we're going to need it. We see the reservoir of language capability drying up on the outside, especially during the 1970s and 1980s, because of lack of funding. Language departments are closing.

The Secretary of Defense has expressed active concem about language training for two or three budget years in a row. The President's budget has zeroed out funding for the Department of Education for foreign language and area study centers, and each year the Secretary of Defense sends out a letter saying this is in the national security interest, please restore the funding. That letter makes its way to Congress, and Congress restores the money. To a certain extent it's a game that's being played, nevertheless, the Department of Defense does recognize that language capability is an intelligence-related skill. That's the phrase that's used.

Now, however, that's one level. The other level is: Can we really afford to maintain the language capabilities, develop and maintain them? How much is available in translation? Given the nature of the military, the rotation of assignments, even the foreign area officers have difficulty maintaining language and the fact that many of the foreign area officers were going into positions where in fact they didn't even use the language and they lose it. Maybe Harvard might be one of those assignments.

It is very costly, obviously, to develop and maintain a language. It's something that everyone at the top gives a great deal of lip service to, about the need to have it. Whether it's actually doable and affordable, I'm not sure. One of the more promising things that has come out, though, is that someone using their head figured out that if the military can't maintain a language capability, the reserves can maintain a language capability. There are several language reserve battalions which have been established in the United States, so that if, in a time of emergency, like an emergency in the Philippines, we find out that there are no Tagalog speakers, the reserves are used.

... There is, I think, an obvious recognition and an obvious commitment that an attache who goes to a country has to have the language. If that is an intelligence function then I think that's understood. I think there's a genuine recognition that an analyst who has a language capability for the country he's dealing with is probably a better analyst, because he understands the cultural milieu and is able to read journals and pick up the nuances. Whether that is attainable, maintainable and cost effective in the government today is debatable. Obviously, it's critical for a National Security Agency to have the language capabilities.

Language therefore is very important. It's one [issue] which I and many other people spend a lot of time thinking about, because we're concerned about the future. But intelligence managers, managers of analysts, tend to think about their daily problems, not about their future problems, and they don't want to build, necessarily, a capability that they might need for 5, or 10, or 15 years from now. To tell people that they really ought to have one Swahili speaker is very hard when they know their budget comes for certain types of intelligence. They know that their immediate problems are this and that, and it's very difficult to get them to send someone out for a long-term study of Swahili or some other language.

... The opportunity that faces defense intelligence is the new missions that are coming. The role that defense intelligence is going to play in arms negotiations. When Mr. Gorbachev decides, for example, that he is going to offer to bargain on weapons in Europe, the questions that get asked are: "What are the weapons? How many? What does that mean to us?" That can mean collection. It's an analysis of their capabilities, our capabilities, and then help during negotiations. I think one of the things we see is that intelligence is taking a front line in terms of arms negotiations. That's something that's new. It's not new that we're having arms negotiations, but the direct involvement of intelligence in this process is new. Verification is going to be one of the issues: Who is verifying intelligence?

... Second, I guess the role for defense intelligence that's relatively new is terrorism—combating terrorism. It's very hard because you don't have a defined enemy. You have an enemy but you're not sure who they are. They don't always wear uniforms. When you find out about them, they're probably so far down the line that it's the ones you don't know about, the small groups that have splintered from a larger group, that very often can be menacing. It's a new type of enemy with a new type of threat. We're trying to figure out how to prepare people to deal with counter-terrorism analysis.

The third, which I mentioned earlier, is narcotics. Those three are kind of new challenges to prepare people for. For example, with the counter-narcotics, that is not necessarily a military intelligence function, but military intelligence may provide some sort of supporting mechanism. We certainly are providing some training right now, and that training is something which has been defined as doable by the Department of Defense. The great difficulty, as I see it, is the problem of evidence. Within the narcotics field individuals have to be brought into a court of law and then there is the whole avenue of where you found out your information, and that gets into the whole issue of sources and methods. There are some problems which have not yet been worked out legally, but yet we can provide analytical training which will be very helpful. (42, 43, 46–47, 55, 56)

Appendices

Appendix A

Seminar Speakers

Dr. Archie D. **Barrett** was a member of the professional staff, House Armed Services Committee at the time of his presentations in 1985 and 1987. A retired Air Force officer, he has extensive experience in NATO general defense, nuclear and logistics plans and policies; Air Staff long-range planning, concepts, and doctrine development; and tactical and strategic flight operations. Dr. Barrett's book, *Reappraising Defense Organization*, was published in 1983 by the National Defense University Press.

Dr. Richard S. **Beal** was Special Assistant to the President for National Security Affairs and Senior Director for Crisis Management Systems and Planning at the time of his presentation. Prior to joining the White House staff, he was an Associate Professor of International Relations and Political Science at Brigham Young University. Dr. Beal had extensive research and teaching experience in Southeast Asia, the Far East, and Europe and contributed widely to general, scholarly, and governmental publications. He died in 1984.

Mr. Stuart **Branch** had recently completed his service as Assistant Secretary for Communications in the Department of State at the time of his presentation. In his career with the department, Mr. Branch served as Chief of the Communications Facilities Staff, African Operations Officer, Communications Officer for the American embassies in Saigon and Mexico City, Chief of the Communications Center Division, and Executive Officer for the Office of Communications.

Mr. Leo **Cherne** was Vice Chairman of the President's Foreign Intelligence Advisory Board, Executive Director of the Research Institute of America, and Chairman of the Lawyers Cooperative Publishing Company at the time of his presentation. A recipient of the Presidential Medal of Freedom in 1983, Mr. Cherne has also been awarded the Legion of Honor by France and the Commander's Cross of the Order of Merit by the Federal Republic of Germany.

Mr. William E. **Colby** was Counsel with Reid & Priest at the time of his presentation. Earlier, he served as Director of Central Intelligence under Presidents Nixon and Ford.

Dr. Robert **Conley** was President, Conley & Associates, Inc., a consulting service, at the time of his presentation. He had served previously as Deputy Assistant Secretary for Advanced Technology and Analysis and Acting Assistant Secretary for Electronic Systems and Information Technology, Department of the Treasury. Prior to then, he was the Navy's Chief Scientist for Command and Control Programs, service which followed 18 years in various assignments with the National Security Agency.

Lieutenant General John H. **Cushman,** US Army (Ret.), was a management consultant at the time of his presentation. During his military career, General Cushman served as a commander and staff officer, culminating in major commands in Vietnam and Korea, as well as stateside command of the Army's Combined Arms Center and a tour as Commandant, Command and General Staff College. His book, *Command and Control of Theater Forces: Adequacy*, was published by AFCEA International Press in 1985.

Mr. Harold **Daniels** was Deputy Director for Information Security of the National Security Agency (NSA) at the time of his presentation. He entered cryptologic service in 1954 as a Navy communications technician serving at NSA and joined the NSA staff in 1957. During his career he has held senior management positions in both SIGINT and COMSEC disciplines, including assignments as Director of Civilian Personnel, and Chief, Asia and Pacific Analysis Group.

Dr. Robert L. **DeGross** was Provost of the Defense Intelligence College at the time of his presentation. He has served on the Advisory Board to the Department of Education on International Education and on the DoD University Forum on Languages and Area Studies. He has also held academic appointments in history at the University of Maryland and at Miami University. He has published on the military-academic relationship and on the relationships between education and work. He has traveled and lectured extensively both in the United States and abroad.

Dr. Richard D. **DeLauer** was Under Secretary of Defense for Research and Engineering and, later, President, Orion Group Limited, a consulting firm, at the time of his presentations in 1981, 1982, and 1985. Previously, at TRW Inc., Dr. DeLauer was responsible for System and Energy activities. He was also director of the Ballistic Missile Program Management and

director of the Titan ICBM development program at TRW. Dr. DeLauer is a member of several technical societies and co-author of two books on nuclear rocketry.

Captain Fred R. **Demech,** Jr., a career cryptologist with the US Navy, was assigned to the National War College at the time of his presentation. During his career, he has held such varied positions as Special Assistant and Personal Aide to the Director for Command Support Programs on the staff of the Chief of Naval Operations; Executive Officer of the Naval Security Group Activity in Winter Harbor, Maine; Executive Assistant for two consecutive directors of the National Security Agency; and Deputy Comptroller for the Naval Security Group Command and the Cryptologic Officer Detail at the Naval Military Personnel Command. He also served as Deputy Executive Director and then Executive Director of the President's Foreign Intelligence Advisory Board from 1981 to 1984, and later as Commanding Officer of the US Naval Security Group Activity in Edzell, Scotland.

Lieutenant General Hillman **Dicklnson,** US Army, was Director for Command, Control, and Communications Systems, Joint Chiefs of Staff at the time of his presentation. He saw service as a commander in Vietnam, but the backbone of his career has been technology: nuclear test detection sensors, combat support systems, target acquisition intelligence, and electronic warfare. He was the first commander of the Army's C^3 Research, Development, and Acquisition Command.

Dr. Gerald P. **Dinneen** was Corporate Vice President, Science and Technology for Honeywell, Inc. at the time of his presentation. He was Assistant Secretary of Defense for Communications, Command and Control, and Intelligence during the Carter Administration. His background lies in MIT's influential Lincoln Laboratory, one of whose prime contributions to modern technology was the pioneering Whirlwind computer. Lincoln was also the birthplace of the long-lived SAGE air defense system.

General Richard H. **Ellis,** US Air Force (Ret.), had recently retired from his position as Commander in Chief, Strategic Air Command when he gave his presentation. General Ellis began his career as an aviation cadet in World War II, rising to Deputy Chief of Staff, Far East Air Forces before the war's end. He was Vice Commander in Chief, USAFE and commanded the 6th Allied Tactical Air Force, Allied Air Forces in Southern Europe, the 16th Air Force in Spain, Allied Air Forces Central Europe, and finally USAFE itself. He directed the Joint Strategic Connectivity Staff at Offutt Air Force Base from its founding in summer 1980 until his retirement and directed the Joint Strategic Targeting Planning Staff, also at Offutt.

Lieutenant General Lincoln D. **Faurer**, US Air Force (Ret.), is a former Director of the National Security Agency, and Chief, Central Security Service, Fort Meade, Maryland. General Faurer's extensive military career included service as Deputy Chairman of the NATO Military Committee in Brussels, Belgium and Director, J-2, for the US European Command in Vaihingen, Germany. He has worked several times for the Defense Intelligence Agency, most recently as Vice Director for Production. General Faurer is also the recipient of numerous decorations and awards, including the Distinguished Service Medal, the Defense Superior Service Medal with one oak leaf cluster, and the National Intelligence Medal of Achievement.

Dr. Greg **Foster**, a former Army officer, was a Senior Fellow with the Institute for National Strategic Studies, National Defense University at the time of his presentation. As first director of the university's Command and Control Research Program, he sought, through a variety of research, publishing, and educational initiatives, to focus the attention of the national security community on a reconceptualization of command and control. Dr. Foster previously served as Director of Research and Manager of Washington Operations for the Foreign Policy Research Institute, and before that as Director of the Center for Security and Policy Studies, Science Applications, Inc. He is co-author, with Adam Yarmolinsky, of *Paradoxes of Power: The Military Establishment in the Eighties*; his most recent book, *The Strategic Dimension of Military Manpower*, co-edited with Alan Ned Sabrosky and William J. Taylor, Jr., was published in 1987.

Mr. John **Grimes** was Director of National Security Telecommunications and Director of Defense Programs (C³) for the National Security Council at the time of his presentation. In previous assignments, he served as Deputy Manager of the National Communications System, from 1981 to 1984, and as Assistant Deputy Chief of Staff for Operations and Plans, US Army Communications Command, from 1973 to 1981. Earlier, he was Deputy Director, Communications Engineering Directorate, and Chief of the Command and Control Division of the Test and Evaluation Directorate, US Army Communications-Electronics Engineering Installation Agency.

General Robert T. **Herres**, US Air Force, the first Vice Commander of the Joint Chiefs of Staff, was Commander in Chief of the North American Aerospace Defense Command (CINCNORAD) at the time of his presentations. As CINCNORAD, he also served as first Commander in Chief of the unified US Space Command, Commander in Chief of the Aerospace Defense Command, and Commander of the Air Force Space Command. Prior to that he was Director for Command, Control, and Communications Systems in the Office of the Joint Chiefs of Staff. General Herres has also commanded the

Air Force Communications Command, Eighth Air Force, and served as Chief of the Flight Crew Division with the Manned Orbiting Laboratory Program. He has held numerous other posts in the fields of intelligence, communications, and systems development and acquisition.

Rear Admiral Robert P. **Hilton,** US Navy (Ret.), was President, Hilton Associates, a consulting firm, at the time of his presentation. He has been a consultant to the International Planning and Analysis Center, Inc., the Center for Naval Warfare Studies, the US Naval War College, and the Institute for Defense Analyses. Before his retirement from the Navy, Rear Admiral Hilton served as Vice Director for Operations, Joint Chiefs of Staff, and was responsible for supervision of the National Military Command Center and Special Operations Forces. He also served as Deputy Director, Plans and Policy, Joint Chiefs of Staff, and as Deputy Assistant Chief of Staff, Plans and Policy for SHAPE, Mons, Belgium.

Professor Samuel P. **Huntington** was Director of the Center for International Affairs at Harvard University and Eaton Professor of the Science of Government at the time of his presentation. One of the founders of the quarterly journal *Foreign Policy*, he was its co-editor for seven years. Mr. Huntington served as Coordinator of Security Planning for the National Security Council, the Policy Planning Council of the Department of State, the Office of the Secretary of Defense, the Institute for Defense Analyses, the US Air Force, and the US Navy. He is the author of numerous scholarly articles and coauthor of several books, including *Living With Nuclear Weapons*, published by Harvard University Press in 1983.

Admiral Bobby R. **Inman,** US Navy (Ret.) made three presentations between 1980 and 1986. In 1981, he became the first Naval Intelligence Specialist to attain four-star rank when he was promoted to Admiral coincident with his appointment as Deputy Director of Central Intelligence. From 1977 to 1981, he directed the National Security Agency, following two years as Director of Naval Intelligence. He was appointed President and Chief Executive Officer of Microelectronics and Computer Technology Corporation in 1983. His volunteer activities include serving as a director of The Atlantic Council, the Council on Foreign Relations, and the Rickover Foundation; a trustee of the Brookings Institution and Southwestern University; and a member of the National Academy of Public Administration, The Trilateral Commission, and the Defense Science Board.

Mr. Donald C. **Latham** was Assistant Secretary of Defense, C³I, at the time of his presentation. He also served as Deputy Under Secretary of Defense, C³I, in the Office of the Under Secretary of Defense for Research and

Engineering. Previously, he was Division Vice President, Engineering, at RCA Government Systems Division, where he reviewed and coordinated engineering activities in various tactical, strategic, and space systems for the military, NASA, and other government agencies. Mr. Latham is also the author of two books and numerous technical papers, and a contributor to many DoD engineering studies and proposals.

Mr. Richard **Levine** was Editorial Director, Data Base Publishing, Dow Jones & Company, at the time of his presentation. In that capacity, he was responsible for the editorial output of Dow Jones's Interactive Information Services Division, which produces Dow Jones News/Retrieval, a videotex service, and DowPhone, a audiotex service. Before moving into electronic publishing, Mr. Levine spent more than 14 years with *The Wall Street Journal*, serving as a general assignment reporter, labor editor, military correspondent, and chief economic writer and front-page columnist.

Mr. James R. **Locher, III** was a member of the professional staff and senior staffer for the Subcommittee on Projection Forces and Regional Defense, Senate Committee on Armed Services at the time of his presentation. From 1985 to 1986, he directed the bipartisan staff effort that resulted in the Goldwater-Nichols DoD Reorganization Act of 1986 and was the principal author of the study *Defense Organization: The Need for Change*. Previously, he was the Senior Committee Adviser on International Security Affairs, responsible for force projection programs, including airlift, sealift, amphibious warfare, and rapidly deployable forces. In addition, he has held several positions in the Office of the Assistant Secretary of Defense for Program Analysis and Evaluation and served as Executive Secretary of the White House Working Group on Maritime Policy, Executive Office of the President, an effort that resulted in the Merchant Marine Act of 1970.

Dr. Mark **Lowenthal** was Acting Director of the Office of Strategic Forces Analysis, Bureau of Intelligence and Research, Department of State at the time of his presentation. In that capacity, he was responsible for intelligence and analysis of issues pertaining to nuclear arms and Soviet activities, providing overall intelligence support to US arms control negotiators, and designing new products for use by policy makers. In a previous assignment, he was a specialist in national defense for the Library of Congress's Congressional Research Service, heading the Europe, Middle East, and Africa Section. Prior to that, he was a Foreign Affairs Officer in the State Department's Office of Policy Analysis, Bureau of Politico-Military Affairs, and was a member of the Consolidated Verification Group. He is the author of *U.S. Intelligence: Evolution and Anatomy* (1984), and of many articles and congressional studies on intelligence-related issues.

General Robert T. **Marsh**, US Air Force, was Commander, Air Force Systems Command (AFSC) at the time of his presentation. His portfolio includes involvement with ballistic missile development and command of the Projects Division in the Directorate of Space in the Pentagon before he returned to the AFSC as Deputy Chief of Staff for Development Plans. He commanded the Electronic Systems Division for nearly four years before being appointed Commander, AFSC in 1981.

Mr. Rodney B. **McDaniel** was Executive Secretary of the National Security Council (NSC) at the time of his presentation. As the administrative head of the NSC staff, he was responsible for the day-to-day functions of the interagency NSC process and providing direct support to the President and the National Security Advisor. He joined the NSC in 1985 as Special Assistant to the President, becoming the Senior Director of the Crisis Management Center, where he developed crisis procedures, systems to support decision-making, and emergency preparedness plans. While in the US Navy, Mr. McDaniel helped draft the Defense Guidance document that laid out the basic strategy for program planning, led a National Security Council-directed study of Navy force requirements, and commanded a guided missile cruiser. He also served as Chief of Staff to the Commander of the Seventh Fleet, with responsibility for day-to-day operational direction of all Navy and Marine Corps forces in the Western Pacific and Indian Ocean, and as Deputy Commander/Comptroller of the Navy's Shipbuilding Command.

Lieutenant General Clarence E. **McKnight**, US Army, was Director for Command, Control, and Communications Systems, Organization of the Joint Chiefs of Staff at the time of his presentation. Prior to that assignment, he was Commanding General, US Army Communications Command, a global responsibility covering 1,400 installations with a total of 33,000 personnel in 14 countries. He also served as the Commandant of the Signal School, the largest technical training center in the Army. His Army career has included assignments in the tactical, strategic, systems engineering, and research and development areas.

Mr. David **McManis** was the National Intelligence Officer for Warning and Director of the National Warning Staff at the time of his presentation. He was also president-elect of the National Security Agency's Computer and Information Sciences Institute. Previously, he had been Chief of the Policy and Management Staff at the Telecommunications and Computer Services Directorate where he was responsible for liaison and support to both the House and Senate Intelligence committees and the Executive Office of the President. Prior to that, Mr. McManis worked for the National Security Agency which he joined originally as an Arabic Voice Transcriber. From

1969 to 1974, he was director of the White House Situation Room and a member of the senior staff of the National Security Council, providing the President and his Assistant for National Security Affairs with current information on international events.

Lieutenant General Thomas H. **McMullen**, US Air Force, was Deputy Commander, Tactical Air Command at the time of his presentation. He has served the Air Force in system acquisition and tactical aviation—flying fighters, seeing command and control work as a forward air controller in Vietnam. He has been a test pilot, worked in R&D, been associated with Gemini, Apollo, and the B–1 bomber and the A–10 attack aircraft, and seen systems from the acquisition side as well.

Mr. William G. **Miller** was Associate Dean and Professor of International Politics, Fletcher School of Law and Diplomacy, Tufts University at the time of his presentation. His career in the Foreign Service brought him from early experience as a political officer in Iran to service as a presidential emissary under President Carter in a 1979 mission that contributed to the release of the first group of Iranian hostages. Along the way, he rose from a staff position in the Senate to staff director of the Senate Special Committee on National Emergencies and Delegated Emergency Powers, and then to equivalent positions on two Senate select committees investigating the US government's intelligence activities. The first, the Church Committee, created the second, the Senate Select Committee on Intelligence, in May 1976, and in doing so brought about a new era of intelligence oversight and a rigorous system of accounting for all intelligence activities.

General William E. **Odom**, US Army (Ret.), was Military Assistant to the Assistant to the President for National Security Affairs at the time of his presentation. He subsequently served as Director of the National Security Agency. He is widely recognized as an authority on Soviet military strategy.

Mr. Lionel **Olmer** was a member of Paul, Weiss, Rifkind, Wharton & Garrison, an international law firm, at the time of his presentation in 1986. He had previously served as Under Secretary for International Trade, US Department of Commerce, where he headed the International Trade Administration, an organization of more than 2,000 persons located in 48 US cities and 124 posts overseas. In this position, he managed the trade promotion, export control regulations, and trade laws of the US government. From 1977 to 1981, he was Director of International Programs for Motorola, Incorporated, where he developed international trade strategies, with emphasis on the opportunities created by the Multilateral Trade Negotiation Agreements.

He also served as Executive Secretary of the President's Foreign Intelligence Advisory Board, a position he had left just prior to his 1980 presentation.

Mr. James M. **Osborne,** former Senior Vice President, E–Systems, Inc., was retired at the time of his presentation. His background includes tactical development for the US Army Signal Corps and 19 years with RCA, during which he rose to Vice President and General Manager of the Government Communications and Automated Systems Division. His career culminated with his Senior Vice Presidency at E–Systems, where he served as Group Executive for the company's Production Electronics Group and General Manager of the ECI Division.

General Lee **Paschall,** US Air Force (Ret.) was a consultant at the time of his presentation. Before retiring from the military, General Paschall directed both the Defense Communications Agency and the National Communications System. That mammoth management job gave him a firsthand basis for judging how C³I is applied in daily reality—political, operational, technical, human.

Vice Admiral David C. **Richardson,** US Navy (Ret.), was a consultant at the time of his presentation. He spent his career in the Navy in a variety of command and staff positions, including command of the Sixth Fleet in the Mediterranean and deputy command of the Pacific Fleet. Since his retirement, he has served on the Defense Intelligence Review Panel, several panels of the Defense Science Board, the Navy Space panel of the National Academy of Sciences, and the C³I panel of the Naval Research Advisory Committee.

Mr. Charles **Rose** was a US Representative (D-NC) at the time of his presentation. He served as Chairman of the Policy Group on Information and Computers, was active in computer and television service to the House as a member of the House Administration Committee, and was Chairman of the Subcommittee on Oversight and Evaluation of the House Permanent Select Committee on Intelligence.

Major General Robert A. **Rosenberg,** US Air Force, was assigned to the National Security Council at the time of his 1980 presentation; when he made his second presentation, in 1984, he was Vice Commander in Chief for the North American Aerospace Defense Command (NORAD) and Assistant Vice Commander for the US Air Force Space Command (SPACECOM). A graduate of the US Naval Academy in Annapolis, General Rosenberg holds a master's degree in aerospace engineering from the Air Force

Institute of Technology and is a graduate of the Industrial College of the Armed Forces, Washington, D.C.

Mr. Charles W. **Snodgrass** was Vice President, Financial Planning and Management, Electronic Data Systems Corporation at the time of his presentation. He is a former Assistant Secretary of the Air Force for Financial Management. During his career with the Federal government, he moved from the Office of Management and Budget through the congressional staff to a cabinet-level office, gaining a view of the federal budgetary process which is both broad and deep. During that time he was associated with many aspects of C³I acquisition, including a successful strategy to protect Air Force interests in defeating an automatic data processing bill in the Senate, and development of means of Congressional oversight of the US intelligence community during his years as a staff assistant to the House Appropriations Committee's Defense Subcommittee.

Lieutenant General James W. **Stansberry**, US Air Force (Ret.), had recently retired from command of the Air Force's Electronic Systems Division when he gave his presentation. His military decorations and awards include the Distinguished Service Medal, the Legion of Merit with one oak leaf cluster, the Air Force Commendation Medal, and the Army Commendation Medal. His military career spanned over thirty years during which he worked in such diverse fields as air science, nuclear safety, atomic energy, and defense procurement. Among the positions he held were Deputy Assistant to the Secretary of Defense (Atomic Energy), Deputy Director of Procurement Policy for the Air Staff at the Pentagon, and Deputy Chief of Staff for Contracting and Manufacturing, Air Force Systems Command at Andrews Air Force Base.

General Richard G. **Stilwell**, US Army (Ret.), was Deputy Under Secretary of Defense for Policy and, later, Chairman of the DoD Security Review Commission at the time of his presentations in 1982 and 1985. His military career spanned 39 years and 14 campaigns in three wars. He was Deputy Chief of Staff for Plans and Operations of the US Army, and held numerous other commands and posts. General Stilwell's many awards include the Department of Defense Distinguished Service medal, the Army Distinguished Service Medal with three oak leaf clusters, and the Purple Heart.

Mr. Raymond **Tate** was President, Raymond Tate Associates at the time of his presentation. He had previously served as Deputy Assistant Secretary of the Navy and Deputy Director of the National Security Agency. His unique background ranges from the environment of the White House basement to the outside world—with vertical integration from the national leadership to

the "grunt" in the field. He has weathered a number of national crises, has had experience in both command situations and intelligence, and thus offers a valuable personal context on national affairs.

Dr. W. Scott **Thompson** was Director of Programs for the American Security Council Foundation, President of Strategic Research Associates in Washington, D.C., and Consultant to the Department of Defense at the time of his presentation. He is a member of the permanent faculty of the Fletcher School of Law and Diplomacy at Tufts University as well as an Adjunct Professor at Georgetown University. He has been a Visiting Fellow at Harvard University's Center for International Affairs, Visiting Research Professor at the University of the Philippines, and Visiting Research Professor at Chulalonkorn University, Bangkok. His non-academic positions include two years as the presidentially appointed Associate Director of the United States Information Agency, a year as Assistant to the Secretary of Defense, and two years as Consultant to the US Navy. He has written or co-edited six books on foreign relations.

Appendix B

Presenters and Presentations

John F. Kennedy School of Government
Seminar: Command, Control, Communications, and Intelligence

Chronological and Alphabetical Listings, 1980–1988

Chronological Listing

1988

Intelligence Sources and Their Applications
Rae Huffstutler
Three Mile Island: A Case Study in C³I for Crisis Management
Richard L. Thornburgh
Special Operations and Low Intensity Conflict: A Congressional Perspective
James R. Locher, III
Strengthening the Chairman of the Joint Chiefs of Staff
Robert T. Herres
The Special Operations Command: Structure and Responsibilities
Robert C. Kingston
Tailoring C³I Systems to Military Users
Jerry Tuttle
The Evolution of Special Operations Forces
Earl Lockwood
Getting in Front of C⁴I² problems
Frank J. Breth
Putting C³I Development in a Strategic and Operational Context
Ruth Davis

1987

The National Defense University's Command and Control Program
Greg Foster
Coming of Age in C³I
Michael J. Zak
Teaching Intelligence
Robert L. DeGross

The Information Management Marketplace
Eugene B. Lotochinski
Ideology and National Competitiveness
George C. Lodge
C³I: A National Security Council Perspective
Rodney B. McDaniel
Making Intelligence Better
Fred R. Demech, Jr.
Defense Reorganization: A View from the Senate
James R. Locher, III
Defense Reorganization: A View from the House
Archie D. Barrett

1986

C³I Systems at the Joint Level
Clarence E. McKnight
Data Security in the Information Age
Robert Conley
Intelligence Techniques for the American Business Community
Lionel Olmer
The Role of the National Security Agency in Command, Control and Communications
Harold Daniels
The Quest for "Good" Intelligence
Mark Lowenthal
Data Base Publishing for Business Intelligence
Richard Levine
Information Technologies and Multinational Corporations
John Grimes
Technological Innovation and the Cost of Change
B.R. Inman

1985

Centralization of Authority in Defense Organizations
Samuel P. Huntington
The Role of Intelligence within C³I
Lincoln D. Faurer
Structure and Mechanisms for Command and Control
Richard G. Stilwell
Politics and the Military—The Climate for Reform
Archie D. Barrett

A Consultant's View
Richard D. DeLauer
A View from Inside OSD
Donald C. Latham
A CINC's View of Defense Organization
Robert T. Herres
Roles of the Joint Chiefs of Staff in Crisis Management
Robert P. Hilton

1984

U.S.–U.S.S.R. Information Competition
W. Scott Thompson
Decision Making, Crisis Management, Information and Technology
Richard S. Beal
Warning as a Peacekeeping Mechanism
David McManis
Television News and the National Interest
Leo Cherne
Cost-Effective Rearmament
James W. Stansberry
Strategic Defense: A Challenge for C³I
Robert A. Rosenberg
C³I and Crisis Management
Stuart Branch
With AT&T in Iran
Hubert L. Kertz with Anthony G. Oettinger

1983 NO SEMINAR

1982

Strategic Connectivity
Richard H. Ellis
Planning for Defense-Wide Command and Control
Hillman Dickinson
A Tactical Commander's View of C³I
Thomas H. McMullen
C³ Priorities
Gerald P. Dinneen
Air Force C³I Systems
Robert T. Marsh

Policy and National Command
Richard G. Stilwell
The View from the Hot Seat
Richard D. DeLauer
Foreign Affairs, Diplomacy and Intelligence
William G. Miller

1981

Meeting Military Needs for Intelligence Systems
James M. Osborne
The Convergence of C³I Techniques and Technology
William O. Baker
A Major Contractor's View of C³I
Richard D. DeLauer
C³I and the Commander: Responsibility and Accountability
John H. Cushman
Funding C³I
Charles W. Snodgrass
The Uses of Intelligence
David C. Richardson
Congress and C³I
Charles Rose
Issues in Intelligence
B.R. Inman

1980

C³I and Telecommunications at the Policy Level
William Odom
Worldwide C³I and Telecommunications
Raymond Tate
The Influence of Policy Making on C³I
Robert Rosenberg
C³I and the National Military Command System
Lee Paschall
Oil Crisis Management
A.K. Wolgast
The Developing Perspective of Intelligence
William E. Colby
Managing Intelligence for Effective Use
B.R. Inman
Watchdogging Intelligence
Lionel Olmer

Alphabetical Listing

William O. Baker	1981
Archie D. Barrett	1985, 1987
Richard S. Beal	1984
Stuart Branch	1984
Leo Cherne	1984
William E. Colby	1980
Robert Conley	1986
John H. Cushman	1981
Harold Daniels	1986
Robert L. DeGross	1987
Richard D. DeLauer	1981, 1982, 1985
Fred R. Demech, Jr.	1987
Hillman Dickinson	1982
Gerald P. Dinneen	1982
Richard H. Ellis	1982
Lincoln Faurer	1985
Greg Foster	1987
John Grimes	1986
Robert T. Herres	1985
Robert Hilton	1985
Samuel P. Huntington	1985
B.R. Inman	1980, 1981, 1986
Hubert L. Kertz	1984
Donald Latham	1985
Richard Levine	1986
James R. Locher III	1987
George C. Lodge	1987
Eugene Lotochinski	1987
Mark Lowenthal	1986
R. Thomas Marsh	1982
Rodney B. McDaniel	1987
Clarence E. McKnight	1986
David McManis	1984
Thomas H. McMullen	1982
William G. Miller	1982
William Odom	1980
Lionel Olmer	1980, 1986
James M. Osborne	1981
Lee Paschall	1980
David C. Richardson	1981
Charles Rose	1981

Robert Rosenberg	1980, 1984
Charles W. Snodgrass	1981
James W. Stansberry	1984
Richard G. Stilwell	1982, 1985
Raymond Tate	1980
Scott W. Thompson	1984
A. K. Wolgast	1980
Michael Zak	1987

Index

The Editor

Thomas P. Coakley was a Senior Research Fellow at the US National Defense University in 1988–89. A lieutenant colonel in the US Air Force, he has served in a variety of positions ranging from executive officer and squadron commander to Professor of English at the US Air Force Academy. He graduated from Villanova University in 1969; he received his masters degree from the University of Texas at San Antonio and his doctorate from Penn State University. Col. Coakley and his wife Katherine have been married 22 years and have four children.

C³I: ISSUES OF
COMMAND AND CONTROL

Text and display composed in Times Roman and Optima
Cover display composed in Helvetica

Advisory readers:
Stuart E. Johnson, National Defense University
Thomas A. Julian, National Defense University

Cover design:
Nancy G. Bressi

Book design and editing:
Mary Loughlin, Editorial Research Associates

NDU Press Editor:
Janis Bren Hietala

NATIONAL DEFENSE UNIVERSITY PRESS
Fort Lesley J. McNair
Washington D.C. 20319-6000