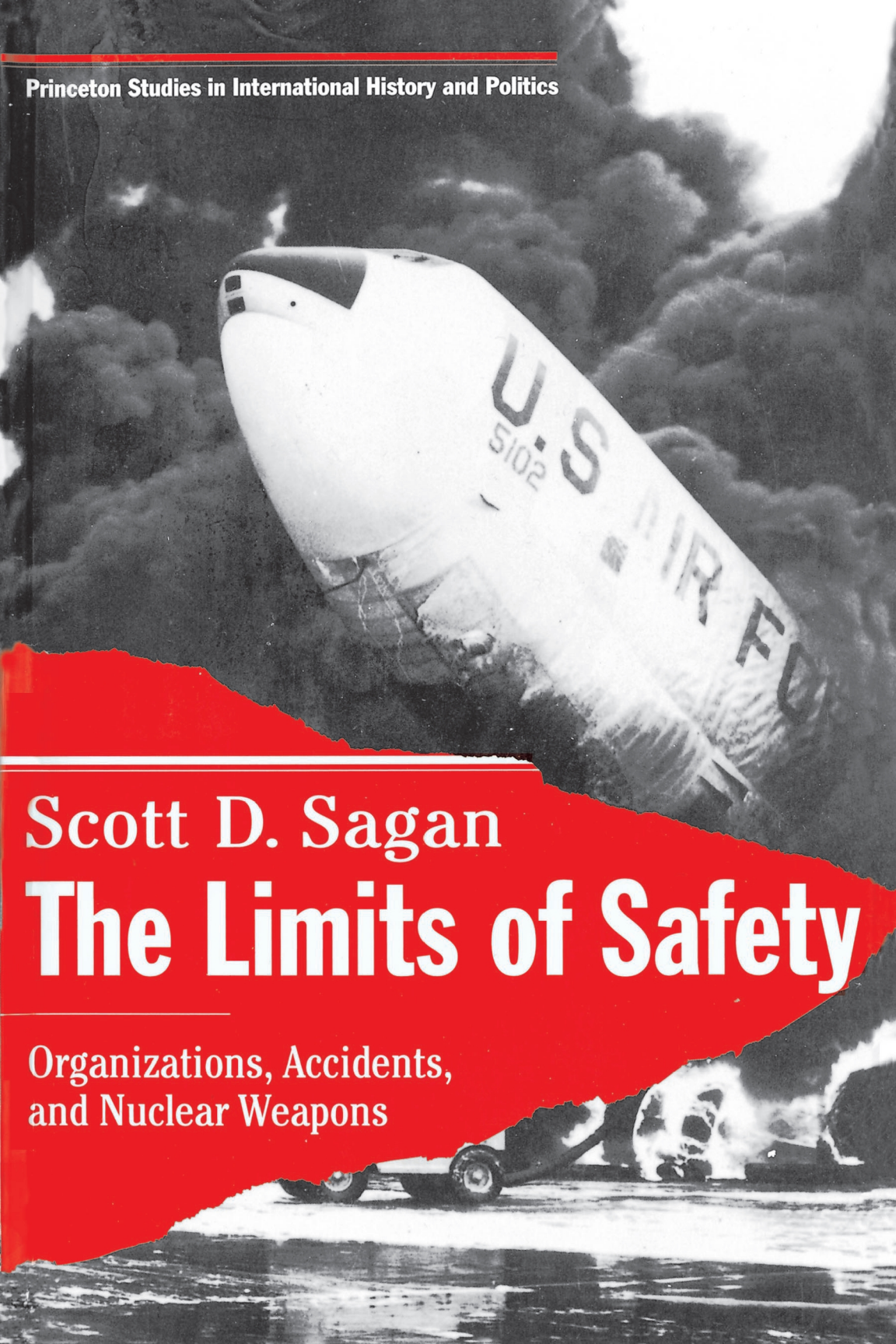
Princeton Studies in International History and Politics



Scott D. Sagan

The Limits of Safety

Organizations, Accidents, and Nuclear Weapons

THE LIMITS OF SAFETY

PRINCETON STUDIES IN INTERNATIONAL HISTORY AND POLITICS

Series Editors
John Lewis Gaddis
Jack L. Snyder
Richard H. Ullman

History and Strategy by Marc Trachtenberg (1991)

George F. Kennan and the Making of American Foreign Policy, 1947–1950 by Wilson D. Miscamble, C.S.C. (1992)

Economic Discrimination and Political Exchange: World Political Economy in the 1930s and 1980s by Kenneth A. Oye (1992)

Whirlpool: U.S. Foreign Policy Toward Latin America and the Caribbean by Robert A. Pastor (1992)

Germany Divided: From the Wall to Reunification by A. James McAdams (1993)

A Certain Idea of France: French Security Policy and the Gaullist Legacy by Philip H. Gordon (1993)

The Limits of Safety: Organizations, Accidents, and Nuclear Weapons by Scott D. Sagan (1993)

Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe by Janice E. Thomson (1994)

We All Lost the Cold War by Richard Ned Lebow and Janice Gross Stein (1994)

Who Adjusts? Domestic Sources of Foreign Economic Policy during the Interwar Years by Beth A. Simmons (1994)

America's Mission: The United States and the Worldwide Struggle for Democracy in the Twentieth Century by Tony Smith (1994)

The Sovereign State and Its Competitors by Hendrik Spruyt (1994)

The Korean War: An International History by William W. Stueck (1995)

Cooperation among Democracies: The European Influence on U.S. Foreign Policy by Thomas Risse-Kappen (1995)

THE LIMITS OF SAFETY

ORGANIZATIONS, ACCIDENTS, AND NUCLEAR WEAPONS

Scott D. Sagan

PRINCETON UNIVERSITY PRESS PRINCETON, NEW JERSEY

Published by Princeton University Press, 41 William Street,
Princeton, New Jersey 08540
In the United Kingdom: Princeton University Press,
Chichester, West Sussex

Library of Congress Cataloging-in-Publication Data

Sagan, Scott Douglas.
The limits of safety : organizations, accidents, and nuclear
weapons / Scott D. Sagan.
p. cm. — (Princeton studies in international history and politics)
Includes index.
ISBN 0-691-03221-1
ISBN 0-691-02101-5 (pbk.)
1. Nuclear weapons—United States—Safety measures. 2. Nuclear
weapons—United States—Accidents. I. Title. II. Series.
U264.3.S24 1993
363.17'9—dc20 93-12196

This book has been composed in Linotron Sabon

Princeton University Press books are printed on acid-free paper and
meet the guidelines for permanence and durability of the
Committee on Production Guidelines for Book
Longevity of the Council on
Library Resources

Fourth printing, and first paperback printing, 1995

Printed in the United States of America

5 7 9 10 8 6 4

For My Parents

JOHN SAGAN AND MARGARET PICKETT SAGAN

Although observers of warfare have often noted the confusions of battle, the ideology of military decision-making emphasizes the imposition of order through organization and command and the importance of clarity, coherence and comprehensiveness. As a result, examining ambiguity in military decision-making is a little like examining the sexual habits of Victorian England. It requires a willingness to accept the possibility that things may not be exactly what they appear to be, or are supposed to be.

(James G. March and Roger Weissinger-Baylon
Ambiguity and Command, 1986)

Contents

Figures and Tables

FIGURES

TABLES

Acknowledgments

AMONG the great joys of finishing a book is the pleasure of thanking those who made it possible. This project has taken more years than I originally anticipated. I have therefore been lucky to receive more than my fair share of assistance, advice, and encouragement along the way.

Financial support for the project was provided by the Carnegie Corporation of New York and the John D. and Catherine T. MacArthur Foundation. Frederic Mosher and David Hamburg of the Carnegie Corporation deserve special thanks for providing me with a discretionary grant, which enabled me to take time away from my teaching responsibilities to complete the first draft of the manuscript. The book would have taken much longer to complete without such generous support.

My research would not have been possible without good access to primary sources of information on the history of nuclear weapons safety. Archivists everywhere seem to be burdened with too much work and too little support; but many somehow overcome the difficulties to provide exemplary professional assistance to researchers. I especially want to thank George Culley at the Air Force Historical Research Center, Suzanne Forbes at the John F. Kennedy Library, David Humphrey at the Lyndon B. Johnson Library, and Edward Reese at the National Archives.

The book would also have been considerably less interesting without the willingness of so many retired U.S. military officers and government officials to be interviewed. Most of these individuals permitted me to identify them in the footnotes. A few preferred "not for attribution" interviews, and in such cases I have only identified their general position so as to permit readers to make at least some judgment as to the reliability of the source. I thank both groups of individuals.

A number of tireless undergraduates at Stanford University have served as my research assistants. They usually found most of what I asked them to find, and they often found important material that I did not realize existed. For all their hard work, I thank Mala Htun, Richard Lobel, John Louie, Trevor Macy, Marlene Rodriguez, Sarah Stevenson, Effie Toshav, and Benjamin Valentino.

Stanford's Center for International Security and Arms Control (CISAC) has been supportive of this project from its conception to its completion. CISAC not only provided an office and a stimulating academic environment, but also organized a special manuscript review meeting in February 1992 in which the following participants offered very helpful suggestions: Barton Bernstein, Lynn Eden, David Holloway, Kurt Gaubatz, John

Harvey, Stephen Krasner, and Richard Scott. The Program on International Political Economy and Security (PIPES) at the University of Chicago also hosted a meeting on the manuscript in April 1992, and I would like to thank all the participants, and especially John Padgett, Brad Thayer, and Stephen Walt for their written comments. In addition, the following friends and colleagues read all or parts of the manuscript in various drafts and saved me from committing many unnecessary errors: John Arquilla, Coit Blacker, James Blight, Kurt Campbell, Chris Demchack, Michael Desch, Daniel Ellsberg, Peter Feaver, John Gaddis, Robert Jervis, Peter Lavoy, Stefan Michalowski, Michael May, James Miller, Susan Okin, Barry O'Neill, Robert Powell, Edward Rhodes, Paul Stockton, Marc Trachtenberg, Stephen Van Evera, Dennis Ward, and Kimberly Zisk.

A number of people deserve very special recognition. Lynn Eden has been a wonderful source of ideas and an apparently inexhaustible reader of numerous drafts. Her enthusiasm for the project was critical at points when mine began to wane. Three scientists affiliated with CISAC—Sidney Drell, Gerald Johnson, and John Harvey—read draft chapters and guided me through many of the technical complexities of nuclear weapon systems, although I must absolve them from any remaining technical errors. I am also very grateful to Richard Scott for his neverending suggestions for further reading and for inviting me to try out some of my ideas at seminars sponsored by the Stanford Center for Organizations Research. In addition, a number of the organization theorists whose work I am building upon—scholars from both the normal accidents school and the high reliability camp—provided extremely valuable criticisms of earlier drafts of this work. I am especially grateful to Jonathan Bendor, Todd La Porte, Charles Perrow, Karlene Roberts, and Gene Rochlin for their ability to debate, their willingness to listen, and their high reliability as scholars.

Finally, I want to thank my wife, Bao Lamsam, and our son, Benjamin, for their love and support. It is good to know that some things in life are beyond the reach of accident.

Acronyms

ADC	Air Defense Command
ADIZ	Air Defense Identification Zone
AFHRC	Air Force Historical Research Center
AFSC	Air Force Systems Command
ANMCC	Alternative National Military Command Center
BMEWS	Ballistic Missile Early Warning System
CC&DF	Command Control and Display Facility
CIA	Central Intelligence Agency
CINCEUR	Commander in Chief, Europe
CINCLANT	Commander in Chief, Atlantic Command
CINCPAC	Commander in Chief, Pacific Command
CINCSAC	Commander in Chief, Strategic Air Command
CINCUSAFE	Commander in Chief, United States Air Forces, Europe
CMEWS	Cuban Missile Early Warning System
DEFCON	Defense Condition
DEW LINE	Distant Early Warning Line
EAM	Emergency Action Message
ECC	Emergency Combat Capability
EMP	Electromagnetic Pulse
ESD	Environmental Sensing Device
EUCOM	European Command
FAA	Federal Aviation Administration
FDA	Food and Drug Administration
FOIA	Freedom of Information Act
GAO	General Accounting Office
GRU	Chief Intelligence Directorate for the Soviet General Staff
HASP	High Altitude Sampling Program
HF	High Frequency
ICBM	Intercontinental Ballistic Missile
IRBM	Intermediate Range Ballistic Missile
JCS	Joint Chiefs of Staff
KGB	Soviet Committee for State Security
LCC	Launch Control Center
NA	National Archives
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NEACP	National Emergency Airborne Command Post

NMCC	National Military Command Center
NORAD	North American Air (or Aerospace) Defense Command
NSA-CMCC	National Security Archives–Cuban Missile Crisis Collection
NSAM	National Security Action Memorandum
PAL	Permissive Action Link
PARCS	Perimeter Acquisition Radar Attack Characterization System
PAVE PAWS	Precision Acquisition of Vehicle Entry New Phased-Array Radars
PCL	Positive Control Launch
PCTAP	Positive Control Turn-Around Point
PG&E	Pacific Gas and Electric
QRA	Quick Reaction Alert
RCA	Radio Corporation of America
ROE	Rules of Engagement
SAC	Strategic Air Command
SACEUR	Supreme Allied Commander, Europe
SAGE	Semi-Automatic Ground Environment
SEAGA	Selective Employment of Air and Ground Alert
SIOP	Single Integrated Operational Plan
SIS	Secret Intelligence Service (United Kingdom)
SLBM	Submarine Launched Ballistic Missile
SRF	Strategic Rocket Forces (USSR)
SWESS	Special Weapons Emergency Separation System
USAF	United States Air Force

THE LIMITS OF SAFETY

INTRODUCTION

Expecting the Unexpected

ON THE NIGHT of October 25, 1962, an air force sentry was patrolling the perimeter of a military base near Duluth, Minnesota. It was the height of the Cuban missile crisis, and nuclear-armed bombers and interceptor aircraft, parked on air base runways and at commercial airports throughout the United States, were alert and ready for war. The sentry spotted someone climbing the base fence, shot at the figure, and sounded the sabotage alarm. At airfields throughout the region, alarms went off, and armed guards rushed into the cold night to prevent Soviet agents from sabotaging U.S. nuclear forces.

At Volk Field in Wisconsin, however, the wrong alarm bell rang: the Klaxon signalling that nuclear war had begun went off. Pilots ran to their nuclear-armed interceptors and started the engines. These men had been told that there would be no practice alert drills during the tense crisis, and they fully believed that a nuclear war was starting as they headed down the runway. Fortunately, the base commander contacted Duluth before the planes took off and discovered what had happened. An officer in the command post immediately drove his car onto the runway, flashing his lights and signaling the interceptors. The pilots saw him and stopped their aircraft. The suspected Soviet saboteur that caused the whole incident was, ironically, a bear.

Unlikely Events

When I began working on this book, I believed that the probability of a serious nuclear weapons accident in the United States was extremely low. I also believed that escalation from a single accident to an accidental nuclear war was even more unlikely. I still hold those beliefs. But new knowledge about bizarre and dangerous incidents within the U.S. nuclear weapons arsenal—like how a bear climbing a fence almost caused nuclear-armed aircraft to be launched—has led to a new appreciation of how often unlikely events occur. In the large and very complex organizations that control hazardous technologies in our society, one should expect that the unexpected will occur, that unimaginable interactions will develop, that accidents will happen.

The historical research presented in this book has discovered a large number of previously unknown "close calls" with U.S. nuclear weapons: serious incidents within the U.S. nuclear arsenal that could have produced an accidental or unauthorized detonation of a nuclear weapon, and potentially even an accidental war, had they occurred under different, though plausible, circumstances. The seriousness of some of these incidents was immediately recognized by the actors involved and the command system problems were properly reported and addressed at higher levels. My research has "discovered" these cases only in the most narrow sense of finding archival material or receiving declassified evidence through the Freedom of Information Act. Other cases, however, were not recognized as serious incidents or even as potential command system problems by the individuals or organizations involved. These incidents have been "discovered" in the more meaningful sense of identifying a real-world problem for the first time. Finally, a number of these events were recognized as being very dangerous by the individuals involved, but were not fully reported, either inadvertently or intentionally, to higher authorities. This research has "discovered" them in the sense that a detective can be said to have discovered hidden evidence about a criminal case, facts that were known to someone, but not to the judge.

Motives and Methods

Why and how was this book written? It began, as most books do, with a puzzle. We live in a world full of hazardous technologies and some risk of catastrophic accidents is therefore ever present. We try to keep these risks as low as possible, yet in recent years, the names of many social and environmental tragedies have been etched into our memory: Chernobyl, the *Exxon Valdez*, Love Canal, the space shuttle *Challenger*, Bhopal. The safety record seems quite extraordinary, however, with the most hazardous technology of all: nuclear weapons. There has never been an accidental or unauthorized detonation of a nuclear weapon, much less escalation to an accidental nuclear war.

Why? How have imperfect humans, working in imperfect organizations and operating imperfect machines, been so successful? Have the military organizations that maintain custody and control over U.S. nuclear weapons done something extremely intelligent to avoid accidents? Have they been designed in such a way to produce reliable safety? Or have they merely been extremely lucky?

The first step toward solving this puzzle was to arm myself with the major scholarly theories that exist about the causes of safety and accidents in complex organizations. Two competing schools of thought—what I call

normal accidents theory and high reliability theory—are analyzed in chapter 1. Such theories are always necessary to understand complex social phenomena; they are the conceptual tools we use to pull disparate events together and understand what caused them. The point is especially obvious for anyone who tries to do historical research with records kept in massive collections like the National Archives: theories are absolutely necessary to tell you where to look for evidence. (The final scene of the movie *Raiders of the Lost Ark*, in which the ark of the covenant is slowly wheeled into a mammoth government warehouse, conveys a sense how effectively historical objects are hidden in the recesses of the archives.) Using the theories discussed in chapter 1 as guides, I was able to explore the historical records of the U.S. military, searching for clues.

Let me give just one example of how the process worked. (See chapter 3 for the substantive details about this particular case study.) The literature on the Cuban missile crisis is immense, but no scholar has previously studied the emergency radar warning system, which the United States deployed on a crash basis in October 1962 after the Soviet missiles were discovered. A study of the activities at the three radars used in this Operation Falling Leaves appeared to me, however, to be a very useful way of comparing the strengths of the two theoretical perspectives outlined in chapter 1, since these theories provide contrasting expectations about this warning system's reliability. Normal accidents theory would predict that Falling Leaves would be a very accident-prone operation: the warning system displayed all the signs of high interactive complexity and tight coupling, the two structural factors that the theory suggests lead to dangerous accidents in other high technology systems. High reliability theory would predict that Falling Leaves would be a relatively safe operation, since the factors that the theory suggests produced safety in other hazardous systems also existed here: significant decentralized decision-making authority was given to operators in the field, redundant radars were used to provide more accurate warning information, and officers' caution was heightened by the crisis environment. I therefore visited the Air Force archives, found a number of relevant declassified documents, and then used the Freedom of Information Act to request that additional related documents be declassified and sent to me.

These historical records confirmed the more optimistic view of the high reliability theorists. They reported on no serious false warning incidents occurring during the crisis. Indeed, the Falling Leaves after-action reports recommended that the emergency radar system be set up again if there was ever another superpower crisis.

This success story was puzzling from a normal accidents perspective. That theory, however, also reminds us to be skeptical of documents that are written by organizational actors who are interested in promoting their

cause. Operators do not want to get blamed for making serious errors and leaders of military organizations want to promote the reputation of their command. I therefore sent the documents to a large number of the retired Air Force officers and civilian contractors who had participated in the Falling Leaves operation, and asked that they comment on them. A number of these men recalled that there had been one or more serious false warning incidents during the crisis and expressed puzzlement as to why such events were not in the unit histories. I did not know whether to trust the documents (which could be faulty) or the memories (which obviously could be faulty too).

Fortunately, one retired officer said that he was sure that he had written something about a false warning incident in the command post log back at Air Defense Command Headquarters in 1962. I had not known that such records existed, but I immediately requested that the Air Force Space Command declassify these command post logs for the dates of October 26–29, 1962. These handwritten notes were like a smoking gun.

They revealed that a serious false warning incident occurred on October 27, 1962, at the height of the Cuban crisis. The radar operators at one site in Moorestown, New Jersey, informed the national command post that a missile had just been launched from Cuba and was about to detonate near Tampa, Florida. The command post officers immediately informed other U.S. military commands that a nuclear attack appeared to be under way. After the event, operators discovered that a software test tape, simulating a missile launch from Cuba, had been inserted into the radar operators' screen and that, simultaneously, a satellite came over the horizon. The operators "became confused," according to the command post log, and therefore reported "the test target as real." Who would have anticipated that a satellite would appear on the radar screen at the exact moment when a test tape was running and at the exact location where a missile launched from Cuba would have appeared? To make matters worse, the Falling Leaves system had been carefully designed to include overlapping redundant radars to provide more reliability, but the other radars were not turned on when the incident occurred. In addition, although the radars were supposed to get advance information on satellites passing overhead, the key facility involved had been taken off that mission, ironically, to help provide warning in the Falling Leaves operation. None of this was reported in the classified after-action reports on the operation.

The research strategy proved laborious, but it also proved necessary. This book thus attempts to show one way in which social science theories can illuminate, indeed even identify, important events in history. It also attempts to show how such historical case studies can be used to evaluate our theories, and thereby improve our broader understanding of how complex organizations manage and mismanage hazardous technologies.

A Note on Sources

Nuclear weapons and military operations are obviously very sensitive subjects within the government. Getting information on nuclear weapons accidents and safety problems has therefore been an extremely difficult task. Four kinds of sources provide the primary evidence used in this book.

First, I made extensive use of the declassified government documents available to researchers at the National Archives, the presidential library system, and the operational archives of the U.S. Air Force and U.S. Navy. I had to visit a number of these archives many times, as new material became available or subsequent ideas suggested new areas of inquiry. Many important pieces of the puzzle were found, however, once I figured out where they might be hidden.

Second, I requested and received literally hundreds of formerly classified documents (some in their entirety and some in sanitized form) through the Freedom of Information Act and the Mandatory Declassification Review process. Responses were forthcoming in anywhere from three weeks to three years. Sometimes my requests were lost; sometimes the wrong documents were declassified. I appealed most decisions to withhold documents in their entirety and occasionally the agency involved released more information. Copies of these documents have been placed in the National Security Archives in Washington, D.C., so that other researchers can use them.

Third, I conducted dozens of interviews with individuals who were involved in these dangerous incidents. These interviews spanned the hierarchy from former senior civilian officials at the Pentagon and the White House, down to individual interceptor pilots and crewmen inside a Minuteman ICBM launch control center. Often I would send the available declassified documents to these individuals to get their views on the accuracy of the records. Evidence from such interviews obviously has to be treated with caution, given the inevitable vagaries of memory and the potential biases of the individuals involved.

Fourth, a great deal of useful information on the subject of nuclear weapons safety can be found in congressional hearings. One must also use the material from such hearings cautiously, however, since testimony given in such hearings may or may not be absolutely accurate. Moreover, critical material is often deleted from the transcript, to protect classified information necessary for national security, and what remains can therefore be misleading.[1]

[1] Difficult detective work is not always necessary to fill in the blanks. For example, I already knew that 30 percent of the U.S. bomber force was kept on day-to-day alert from the following sanitized testimony: "With regard to the bomber force, we keep approximately (*deleted*) *percent* of the bombers and supporting tankers—roughly (deleted) aircraft—on

Given the extreme sensitivity of the whole subject of nuclear weapons safety, many relevant documents remain classified even after thirty years. A special caveat is therefore in order. This is not, and could not be, the definitive story of accidents and near-accidents with U.S. nuclear weapons and command and control systems. Much more information would have to be declassified in order to provide a full glimpse into the heart of the problem. I have done the best I can with the limited material available, and try to provide enough detail so that each reader can develop his or her own judgment about the seriousness of each incident I discuss. I suspect that declassification of further documents may lead to reevaluation of some of my cases; I also suspect that such material will make some incidents seem more dangerous, and some less dangerous, than they appear in the light of the current evidence. And I strongly believe that more nuclear safety problems than are reported here will eventually surface from the recesses of the classified archives.

Outline of the Book

The structure of this book is straightforward. Chapter 1 presents and develops two theoretical perspectives on the ability of complex organizations to manage hazardous technology. These two theories are lined up in a kind of comparative test to determine which provides better insights into the history of U.S. nuclear weapons safety. Chapter 2 and chapter 3 are a series of case studies of nuclear weapons operations during the Cuban missile crisis of October 1962. In chapter 2, I present what the logic of each theory would lead one to expect would happen when the United States put its nuclear forces on alert during the crisis, and then compare these expectations to the historical record. I follow the same approach, only this time looking at U.S. warning and intelligence operations, in chapter 3.

Chapter 4 moves forward to January 1968 and presents a detailed study of the causes and consequences (both real and potential) of the crash of a nuclear armed B-52 bomber near Thule, Greenland. The purpose of the chapter is to explore the consequences of a strategy for improved safety that attempts to produce high reliability by adding redundancy to the system. Chapter 5 focuses on the issue of organizational learning. It presents two case studies. The first is an examination of U.S. nuclear alert operations during the October 1973 Yom Kippur War, which examines the

---

constant alert. They are at the appropriate alert levels, so that they could escape prior to the impact of SLBM weapons. If we suffer a strike out of the blue, a surprise attack, we accept the probability that *the other 70 percent of the force* would be destroyed." Testimony of General Richard Ellis, Senate Armed Services Committee, *Hearings on DOD Appropriation for FY 1982*, part 7, p. 3799 (emphasis added).

degree to which the U.S. government and U.S. military commands learned from the experience with nuclear weapons operations during the Cuban crisis eleven years earlier. The second case study examines a series of false warning incidents that occurred within the North American Aerospace Defense Command in 1979 and 1980. Why did these incidents occur and what was learned from the experience?

Chapter 6 presents my conclusions. The implications of the study for organization theory, especially for our understanding of the causes of accidents involving hazardous technologies, are outlined first. Then the implications for deterrence theory and the study of nuclear weapons are presented. Finally, I conclude with a brief discussion of the policy implications of this book. What, if anything, can be done to reduce the dangers identified within?

Beyond the Cold War

Like many books about international politics that have been published in recent years, this one was started during the Cold War and was completed in the post–Cold War era. Unlike some of these books, however, this one is, I believe, as relevant to the emerging new world as it was to the old. This is the case for two basic reasons.

First, while the end of the Cold War has clearly and dramatically reduced the risk of a deliberate conflict between the United States and the former Soviet Union, its impact on the likelihood of nuclear weapons accidents, and even accidental war, is less clear cut. A number of factors do appear to have reduced these risks. The likelihood of serious accidents is highest during a crisis, when nuclear forces are placed on a heightened state of alert readiness; and since the end of the Cold War reduces the likelihood of major crises, it thereby also lowers the likelihood of accidents. The major achievements in Russian and American arms control in 1991 and 1992—especially the U.S. decision to take Strategic Air Command bombers off day-to-day nuclear alert status and the Russian decision to take its largest ICBM, the SS-18, off alert—have further reduced the risks. Finally, it appears much less likely after the Cold War that Russian or American political or military authorities would react to a false warning of an attack against their country with rash orders to retaliate immediately.[2]

That is the positive side of the ledger. A number of important factors, however, appear on the negative side. The collapse of the Soviet Union has

[2] One should not, however, be too optimistic here. Imagine that a serious false warning that a nuclear attack was under way, like the events described in chapter 5, had occurred during the August 1991 coup attempt in Russia. Can we be certain that such a warning would have been treated with skepticism?

subjected its nuclear command and control system to unprecedented and unanticipated tensions. Short-range tactical nuclear weapons have reportedly all been successfully withdrawn, in great haste (and thus probably with considerable risk of accident), to Russia from other former Soviet republics. Yet, intercontinental-range strategic nuclear weapons are likely to continue to be deployed in Russia, Kazakhstan, and Ukraine for many years to come, and the safety of these weapons will likely be strained by emerging political, ethnic, and civil-military conflicts in the region. The elaborate system of nuclear weapons control there was simply not designed to cope with such events as a coup attempt or large-scale social unrest, and its ability to provide safety in such an environment is uncertain. In addition, for reasons spelled out in chapter 6, the danger of accidents with nuclear weapons, and the danger of accidental nuclear war, are more likely with new states that are developing their own nuclear arsenals in the post–Cold War world.

Finally, there is a serious problem of overconfidence here in the United States. If the theories and evidence presented in this book are correct, then there are likely to be a number of hidden bugs in the U.S. nuclear weapons system, latent technical and organizational safety problems that have not been recognized over time. To the degree that we become complacent, believing that the end of the Cold War has solved the problem of nuclear weapons safety, fewer of these problems will be identified and fixed. Some day, when we expect it least—during a military exercise, while transporting nuclear weapons to storage sites, during a missile flight test, or even during a routine missile maintenance operation—the unexpected will occur. That would indeed be an ironic and tragic consequence of the end of the Cold War rivalry.

The second basic reason that this book is relevant to the post–Cold War world is that the hidden history of nuclear weapons safety problems has many broader implications for other organizations that attempt to manage hazardous technologies. The U.S. military organizations studied here are widely considered to be models of discipline and reliability. Some of the problems they have experienced can therefore reasonably be expected to be repeated—in one form or another, and sometimes with a vengeance—in more "ordinary" civilian organizations, such as nuclear power plants, oil tankers, petrochemical factories, and biotechnology firms.

We will continue to live in a world filled with hazardous technologies and our understanding of how to control them is both terribly important and very incomplete. This book is an effort to identify some persistent problems that might be fixed, as well as some that probably cannot. It attempts to illuminate both the prospects for progress and the inherent limits of safety.

CHAPTER 1

The Origins of Accidents

An examination of page 752 of the reference (Emergency Actions File) indicates that the President is not included in the list of personnel to be notified under declared conditions of an Air Defense Emergency or a Defense Emergency or DEFCON 1.

(Rear Admiral J. H. Wellings, Acting Director of the Joint Staff, Memorandum, December 27, 1960)

Accidents will happen.

(Anon.)

ACCIDENTAL nuclear war is a very difficult subject to study. The first reason for this difficulty is the most obvious, the most important, and the most fortunate one: there has never been a single accidental nuclear detonation, much less an accidental nuclear war. The traditional comparative methodology used by social scientists to explain complex political phenomena—comparing and contrasting cases in which the phenomena occurred against cases in which it did not—cannot be used here. There are, of course, many other difficulties involved in a thorough investigation of this subject. Many important pieces of evidence about past nuclear weapons incidents remain classified; some critical documents about sensitive military operations have been destroyed; faulty historical records have sometimes been created by military units; and inadequate social science theories exist to help us understand both the causes of war and the origins of accidents. But these difficulties pale next to the basic conceptual dilemma posed by the problem of accidental nuclear war. How does one even begin to study something that has never occurred?

One possibility is to assume that this central fact proves that the danger of nuclear weapons accidents and accidental nuclear war is minimal. Such an optimistic assessment is not unusual, in fact, since it can be argued that history has demonstrated that nuclear weapons can be maintained and operated in a safe and secure manner.[1] This assessment, however, is inade-

[1] See, for example, Kenneth N. Waltz, *The Spread of Nuclear Weapons: More May Be Better*, Adelphi Paper 171 (London: International Institute for Strategic Studies, 1981), p. 16.

quate for at least three reasons. First, things that have never happened before happen all the time in history. There must be a first time for every type of historical event that has occurred in the past, and the lack of earlier nuclear accidents is therefore insufficient evidence for making such a strong statement about future possibilities. Second, nuclear weapons have existed for less than fifty years and have been in the possession of only a small number of nations. This is a very limited pool of experience on which to base confident assessments of long-term nuclear weapons safety, especially under what could be quite different conditions during the next century. Third, an assessment of the risk of accidental nuclear war should examine close calls to catastrophe, and not be satisfied with the simple fact that accidental nuclear war has never occurred. For if we have had numerous "near-accidents" with nuclear weapons—incidents that could have resulted in an accidental nuclear war had they occurred under other plausible circumstances[2]—even an apparently perfect final safety record may not inspire extreme confidence.

A more thorough assessment therefore requires a deeper investigation into the hidden history of nuclear weapons. What has been the complete safety record, of accidents and near-accidents, with these weapons and their command and control systems? How have the military organizations that have custody over nuclear weapons been able to manage their complex operations with such apparent success? Have these organizations done something extremely intelligent to avoid accidents or have they merely been extremely lucky?

A useful place to start is to examine the causes of accidents and safety problems in other similar sociotechnical systems. For although there has never been an accidental nuclear weapons detonation or war, there have been numerous serious accidents in recent decades in other complex high-technology systems such as nuclear reactors, commercial and military aircraft, space programs, international shipping, and large petrochemical plants. Fortunately, a rich scholarly literature studying the causes of reliability and safety in these industries exists. What has caused serious accidents with these hazardous technologies? What organizational designs and strategies have been used to prevent accidents and enhance safety? A number of scholars have sought to explain successes and failures in organizational safety, and their ideas, if used very carefully, can help us understand the risks of serious accidents with nuclear weapons.

This chapter will examine the two most important schools of thought within the organization theory literature concerning the issue of safety and

[2] Here I am following the National Research Council's definition of a safety "incident." See National Research Council, Assembly of Engineering, *Improving Aircraft Safety: FAA Certification of Commercial Passenger Aircraft* (Washington, D.C.: National Academy of Sciences, 1980), p. 107.

reliability in complex technological systems. Subsequent chapters will then apply these theories to the military organizations that control U.S. nuclear weapons and test the theories competitively against one another by probing into the historical record of nuclear weapons accidents and "close calls" to accidental nuclear war. The goal is to provide a clearer understanding of the origins of accidents and the causes of safety.

ORGANIZATION THEORY AND ACCIDENTS

Even a brief glance at the recent history of high-technology industries cautions against complacency. Why have such tragedies as Chernobyl, the *Exxon Valdez*, and Bhopal occurred? Are such accidents preventable? Or are they the inevitable consequence of the widespread use of hazardous technologies in the modern world?

The scholarly literature about complex organizations is large and diverse, but two general competing schools of thought on this specific issue exist. The first is the optimistic view of what I will call "high reliability theory," whose proponents argue that extremely safe operations are possible, even with extremely hazardous technologies, if appropriate organizational design and management techniques are followed. The second school, what I will call "normal accidents theory," presents a much more pessimistic prediction: serious accidents with complex high technology systems are inevitable.

The term *schools of thought* was used deliberately, since it is in many ways a better description of what exists in this literature on hazardous technologies than the term *theories*. The scholarship I will be analyzing is based on mixtures of abstract deductive logic and inductive empirical observation, and the authors within each school by no means agree on all details concerning organizational safety. Specific terms that appear often in this literature are not always used in a consistent manner. And perhaps most importantly the predictions of both schools are often imprecise. Nevertheless, proponents of each school do focus attention on a specific set of factors that they believe contributes to or decreases safety, and each school develops a set of general hypotheses that is meant to hold true in a variety of organizations across space and time. These ideas can therefore be viewed as nascent social science theories and can usefully be tested against one another.

These two schools of thought have intellectual roots in different traditions within the organization theory literature; they have different basic understandings of how organizations work and hold different views on how best to analyze complex organizations. The theories offer competing general explanations for the causes of accidents with hazardous technolog-