APPENDIX A
UKRAINIAN PROJECT DEPARTMENTS AND PERSONNEL CONTACTED

Ukrainian Psychological Institute
2 Pankovskaya Street
Kiev, Ukraine 252033

Director, Professor A. K. Wasilewich
Director of the Children's Center for Chernobyl, Dr. S. Yakovenko
Project Manager, Adults of Chernobyl, Dr. Y. Sewalb
Child Psychologist, Natalia A. Bastun
Director, Ukrainian Guidance Center, Dr. V. Panok

Institute for Psychiatry
103 Frunze Street
Kiev, Ukraine 252053

Director, A. P. Chuprinov, M.D.

Ministry of Forests
5 Kreshechatik Street
Kiev, Ukraine 252601

Head of the Scientific and Technical Office, N. Kaletnik

Minister of Chernobyl Affairs
1 Lesi Ukrainki Square
Kiev, Ukraine 252196

Chief, Protection of the Population Department, L. Tabachny
First, Vice-Minister, Boris S. Prister
Director, International Cooperation, Y. Pavlov
Department Head, Statistics, N. Repina

Shevchenko University
64 Vladimirskaya Street
Kiev, Ukraine 252601

Chairman, Psychodiagnostics and Medical Psychology, Prof. L. Burlatchuk
First, Vice-Rector, Prof. O. Tretyak
Vice-Rector of Education, Prof. L. Gubersky

Ukrainian Academy of Sciences

Dr. V. V. Gudzenko
Dr. E. V. Sobodovych

APPENDIX B
PHOTOGRAPHS OF CHERNOBYL
AND
TESTING SITES

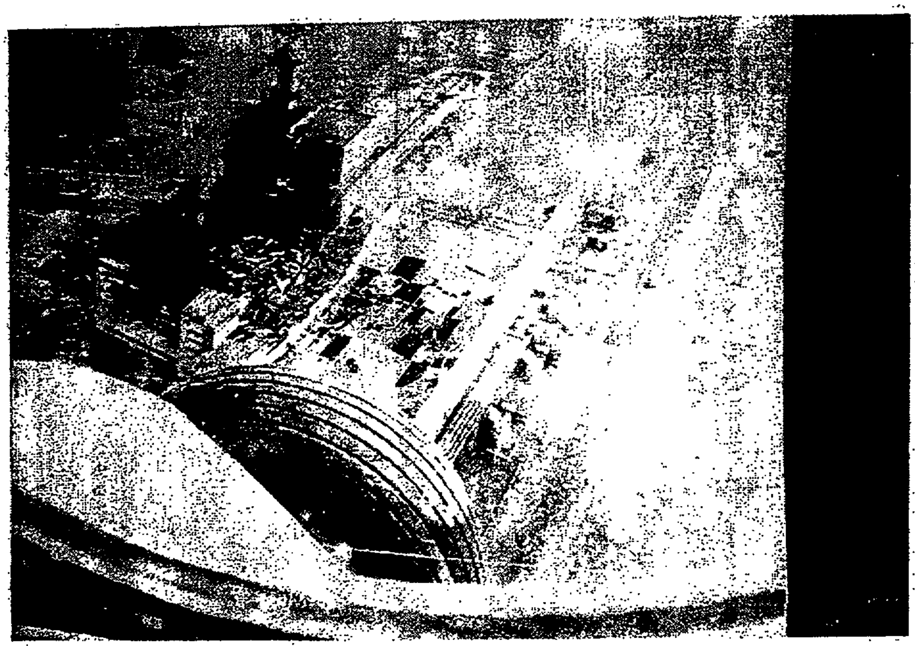

Figure B-1. Chernobyl site after explosion, 26 April 1986.

Figure B-2. Russian monitors, 26 April 1986.

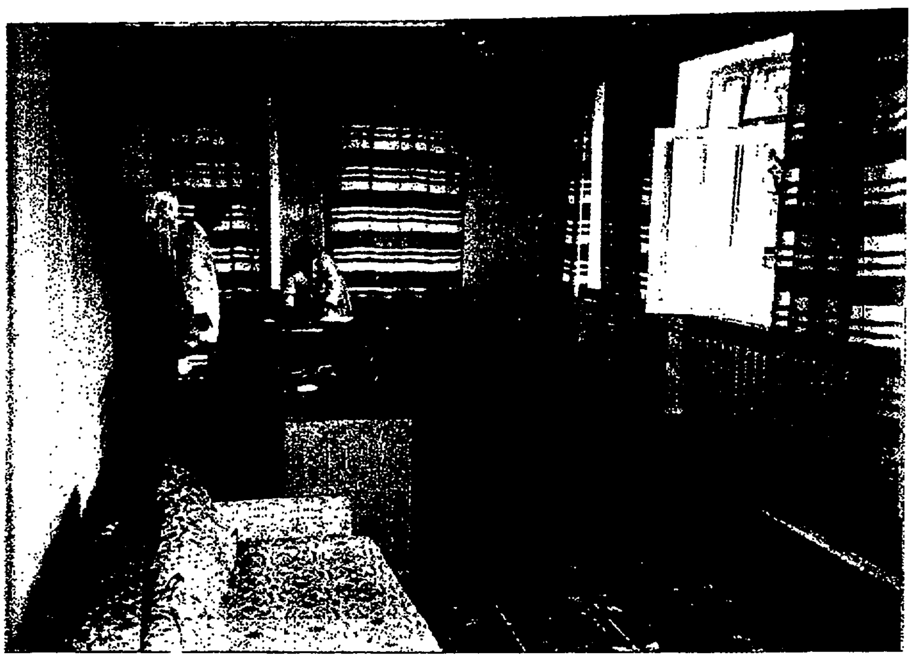

Figure B–3. Setting up to test eliminators.

Figure B-4. Agricultural workers ready for testing on ANAMUKR.

Figure B-5. Agricultural workers walking on balance beam.

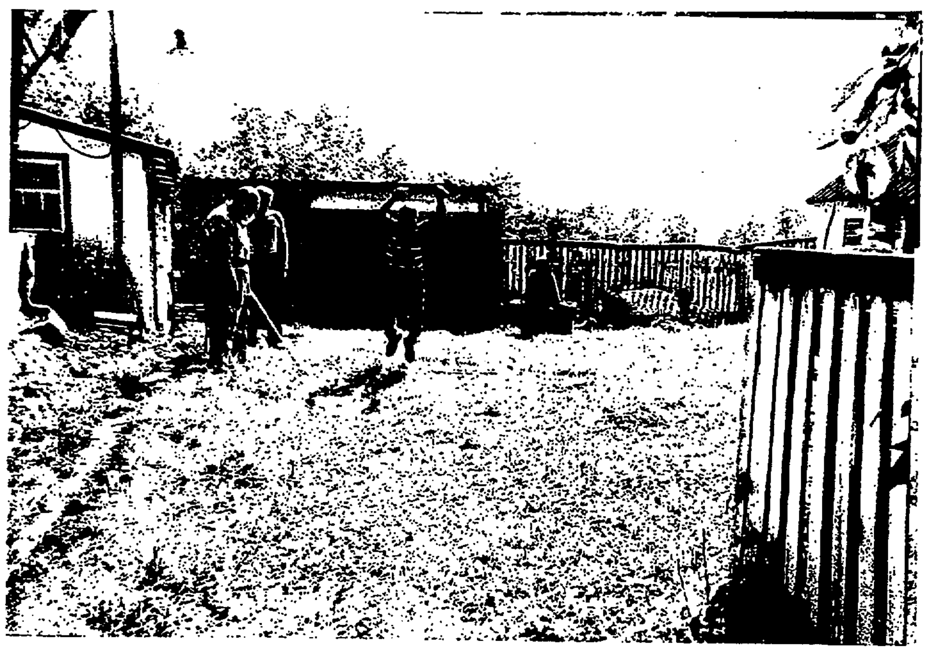

Figure B-6. Agricultural workers performing broad jump.

Figure B-7. Control person carrying weights.

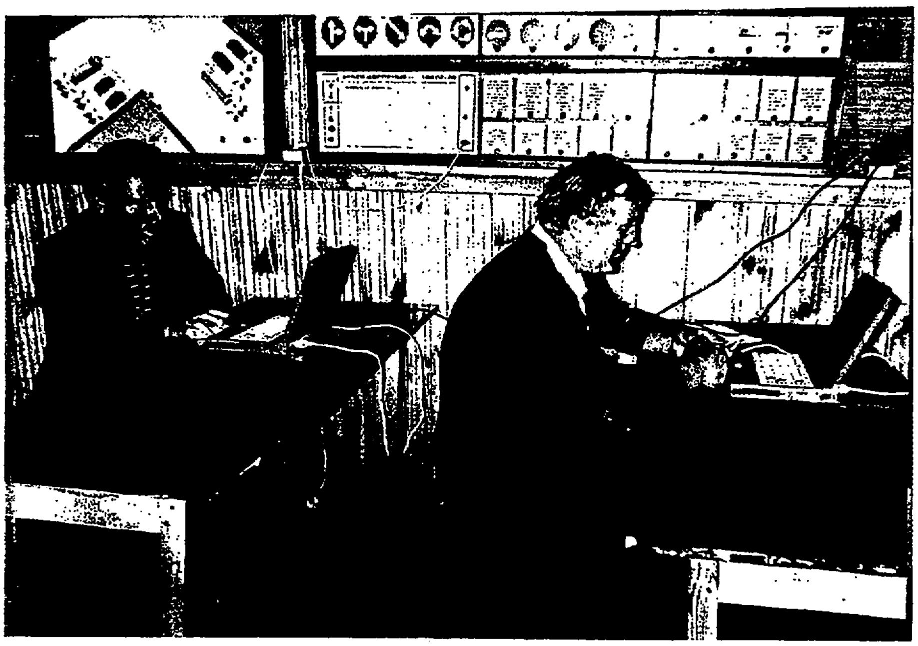

Figure B-8. Forestry workers performing ANAM.

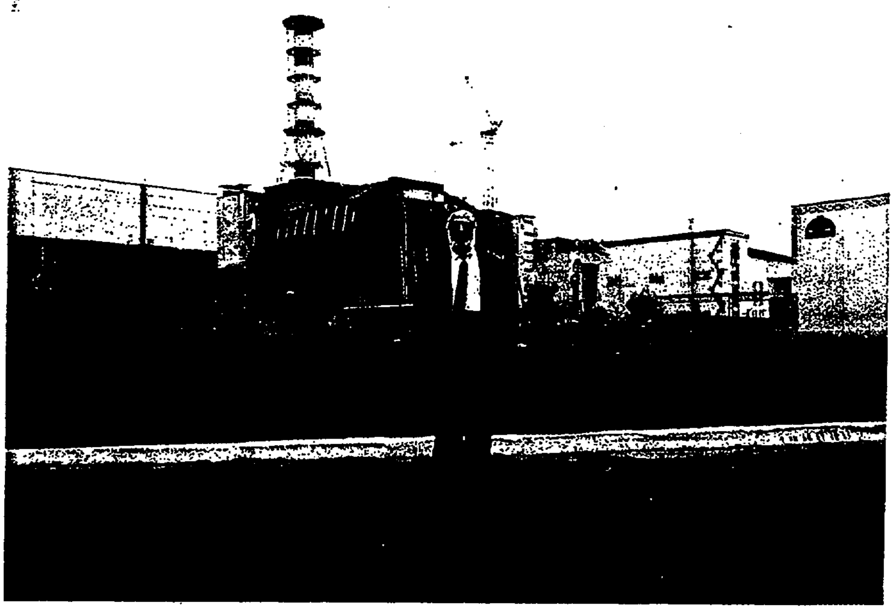

Figure B-9. Dr. Gamache at Chernobyl Nuclear Power Plant, 1997.

APPENDIX C
CONSENT FORM

Dear____

You are invited to participate as a VOLUNTEER in a 4-year MINIMAL RISK research project designed to test your physical and cognitive performance. This research is conducted by KGA International, Kiev Polytechnic Institute, and the Ukraine Center for Radiation Medicine. The research is planned for 1995-1998, and the testing will be carried out in the summer months and will require you to be tested, as scheduled. Complete testing will take one-half day.

Prior to testing you will be provided with instructions how to perform the tests. The physical part of testing is based on simple exercises that are easy to perform for any individual. The cognitive test will be performed on a computer with appropriate instructions in Russian.

If, during the testing, you feel ill or want to ask a question, notify your instructor immediately. If you are ill, the instructor will refer you to the medical staff. Inquries regarding instructions given MAY necessitate starting testing over again. Make sure to ask ALL questions prior to commencing the test procedure.

I, certify that I am a volunteer and all procedures and risks have been thoroughly explained to me. I also have the choice NOT to participate at any time.

Signature____
Date________________

APPENDIX D
GLOSSARY

2CH	Two-choice Reaction Time
AC	Control group
ACC	Accuracy
AE	Eliminator group
AF	Forester group
AG	Agricultural group
ANAM	Automated Neuropsychological Assessment Matrices
ANAM-ACC	ANAMUKR – accuracy scores
ANAM-EFF	ANAMUKR – efficiency sores
ANAMUKR	Special subset of ANAM created for this study
BALBEAM	Balance Beam
BROADJMP	Broad jump
CARRYWGT	Carrying weights
CDD	Code Substitution – delayed recall
CDI	Code Substitution – immediate recall
CDS	Code Substitution – visual search
COMP	Composite measure
CPT	Running Memory Continuous Performance Task
DECL	Decline
DECR	Decrement
DGS	Digit Symbol
EFF	Efficiency
GPAB	Gamache Physical Abilities Battery
MSP	Matching to Sample
SLP	Stanford Sleepiness Scale
SPD	Spatial Processing
SQUATTHR	Squat thrusts
SRT	Simple Reaction Time
TAP-L	Tapping – left index finger
TAP-R	Tapping – right index finger

DISTRIBUTION LIST

DEPARTMENT OF DEFENSE

DIRECTOR
ARMED FORCES RADIOBIOLOGY RSCH INST
INFORMATION SERVICES DEPARTMENT
8901 WISCONSIN AVENUE
BETHESDA, MD 20889-5603
ATTN: BHS
ATTN: EXH
ATTN: MRA
ATTN: RSD
ATTN: TECHNICAL LIBRARY

DEFENSE TECHNICAL INFORMATION CENTER
8725 JOHN J. KINGMAN ROAD, SUITE 0944
FORT BELVOIR, VA 22060-6218
ATTN: DTIC/OCP

DEFENSE THREAT REDUCTION AGENCY
6801 TELEGRAPH ROAD
ALEXANDRIA, VA 22310-3398
ATTN: TDA, C. MCFARLAND
ATTN: TDAC
ATTN: TDACC
ATTN: TDANP, TRC

DEFENSE THREAT REDUCTION AGENCY
ALBUQUERQUE OPERATIONS
1680 TEXAS STREET, SE
KIRTLAND AFB, NM 87117-5669
ATTN: TDTO

DIRECTOR
DISA
TECHNICAL RESOURCES CENTER
7010 DEFENSE PENTAGON
WASHINGTON, DC 20301-7010
ATTN: JNGO

PRESIDENT
NATIONAL DEFENSE UNIVERSITY
FORT LESLEY J. MCNAIR
WASHINGTON, DC 20319-6000
ATTN: ICAF, TECH LIB
ATTN: LIBRARY, STOP 315

DIRECTOR
NET ASSESSMENT
OFFICE OF THE SEC OF DEFENSE
ROOM 3A930, THE PENTAGON
WASHINGTON, DC 20301
ATTN: DOCUMENT CONTROL

HEADQUARTERS
US EUROPEAN COMMAND
UNIT 30400 BOX 1000
APO AE 09128
ATTN: ECJ5-N

USSTRATCOM/J531T
901 SAC BOULEVARD, SUITE-BB11
OFFUTT AFB, NE 68113-5160
ATTN: J-521

DEPARTMENT OF DEFENSE CONTRACTORS

INSTITUTE FOR DEFENSE ANALYSES
CONTROL & DISTRIBUTION
1801 N. BEAUREGARD STREET
ALEXANDRIA, VA 22311
ATTN: D. SCHULTZ

ITT INDUSTRIES
ITT SYSTEMS CORPORATION
ATTN: AODTRA/DTRIAC
1680 TEXAS STREET, SE
KIRTLAND AFB, NM 87117-5669
ATTN: DTRIAC
ATTN: DTRIAC/DARE

JAYCOR
1410 SPRING HILL ROAD, SUITE 300
MCLEAN, VA 22102
ATTN: DR C. P. KNOWLES

PACIFIC-SIERRA RESEARCH
OPERATING COMPANY OF VERID
29801 28TH STREET, 2ND FLOOR
SANTA MONICA, CA 90405
ATTN: G. ANNO
ATTN: H. BRODE
ATTN: L. MATHESON

PACIFIC-SIERRA RESEARCH CORPORATION
WASHINGTON OPERATIONS
1400 KEY BOULEVARD, SUITE 700
ARLINGTON, VA 22209
ATTN: G. MCCLELLAN

PSYCHOLOGICAL RESEARCH CENTER
8 ALTHEA STREET
ST AUGUSTINE, FL 32095
ATTN: D. L. REEVES
ATTN: D. M. LEVINSON
ATTN: L. GAMACHE
ATTN: P. I. BIDIOUK

SCIENCE APPLICATIONS INT'L CORPORATION
10260 CAMPUS POINT DRIVE
SAN DIEGO, CA 92121-1578
ATTN: D. KAUL, MS-33
ATTN: E. SWICK, MS-33

UNIVERSITY OF CINCINNATI MEDICAL CENTER
MAIL LOCATION 577
CINCINNATI, OH 45267
ATTN: E. SILBERSTEIN

DEPARTMENT OF ENERGY

UNIVERSITY OF CALIFORNIA
LAWRENCE LIVERMORE NATIONAL LAB
P. O. BOX 808
LIVERMORE, CA 94551-9900
ATTN: Z. DIVISION LIBRARY

SANDIA NATIONAL LABORATORIES
ATTN: MAIL SERVICES
P. O. BOX 5800
ALBUQUERQUE, NM 87185-0459
ATTN: TECH LIB, MS-0899

DEPARTMENT OF THE AIR FORCE

AIR UNIVERSITY LIBRARY
600 CHENNAULT CIRCLE
BUILDING 1405 - ROOM 160
MAXWELL AFB, AL 36112-6424
ATTN: AUL-LSE
ATTN: LIBRARY
ATTN: STRATEGIC STUDIES

ASSISTANT CHIEF OF STAFF
STUDIES AND ANALYSES AGENCY
1570 AIR FORCE PENTAGON
WASHINGTON, DC 20330
ATTN: AFSAA/SAMI

DIRECTORATE OF NUCLEAR
AND COUNTERPROLIFERATION
DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC 20330
ATTN: XOOSS

US AIR FORCE ACADEMY
2354 FAIRCHILD DRIVE, SUITE 3A22
USAF ACADEMY, CO 80840-6214
ATTN: LIBRARY

DEPARTMENT OF THE ARMY

DEPARTMENT OF THE ARMY
DEPUTY CHIEF OF STAFF FOR
OPERATIONS AND PLANS
THE PENTAGON
WASHINGTON, DC 20310-0460
ATTN: DAMO-SWN
ATTN: DAMO-ZXA

US ARMY MEDICAL RESEARCH &
DEVELOPMENT COMMAND
FORT DETRICH, BUILDING 722
FREDRICK, MD 21702-5012
ATTN: SGRD-PLE

US ARMY MODEL IMPROVEMENT STUDY
MANAGEMENT AGENCY
CRYSTAL SQUARE 2
1725 JEFFERSON DAVIS HIGHWAY SUITE 808,
ARLINGTON, VA 22202
ATTN: SFUS-MIS

COMMANDER
US ARMY NUCLEAR & CHEMICAL AGENCY
7150 HELLER LOOP, SUITE 101
SPRINGFIELD, VA 22150-3198
ATTN: MONA-NU

US ARMY RESEARCH LAB
5232 FLEMING ROAD
ABERDEEN PROVING GROUND, MD 21001-5067
ATTN: DIRECTOR
ATTN: SLCBR-D
ATTN: SLCBR-DD-T, TECH LIB
ATTN: SLCBR-TB

US ARMY RESEARCH LABORATORIES
2800 POWDER MILL ROAD
ADELPHI, MD 20783-1197
ATTN: TECH LIB

COMMANDER
US ARMY TEST & EVALUATION COMMAND
BUILDING 860
ABERDEEN PROVING GROUND, MD 21005
ATTN: STECS-NE, 70

DIRECTOR
US ARMY VULNERABILITY/LETHALITY
ASSESSMENT MANAGEMENT OFFICE
ABERDEEN PROVING GROUND, MD 21005-5001
ATTN: AMSLC-VL-NE, DR J. FEENEY

SUPERINTENDENT
US MILITARY ACADEMY
WEST POINT, NY 10996
ATTN: DEPT OF BEHAVORIAL
SCI & LEADERSHIP

DIRECTOR
WALTER REED ARMY INSTITUTE OF RESEARCH
6825 16TH STREET, NW
WASHINGTON, DC 20307-5100
ATTN: SLRD-UWI

DEPARTMENT OF THE NAVY

PRESIDENT
NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207
ATTN: LIBRARY, CODE 1E22

OTHER GOVERNMENT

NATIONAL ARCHIVES & RECORDS
ADMINISTRATION
8601 ADELPHI ROAD, ROOM 3360
COLLEGE PARK, MD 20740-6001
ATTN: USER SERVICE BRANCH

Exhibit 3

Dumas, Lloyd J. 1999. *Lethal Arrogance: Human Fallibility and Dangerous Technologies*. St. Martin's Press, New York, NY.

Excerpts:

Prologue: *Will Twentieth-Century Incidents Become Twenty-First-Century Nightmares?*
Chapter Two: *Terrorism and Dangerous Technologies*
Chapter Seven: *The Fallability of Individuals: The Nature and Conditions of Life and Work.*
Chapter Nine: *The Failure of Technical Systems*
Notes

Lethal Arrogance

HUMAN FALLIBILITY AND DANGEROUS TECHNOLOGIES

Lloyd J. Dumas

St. Martin's Press

LETHAL ARROGANCE

For information, address St. Martin's Press, 175 Fifth Avenue, New York, N.Y. 10010.

ISBN 0-312-22251-3

Library of Congress Cataloging-in-Publication Data

Lethal Arrogance : human fallibility and dangerous technologies / Lloyd J. Dumas.
p. cm.
Includes bibliographical references and index.
ISBN 0-312-22251-3 (cloth)
1. Technology—Risk assessment. 2. Technology—Social Aspects.
I. Title.
T174.5.D86 1999
303.48'3—dc21 99-31677
CIP

Book design by ACME Art Inc.

10 9 8 7 6 5 4 3 2 1
08 07 06 05 04 03 02 00 01 99

TABLE OF CONTENTS

PART III
WHY IT CAN HAPPEN HERE:
THE MANY SIDES OF HUMAN FALLIBILITY

PART IV
WHY IMPROVING TECHNOLOGY WON'T SAVE US

PART V
WHAT CAN AND MUST BE DONE

PROLOGUE

Will Twentieth-Century Incidents Become Twenty-First-Century Nightmares?

NUCLEAR DISASTER: WAITING IN THE WINGS?

Suddenly, tons of highly toxic nuclear waste erupt like a volcano. Hundreds of people are killed outright, many thousands more exposed to dangerous ionizing radiation and forced to relocate. Close to 400 square miles of land becomes so contaminated with deadly radioactivity that it is rendered uninhabitable.

A scenario from the fertile if paranoid mind of a television screenwriter? No, a real-life disaster in the former Soviet Union, covered up for more than thirty years. In the late 1950s, during the height of the Cold War, the buildup of heat and gas in stored nuclear weapons waste caused an explosion that devastated the countryside near Kyshtim in the Ural Mountains. Think it couldn't happen here?

On July 23, 1990, more than 30 years after disaster at Kyshtim, the report of a U.S. government advisory panel warned that something very much like it could indeed happen here. The panel was headed by John Ahearne, a physicist who was formerly a high official in the Departments of Defense and Energy and chair of the U.S. Nuclear Regulatory Commission.

There are millions of gallons of highly radioactive waste, accumulated during four decades of producing plutonium for nuclear weapons, stored in 177 tanks at the Department of Energy's Hanford nuclear reservation in Washington state. The study argued that heat generated inside the tanks or a shock from the outside could cause one or more of them to explode. Although the explosion would not itself be nuclear, it would throw a huge amount of radioactivity around. How imminent is the danger?

According to the panel, "Although the risk analyses are crude, each successive review of the Hanford tanks indicates that the situation is a little worse." According to the *New York Times*, as of July 1990, "Experts outside the Department of Energy say the risk of explosion is now so high that the department has imposed a moratorium on all activity at one tank because of fear that a jolt or spark could detonate the hydrogen that has built up inside the tank."[1]

Hanford's long-term plan to solve the problem is to get the liquid wastes out of the sometimes leaky tanks, turn them into a glass-like solid form and bury them. But some engineers are afraid that parts of this very process that is intended to make waste storage safer will actually make an explosion more likely.

THE TERROR UNDERGROUND

Like characters in a grade-B horror film, they emerged from under the ground by the thousands, choking and gasping for air, some with blood streaming from the nose or mouth. But this horror was all too real. In a carefully timed attack, terrorists had set off at least five canisters of deadly nerve gas at almost the same time in the tunnels of three different subway lines beneath the streets of Tokyo.

More than 5,500 people were injured in the attack, which came at the peak of the Monday morning rush hour, 12 of them fatally. It is something of a miracle that many more did not die. Tokyo subway trains are packed at rush hour, and sarin, the Nazi-era nerve gas released, is 500 times more toxic than cyanide, the gas used for executions in the United States. Half a milligram is a lethal dose.

Leaders of the wealthy Japanese end-time religious cult known as Aum Shinrikyo were later arrested and charged with the attack. It seems that the ghastly assault on Tokyo was to be just the beginning. When thousands of police officers raided dozens of Aum Shinrikyo buildings around Japan, they found gas masks, tons of chemicals and sophisticated chemical manufacturing equipment. They also found evidence that the cult might have been trying to develop biological weapons. And they found a cult newsletter warning that by the end of 1996, 90 percent of the people living in major cities like Tokyo would be killed by earthquakes, epidemics—or poison gas.

Sarin was specifically mentioned by name.

"HOLES IN THE FENCES EVERYWHERE"

Enriched uranium is standard fuel for the Russian nuclear navy. If it is enriched enough, it is also the stuff of nuclear weapons.

In the early afternoon of November 27, 1993, two guards patrolling the Sevmorput shipyard, one of the Russian navy's main nuclear fuel storage depots, saw a discarded padlock lying on the ground. They noticed that the door of a nearby storehouse was open. When they looked inside, they found that 4.5 kilograms (10 pounds) of enriched uranium was missing.

Six months later, three men were arrested and the stolen fuel recovered. The man charged with breaking the padlock on the door and stealing the uranium was the deputy chief engineer at the shipyard. The man accused of hiding the stolen uranium was a former naval officer. And the alleged mastermind of the operation was the manager in charge of the refueling division at the shipyard!

Although this theft had been an inside job, stealing uranium from Sevmorput was apparently not that big a challenge. According to Mikhail Kulik, the chief investigator, "'On the side [of the shipyard] facing Kola Bay, there is no fence at all. You could take a dinghy, sail right in—especially at night—and do whatever you wanted. On the side facing the Murmansk industrial zone there are . . . holes in the fences everywhere. And even in those places where there aren't holes, any child could knock over the half-rotten wooden fence boards.'"[2] In Kulik's view, if the amateur thief had not made the bush-league mistake of leaving the door open, the theft at Sevmorput "could have been concealed for ten years or longer."

BAD YEAR AT BANGOR

At the end of the Cold War, Bangor, Washington, was one of the most heavily armed cities in the world. With some 1,700 nuclear weapons at the Bangor Submarine Base and more stored at the Strategic Weapons Facility nearby, there was enough nuclear firepower in Bangor to destroy any country on earth many times over.

More than a thousand military personnel in the area were on active nuclear duty, certified by a special Pentagon program as physically and mentally reliable. Yet just how reliable were they?

One of those certified as reliable was an 18-year-old marine, Lance Corporal Patrick Jelly. Claiming to be a reborn soldier killed in Vietnam, he punctured his arms with a needle and thread. For weeks he had threatened to kill himself. Still he was kept on active duty. At 9:30 P.M. on January 14, 1989, while standing guard over the fearsome nuclear arsenal stored at the Strategic Weapons Facility, Jelly finally made good on his threat. The troubled young marine aimed an M-16 rifle at his head and pulled the trigger. Jelly had remained certified as reliable until the night he died.

Tommy Harold Metcalf was also certified as physically and mentally fit. He was a fire-control technician aboard the Trident submarine *Alaska*, part of the team directly responsible for launching the ship's nearly 200 city-destroying nuclear warheads. On July 1, 1989, Metcalf suddenly went to the home of an elderly couple and murdered both of them by suffocation.

William Pawlyk had been commander of Submarine Group 9 at Bangor and had served aboard the nuclear submarine *James K. Polk* for five years. In early August 1989, Commander Pawlyk was arrested after stabbing a man and a woman to death. He was head of a naval reserve unit in Portland, Oregon, at the time of the murders.

Shyam Drizpaul was assigned to duty aboard the nuclear submarine *Michigan*. Like Tommy Metcalf, he was part of the missile launch team, certified as physically and emotionally healthy. On January 15, 1990, he shot and killed a fellow crew member in the lounge at his living quarters, then another in bed. Afterward, while attempting to buy a pistol at a pawnshop, Drizpaul grabbed the gun from the clerk, shot her to death and critically wounded her brother. Fleeing the scene of that crime, he checked into a motel near Vancouver and used the same weapon to kill himself. A subsequent Navy investigation discovered that Drizpaul drank heavily, carried an unregistered hand gun, and boasted of having been trained as an assassin.

All of these incidents occurred between mid January 1989 and mid January 1990. It had been a bad year at Bangor.[3]

A WARNING

If you are thinking that there is something unreal, something unique about this set of stories, think again. Not only are these stories real, they are anything but unique. They turn on problems of human fallibility and technical failure that are embedded in the fabric of everything we do.

Our brilliant technological accomplishments have made us too complacent, too arrogant about our ability to control even the most dangerous technologies we create and permanently avoid disaster. But we will not, because we cannot.

We humans are fallible. We are not perfect, and never will be. Understanding the many-sided nature of our unavoidable fallibility and how it interacts with the most dangerous technologies we create is the key to the fundamental change that can lead us away from disaster. It is what this book is all about.

If we do not fundamentally change the way we do things, these frightening twentieth-century incidents may just be the forerunners of still more horrifying twenty-first-century nightmares.

If you think that I am exaggerating, that it can't really be that bad, read on.

CHAPTER TWO

Terrorism and Dangerous Technologies

Eighteen minutes after noon on February 26, 1993, a blast shook the twin 110-story towers of New York's World Trade Center with the force of a small earthquake. A van loaded with some 1,200 pounds of powerful explosive had blown up in the underground garage. Walls and floors collapsed, fires began to burn and smoke poured into hallways and stairwells darkened by the loss of power. Dozens were trapped for hours in many of the Center's 250 elevators caught between floors. An estimated 40,000 people in the hundreds of offices and miles of corridors of Manhattan's largest building complex had to find their way out amidst the smoke, darkness and confusion. It took some of them most of the day to escape. When it was all over, six people were dead, more than a thousand were injured and property damage was estimated at half a billion dollars.[1]

The bombing of the World Trade Center was the worst terrorist incident on American soil—until the morning of April 19, 1995. A rented truck packed with more than 4,000 pounds of explosive made of widely available fertilizers, chemicals and fuel sat parked by the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma. Just after 9:00 A.M., when the building's workers were at their jobs and the second floor day care center was filled with young children at play, the truck blew up with a deafening roar. Walls, ceilings and much of the building's north face came down in an avalanche of concrete, steel and glass. The blast left a crater 20 feet wide and 8 feet deep, overturned cars, damaged 6 nearby buildings, and set dozens of fires. Nearly 170 people were killed, including many of the children in the day-care center, and hundreds were injured. A building that was much smaller than the World Trade Center, in a city a fraction of the size of New York, had sustained a terrorist attack that took nearly 30 times as many lives.[2] Terrorism had come to America's heartland.

As terrible as these attacks were, they are dwarfed by the mayhem that could be caused by a successful terrorist assault on a nuclear power plant, toxic chemical manufacturing facility or radioactive waste storage site. Worse yet, imagine the magnitude of disaster that could be unleashed by terrorists armed with weapons of mass destruction. Even a crude, inefficient, homemade nuclear weapon would have turned the World Trade Center into rubble and taken the lives of more than 40,000 people. A more efficient weapon could have leveled much of Oklahoma City.

THE NATURE OF TERRORISM

Not every form of violent, destructive, antisocial activity is terrorism. Nor is terrorism defined by the ultimate goals terrorists seek to achieve. Calling violent groups "terrorists" when we don't like their objectives and "freedom fighters" when we do is a political game. It won't help us understand what terrorism is, judge how likely terrorists are to use dangerous technologies, or figure out what can be done about it. Instead, we need a working definition that is more than just propaganda or opinion.

Terrorism can be defined by its tactics and strategy: it is violence or the threat of violence carried out with the express purpose of creating fear and alarm. When an armed gang shoots bank guards in order to steal money, that is a violent crime, not an act of terrorism. The violence is perpetrated to stop the guards from interfering with the theft, not to frighten the wider population. But when a gang randomly plants bombs on city buses, they are not trying to stop the passengers from interfering with them, they are trying to frighten people. Their acts are intended to have effects that reach well beyond the immediate damage they are causing or threatening to cause. Whether their objective is to force the government to release political prisoners or to extort a ransom, they are terrorists because they are trying to terrorize.[3] Unlike other criminals, terrorists usually try to draw attention to themselves, often claiming "credit" for the acts they have committed. In many ways, terrorism is a perverse form of theater in which terrorists play to an audience whose actions—and perhaps, opinions—they are trying to influence. When terrorists hijack an aircraft, they may be playing to an audience of corporate managers who can assemble a ransom, government officials who can order their imprisoned comrades released, or whoever else has the power to meet their demands. But they are also playing to the public, whose mere presence as well as opinions and actions can put pressure on those in power to do what the terrorists want done. Those actually taken hostage on the plane cannot meet the terrorist demands, any more than can those maimed when a pub is bombed or killed by a murderous spray of gunfire in a hotel lobby. Nor are they in any position to apply pressure to the people who have that power. They just happened to be in the wrong place at the wrong time. Innocent victims, they have become unwitting players caught up in a real-life drama, the cannon fodder of terrorism.

Terrorists are trying to make the public feel vulnerable, unsafe, helpless. In some cases, choosing victims at random is the best way to accomplish this. If there is no clear pattern as to which particular bus is blown up, which airliner hijacked, which building bombed, there is no obvious way to avoid becoming a victim. That is very frightening. On the other hand, if the terrorist objective is more targeted, choosing victims randomly but within broadly defined categories may be more effective. The mercury poisoning of Israeli oranges in Europe in the late 1970s was targeted randomly but only at consumers of Israeli produce. It was intended to damage Israel's economy by creating fear that their agricultural exports were unsafe.[4] Economic damage was also the goal of the terrorist who poisoned some of the Johnson & Johnson Company's painkilling Tylenol capsules with lethal cyanide in the early 1980s.[5] The targets of the Oklahoma City bombing were also neither purely random nor very specific, but were chosen to intimidate federal employees and users of federal services, to express broad ideological antipathy to the government.

In sum, acts intended to instill fear in the public, committed against more or less randomly chosen victims not themselves able to meet the attackers' demands, define terrorism and set it apart from many other forms of violence. Bombing the barracks of an occupying military force is an act of war, violent and murderous, but it is not an act of terrorism. It attacks those who are directly involved in the activity the attackers are trying to oppose, not randomly chosen innocent victims. The act of a habitual sex offender in kidnapping, raping and murdering a more or less randomly chosen innocent victim is a vicious and brutal crime, but it is also not terrorism. Though it may well instill fear in the public, it is not done for that purpose, and it is not done to influence public opinion or behavior. Suicide bombing a city marketplace to precipitate a change in government policy is an act of terrorism. The more or less randomly chosen victims cannot directly change government behavior, but the indiscriminate slaughter is intended to shock and frighten people into demanding that the government change direction by convincing them that they will be in danger until those policies change. Whether or not the bombing achieves that objectiv the act itself is still an act of terrorism.

It is important to emphasize that there is nothing in the definition of terrorism that prejudges the legitimacy or desirability of the terrorists' ultimate goals. Whether a group is trying to overthrow a legitimate democratic government and establish a rigid dictatorship, create a homeland for a long-disenfranchised people, trigger a race war, or get more food distributed to malnourished poor people, if the group uses terrorist means, it is a terrorist group.

Terrorism may be despicable, but it is not necessarily irrational. There are a variety of reasons why subnational groups with clearly political goals sometimes choose terrorist tactics to undermine support for the government and/or its policies. Domestic terrorist groups may believe that this is an effective way of convincing the public that the government does not deserve their support because it cannot keep them safe. Or they may believe that provoking widespread and repressive counterterrorist measures will turn the public against the government by exposing just how brutal and overbearing it can be. As paradoxical as it may seem, terrorist groups clearly believe that the end result of their terrible random acts of violence will be an uprising of the public against the government and increased support for the group's political agenda.

Since international terrorists attack only foreigners and their property ar usually claim to be the avenging arm of their oppressed brothers and sisters, is easier to understand why they might believe that their brutal actions will build public support for their cause at home. They may also see international terrorism as the only way to shock the world into paying attention to the plight of their people. For subnational groups, it is certainly true that terrorism is the "weapon of the weak." A powerful and influential group would not need to resort to such desperate and horrible tactics to make itself heard.

There is a tendency to think of terrorists as either small, disconnected groups of half-crazy extremists or expert paramilitary cadres bound tightly together in grand international conspiracies. In fact, the reality most often lies in between. It is true that terrorist groups do cooperate across ideological and political boundaries, sometimes even "subcontracting" with each other or carrying out joint attacks. But these coalitions are typically loose and transitory. Japanese Red Army terrorists, for example, carried out a grenade and rifle attack planned by the Popular Front for the Liberation of Palestine (PFLP) against a crowd of 250 people at Lod Airport near Tel Aviv in 1972, killing 27 and wounding 80 more.[6] Yet this was not a stable, tightly organized alliance. By the mid 1990s, white supremacist, antisemitic, paramilitary groups in the United States had established extensive networks of communication, cooperation and support, but th had by no means coalesced into a single, centrally controlled organization.[7]

Governments and Terrorism

Terrorism is not only a tactic of subnational groups. Governments can, and all too often do, carry out terrorist acts. In fact, the term "terrorist" appears to have first been applied to the activities of a government, the Jacobin government of France after the French Revolution.[8] The Nazi Gestapo, Iranian Savak and many other "secret police" organizations in many other countries have deliberately terrorized the population to suppress opposition and force the public to submit to the edicts of brutal governments. Because of the resources at their command, when governments engage in terrorism, their actions are often far more terrifying than the acts of subnational terrorists.

Governments have sometimes carried out official campaigns of terrorism. The Ethiopian government launched what it called the "red terror" in reaction to a revolutionary group's "white terror" campaign in the late 1970s. Within two months, more than a thousand people were killed, many of them teenagers. Their dead bodies were displayed in public squares with signs hung on them saying "The red terror must crush the white terror."[9] In 1998, testimony before South Africa's Truth and Reconciliation Commission revealed an apartheid-era campaign of chemical and biological attacks intended to murder political opponents.[10]

State-Sponsored Terrorism

The term "state-sponsored terrorism" has at times been used too loosely to brand the activities of governments with which we disagree. But there is a reality beyond the name-calling. Governments sometimes do directly aid subnational groups that stage attacks in the homelands or against the interests of opposing governments, groups that are "terrorist" by any reasonable definition of the term. Governments have provided safe havens, intelligence, weapons and even training. On the specious theory that "the enemy of my enemy is my friend," the United States, Saudi Arabia and others flooded Afghani revolutionary forces with weapons and money after the Soviet military intervened in support of the Afghan government in 1979. Much of it went to groups in Peshawar, the capital of Pakistan's Northwest Frontier province bordering Afghanistan. Long a violent area, the money and guns helped Peshawar descend deeper into lawlessness. According to a high-ranking officer, the Pakistani military was directly involved in training something like 25,000 foreign volunteers to fight with the Afghan guerillas. Most were Arabs, but there were also Europeans, Asians and some Americans. After the Soviets withdrew from Afghanistan in 1989, a large number of the foreign volunteers who survived the war stayed in and around Peshawar, working with organizations that have been accused of being fronts for international terrorist groups.[11]

In 1995, Pakistani police officials had the University of Dawat and Jihad in Peshawar under investigation. The officials claimed that the university may actually have been the training ground for terrorists responsible for attacks in the Philippines, Central Asia, the Middle East, North Africa and possibly North America. Ramzi Ahmed Yousef, convicted of both the 1993 bombing of New York's World Trade Center and a 1995 plot to blow up a dozen American airliners in East Asia, had used Peshawar as a base.[12] Several of the eight men arrested by the FBI later in 1993 and accused of plotting to blow up car bombs at UN headquarters, the Lincoln and Holland Tunnels and several other sites in New York City were involved in the Afghan War.[13] So too was Osama bin Laden, the Saudi businessman widely touted by the United States as a financier of anti-American terrorists in the 1990s. In the words of one senior Pakistani official, "Don't forget, the whole world opened its arms to these people. They were welcomed here as fighters for a noble cause, with no questions asked.... [N]obody thought to ask them: when the Afghan Jihad is over, are you going to get involved in terrorism in Pakistan? Are you going to bomb the World Trade Center?"[14]

Nuclear deterrence, a mainstay of the official security policy of the nuclear weapons states, is itself a form of international terrorism. Nuclear deterrence does not so much threaten to annihilate the leaders of opposing governments—those with the power to make decisions of war or peace—as it holds hostage and threatens to destroy the ordinary people of the opposing nation if their government decides to attack. Even in democracies, the general public under threat is not in a position to control the decision of their government to launch a nuclear attack. No referendum has ever been planned for "button pushing" day. That is even more true of the public in authoritarian countries.

Furthermore, the underlying objective of threatening nuclear attack is precisely to create such widespread fear that the opposing government will feel enormous pressure to avoid any behavior that would result in the threat being carried out. This is terrorism, plain and simple. In fact, during the Cold War, the threat of "mutually assured destruction" was officially called a "balance of terror." And a balance of terror is still terror.

Though it does not legitimize or excuse the use of terrorist tactics by subnational groups, the fact is even democratic governments have provided th something of a model for this type of behavior.

THE TERRORIST THREAT OF MASS DESTRUCTION

Terrorists have not yet committed violence on anywhere near the scale that would result from a successful attack on a nuclear power plant, toxic chemical manufacturing facility or hazardous waste dump. They have not yet used a homemade, store-bought or stolen nuclear weapon. They have not yet contaminated the water supply of a city or the air supply of a major building with deadly chemicals or virulent bacteria. Why not?

If it is because they do not have and cannot develop the capability to use dangerous technologies as a weapon or a target, we can relegate these frightening scenarios to the realm of science fiction and breathe a collective sigh of relief. But if instead the capability to do such nightmarish damage is within their reach, it is important to know what is holding them back. Is it just a matter of time before this modern-day horror becomes real?

Because their actions seem so immoral, abhorrent and repulsive, we usually assume that terrorists will do whatever harm they are capable of doing. But though their methods are similar, not all terrorists are alike. Some may actively seek the capability for committing mayhem that dangerous technologies provide, while others have no desire to do that much damage. It would be very useful to know which is which. At best, that might help us formulate more effective strategies for preventing a terrorist-induced catastrophe. At least, we would know what kinds of groups need to be most closely watched.

Then there is the biggest question of all: whatever the reason terrorists have not yet committed such atrocities, is there any reason to believe this restraint will continue?

Can Terrorists "Go Nuclear"?

Despite high priority and lavish government funding, it took years for a collection of the most brilliant scientific minds of the twentieth century to develop the first nuclear weapon. Potent nerve gas weapons emerged from technically advanced laboratories run by teams of highly trained chemists. A great deal of engineering and scientific effort has gone into designing nuclear power plants. They are protected by layers of backup and control systems intended to make catastrophic failure very unlikely, whether by accident or sabotage. Are terrorists really sophisticated enough to get their hands on and successfully use dangerous technologies as weapons or as targets of their attacks?

The image of the terrorist as a demented fanatic who stashes a suitcase full of dynamite sticks wired to a crude timing device in some forgotten corner of a building is out of step with the times. Such crude forms of terrorism can still be very effective. But terrorists and criminals using terrorist tactics have long sir shown themselves capable of much greater tactical and technological sophistication. In August 1980, a box as big as a desk was delivered to the executive offices of Harvey's Casino in Stateline, Nevada. A three-page extortion note sent to the management warned that the box contained a bomb that would explode if any attempt was made to move it. Not knowing whether the threat was real, casino managers called in bomb experts from the FBI, the Army bomb disposal team and the U.S. Department of Energy (the agency in charge of nuclear weapons research and manufacture). They examined the plastic covered box carefully. X-rays revealed that it contained 1,100 pounds of explosives. The experts were struck by the highly sophisticated design of the device, but nevertheless believed they could safely disarm it. They were wrong. The bomb exploded, doing $12 million worth of damage to the casino.[15]

If there was any lingering doubt about the possibility that technologically advanced subnational terrorist groups could arise, it was dispelled in the mid1990s by the emergence of the Japanese doomsday cult Aum Shinrikyo. Nearly a dozen of the sect's top leaders were educated in science and engineering at top Japanese universities, as were some other members. When the police arrested members of the cult and accused them of using sarin nerve gas in a March 1995 attack on the Tokyo subways, they found hidden laboratories at the cult's compounds that could manufacture the gas. They charged that Aum also had facilities capable of producing biological warfare agents. Furthermore, Japanese police reportedly suspected that the purpose of the 1993 visit of a high cult official to Australia was to obtain uranium to be used in building nuclear weapons.[16]

As discussed in chapter one, thousands of people have been trained in designing nuclear weapons in the United States, the former Soviet Union, Britain, France and China over the past 50 years. These are people of widely differing political, ideological and religious views, personalities and life circumstances. Many of Russia's nuclear scientists are now living in such economic deprivation that the United States allocated $30 million in 1999 to help create nonmilitary jobs for them in the hope of discouraging them from selling their expertise to rogue nations or terrorists.[17] Can we really be sure that no terrorist political group or religious cult will ever be able to recruit, coerce or buy off any of these experienced weapons designers?

Unfortunately, the degree of technical sophistication required to acquire or use dangerous technologies as weapons is actually much lower than many people think. Poison gas can be made with the chemicals most of us have around the house. As long ago as 1977, a British military research laboratory was openly advertising the sale of infectious organisms at bargain-basement prices, including three strains of *Escherichia coli.*[18] That is the same bacterium that was responsible for a mysterious epidemic of food poisoning that shut down the entire Japanese school system during the summer of 1996. More than 9,400 people were sickened and 10 died.[19]

In March 1995, four members of the right-wing Minnesota Patriots Council were convicted in federal court of conspiracy to use ricin, a deadly biological toxin, to kill federal agents. They had manufactured enough to kill 1,400 people using information in a manual they bought from a mail order house.[20] Two months later, a member of the American white supremacist group Aryan Nations was arrested for (and subsequently pled guilty to) making another mail-order purchase—three vials of frozen bubonic plague bacteria—obtained using false credentials from the food-testing laboratory at which he worked.[21] What about nuclear weapons?

Designing a Terrorist Nuclear Weapon

The "secret" of designing nuclear weapons is out, accessible in the public literature to anyone moderately well trained in the physical sciences or engineering. More than 20 years ago, the Public Broadcasting System's *NOVA* science television series recruited a 20-year-old chemistry student at the Massachusetts Institute of Technology and gave him the assignment of designing a workable atomic bomb. He was required to work alone, without any expert assistance, and to use only publicly available information. He began by simply looking up references in the college science library. In the student's words,

> the hard data for how big the plutonium core should be and how much TNT I needed to use I got from Los Alamos reference books [purchased from the National Technical Information Service in Washington for about $5 each] and also other reference books I checked out of the library.
>
> . . . I was pretty surprised about how easy it is to design a bomb. When I was working on my design, I kept thinking there's got to be more to it than this, but actually there isn't.[22]

Only five weeks later, the student's fully documented, detailed report was given to a Swedish nuclear weapons expert for evaluation. The verdict: a fair chance that a bomb built to this design would go off, though the explosion would probably be no more than the equivalent of 1,000 tons of TNT, more likely less than 100.

The design was crude and unreliable, the yield unpredictable and small by nuclear standards—it would not be an acceptable military weapon. But none of these deficiencies is much of a problem for terrorists used to unreliable bombs with unpredictable yields. An explosion equivalent to even 50 tons of TNT would be gigantic by terrorist standards. That is 25 times as powerful as the explosives used in the Oklahoma City and World Trade Center bombings. Imagine what would have happened had those blasts been 25 times as powerful. Then add the death and destruction that would have been caused by the enormous release of heat and radiation from this crude nuclear weapon—designed by one undergraduate student in less than two months.

One year later, a senior at Princeton University duplicated this design feat, and then some. Working from publicly available sources and taking more time, he designed a 125-pound device about the size of a beach ball, which he estimated would explode with the force of about 5,000 tons of TNT. A specialist in nuclear explosives engineering reviewed the student's 34-page term paper, declaring that the bomb design was "pretty much guaranteed to work."[23]

In April 1979, FBI Director William Webster said that sufficient information was available in public libraries to design a nuclear weapon small enough to be carried on a terrorist's back.[24] A few months later, the *Progressive* magazine published an article called "The H-Bomb Secret."[25] The author, a journalist named Howard Morland, had unearthed enough detail about the design of the much more powerful hydrogen bomb that the U.S. government took Morland and the *Progressive* to court to prevent the article's publication on grounds of national security. After a long battle, the court refused to enjoin its publication because all of the information it contained was shown to be available in sources that had already been public for years. This included a report giving precise specifications for the key hydrogen bomb trigger mechanism and other important design details. It had been on the public shelves in Los Alamos since 1975. The Department of Energy argued that they should never have declassified the report and made it available. Why did they? It was simply a matter of human error.[26]

Building a "Homemade" Nuclear Bomb

Skeptics often argue that designing a weapon on paper may not be all that difficult, but actually building a nuclear bomb would require large teams of people with advanced skills and access to materials and equipment that is expensive and difficult to come by. Ted Taylor, a noted physicist and the Los Alamos nuclear weapons designer credited with the most efficient A-bomb ever designed, disagrees. In his view,

> Under conceivable circumstances, a few persons, possibly even one person working alone, who possessed about ten kilograms of plutonium oxide and a

substantial amount of chemical high explosive could, within several weeks, design and build a crude fission bomb . . . that would have an excellent chance of exploding, and would probably explode with the power of at least 100 tons of chemical high explosive. This could be done using materials and equipment that could be purchased at a hardware store and from commercial suppliers of scientific equipment for student laboratories.

The key person or persons would have to be reasonably inventive and adept at using laboratory equipment and tools of about the same complexity as those used by students in chemistry and physics laboratories and machine shops.[27]

The M.I.T. undergraduate who designed the workable A-bomb for *NOVA* estimated that if he had the plutonium, he could actually build the bomb from scratch in a year or less, with the help of three to four people and no more than $30,000 for supplies purchased from ordinary commercial sources. The finished product would be about as big as a desk, and weigh 550 to 1000 pounds.[28] In other words, it would be roughly the size and weight of the box terrorists delivered to Harvey's Casino in Nevada five years later. A 1980 article published in the British magazine *New Scientist* gave new meaning to the phrase "home-made bomb." It outlined a method for turning an ordinary two story house (with basement) into an atomic bomb! Aside from the 30 to 37 pounds of nuclear material required, the plan only called for about 20 feet of black iron pipe, 2 sticks of dynamite, 15 sacks of cement, 20 cubic yards of sand and gravel and a few easily obtainable miscellaneous bits and pieces. According to the author, such a bomb "detonated in New York City, ought to kill perhaps 250,000 people and injure another 400,000 . . . more than adequate for the average terrorist."[29]

Are the Necessary Nuclear Materials Available?

There are about a thousand metric tons of plutonium contained in stored spent fuel from nuclear power plants. That is four times as much plutonium as has been used in making all of the world's nuclear weapons.[30] For a long time now, the public has been told that nuclear weapons cannot be built from this "reactor grade" plutonium without an expensive and technically complex refinement process: it is much too heavily contaminated with plutonium-240 to be usable for a weapon. Not only is that untrue, it has definitively been known to be untrue for more than 30 years.

In 1962, the U.S. government assembled a nuclear bomb from the kind of low-grade, contaminated plutonium typically produced by civilian nuclear power plants, and brought it to the Nevada desert for secret testing. It blew up, producing "a nuclear yield."[31] Fourteen years later, a study done at the Lawr- Livermore nuclear weapons lab in California came to the conclusion "that the distinction between military and civilian plutonium was essentially false—that even relatively simple designs using any grade of plutonium could produce 'effective, highly powerful' weapons with an explosive yield equivalent to between 1,000 and 20,000 tons of TNT."[32]

Is it also possible to use uranium taken directly from nuclear power reactors? Natural uranium contains only 0.7 percent U-235, much too low a concentration to sustain a chain reaction in weapons. Although some nuclear power reactors use natural uranium, most use uranium enriched to higher levels of U-235. Uranium enriched to more than 90 percent is an excellent nuclear explosive, and is typical military weapons grade. But according to Ted Taylor, "It is probable that some kind of fission explosive with a yield equivalent to at least a few tens of tons of high explosive could be made with metallic uranium at *any enrichment level significantly above 10 percent*" (emphasis added).[33]

There are civilian nuclear power reactors fueled by 90 percent enriched uranium, but most use uranium less than 10 percent enriched. Military nuclear power reactors may use more enriched uranium. For example, most of the Russian Navy uses uranium fuel enriched to 20 to 45 percent.[34] Thus, the uranium used as fuel in many, but not all, nuclear power reactors could be u to make bombs without further enrichment. Lower enriched reactor fuel can still be used, but it would have to be processed to raise its concentration of U-235.

In 1996, *Time* reported that 17 scientists at the Los Alamos nuclear weapons laboratory were given the assignment of trying to design and build terrorist-type nuclear weapons using "technology found on the shelves of Radio Shack and the type of nuclear fuel sold on the black market." They successfully assembled more than a dozen "homemade" nuclear bombs.[35]

If terrorists were willing to settle for a device that dispersed deadly radiation without a nuclear blast, they would have a much wider variety of designs and nuclear materials from which to choose. The skills and equipment needed to build a dispersal device are also much simpler than those required for building a bomb.

Plutonium is so toxic that even a few grams would be enough for a radiological weapon. Dispersed as an aerosol in the ventilating system of a major office building, a few grams would pose a deadly threat to thousands of people. It wouldn't be an effective military weapon, but it would be nearly ideal for terrorists. Many other radioactive materials could also be used. Biological or chemical weapons dispersal devices would be even simpler. By one estimate, terrorist biological weapons might be developed at a cost of $100,000 or less "require five biologists, and take just a few weeks, using equipment that is reac available almost anywhere in the world."[36]

Getting Access to Nuclear Explosives

The problems of record keeping and protection of inventories detailed in the next chapter raise the possibility that it may not be as difficult as one might hope for terrorists to get their hands on the "any grade of plutonium" or the "uranium at any enrichment level significantly above 10 percent" that they would need to build a crude nuclear weapon. Using a conservative estimate of error in best practice U.S. plutonium record keeping and a conservative estimate of the size of plutonium inventories worldwide, enough plutonium could have been diverted to make more than 200 crude nuclear weapons (or deliver millions of lethal doses in dispersal devices) without the record keeping system ever noticing that anything was missing.

More than 200 pounds of highly enriched uranium disappeared under suspicious circumstances from the privately owned Nuclear Materials and Equipment Corporation (NUMEC) plant in Apollo, Pennsylvania in the 1960s. Two decades later, during exercises run by the U.S. Department of Energy, "mock" terrorists successfully stole plutonium from the Pantex nuclear weapons plant in Texas and the Savannah River Plant in South Carolina. Both Savannah River and Pantex are facilities at which protection was presumably a very high priority, since they not only handle plutonium, but are involved in assembling and disassembling nuclear weapons. The U.S. Nuclear Regulatory Commission (NRC) also tested the ability of armed terrorists to penetrate commercial nuclear power facilities. Serious security problems were discovered at almost half of the nation's nuclear plants. In at least one mock attack, "terrorists" were able to sabotage enough equipment to cause a core meltdown. Yet in 1998, the security testing program was eliminated in the interests of cutting costs.[37]

Then there is the problem of safeguarding inventories of plutonium, enriched uranium and nuclear weapons in the former Soviet Union. The Soviet system of record keeping was so poor that even by 1996, Russia still did not have accurate records of the quantity, distribution and status of nuclear materials at many of the 40-50 nuclear locations and 1,500-2,000 specific nuclear areas throughout the former Soviet Union.[38] Economic and political turmoil in Kazakhstan, Ukraine and Russia have greatly increased the chances of nuclear theft. We know that enriched uranium was stolen from Russian facilities at Podolsk and Sevmorput in the 1990s. And persistent reports of "holes in the fences" and other poor security practices in Russia do not bode well for the future.

There is no doubt that conventional weapons, explosives and all manner of related goods stolen from Russian and American military arsenals have found their way into the hands of terrorists around the world. There is also little doubt that a black market in nuclear materials now exists, most likely fed in part by criminal sources in the former Soviet Union. Between 1991 and 1994, German police recorded more than 700 cases of nuclear smuggling (though at least some of these were hoaxes). Speaking in April 1996, CIA Director John Deutch put it this way: "The chilling reality is that nuclear materials and technologies are more accessible now than at any other time in history."[39]

Once "nuclear materials and technologies" are acquired, they can be smuggled across international borders. In 1985, a West German businessman was convicted of illegally shipping an entire $6 million nuclear processing plant to Pakistan—along with a team of West German engineers to supervise its construction![40]

U.S. borders are so porous that it would be relatively easy to bring nuclear materials into the United States that had been stolen from poorly guarded nuclear facilities elsewhere. It wouldn't be all that difficult to bring stolen or homemade nuclear weapons or components into the United States either. In early 1996, *Time* reported that "U.S. intelligence officials admit that a terrorist would have no more difficulty slipping a nuclear device into the U.S. than a drug trafficker has in bringing in bulk loads of cocaine."[41] Decades earlier, special forces teams actually tried to smuggle simulated nuclear bombs into the United States dozens of times to see if it could be done. They carried the dummy weapons across the borders in trucks, small planes and boats. None of them were ever intercepted.[42]

Some Incidents

There is a long history of nuclear threats and related plots by terrorists and criminals.

- In 1978, the FBI arrested two men after they tried to recruit an undercover agent to take part in a plot to steal an American nuclear submarine. The men had showed him their plan to use a gang of 12 to murder the crew of the nuclear submarine USS *Trepang*, sail it from its dock in New London, Connecticut, to the mid Atlantic and turn it over to a buyer they did not identify. The plan included the option of using one of the ship's nuclear missiles to destroy an East Coast city as a diversion to help with the getaway.[43]
- Hours after Uganda's megalomaniacal dictator Idi Amin was overthrown in June 1979, top secret documents were discovered that allegedly revealed a plot Amin was preparing. Nuclear weapons small enough to fit into suitcases were to be built and carried into the nation's embassies around the world by teams of Ugandan diplomats, possibly for purposes

of nuclear blackmail. It was further reported that Amin was actively seeking terrorist help and expertise to carry out this grotesque plan.[44]

- On April 1, 1985, New York City officials received an anonymous letter threatening to contaminate the city's water supply with deadly plutonium trichloride unless all charges against Bernhard Goetz were dropped. Goetz was accused shooting four young black men in a subway confrontation. The charges were not dropped. Two and a half weeks later, tests of the city's water showed levels of plutonium 35 times greater than normal.[45]
- In December 1994, a Czech scientist named Jaroslav Vagner and two colleagues were arrested for nuclear smuggling when Prague police found nearly six pounds of weapons grade uranium in the back seat of his car. Eighteen months later, interviews with Czech police and newly released documents revealed that allies of the three conspirators had threatened to explode a nuclear weapon at an unspecified Prague hotel unless the prisoners were released. According to the Czech police detective handling the investigation, "It is possible they have the nuclear material to do it. We found out they were planning to bring out [of Russia] 40 kilos of uranium within several days and . . . one ton within several years."[46]

In an attempt to deal with the threat of nuclear terrorism, the United States put together the multiagency Nuclear Emergency Search Team (NEST) in 1975. NEST was set up to evaluate criminal or terrorist nuclear threats and if necessary, to conduct extensive high-tech bomb searches to find and disable nuclear devices. By early 1996, NEST's annual budget was up to $70 million. The team had evaluated 110 threats (including some nuclear emergencies not involving weapons) and mobilized to search or take other action 30 times. All but one of the threats were reportedly hoaxes.[47]

What are the chances that this specialized team could actually find a real terrorist nuclear device? In 1980, NEST's assistant director put it this way: "If you can cut it down to a few blocks, we have a chance. But if the message is to search Philadelphia, we might as well stay home."[48]

THREATENING DANGEROUS TECHNOLOGY FACILITIES

Terrorists would not have to steal or build weapons of mass destruction to wreak havoc. They could achieve much the same effect by sabotaging plants that produce or use large quantities of toxic chemicals, attacking nuclear or toxic chemical waste storage areas or triggering the catastrophic failure of nuclear power plants. Ordinary explosives or incendiary devices, placed in the right

TABLE 2-1

NUCLEAR SAFEGUARDS INCIDENTS BY CATEGORY, 1976-19

CATEGORY	NUMBER OF EVENTS	PERCENT OF TOTAL
Bomb-Related	690	38.9%
Firearms-Related	540	30.4%
Tampering/Vandalism	120	6.8%
Intrusion	43	2.4%
Missing or Allegedly Stolen	29	1.6%
Arson	21	1.2%
Transport-Related	12	0.7%
Miscellaneous	321	18.1%
TOTAL	1776	100%

Notes: (1) The NRC's definitions for the categories are:
"Bomb-Related: Events concerned with explosives or incendiary devices"
"Firearms-Related: Events typically describe the discharge, discovery or loss of firearms"
"Tampering/Vandalism: Incidents of destruction or attempted destruction . . . which do not directly cause a radioactive release"
"Intrusion: Incidents of attempted or actual penetration of a facility's barriers or safeguards systems"
"Missing or Allegedly Stolen: Events in which safeguarded material was stolen, alleged to be stolen, discovered missing or found [includes material missing or stolen during transport]"
"Arson: Intentional acts involving incendiary materials resulting in damage to property"
"Transport-Related: Events . . . where safeguarded material was misrouted or involved in an accident"
(2). Even though there is some overlap in categories, each event was only included in a single category. There is thus no "double-co

Source: Operations Branch, Division of Fuel Safety and Safeguards, Office of Nuclear Material Safety and Safeguards, Safeguards Summary Eve List (SSEL) (Washington D.C.: U.S. Nuclear Regulatory Commission, NUREG-0525, Vol. 2, Rev. 3; July 1995), pp. vii and A-7.

places and ignited at the right time, could cause more damage than that cause by the terrible accidents at Bhopal and Chernobyl. Many threats have been mac against nuclear facilities over the years. NRC data on "safeguards event involving nuclear materials, power plants and other facilities show nearly 1,80 threatening events during the 19 years from 1976 through 1994 (see Table 2-1).[49] Close to 700 events (almost 40 percent) were bomb related.

Like terrorist incidents in general, these events follow an uneven pattern ov time, as shown in Table 2-2. It is good news that there were many fewer boml related incidents during the first half of the 1990s than in any earlier five-ye period. But that is a slender reed on which to build up hope. Even in those fi years there were 76 bomb-related incidents, an average of more than one a montl And the decline in bomb-related events was more than made up by a sharp rise i the number of other incidents. There does not seem to be any good rea believe that credible threats against nuclear facilities will stop anytime soon.

TABLE 2-2

NUCLEAR SAFEGUARDS INCIDENTS BY YEAR, 1976-1994

YEAR	TOTAL NUMBER OF INCIDENTS	REACTOR EVENTS ONLY	BOMB-RELATED INCIDENTS
1976	72	66	55
1977	34	29	28
1978	47	40	29
1979	118	111	94
1980	109	103	73
1981	74	70	48
1982	82	80	57
1983	56	54	39
1984	58	57	28
1985	67	58	23
1986	96	84	43
1987	95	91	35
1988	137	128	37
1989	148	142	25
1990	103	100	11
1991	152	150	32
1992	94	94	12
1993	116	116	12
1994	118	118	9
TOTAL	1776	1691	690

Source: Operations Branch, Division of Fuel Safety and Safeguards, Office of Nuclear Material Safety and Safeguards, Safeguards Summary Event List (SSEL) (Washington D.C.: U.S. Nuclear Regulatory Commission, NUREG-0525, Vol. 2, Rev. 3; July 1995), pp. A-1, A-2, and A-8.

Many of the safeguards events in these tables were only threats or hoaxes. Even so, they indicate the extent to which nuclear facilities are seen as vulnerable enough to make the threats and hoaxes credible. In any case, it is very clear from these data that nuclear facilities have been considered attractive targets by terrorists and criminals for some time now.

A Chernobyl by Design?

The same month that terrorists used a truck bomb to blow up the World Trade Center in Manhattan, a mental patient crashed his station wagon through a door at the infamous Three Mile Island nuclear power plant.[50] Coming so close together, these two events naturally raised the question of what would happen if a disturbed individual or terrorist gang attacked a nuclear plant with a truck bomb as powerful as the one that ripped apart six stories of the Trade Center. The devastating Oklahoma City bombing two years later and the deadly 1996 truck bombing that destroyed part of an American military housing complex in Saudi Arabia (despite barriers that kept the vehicle 35 yards away) further strengthened this concern.[51]

The reinforced containment structure that covers a nuclear power reactor is the last line of defense against the release of large amounts of radioactive material. Its presence at Three Mile Island and its absence at Chernobyl was one of the most important reasons why the Chernobyl accident did so much more damage. Early in a severe reactor accident, high pressure from the heat of fission products, gas generation and the like threaten the containment. At the same time, it is filled with many radioactive materials in vaporized and aerosol form, easily carried by the wind and easily inhaled. It is the worst possible time for the containment to fail. If a terrorist group were to trigger a major nuclear accident, perhaps by sabotaging the plant with the help of insiders, anything they could do to weaken the containment enough to make it fail would greatly increase the magnitude of the disaster. Coordinating sabotage of the plant with a vehicle bomb attack might just do the trick. Is such a scenario possible?

In 1984, Sandia National Laboratories completed a study of the truck bomb threat to nuclear facilities for the Nuclear Regulatory Commission. In April, NRC staff reported to the commissioners that "The results show that unacceptable damage to vital reactor systems could occur from a relatively small charge at close distances and also from larger but still reasonable size charges at large setback distances (greater than the protected area for most plants)."[52] The Sandia study concluded that nuclear facilities in the United States were vulnerable to terrorist truck bombs, and that putting a few barricades near the reactor building would not solve the problem. "Unacceptable damage to vital reactor systems" could be done by bombs detonated some distance away, in some cases possibly even off-site.[53]

Trucks are not the only vehicles that terrorists could use to attack a nuclear plant. In the early 1970s, Atomic Energy Commission Chairman James Schlessinger put it this way: "If one intends to crash a plane into a facility . . . there is, I suspect, little that can be done about the problem. . . . The nuclear plants that we are building today are designed carefully, to take the impact of, I believe, a 200,000 pound aircraft arriving at something on the order of 150 miles per hour. It will not take the impact of a larger aircraft."[54]

At least a few dozen nuclear plants still operating in the United States today have containments no stronger than that to which Schlessinger was referring. Quite a few jumbo jets have been hijacked by terrorists by now, and they are considerably heavier and faster than the aircraft whose impact those containments were designed to resist. A Boeing 747, for example, weighs more than 300,000 pounds and can travel at speeds over 500 miles per hour. But even a much smaller plane could seriously damage the containment if it were filled with explosives.

As to sabotaging a nuclear plant, documents written to help nuclear plant operators test their security have been publicly available since the 1970s. They would be very useful to a potential saboteur. One includes a computer program that could be used to determine the best route for a saboteur to follow. According to a former nuclear safeguards inspector, to use the program, "All you need is the values (dimensions) of the plants, some of which are available in the library."[55]

Then there is the *Barrier Penetration Database,* prepared by Brookhaven National Laboratory under contract to the NRC. It gives detailed information on the types of tools and explosives necessary to break through dozens of barriers, from chain-link fences to reinforced concrete walls. It includes other information important to planning an attack, such as the weight of the equipment required and how long it should take to break through each barrier.[56] A 1993 RAND study (sponsored by the Department of Energy) looked at 220 direct attacks by armed bands of guerrillas or terrorists that the researchers believed were analogous to the kinds of direct armed assault such groups might launch against American nuclear facilities. They found that the attackers were successful 74 percent of the time.[57]

Of course, sabotage would be easier with the help of insiders working at the facility. In a 1990 study, *Insider Crime: The Potential Threat to Nuclear Facilities,* RAND found that financial gain was the main motivation in the overwhelming majority of insider crimes they studied.[58] Terrorists might need to do little more than find a sufficiently money-motivated insider and pay him/her off. Guards themselves were responsible for more than 40 percent of the crimes against guarded targets. Their overall conclusion? "[N]o organization, no matter how ingeniously protected can operate without some trust in individuals on all levels. Beyond a certain point, security considerations in hiring, guarding, controlling, and checking people can become so cumbersome as to actually impede the operation of a facility. This creates a serious dilemma in the case of a nuclear facility. . . . total security can never be attained."[59]

It would be much simpler to attack a toxic chemical plant, radioactive or toxic chemical waste storage dump and the like than a nuclear power plant. If a successful terrorist assault on a nuclear plant is possible, terrorist assaults on oth dangerous-technology facilities are even more likely to succeed.

Why Haven't Terrorists Yet Engaged in Acts of Mass Destruction?

Experts have warned about the dangers of nuclear terrorism and its equivalents at least since the 1960s. Dangerous technologies have already been used to do damage on a scale similar to conventional terrorism (such as in the 1995 Tokyo nerve gas attack). There have also been threats of mass destruction and hoaxes involving nuclear weapons. But as yet, there has been no publicly reported case of terrorists (or criminals) doing the kind of massive damage that could result from large-scale use of dangerous technologies as either a weapon or target. Why not?

It is clearly not because this kind of attack is beyond their capabilities. It cannot be because of a moral revulsion against taking innocent lives, since the taking of innocent lives is the terrorist's stock in trade. It is possible that terrorists might be inhibited by a belief that murder and destruction on a massive scale would invite ferocious retaliation. But decades of experience show that terrorists are willing to risk ferocious retaliation, and may even b trying to provoke it. Many who seek to retaliate against terrorists are already prepared to do them grievous, even deadly harm. Even in free societies, where the search for terrorists is complicated by constraints against hurting innocent people and forfeiting personal freedoms, terrorists are already pursued with dogged determination and severely punished (witness the death sentence meted out to Timothy McVeigh, convicted of the Oklahoma City bombing).

More likely, terrorists have simply not found acts of mass destruction necessary up to now. If acts of conventional terrorism still provoke enough fear to put pressure on decision makers to do what terrorists want done, there is no particular reason for them to go to the trouble, danger and expense of acquiring and using the means of mass destruction. If acts of conventional terrorism come to be more routine and so generate less shock and fear, terrorists may someday conclude that they must commit much greater violence to frighten people enough to achieve their objectives. They will find the tactics of mass destruction waiting in the wings.

Another possibility is that so far, terrorists have believed that committing acts of mass destruction would get in the way of achieving their objectives. The credibility of this explanation depends on what kind of group we are considering. Terrorist groups are not clones of each other. Understanding what makes them different is important to judging how likely it is that any particular group will use dangerous technologies. It is also the key to developing more effective countermeasures.

A Taxonomy of Terrorists

The first and perhaps most obvious distinction is between domestic groups and international terrorists. Germany's left-wing Red Army Faction, France's right-wing Federation for National European Action, America's white supremacist The Order, Spain's Basque separatist ETA and Peru's revolutionary Shining Path are examples of domestic terrorist groups active in the 1980s.[60] On the other hand, the Popular Front for the Liberation of Palestine, the Japanese Red Army, Hamas, the Jewish Defense League and the Armenian Secret Army are historical examples of internationally focused terrorist groups.[61] Some have straddled the boundary. The Irish Republican Army (IRA) carried out most of its attacks inside Northern Ireland (against both Irish and English targets), but it was also responsible for more than a few terrorist bombings in England.

Secondly, some terrorists have relatively well-defined, specific political goals, while the goals of others are much more vague, general, ideological and/or anarchic. The Palestine Liberation Organization (PLO) used terrorist tactics to raise public awareness of the plight of disenfranchised Palestinian Arabs and gain support for establishing an independent Palestinian state. Similarly, the goal of IRA terrorism was also clear, specific and political: to end British rule in Northern Ireland. By contrast, the Symbionese Liberation Army, made famous by its kidnapping of newspaper heiress Patricia Hearst, had only the most general, ideological, anticapitalist goals. The long terrorist career of the infamous Unabomber was aimed at promoting vague antitechnology goals. And the self-proclaimed goal of Shoko Asahara, the leader of the Japanese terrorist cult Aum Shinrikyo, was to "help souls on earth achieve 'ultimate freedom, ultimate happiness and ultimate joy.'"[62]

Asahara's statement leads naturally to a third, related characteristic that differentiates terrorists from each other: some are rational and some are not. There is a temptation and a desire to believe that anyone who would engage in brutal terrorist actions cannot be rational. But that is not true. Rationality is a matter of logic, not morality. It simply means that the tactics used are logically related to the goals being pursued. The German Nazis were vicious and their behavior despicable and profoundly immoral, but not illogical. At least in the short term, their tactics led them step by step toward their goals of conquest and control.

Nonrational behavior includes both irrationality (in the sense of craziness) and behavior that is not necessarily crazy, but is driven by something other than logic. Emotion, culture, tradition and religion are important nonrational drivers of human behavior. To refuse to do business with the lowest-cost supplier because that firm is run by someone who once caused you personal emotional pain may not be rational, but it is easy to understand and certainly not crazy. To sit for hours in the hot sun at a graduation ceremony wearing long, black robes appropriate to the much colder climate from which they came is not logical behavior, but neither is it a sign of mental imbalance. It is driven by culture and tradition. Similarly, belief in God and adherence to the ceremonies of a particular religion is not a matter of logic, it is a matter of faith. And while faith may not be logical, it is not irrational.

Whether or not terrorist tactics actually advanced the political goals of the PLO or the IRA, the decision to use them, though reprehensible, was still rational: terrorism might logically have led them where they wanted to go. It is difficult, however, to imagine by what logic the terrorist activities of Aum Shinrikyo can be related to their spiritual goal of helping people on Earth to attain "ultimate freedom, ultimate happiness and ultimate joy." Similarly, the brutal murders perpetrated in Los Angeles decades earlier by the "Manson Family" (see Chapter 8) were driven by Manson's psychotic fantasies, not some logical process of choosing among available tactics in the service of an achievable goal.

A fourth factor that differentiates terrorist groups is the degree of support for their underlying goals. Whether or not the public approves of their tactics, terrorist groups fighting for a popular cause behave differently than those whose *goals* are considered extremist and out of touch. Everything else being equal, when the cause is popular, it will be easier for the group to recruit members, raise funds and find hiding places for their weapons and for themselves. Those that are rational will cultivate this sponsorship, and take care when choosing their targets and tactics to avoid alienating their supporters. They will try to avoid catching their potential allies in the web of innocent victims. Groups with little or no public support are less inhibited in their choice of victims. They may believe that acts of horrific violence are the only way to shock what they see as a complacent or submissive public into action. It is a safe bet that, despite their lack of support, most see themselves as the leading edge of a great movement, and think that once the public awakens, a mass of supporters will rise up and carry them to victory.

Finally, different terrorist groups face off against different kinds of opponents. Some see a very specific enemy, such as the top executives of a particular company (or industry) or the political leaders of a specific country. Others see a much larger enemy, such as all nonwhites or all non-Christians, or a vaguely defined group, such as the "international Jewish financial conspiracy." The nature of their perceived enemy affects the kinds of actions they take and the intensity of the violence they commit. The range of likely targets and the degree of violence tend to be greater when the enemy is "the federal government" or "the Jews" than when the target is the management of Exxon or the ruling party in Britain.

To summarize, the five distinguishing factors are:

- *geopolitical focus* (Are they domestic or international in focus and if international are they state sponsored?)
- *nature, specificity and achievability of goals* (Are their goals vague and ideological or specific and political?)
- *rationality* (Is their behavior driven by logic?)
- *public support for their goals* (How much public support is there for their goals as opposed to their tactics?)
- *size and character of their enemy* (Is their opponent a relatively small and specific group of decision makers or a much larger and more generalized class of people?)

Domestic terrorists with clearly defined and potentially achievable political objectives are most likely to see the terrorism of mass destruction as counterproductive. Because they see their terrorist acts as acts of resistance and rebellion that will eventually rally their silent, disempowered supporters to the cause, they must always balance the shock effect of the damage they do against the support they will lose if their violence becomes too extreme. Except in situations of complete desperation, groups of this type are almost certain to see in advance that acts of mass destruction would be disastrous tactical blunders.

International terrorist groups with clearly defined and potentially achievable political objectives are somewhat more likely to escalate the level of violence. If they are playing to a domestic audience and if most of the violence they do is outside the borders of their home country, they may feel that spectacular acts of destruction will not alienate and may even encourage those who support their cause at home. This might be especially true of a terrorist group attacking targets inside the borders of a nation whose military is occupying the terrorists' home country. However, if the terrorists are also trying to influence the wider international community to support their cause, acts of extraordinary violence are not likely to seem appealing.

Domestic or international terrorist groups whose objectives are much more general or ill formed and whose attitudes are much more nihilistic—such as doomsday religious cults, racist and ideological extremists, and nuts—are an entirely different story. They are less likely to be deterred by worries about alienating supporters and may find devastating of acts of mass destruction an appealing, unparalleled opportunity to exercise their power. Doomsday cults could even see such acts as a way of hastening the salvation they believe will follow the coming cataclysm. Groups of this sort a extremely dangerous.

With a doomsday philosophy and considerable scientific talent on board, Aum Shinrikyo is a good case in point. This well-financed cult was accused not only of committing an act of nerve gas terrorism, but of preparing for much more deadly and devastating uses of chemical, biological and even nuclear weapons. The powerful control exerted over Aum's members by its charismatic but apparently mentally disturbed founder combined with the group's nihilistic orientation and substantial resources is an almost perfect recipe for the terrorism of mass destruction.

By 1997, there were more than 200 right-wing, violence-oriented, white-supremacist militias in the United States, active in some 40 states.[63] The agendas of many of these groups are extremist by any reasonable definition of the word. Collectively calling themselves the "Patriot" movement, they picked up on the antigovernment rhetoric of mainstream political conservatives and distorted it to the extreme. Many Americans believe that some federal agencies are oversized, inefficient and sometimes abusive. But the rhetoric of the Patriots goes much farther. In the words of one analyst who has closely tracked the movement, "those in the Patriot movement are convinced that the government is evil. It is run by a secret regime ('The New World Order') that seeks to disarm American citizens and subjugate them to a totalitarian world government. Just about anything that can be described with the adjectives 'global,' 'international' or 'multicultural' is a Patriot menace."[64]

These groups are heavily armed, and not without financial resources. In 1995, 11 individuals associated with the Patriot group "We the People" were indicted on felony charges related to a scheme in which they allegedly collected almost $2 million from thousands of people they charged $300 each to be part of a phony class-action lawsuit against the federal government. A year before, the host of a popular Patriot radio program and founder of the Patriot group "For the People" took in more than $4 million.[65]

America's right-wing, extremist, paramilitary militias have many characteristics that make them prime candidates for the terrorist use of dangerous technologies. Some rank high on each of the five factors in the taxonomy of terrorist groups:

> *Factor 1:* While they are domestic rather than international, they see themselves as fighters against a national government that has become the pawn of an international conspiracy ("The New World Order"). They believe the U.S. federal authorities constitute an "occupation government," and some think that no level of government higher than the county has any legitimacy. Thus, they see themselves more as fighters against a foreign government than as domestic revolutionaries.

Factor 2: Their goals are ideological, general and anarchic, rather than specific, limited and politically achievable.

Factor 3: They are not particularly rational. Living in a paranoid world of conspiracies, they are motivated by nonrational beliefs often clothed in the garb of some form of end-time religion. Some have been tied to the violence-oriented, postmillenial Christian Identity movement.

Factor 4: Though there is considerable cynicism about the federal government among many Americans, there is very little support for the nihilistic goals of the Patriot movement.

Factor 5: Rather than having a very specific and limited enemy, many of the Patriot militias consider all nonwhites, non-Christians and many mainstream Christians as well to be the enemy.

After studying a wide range of terrorist groups for the Department of Energy in 1986, RAND concluded, "Of the terrorist organizations active in this country, the right-wing extremists appear to pose the most serious threat to U.S. nuclear weapons facilities."[66]

To date, the lack of unity and coordination among the extremist militia has limited the scope of their terrorist efforts. There is, however, growing cross-fertilization among them. They count well-trained American military personnel (including at least some former Green Berets) among their members and are always trying to recruit more. They have not yet been able to attract many highly educated and technically skilled people to the movement, but the movement is relatively new and does seem to have significant financial resources. There is no reason to believe that the scope of their terrorist activities will stay limited indefinitely. These "Patriots" are prime candidates for becoming nuclear terrorists.

IS THE TERRORIST THREAT GROWING?

There are some useful data available on the frequency and severity of terrorist attacks and credible threats of attack, but they are limited and flawed. Because the "terrorist" label is so politically loaded, governments and other organizations that gather and publish such data often use different definitions of what is a terrorist incident. Beyond this, incidents that involve grave potential danger—such as threats against nuclear power plants, nuclear weapons facilities or radioactive waste

TABLE 2-8

INCIDENTS OF INTERNATIONAL TERRORISM*

YEAR	NUMBER OF INCIDENTS**	FATALITIES†	INJURIES	TOTAL CASUALTIES††
1968	120	20		
1969	200	10		
1970	300	80		
1971	280	20		
1972	550	140		
1973	350	100		
1974	400	250		
1975	345	190		
1976	457	200		
1977	419	150		
1978	530	250		
1979	434	120		
1980	499	150		
1981	489	380		
1982	487	221	840	1061
1983	497	720	963	1683
1984	565			1100
1985	635	825	1217	2042
1986	612	576	1708	2284
1987	665	633	2272	2905

storage areas—tend to be covered up, on the belief that making them public would spread undue fear and thus give the terrorists a partial victory. Clearly, such incidents are also kept secret to create a false sense of security so that the public will continue to support particular government institutions or policies.

It is easier to keep the attacks quiet when they are carried out by domestic terrorists than when international terrorists are involved. The incentives are also greater: the frequency and severity of domestic terrorist incidents are mea of internal opposition and political turmoil, something no government likes to

TABLE 2-3 CONTINUED

YEAR	NUMBER OF INCIDENTS**	FATALITIES†	INJURIES	TOTAL CASUALTIES††
1988	605	658	1131	1789
1989	375	407	427	834
1990	437	200	677	877
1991	565	102	242	344
1992	363	93	636	729
1993	431	109	1393	1502
1994	321	315	663	977
1995	440	165	6291	6456
1996	296	314	2912	3226
1997	304	221	693	914
TOTAL	12,971	7,619	22,065	28,723††
	(OVER 30 YRS)	(OVER 29 YRS)	(OVER 15 YRS)	(OVER 16 YRS)
AVERAGE	432/YR	263/YR	1471/YR	1795/YR††

* The U.S. State Department excluded intra-Palestinian violence beginning with 1984, apparently because it was considered to be domestic rather than international terrorism. Such terrorism had previously been included because the "statelessness" of the Palestinian people made the violence seem inherently international.

** Data for 1968-74 were extracted from a bar graph that was not specifically numbered, so they should be considered approximations, rounded to the nearest ten. The underlying data were not published.

† Data for 1968-81 were extracted from a line graph that was not specifically numbered, so they should be considered approximations, rounded to the nearest ten. The underlying data were not published.

†† Includes only years for which data on the sum of both fatalities and injuries were available. Therefore, the total of this cdumn is less than the sum of the totals of the separate columns for fatalities and injuries.

Sources: Data on number of incidents for 1975-94 from the Office of the Coordinator for Counterterrorism, U.S. Department of State, Patterns of Global Terrorism, 1994, p. 65, 1995 data from the 1995 edition, p. 4, 1996 and 1997 data from the 1997 edition; data on number of incidents for 1968-74 from Office of Counterterrorism, U.S. Department of State (unpublished) as cited in Kegley, Charles W. Jr, International Terrorism: Characteristics, Causes, Controls (New York: St. Martin's Press, 1990), p. 15.
Data on fatalities for 1968-83 and injuries for 1982-83 from Cordes, Bonnie, et al., Trends in International Terrorism, 1982 and 1983 (Santa Monica, California: Rand Corporation, August 1984), pp. 6-7; these data were apparently based U.S. State Department data. Data for fatalities and injuries for 1985-97 from Patterns of Global Terrorism annual editions for 1985-97; approximate total casualties data for 1984 were from the 1992 edition, p. 60.

publicize. As a result, while all data on terrorism must be treated with caution, data on international terrorism are likely to be more reliable (see Table 2-3).

According to the U.S. Department of State, there were nearly 13,000 separate incidents of international terrorism from 1968 through 1997—an average of more than 430 per year for three decades. The average number of terrorist incidents per year rose from 160 in the late 1960s to more than 400 during the 1970s, peaking at more than 540 in the 1980s. With the end of Cold War rivalries and the beginning of serious ongoing peace negotiations in the

Middle East, the first eight years of the 1990s saw a significant drop in the average number of terrorist incidents per year to just under 400. Still, there were *almost two and a half times* as many incidents per year on average in the period 1990-97 as there had been in 1968-69.

International terrorism has also become a more deadly business over the years. The average number of people killed each year skyrocketed from 15 in 1968-69 to 150 during the 1970s, then grew rapidly to more than 500 in the 1980s. Fatalities dropped even more sharply than incidents in 1990-97, falling to about 190 per year. Even so, despite the Middle East peace process and the end of the Cold War, the average number of people killed each year by international terrorists was more than 25 percent higher in 1990-97 than it had been in the 1970s, and almost 13 times as high as it had been in the late 1960s.

These data are far from perfect, but they would have to be very far off the mark to overturn the basic picture they paint. International terrorism is, sad to say, still going strong. It shows no signs of fading away anytime soon.

In the United States, we have become accustomed to thinking of international rather than domestic terrorism as the gravest threat to life and limb. Yet fewer people were killed worldwide in 1995 in all 440 international terrorist incidents than died that year in the single domestic terrorist bombing in Oklahoma City.

Terrorists have not yet used dangerous technologies to do catastrophic damage, as weapons or as targets. But there is nothing inherent in the nature of terrorism that makes it self-limiting. Those who are ready, even eager, to die for their cause, who stand willing to abandon every constraint of civilized behavior and moral decency against the slaughter of innocents, cannot be expected to permanently observe some artificial restriction on the amount of havoc they wreak.

Many terrorists are political rebels, in the classic sense. They have chosen reprehensible methods to fight for rational, limited, clearly defined objectives. But others are striking out against a vast array of faceless enemies, out of touch with reality and trying to punish, even to destroy a world they cannot live in and do not understand.

CHAPTER SEVEN

The Fallibility of Individuals: The Nature and Conditions of Life and Work

In *Space/Aeronautics* magazine in the late 1960s, Charles Cornell wrote, "Seemingly inexplicable, inconsistent and unpredictable human 'goofs' account for 50-70 percent of all failures of major weapons systems and space vehicles. That puts human errors . . . ahead of mechanical, electrical and structural failures...as a source of system troubles. . . . The consequences range from minor delays to major disasters."[1] In the aftermath of the tragic midair destruction of off-course Korean Airlines Flight 007 by the Soviet military in 1983, a National Aeronautics and Space Administration (NASA) official testified before Congress that human error was responsible for more than two-thirds of the 950-plus incidents in which civilian airliners had strayed off course in the preceding five years.[2] According to an analysis by the Safety Studies and Analysis Division of the National Transportation Safety Board, pilot error caused or contributed to 54 of the 76 fatal crashes on major airlines in the United States from 1967 through 1981.[3]

In the preceding chapter, we considered how substance abuse and mental illness contribute to human error. But that is only part of the problem. Error is pervasive in human activity, even when lives and treasure hang in the balance. In the airline industry, in the space program, in the field of medicine, in the world of high finance, in the criminal justice system—nowhere are we completely insulated from its consequences. Witness:

- On a clear night in December 1995, the pilots of American Airlines Fligh 965—both with thousands of hour of flying time and spotless records—made a series of "fatally careless mistakes" as they approached Cali, Colombia. After flying past the locational beacon 40 miles north of the airport, they programmed their navigational computers to fly toward it, and steered their plane into the side of a mountain. Flight recorders showed no evidence that they had discussed approach procedures, as is mandatory before every landing. It was the worst accident involving an American air carrier in seven years.[4]
- A Boeing 757 crashed off the coast of Peru in early October 1996, killing all 70 people on board. According to the National Transportation Safety Board, the plane went down "because maintenance workers forgot to remove tape and paper covers they had put over sensors while polishing the plane."[5]
- On July 17, 1997, one of three astronauts aboard the already troubled Russian *Mir* space station disconnected a critical electrical cable by mistake. That disabled the computer that controlled *Mir's* position in space, causing the space station to drift. A backup system took over too late to correct the problem. With the solar panels no longer pointed at the sun, the power drained slowly out of the batteries. Data transmission to the ground was cut off, and the key lighting, temperature-control and oxygen-generation systems had to be shut down to save energy.[6]
- Six people attached to dialysis machines at the Albuquerque Kidney Center suddenly began to scream in excruciating, unexpected pain as a technician mistakenly threw a switch that sent a cleaning solution intended to rinse the machines into the patients' bloodstreams. Five of the patients recovered, one died.[7]
- In May 1995, the chief of neurosurgery at the world-renowned Memorial Sloan-Kettering cancer center in New York operated on the wrong side of a patient's brain. Six months later, the New York State Department of Health reported that "systemic deficiencies" at the hospital, such as failure to always follow medical practices as basic as reviewing diagnostic reports and medical records prior to surgery, had played a role in the incident.[8]
- Four minutes before the end of trading on March 25, 1992, the prestigious Wall Street firm Salomon Brothers unexpectedly sent huge "sell" orders for the shares of 400 companies to the floor of the New York Stock Exchange. The market was thrown into turmoil as the flood of sell orders alarmed traders and caused the Dow Jones industrial average to drop some 15 points. It was all a mistake. An investor had sent the firm

an order to sell $11 million worth of stock in 400 companies, but a clerk put the figure in the wrong column, turning it into an order to sell 11 million shares. Even at an average price of $30 per share, that simple human error would have turned the $11 million sell order into an order to sell nearly one-third of a billion dollars worth of stock.[9]

- In April 1997, the inspector general of the Justice Department found that flawed scientific practices and sloppy performance were common at the FBI's world-famous crime laboratory. These "extremely serious and significant problems" jeopardized dozens of criminal cases, including the bombing of the Murrah Federal Building in Oklahoma. In that case, lab workers accused superiors of engaging in sloppy, improper or unscientific practices that so compromised bomb debris evidence that none of it could be tested.[10]
- At 4:00 A.M. on August 31, 1997, five bounty hunters wearing body armor and ski masks forced their way into a house in Phoenix, Arizona. They tied the hands and feet of a woman in the house, and held her, her daughters and her 11-year-old son at gunpoint. They then opened fire into another bedroom, killing a couple who had been sleeping there. The bail jumper the bounty hunters were tracking was not in the house, had never lived there, and was apparently unknown to the people whom they attacked. When asked why the bounty hunters had chosen that house, the Phoenix police said, "It's a mystery to us. There is nothing to indicate that the person they were looking for was at that house."[11]

It was not drug addiction, alcoholism or mental illness that caused these problems. People are prone to make mistakes even under the best of circumstances. But the physical, psychological and sociological circumstances in which we live and work are often not the best. They have powerful effects on our state of mind and thus our behavior on (and off) the job. Even emotionally, physically and mentally healthy people, not abusing drugs or alcohol, have real limits when subjected to the stress, boredom and isolation that are so often an inherent part of working with dangerous technologies. Spending endless hours interacting with electronic consoles, repeating essentially the same lengthy and detailed routine over and over, watching lighted panels and screens, flipping switches, checking and double-checking, sitting hour after hour in the control room of a nuclear power plant or missile silo, sailing for months in a submerged submarine isolated from most of humanity yet poised to destroy it—these are working conditions bound to aggravate the already strong human tendency to make mistakes.

The working environment in the nuclear military is among the most difficult of dangerous-technology work environments. It is isolating because it is enveloped in secrecy. No one on nuclear duty is permitted to talk about the details of their work with anyone lacking the proper security clearance. They cannot share what they do with friends and family. For much of the nuclear military, the work is also isolating because it requires long periods away from friends and loved ones.

Because of the constant repetition of routines and because it is so isolating, life in the nuclear forces is boring too. And it is stressful as well, for at least five reasons: (1) boredom itself is stressful; (2) isolation also creates stress (that's why solitary confinement is considered such a severe punishment for prisoners who behave badly); (3) for safety and security reasons, people on nuclear duty are always "on call," even when they are "off duty"; (4) Being highly trained to carry a task through, but never being able to take it to completion is frustrating and stressful; (5) many on nuclear duty are aware that if nuclear war comes, they will be part of the largest-scale mass murder in human history.

The nuclear military may be the maximum case of a stressful, boring and isolating dangerous-technology work environment, but it is far from the only case. One or more of these reliability-reducing characteristics are found in many other dangerous-technology workplaces. Nuclear power plant operators do work that is boring most of the time and stressful some of the time, though it isn't all that isolating. Working around highly toxic chemical or dangerous infectious biological agents has significant levels of background stress, punctuated by periods of intense stress when something goes really wrong. But because it combines most of the reliability-reducing elements relevant to dangerous-technology workplaces in general, the military work environment is worth special attention.

BOREDOM AND ROUTINE

In 1957, Woodburn Heron described laboratory research funded by the Canadian Defence Research Board in which subjects lived in what amounted to an exceedingly boring environment. There were sounds, but they were constant droning sounds, like the hum of a fan; there was light, but it was constant, diffuse light. There was no change in the pattern of sensory stimuli. The subjects became so eager for some kind of sensory stimulation that they would whistle, sing or talk to themselves. Some had a great deal of difficulty concentrating. Many lost perspective and found themselves on an emotional roller coaster, shifting suddenly and unpredictably from one emotion to another. Many also began to see or hear things that were not there.

People vary widely in their sensitivity to boredom. It is difficult to predict the threshold of monotony that will trigger these reactions in any particular individual "real world" situations. Yet there is ample evidence that grinding boredom and dulling routine can and do produce such problems. For example, in 1987 it was reported that "Congressional committees, watchdog groups and the [Nuclear Regulatory] commission have repeatedly found operators of nuclear plants asleep or impaired by alcohol and drugs." Attempting to explain such behavior, a representative of the Atomic Industrial Forum (the industry lobbying group) said, "The problem is that it's an extremely boring job. It takes a great deal of training. Then you sit there for hours and hours and take an occasional meter reading."[12]

Boredom can be so painful that people feel compelled to try to escape, sometimes taking refuge in drugs and alcohol. In interviews of Vietnam veterans conducted by the Psychiatry Department of the Walter Reed Army Institute of Research during the Vietnam War (1971), soldiers often cited boredom as the main reason they used drugs. "Descriptions of work activities invariably included statements like, 'There was nothing to do, so we smoked dope. . . . We just sat around. . . . You had to smoke dope, or drink, or go crazy doing nothing. . . . It was boring until I started smoking skag [heroin]; then I just couldn't believe how fast the time went.'"[13]

A sailor who served as helmsman on the nuclear aircraft carrier USS *Independence* claimed that he regularly used LSD *on duty* during the late 1970s and early 1980s. It was the only way, he explained, to get through eight hours of extremely boring work. He said that there was almost never a day in his whole tour of duty that he was not on either LSD or marijuana, most often LSD.[14]

The dulling effects of routine can create great danger in systems subject to sudden criticality. According to Marrianne Frankenhaeuser of the Karolinska Institutet Department of Psychiatry and Psychology in Stockholm,

> An early sign of understimulation is difficulty in concentrating . . . accompanied by feelings of boredom, distress and loss of initiative. One becomes passive and apathetic. . . . [Then] when a monotonous situation all of a sudden becomes critical . . . the person on duty must switch instantaneously from passive, routine monitoring to active problem solving. . . . The sudden switch . . . combined with the emotional pressure, may cause a temporary mental paralysis. During a brief but possibly critical interval, the person in charge may be incapable of making use of the information available. The consequences of such mental paralysis—however brief—may be disastrous.[15]

Eastern Airlines Flight 401 was on a routine final approach to Miami International Airport on a dark night in December 1972. The crew included three able-bodied and experienced pilots. Weather conditions were fine. As they prepared to land, the crew noticed that the nose landing gear light wasn't working, so they couldn't tell whether the gear was extended and locked. An emergency landing with a possible nose gear problem is neither very risky nor particularly rare. But because of the otherwise routine conditions, the crew was so removed from the primary job of flying the plane that they became fixated on the light bulb. They didn't notice that the autopilot had disengaged and the plane was slowly descending. They ignored the altimeter, and didn't even react when the altitude alert sounded. By the time they realized what was happening, they were "mentally paralyzed," unable to react fast enough to prevent disaster. The jumbo jet crashed into the Florida Everglades, killing 99 people.[16]

The pilot, first officer, flight engineer and a guest crew member aboard Pacific Southwest Airlines Flight 182 were talking intensely about retirement benefits as the plane made a routine visual approach to San Diego in clear weather on the morning of September 25, 1978. The San Diego air traffic controller gave standard landing instructions, twice advising of a light aircraft in the area. Each time, the flight crew acknowledged the information. The second time, the captain said he had the Cessna in sight and would maintain visual separation. The approach seemed so routine that the conversation about retirement benefits continued unabated. The crew paid no attention to the fact that they had lost sight of the light plane. Shortly after 9:00 A.M., the jet slammed into the Cessna, and 144 people died.[17]

In 1904, Sigmund Freud published a very popular book, *The Psychopathology of Everyday Life.* He had collected hundreds of examples of inconsequential everyday errors: misreadings, misquotes, slips of the tongue, etc. Freud interpreted these not as meaningless accidents, but as unintended revelations of the unconscious mind, the famous "Freudian slip." His interpretation aside, the fact is that such seemingly trivial errors—trying to open the house door with the office key, calling one child by another child's name, misdialing the telephone—are exceedingly common.

Having analyzed many slips reported by some one hundred subjects over a number of years, psychologist James Reason of Manchester University reported that nearly half the absent-minded errors involved deeply ingrained habits: "The erroneous actions took the form of coherent, complete sequences of behavior that would have been perfectly appropriate in another context. In each case the inappropriate activity, more familiar to the subject than the appropriate one, had been carried out recently and frequently, and almost invariably its locations, movements and objects were similar to those of the appropriate action."[18]

Under normal circumstances these errors are easily corrected and of little consequence. Under abnormal circumstances, following familiar routines can lead to disaster. It is important to understand that *the difference between a trivial and a catastrophic error is situational, not psychological.* What creates the disaster is the context within which the error occurs, not the mental process that caused it. During special NATO training exercises over West Germany in the 1980s, a Royal Air Force Phantom jet pilot followed the same routine he had followed in the more common training missions he had been flying for eight years. Completely forgetting that this time he was carrying live Sidewinder missiles, he fired one and destroyed a multimillion-dollar Royal Air Force Jaguar aircraft.[19] In 1977, the experienced Dutch pilot of a Boeing 747 jumbo jet departing from Tenerife in the Canary Islands failed to wait for takeoff clearance, roared off and crashed into another 747 that was still taxiing on the runway. How could a well-trained, experienced pilot who had actually been head of KLM Airlines' flight training department for years make such an elementary error? He had spent some fifteen hundred hours in flight simulators over the preceding six years and had not flown a real aircraft for three months. To save costs, simulator pilots are never required to hold position while waiting for takeoff clearance. Apparently, the pilot simply reverted to the routine of the flight simulator with which he was so familiar. What in a different context might have been a trivial error, instead cost 577 lives.[20]

STRESS

Though we often think of stress as an unalloyed problem, a little stress "gets the juices flowing," increasing alertness, effectiveness and reliability. But as the pressure continues to mount, performance tends to level off, then decline, sometimes very sharply. Excessive stress can create all sorts of physical, mental and emotional problems that affect reliability, ranging from irritability to high blood pressure to complete mental breakdown. On the physical side, there is evidence that high levels of mental stress can adversely affect the body's immune system. In research reported in the early 1990s, hundreds of healthy British adults were exposed to cold viruses under controlled conditions. Those in the highest-stress group were found five times as likely to become infected and twice as likely to develop full-fledged colds as those in the lowest-stress group.[21] In late 1991, a team of cardiologists showed that stress can cause abnormal constriction of blood vessels in patients whose coronary arteries are already clogged with atherosclerotic plaque. The stress-linked narrowing of the arteries further impedes blood flow to the heart, raising the chances of heart attack.[22]

Psychiatrists widely accept the notion that stress can play a significant role in triggering episodes of severe depression. In the late 1980s, National Institute of Mental Health psychiatrist Philip Gold suggested how this linkage might work: When confronted by a threat, we naturally experience a "fight or flight" response—a complex biochemical and behavioral mobilization of the mind and body that includes increased respiration rate, a general sense of alertness, and a feeling of released energy. In the short run, this is a healthy, normal reaction that is vital to our survival individually and as a species. But sustaining this level of arousal for long periods produces serious, even dangerous effects.

Gold's work focused on melancholic depression, a relatively common form of severe depression with a clear and consistent set of symptoms (including low self-esteem, hopelessness and intense anxiety about the future). He suggests that depression results when the mechanisms that normally regulate the stress response go awry and a free-running state of constant stress develops. The "fight or flight" stress response may work well as a reaction to an acute, short-lived physical threat, the kind of threat for which it evolved. But the emotional stress so common to modern life tends to be ongoing, longer term and cumulative. Extended periods of high stress (particularly emotional stress) can overload the system, leading to maladaptive reactions like severe depression.[23]

The effects of chronic stress may be temporary, subsiding when the sources of stress are removed, or they may have a very long reach, possibly even affecting the physical structure of the brain.[24] Acute stress from emotional traumas such as job loss, divorce and the death of a loved one can have both powerful short-term effects and long-term impacts that can last from a few years to a lifetime. The most extreme, longest-term reactions to stress seem to occur where the level of stress is both high and prolonged.

In recent years, one of the more celebrated effects of stress has been post-traumatic stress disorder (PTSD), discussed briefly in the previous chapter. An immediate or delayed aftermath of trauma, the disorder involves recurring dreams, memories and even flashbacks of the traumatic events sometimes triggered by a sight, sound, smell or situation with some relationship to the original crisis. PTSD typically involves emotional detachment from loved ones, extreme suspicion of others and difficulty concentrating.

At least 500,000 of the 3.5 million American soldiers who served in Vietnam have been diagnosed as suffering from PTSD.[25] An estimated 30 percent suffer from such a severe version of the disorder that they will never lead a normal life without medication and/or therapy.[26] A quarter of those who saw heavy combat were involved in criminal offenses after returning to the United States. Only 4 percent of those had had prior psychological problems.[27] A 1997 study of Vietnam veterans with PTSD found that they were also more likely to be suffering from serious physical ailments, such as heart disease, infections, and digestive and respiratory disorders.[28]

It is testimony to the basic soundness of the human mind that the horrors of war often create psychological wounds in combat troops. In the early 1980s, Israeli soldiers suffered nearly a quarter as many psychiatric casualties as physical casualties during the invasion of Lebanon. Israeli Army psychologists claim that the rate of psychiatric to physical casualties was even higher during the 1973 Middle East war, some 40 to 50 percent.[29]

The diagnostic manual of the American Psychiatric Association indicates that PTSD is induced by events that lie "outside the range of usual human experience." But there is evidence that PTSD may be triggered by experiences that are not nearly as unusual as the manual implies. A study of young adults in metropolitan Detroit revealed that some 40 percent of the more than one thousand randomly selected subjects had experienced one or more of the traumatic events that were defined as "PTSD stressors." These included sudden serious injury or accident, physical assault or rape, seeing someone seriously hurt or killed, and receiving news of the unexpected death of a friend or close relative. About a quarter of those who reported these experiences (93 of 394) developed PTSD.[30] If these data are generalizable, PTSD would rank fourth among the most common psychiatric disorders troubling young urban adults.[31]

Trauma can have a very long reach. A 1991 report of psychologists at the VA Medical Center in New Orleans that studied 22 U.S. soldiers who had been taken prisoner during the Korean War found that as many as 19 of them (86 percent) were still suffering from PTSD and other mental problems more than 35 years after their release. More than half of the former POWs who developed PTSD also suffered from other forms of anxiety disorder, such as panic attacks, and about a third experienced severe depression. Prisoners of war appear to be far more likely to develop PTSD than combat veterans.[32] The traumas that they experienced were both prolonged and extreme, involving random killings, forced marches, months of solitary confinement, torture and the like. Yet trauma need not be this extreme to have very long-lasting effects on emotional health and mental stability.

From the perspective of human reliability in dangerous-technology systems, two characteristics of trauma-induced disorders are particularly relevant. First, since the onset of the problems that result from stress disorders may be delayed days, months or even years, someone who appears to be completely recovered from trauma and untouched by such disorders may still harbor them. Psychiatrist Andrew Slaby used the general term "aftershock" to describe "any significant delayed response to a crisis, whether this reaction is anxiety, depression, substance abuse or PTSD."[33] According to Slaby, "everyone, even the calmest, most levelheaded person, has a breaking point that a trauma, or a series of traumas, can set off and bring on aftershock."[34] Second, even if someone who has been severely traumatized in the past does not appear to be dysfunctional or unreliable, his/her ability to cope with stress can be severely compromised. Either chronic stress or the acute stress of a future crisis might overwhelm him/her well before it became severe enough to render a person without such problems unreliable. Because these disorders are common in the human population and can be difficult or impossible to detect, it is impossible to completely avoid them when recruiting large dangerous-technology work forces.[35]

CIRCADIAN RHYTHMS: DISRUPTING THE BIOLOGICAL CLOCK

The behavior and metabolism of most biological organisms seems to be partly regulated by an internal biological clock. For many centuries, it was believed that this rhythmic time pattern was simply the result of plants or animals responding passively to natural cycles in their environment (such as the day-night cycle). But even when an organism is deprived of all environmental time cues (by keeping light, sound, temperature and food availability constant), the majority of its time patterns continue—with a period close to but not exactly 24 hours.[36] Such patterns are called "circadian" rhythms (from the Latin for "approximately one day"). Apparently, most organisms on this planet have internalized the naturally occurring 24-hour period of an earth day.

The part of the human circadian pattern most important to reliability is the sleep-wake cycle, or, more generally, the variation in alertness and psychomotor coordination over the course of a day.[37] When time patterns are abruptly shifted, the internal biological clock is thrown out of phase with the external time of day. For example, flying at jet speed across a number of time zones causes "jet lag," which disrupts sleep, dulls awareness, reduces attention span and produces a general feeling of disorientation and malaise. It takes several days for most people to completely adjust to the simple twice a year, one-hour time shift between standard time and daylight saving time.[38] It is no surprise then that rapidly crossing five, six or more time zones can throw our biological clocks out of balance.

The fundamental problem with being out of phase with external time is that the external world may be demanding highest alertness and capability just when the internal cycle is at lowest ebb. A businessperson flying from New York to London crosses five time zones. When it is 9:00 A.M. in London, he/she will want to be bright and alert to deal with typically high demands at the beginning of a new business day. But his/her internal clock will be set at 4:00 A.M., a time when the level of alertness and psychomotor performance tends to be at or near its daily minimum.[39]

Many dangerous-technology workers must staff all critical duty stations throughout the 24-hour day, every day. That kind of round-the-clock shift work inevitably plays havoc with the biological clock. There appears to be an underlying circadian rhythm that reaches its lowest levels at night, regardless of sleep-wake schedules. Thus, night-shift workers inherently tend to perform less well than day-shift workers. Swedish studies showed that the normal performance of night-shift workers was similar to that of day-shift workers who had lost an entire night's sleep.[40]

Rotating the work schedules of shift workers both aggravates the problem and spreads it to the day shift. Yet a survey by the National Center for Health Statistics in the U.S. showed that by the late 1970s, more than 27 percent of male workers and 16 percent of female workers rotated between day and night shifts. Over 80 percent of these shift workers suffered from insomnia at home and/or sleepiness at work, and there is evidence that their risk of cardiovascular problems and gastrointestinal disorders also increased.[41]

Even if it were possible to keep the same workers on the night shift permanently, that would not solve the problem. Night-shift workers usually try to function on something approaching a day schedule on their days off, so they won't be completely out of step with the world around them. Consequently, their circadian rhythms are in a continual state of disruption. If they don't try to follow a more normal schedule on their days off, they will be much more socially isolated, and that will subject them to increased stress, which will also degrade their performance.

In the early 1980s, a group of applied psychologists in England studied sleep and performance under real-life conditions.[42] They monitored and recorded the sleep of a dozen male factory shift workers in their own homes, then measured their performance at the factory where they all worked. The men were followed over one complete three-week cycle during which they rotated between morning (6:00 A.M. - 2:00 P.M.), afternoon (2:00 P.M. - 10:00 P.M.) and night (10:00 P.M. - 6:00 A.M.) shifts. The researchers found that, compared to night sleep, sleep during the day was lighter, more "fragile." The normal pattern of sleep stages was disrupted. As a result, not only were reaction times significantly slower on night-shift work, but performance tended to get worse as the week progressed. Performance of workers on the morning and afternoon shifts remained nearly stable. Even if night-shift workers took more or longer naps, they could not compensate successfully for the lower quantity and poorer quality of day sleep.[43] "The night-shift worker must sleep and work at times when his or her body is least able to perform either activity efficiently. The body is programmed to be awake and active by day and asleep and inactive by night, and it is extremely difficult to adjust this program in order to accommodate artificial phase shifts in the sleep-wake cycle. . . ."[44]

Circadian rhythms also play a role in disease. The timing of death of both surgical and nonsurgical patients follows a circadian rhythm. Studies of ongoing disease processes in animals show real circadian variation in the average dose of toxins and the severity of injuries that prove fatal. Thus, shift workers may also be more vulnerable to health-related reliability problems. Further, the effectiveness or toxicity of a variety of drugs has been shown to follow a circadian rhythm as well, apparently because of underlying circadian rhythms in drug absorption, metabolism and excretion.[45] Drug and alcohol abuse might therefore reduce the reliability of dangerous-technology shift workers even more than it reduces the reliability of workers on a stable day schedule.

The timing of the accident at the Three Mile Island nuclear power plant in 1979 strongly suggests that circadian factors played a significant role. The operators at Three Mile Island had just passed the middle of the night shift when the accident occurred, at 4:00 A.M. They had been on a six-week slow shift rotation cycle.[46] In general, the incidence of work errors seems to be much higher in the early morning hours for rotating shift workers whose circadian rhythms have not been fully synchronized to their work schedules. According to a study by the National Transportation Safety Board, truck drivers falling asleep at the wheel are a factor in 750 to 1,500 road deaths each year. Fatigue is a bigger safety problem for truckers than drugs or alcohol.[47] According to another study, they are three times as likely to have a single-vehicle accident at 5:00 A.M. than during usual daytime hours.[48]

Poor circadian adjustment is also an important problem in aviation. Late one night, a Boeing 707 jetliner whose crew had filed a flight plan to land at Los Angeles International Airport passed over the airport at 32,000 feet headed out over the Pacific. The aircraft was on automatic pilot and the whole crew had fallen asleep! When local air traffic controllers could not get a response from the aircraft, they managed to trigger a series of alarms in the cockpit. One of the crew woke up. The plane, which had flown a hundred miles over the Pacific, still had enough fuel to turn around and land safely in Los Angeles. The pilot of another jetliner coming in early one morning after a night flight from Honolulu was in the process of landing the plane when he fell asleep only 200 feet above the ground. The copilot realized what had happened and was able to land the plane safely. Not all such incidents have a happy ending. Pilot error was cited as the main cause of the 1974 crash of a Boeing 707 in Bali that killed 107 people. The crew had flown five legs on this flight since it had begun in San Francisco, combining night and day flying across 12 time zones. It is likely that disrupted circadian rhythms were a major contributor to the "pilot error" officially listed as the cause of this accident.[49]

Because most circadian rhythms follow a more or less 24-hour day, forcing workers into an average day length radically different from 24 hours can also interfere with the normal functioning of the biological clock. Yet American nuclear submarine crews normally operate on an 18-hour day. Each sailor is at work for 6 hours, off duty for 12 hours, then back at work for another 6-hour shift. Short-term studies have shown that the 18-hour day can cause insomnia, impaired coordination and emotional disturbance. This schedule is probably one reason for the extremely high turnover rate of American submarine crews. After each voyage, as much as 30 to 50 percent of the enlisted crew does not sign up for another tour. Only a small number of sailors undertake more than two or three of the 90-day submarine missions.[50] The high turnover rate means that a large fraction of the crew on any given voyage is not fully experienced in the operation and maintenance of the ship on which they are sailing, and not used to being confined to a tube sailing under water for three months. This too is a potential source of unreliability.

Finally, disturbances of circadian rhythms have long been associated with certain forms of mental illness.[51] Waking up early in the morning, unable to fall back asleep, for example, is one of the classic symptoms of depression.[52] There is evidence that sleep-wake disorders in manic-depressive individuals may result from misfiring of their circadian pacemakers. It is even possible that those malfunctions may help cause manic-depressive syndrome. In general, studies suggest that disturbances of the biological clock caused by abnormalities in circadian pacemakers may contribute to some forms of psychiatric illness. If so, the circadian disruptions so common among dangerous-technology workers may create reliability problems through this route as well.[53]

LEADERS AND ADVISORS

There is nothing in the exalted positions of political leaders (or the advisors on whose counsel they depend) that makes them immune to any of the reliability problems we have already discussed. There is also nothing in the process of achieving those exalted positions that insures that failures of reliability will not occur. Quite the opposite; in nearly all modern governments, most political leaders follow a long and arduous path to the pinnacles of power. By the time they get there, they have been exposed to a great deal of physical and mental stress, and have often reached an advanced age. By the time they relinquish power, they are older and usually have been subjected to even greater stress. On the positive side, that means that those who reach high political positions have lived enough years to accumulate valuable experience and have shown that they can cope with stress. On the negative side, stress and advanced age certainly do take their toll.

Some people show significant physical or psychological effects associated with aging before they leave their fifties, while others suffer little or no deterioration in intellectual and creative ability well into their seventies or eighties. Bernard Baruch authored the American plan for the control of atomic energy after World War II at age 76; Goethe completed *Faust* at age 80; Michaelangelo was still creating extraordinary sculpture in his 80s.[54] With the right lifestyle, nutrition and exercise, it is possible for individuals to maintain their critical physical capacities much longer as well. Still, the mental and physical capability to cope successfully with the pressures of an acute crisis does tend to diminish with age.[55]

A variety of physical and psychological problems relevant to reliability are more common among people in the later stages of life. And when these problems occur, the process of aging tends to aggravate them. Psychiatrist Jerrold Post cites a series of psychological difficulties that tend to grow worse with age "once the march of symptomatic cerebral arteriosclerosis or other presenile cerebral degeneration has begun": (1) thinking tends to become more rigid and inflexible, with things seen more in terms of black and white, right or wrong; (2) concentration and judgement are impaired, and behavior becomes more aggressive and less tolerant of provocations; (3) there is less control of emotions, with anger, tears and euphoria more easily triggered and a greater tendency to depressive reactions; (4) rather than mellowing, earlier personality traits can become exaggerated (for example, someone who has generally been distrustful can become truly paranoid); (5) the ability to perform mental tasks is degraded, but wide day-to-day fluctuations in mental function can lead others to underestimate the seriousness of the deterioration that has taken place; (6) there is a marked tendency to deny the seriousness and extent of disabilities—a failing leader may therefore "grasp the reins of power more tightly at the very time when he [or she] should be relinquishing them."[56]

Political leaders who have manifested some of these difficulties are as diverse as Joseph Stalin and Woodrow Wilson. Stalin was never a particularly trusting soul. That trait became exaggerated with time, and according to Post, "Joseph Stalin in his last years was almost surely in a clinically paranoid state."[57] Woodrow Wilson became quite ill while president, yet refused to acknowledge the extent of his illness. He "suffered a major cerebrovascular accident [a stroke] in September 1919 which left him paralyzed on the left side of his body and was manifested by severe behavioral changes. The manner in which Wilson stubbornly persisted in fruitless political causes was in part to sustain his denial of disability."[58] The European political leaders of the 1930s have often been condemned for failing to stop the rise to power of aggressive dictators in Germany and Italy short of World War II. But "All the evidence suggests that . . . [the leaders of Europe] were sick men rather than sinners."[59]

The remarkable career of Franklin Delano Roosevelt was filled with physical challenges. He had scarlet fever at school, typhoid fever at age 30, and was stricken by crippling poliomyelitis nine years later. Throughout his life he suffered from serious nose, throat and sinus infections. In 1937 a member of Roosevelt's cabinet said, "the President . . . looks all of fifteen years older since he was inaugurated in 1933."[60] After late 1943, Roosevelt's physical and mental condition continually deteriorated. It was dangerous, and probably irresponsible, for a seriously ill Roosevelt to run for a fourth term in 1944. Aside from the personal consequences, it was not a good idea to have a man as ill as FDR negotiating with Stalin and Churchill over the political future of Asia and Europe and the lives of hundreds of millions of people.

The World War II leader of Britain, Winston Churchill, became prime minister at age 65. Churchill has been described as "a medical textbook in himself." Lord Allanbrooke was chief of the Imperial General Staff, and in daily contact with Churchill. Referring to the prime minister's exhaustion and deterioration in 1944, Allanbrooke noted: "He seems quite incapable of concentrating for a few minutes on end, and keeps wandering continuously"; and "Winston had been a very sick man with repeated attacks of pneumonia and frequent bouts of temperature."[61] In May 1944, the Polish ambassador observed, "I began to wonder whether Churchill . . . really grasped all that was going on. . . Perhaps, however, he has his own reasons for repeating certain things to us over and over again."[62] After Churchill's second serious stroke in 1952, his personal physician noted, "he was not doing his work. He did not want to be bothered by anything." His physician also revealed that Churchill apparently suffered from bouts of severe depression. By the time he resigned in April 1955, his various disabilities caused him to spend most of the day in bed.[63]

At age 65, in his third year as president, Dwight Eisenhower suffered a myocardial infarction (heart attack), apparently as a result of both chronic and acute stress. Fortunately, it came at a quiet time, domestically and internationally. But Eisenhower later commented that if a dangerous situation, such as the Lebanon crisis of 1958, had arisen early in his illness, "the concentration, the weighing of pros and cons, and the final determination would have represented a burden . . . which the doctors would likely have found unacceptable for a new cardiac patient to bear. . . . [However] had there been an emergency, such as the detection of incoming enemy bombers, on which I would have had to make a rapid decision regarding the use of United States retaliatory might, there could have been no question, after the first forty-eight hours of my heart attack, of my capacity to act."[64] Clearly, even in the President's own view, his ability to make critical decisions *within* the first 48 hours after his heart attack was at least questionable.

Sitting at his desk on November 25, 1957, Eisenhower felt a brief giddiness. He could not pick up a piece of paper or grip his pen. It fell to the floor. He could not read or find the right words to express his thoughts or needs. The president had suffered a mild stroke. Understanding that another stroke or heart attack could happen again at some unpredictable time, Eisenhower wrote a detailed letter to Vice President Nixon early in 1958, specifying the procedures under which Nixon would temporarily or permanently take control, in the event he became medically disabled.[65]

The youngest man to be elected to the U.S. presidency (in 1961, at age 43), John F. Kennedy was also troubled by serious medical problems. He suffered from Addison's disease, a condition of the adrenal cortex that results in decreased production of steroid hormones over time. Symptoms include tiredness, weakness, anemia, bouts of diarrhea and indigestion with nausea and vomiting. In a patient with Addison's, even a mild infection can create sufficient stress to cause acute adrenal failure resulting in dehydration and loss of consciousness (among other things) in the absence of careful medical attention.[66] Because of this condition, Kennedy was treated almost continually with steroids from 1947 on. He had injured his back while playing football in 1937, an injury later aggravated during his stint in the Navy in World War II. In 1944, and again in 1954, he underwent back surgery. He used braces and crutches periodically beginning as early as 1952. Kennedy's back problems caused him to suffer from recurrent pain and disability throughout his life.[67]

During the final days of his presidency, Richard Nixon was under enormous pressure as a result of the Watergate scandal. Investigative journalists Bob Woodward and Carl Bernstein reported that General Alexander Haig, White House chief of staff, said Nixon was a battered man, strained to his limit, and he was afraid the president might try to kill himself. Woodward and Bernstein described a meeting between Nixon and Secretary of State Kissinger on August 7, 1974—two days before Nixon resigned in disgrace: "The President was drinking. He said he was resigning. . . . The President broke down and sobbed. . . . Nixon got down on his knees . . . prayed out loud. . . . He was weeping. And then, still sobbing, Nixon leaned over, striking his fist on the carpet, crying, 'What have I done? What has happened?' Kissinger touched the President, and then held him, tried to console him, to bring rest and peace to the man who was curled on the carpet like a child. The President of the United States."[68] Later that night, Nixon telephoned Kissinger. According to Woodward and Bernstein, "The President was slurring his words. He was drunk. He was out of control. . . . He was almost incoherent."[69]

Whatever one's opinion of Richard Nixon and his political career, it is possible to empathize with the specter of a man whose life was coming apart at the seams. Nevertheless, that same man was at this very time commander-in-chief of the world's most powerful armed forces, the only person authorized to order the use of American nuclear weapons on his own judgement. He was at the head of the nuclear chain of command as his life slowly descended into chaos. As long as there are nuclear weapons, it is impossible to insure that no leader of a nuclear-armed nation will ever get into an emotionally tortured state like this again.

On March 30, 1981, three months into his administration, Ronald Reagan was wounded when one of six bullets fired at his entourage ricocheted off his limousine and buried itself in his chest. The Twenty-Fifth Amendment to the Constitution (passed in 1967) provided for the orderly temporary or permanent transfer of power in the event of presidential illness or incapacity. Yet there was no attempt to transfer power when Reagan was shot.[70] Even as he lay in the operating room, undergoing surgery under anesthesia, Reagan still held all presidential powers.

The public was led to believe that Ronald Reagan was not badly wounded. However, according to Stanford University medical professor Herbert Abrams, Reagan's condition was much more serious than was admitted at the time.[71] By the time he was wheeled into the operating room to have the bullet removed from just behind his heart, he had lost 35 percent of his blood, though the bleeding had been slowed and his blood pressure kept up by transfusions. By the time he entered the recovery room he had lost about 50 percent of his total blood volume. He continued to cough up blood the next day. Speaker of the House Tip O'Neill visited Reagan that day, and, shocked by his appearance, later commented, "in the first day or two after the shooting he was probably closer to death than most of us realized." Yet that day a White House staffer was quoted in the *Wall Street Journal* as saying, "If a really grave crisis occurs, Mr. Reagan would be on top of it."[72]

Reagan was still seriously debilitated nearly two weeks after the attack: "A visitor describes him as 'pale and disoriented, walking with the hesitant steps of an old man.' Entering a room, Reagan starts to sit down and 'falls the rest of the way, collapsing into his chair.' He can concentrate for only a few minutes at a time and is able to work and remain attentive for only an hour or so a day."[73] In the opinion of his personal physician, Reagan was not fully recovered until October, more than half a year after the attack.[74] Then in 1994, six years after leaving the presidency, Ronald Reagan was diagnosed as having Alzheimer's disease, a disease characterized by progressive deterioration of mental faculties. Alzheimer's can proceed so slowly that it can significantly affect the kind of mental functions critical to decision making for years before it is finally diagnosed.[75]

Fourteen of the eighteen U.S. presidents who held office during the twentieth century had significant illnesses during their terms. Four had strokes; five suffered from various kinds of chronic respiratory illness; six underwent major surgery at least once; seven suffered from serious gastrointestinal disorders; and nine had heart disease. Wilson, Franklin Roosevelt, Eisenhower, Johnson and Reagan were medically incapacitated while president; Harding, FDR, McKinley and Kennedy died in office (the latter two by assassination). Four of the seven leaders of the USSR suffered from serious heart conditions and five died while in office.[76]

After the collapse of the Soviet Union, Boris Yeltsin became the first president of Russia. He had been first hospitalized for heart trouble in the late 1980s. In July 1995, he was rushed to the hospital with "acute heart problems." It appears that he had yet another heart attack that was kept secret in the spring of 1996, and subsequently had major coronary-bypass surgery. In the first six months after his re-election, he was able to work in his office for only two weeks.[77] As of early 1999, it was clear that Yeltsin remained a very sick man, still holding the reins of power in an economically and politically deteriorating nation, a nation armed with the world's second-largest nuclear arsenal.

The kinds of illness and trauma that have so frequently plagued political leaders do not simply affect physical function. They can impair psychological function as well. Heart attacks, for example, are often followed by anxiety, depression and difficulties in sleeping and concentrating. In more than half the patients, some of these psychological disturbances persist for months after the attack. According to one study, more than 30 percent suffer from irritability, fatigue, impaired memory, inability to concentrate and emotional instability for six months to two years after their heart attack.[78]

Strokes, another common problem in aging leaders, cause many patients to suffer from depression, anxiety and emotional volatility; 40 to 60 percent are cognitively and emotionally impaired. Inability to sleep and feelings of hopelessness are also common. Severe depression may persist for 6 to 24 months. Major surgery also produces important psychological side effects, including confusion serious enough to make it hard to think clearly (especially in elderly patients). It can produce disorientation and an inability to grasp concepts and use logic.[79]

Depression and anxiety are both common effects of serious physical illness and trauma in general. People who are depressed have a hard time focusing their attention, concentrating and remembering. They tend to overemphasize negative information; their analytic capabilities can be seriously impaired. Anxiety also degrades learning and memory, as well as interfering with the ability to reason. These are extremely serious problems for any leader having to make crucial decisions, or any advisor upon whose counsel a leader must depend in a crisis.

FAMILIARITY

There is one more issue of individual fallibility that is often overlooked. When put into a novel work situation, especially one which involves expensive, dangerous or otherwise critical systems, people tend to be very careful of what they do—for a while. But no matter how expensive or dangerous the systems might be, if things go well and all is calm for a long time, most people begin to assume that nothing will go wrong. The cutting edge of their vigilance begins to dull. Even if familiarity does not breed contempt, it does breed sloppiness.

There is no reason to expect that it is any different in dangerous technological systems. Military personnel assigned to duty that brings them directly in contact with nuclear weapons undoubtedly feel a sense of awe and danger at first. But after months of guarding them, loading them on ships or planes, etc., nuclear weapons are just another bomb, if not just another object. If this seems exaggerated, consider how careful most people are when they first learn to drive. Being aware that they could get hurt or killed in a car crash tends to make beginning drivers more careful—for a while. But once they get comfortable with the act of driving, most people pay much less attention its inherent dangers. The car is just as deadly, but the act of driving has become much more routine.

The tendency to relax once we become familiar with a task is not only a common human trait, it is useful in most situations. But when it causes vigilance to fail in dealing with critical dangerous technological systems, it can lead to catastrophe. There is no way to completely avoid this or any of the other fundamental problems of individual fallibility we have discussed, no way to be sure that we can completely avoid recruiting workers whose reliability has been compromised by the vulnerabilities, traumas and afflictions that are part of every human life.

Because we humans are, after all, social animals, programmed to interact with each other, it is not enough to consider our behavior as individuals. When we function as part of a group, as we so often do, the behavior of the group can be very different from the sum of our individual behaviors. It is now time to consider just how dramatically that difference can affect the reliability of those who interact with dangerous technologies.

CHAPTER NINE

The Failure of Technical Systems

More than ever before, we are dependent on a web of interconnected technical systems for our most basic needs and our most fleeting whims. Technical systems are integral to providing us with water, food and energy, to getting us from place to place, to allowing us to communicate with each other and coordinate all the activities on which our physical and social lives depend. The more technical systems have become central to our way of life and critical to the normal functioning of society, the greater the disruption caused when they fail.

Most of us don't really understand how any of these complex and sophisticated technical systems work, and no one understands them all. Most of the time, that isn't much of a problem. We don't have to know how they work to use them, and often don't need detailed technical knowledge to maintain or repair them. Knowing which pedal to push to speed up or slow down, when and how much to turn the steering wheel, how to back up and so on is all you need to know to drive a car. You don't have to understand what actually happens inside. Even those who repair cars don't need engineering or scientific knowledge of the electrical, chemical, and mechanical processes that make the car work. All they need to know is what each part does and how to adjust, repair or replace it.

Technical expertise is also not necessary to understand why technical systems fail and why the possibility of failure cannot be completely eliminated. It is enough to generically comprehend the inherent problems involved in developing, producing and operating them, as well as in assessing their costs, benefits and risks. There is great power in technology, but there are also inherent limits to that power.

COMPLEXITY AND RELIABILITY

The reliability of a technical system depends on both the reliability of its parts and the complexity of the system. Complexity, in turn, depends upon the number of parts and how they interact with each other. All other things being equal, the more parts there are that must perform properly for the system to work, the less reliable the system will tend to be.[1] Multiplying the number of parts can make the whole system less reliable even if each part is made more reliable.[2] Greater interdependence among components also tends to make the system less reliable.[3]

In a system with more parts, there are more ways for something to go wrong. Given the same quality of materials, engineering and construction, a system with more parts will thus fail more often. When the parts of a system are tied together more tightly, the failure of any one part is more likely to overload or otherwise interfere with the other parts. One failure tends to lead to others, dragging the system down. At first this may only degrade performance, but if it produces a cascading series of failures, it can cause the whole system to break down completely.

The complex of satellites orbiting the earth has, in effect, become just such an increasingly interdependent technical system. Some near-earth orbits are so full of active satellites, dead satellites, discarded rocket booster stages, and an enormous amount of small, miscellaneous debris that even a small scrap of very high speed space junk smashing into a large orbiting object could shatter it into hundreds of pieces, which would then shatter other objects in a continuing chain reaction. Although it would take decades for this slow-speed chain reaction to run its course, it could destroy many billions of dollars worth of vital satellites. Some experts believe we are already near the critical point at which a random collision could start this expensive disaster in motion.[4]

Sometimes complexity is unavoidable. Achieving the required performance might require a complex design. The more complex version might also be faster, safer, cheaper to operate, or higher precision than a simpler design. Still, increasing the number of and interdependence of components rapidly overwhelms attempts to make the system more reliable by improving the reliability of each of its parts. Despite our best efforts, complicated technical systems tend to fail more often than simpler ones.

The Therac 25 linear accelerator, an electron-beam and X-ray radiation therapy machine, was designed to destroy tumors deep inside a cancer patient without damaging skin tissue. On three separate occasions in 1985 and 1986, the machine failed, delivering a dose 100 times larger than the typical treatment dose. Two patients died, the third was severely burned. Therac 25 had a metal target designed to swing into place and convert its high-energy electron beam into lower energy X-rays. A minor error in the machine's software made it unable to keep up when instructions were typed at unusually high speed. The critical target apparently failed to swing into place. It is not even clear that complex and sophisticated computer controls were needed for this function. A simple on-off switch and timer might have done the job just as well, with a much lower probability of failure.[5]

In an internal briefing for the Air Force in 1980, military analyst Franklyn C. Spinney documented the reliability-reducing effects of complexity.[6] Using several different measures, he compared the reliability of aircraft of varying complexity in both the Air Force and Navy arsenals. Data drawn from his analysis are given in Table 9-1.

All modern combat aircraft are very complex, interdependent, high-performance technical systems. Even the most reliable of them breaks down frequently. None of the aircraft in the sample averaged more than 72 minutes of flying time between failures (problems that require maintenance), averaged fewer than 1.6 maintenance events per flight or had all of the equipment essential for its mission operating properly more than 70 percent of the time. Anyone whose car broke down anywhere near this often would consider that car a world-class lemon.

Even so, substantial differences in complexity do give rise to major differences in reliability. While the complexity designations in the table are necessarily general, there is a clear pattern of reduced reliability with increasing complexity, by any of the measures used. The contrast between the most and least reliable aircraft is striking. The highly complex F-111D averaged only 12 minutes of flying between failures, while the much simpler A-10 flew six times as long between problems. At least one piece of equipment essential to the F-111D's mission was broken nearly two-thirds of the time, while the A-10 was fully mission capable twice as often. And the F-111D averaged more than six times as many maintenance problems as the A-10 every time it flew.

Complexity-induced failures of reliability are an inherent feature of all technical systems, be they single machines or large interconnected networks of equipment. The primary air traffic control system is based on computerized radar tracking. Computers in the regional air route traffic control centers receive a continuous flow of data from radars transmitted via telephone lines. The computers are designed to diagnose and correct a variety of malfunctions. Nevertheless, in 1980 the system was experiencing an average of one interruption

TABLE 9-1
COMPLEXITY AND RELIABILITY IN MILITARY AIRCRAFT
(FY 1979)

AIRCRAFT (AF=AIR FORCE; N=NAVY)	RELATIVE COMPLEXITY	AVERAGE PERCENTAGE OF AIRCRAFT NOT MISSION CAPABLE AT ANY GIVEN TIME	MEAN FLYING HOURS BETWEEN FAILURES	AVERAGE NUMBER OF MAINTENANCE EVENTS PER SORTIE
A-10 (AF)	Low	32.6%	1.2	1.6
A-4M (N)	Low	31.2%	0.7	2.4
A-7D (AF)	Medium	38.6%	0.9	1.9
F-4E (AF)	Medium	34.1%	0.4	3.6
A-6E (N)	High	39.5%	0.3	4.8
F-14A (N)	High	47.5%	0.3	6.0
F-111D (AF)	High	65.6%	0.2	10.2

Source: Spinney, F.C., *Defense Facts of Life* (December 5, 1980: Department of Defense unreviewed preliminary staff paper distributed in typescript by author).

of service of a minute or longer per center per week. That doesn't sound like much . . . until you realize that a modern jetliner flies about nine miles in one minute (at normal cruising speed). On average, these disruptions lasted seven minutes.[7] For most of us, a one-minute telephone outage or switching error is little more than a nuisance. We just hang up and dial again. But even short-lived interruptions in transmission or switching failures can create serious, even deadly problems in critical systems such as those used for air traffic control.

The complex, interconnected telephone system fails fairly often, though most of these failures are so fleeting and trivial we scarcely notice them. Every once in a while, though, we get a spectacular illustration of just how wrong something can go when something does go wrong. At 2:25 P.M. on January 15, 1990, a flaw in a single AT&T computer program disrupted long-distance service for nine hours. Roughly half the national and international calls made failed to connect.[8] Robert Allen, AT&T's chairman, called it "the most far-reaching service problem we've ever experienced."[9]

The program involved was part of a switching-software update designed to determine routings for long-distance calls. Because of the flaw, a flood of overload alarms was sent to other computers, stopping them from properly routing calls and essentially freezing many of the switches in the network.[10] Ironically, the system had been designed to prevent any single failure from incapacitating the network.[11] Furthermore, there was no sign that anything was wrong until the problem began, but once it did, it rapidly spun out of control. In the words of William Leach, manager of AT&T's network operations center, "It just seemed to happen. Poof, there it was."[12]

Ten years earlier, a forerunner of the Internet called "Arpanet," then an experimental military computer network, failed suddenly and unexpectedly. Its designers found that the failure of a small electronic circuit in a single computer had combined with a small software design error to instantly freeze the network.[13] In 1987, a complex network of hundreds of computers TRW had created for U.S. intelligence in Europe began to behave in peculiar and unpredictable ways. On careful investigation, engineers could not find anything wrong with the way it had been designed. Yet it was clearly not performing as intended.[14]

Opacity

As technical systems become more complex, they become more opaque. Those who operate ever more complex systems usually cannot directly see what is going on. They must depend on readings taken from gauges and instruments, and this can be very misleading. During the buildup to the massive power failure New York City experienced in 1977, one of the operators checked a current-flow reading on a particular line and saw it was zero. Since that line normally carried little if any current, that part of the system seemed to be operating normally. But what the operator was really seeing was the combined result of two switching failures, one of which would have sent current surging through that line if the second failure hadn't blocked the flow of any current to the line. The indirect information on which the operator was relying created a false sense of confidence. When the lights finally went out in the operator's control room, it became clear enough that something was very wrong.[15]

When a system becomes so complex that no one—including its designers—can really visualize how the system as a whole works, patchwork attempts to fix problems or enhance system performance are likely to create other hidden flaws. Just such an attempt seems to have caused the great AT&T crash of 1990. In 1976, AT&T pioneered a system called "out of band" signalling, which sent information for coordinating the flow of calls on the telephone network as each call was made. Engineers who were updating the out-of-band system in 1988 inadvertently introduced the software flaw that caused the system to crash two years later.

Those who modify very complex systems often do not understand enough about how they work to completely analyze all the ways in which changing one part will affect the rest of the system under all conceivable conditions. If they are careful and do the job properly, they may avoid creating problems in the part of the system they are changing. But it is virtually impossible for them to see all the subtle ways in which what they are doing will alter the overall system's characteristics and performance.

If patchwork change can open a Pandora's box, why not redesign the whole system when it fails or needs updating? Fundamental redesign may be a good idea from time to time, but it is much too time consuming and expensive to do whenever a problem arises or a way of improving the system occurs to someone. And frequent fundamental redesign has a much higher chance of introducing more serious problems than does patchwork change.

Although it sounds unbearably primitive, trial and error is still very important in getting complicated systems to work properly. "Bugs" are inevitable, even in the most carefully designed complex systems, *because* they are complex systems. Only by operating them under realistic conditions can we discover and correct unexpected (and sometimes unpredictable) problems and gain enough experience to have some confidence in their reliability. That is why engineers build and test prototypes. How confident would you feel flying in an airliner of radically new design that had never actually been flown before?

On April 24, 1990, the National Aeronautics and Space Administration (NASA) successfully launched the Hubble Space Telescope. Nearly a month later, Hubble produced its first blurry light image. Euphoria soon turned to concern, as the telescope just would not come into perfect focus, despite repeated commands from ground controllers at the Goddard Space Center outside Washington. Two months after launch, it became clear that the telescope suffered from spherical aberration, a classic problem covered in basic optics textbooks. A very slight flaw in the curvature of the Hubble's 2.4-meter primary mirror resulted in the optical system's failure to focus all incoming light at precisely the same spot. More than a decade of painstaking development had failed to prevent this crippling defect, and an extensive program of testing had failed to detect it. Scientists estimated that up to 40 percent of the scientific experiments the $1.6 billion space telescope was designed to carry out would have to be completely given up, and most of the remainder would be negatively affected. It would be years before the Hubble could be fixed.[16]

In December 1993, the telescope was finally repaired by a team of astronauts riding the space shuttle *Endeavor* into orbit. After more than a year of painstaking earthbound rehearsals, the astronauts were able to replace some defective equipment and install carefully designed corrective devices during an unprecedented series of space walks.[17] The next month, NASA jubilantly announced that the long-awaited repairs had been successful. Although Hubble still did not meet its original design specifications, it had finally been brought into clear focus and was producing remarkable images of the heavens.[18] By late March 1999, the space telescope was once more in trouble. Only three of Hubble's six gyroscopes were working properly. If one more failed, the telescope would become too unsteady to do observations and would shut down. NASA prepared to launch an emergency repair mission by October, but there was an estimated 20 percent chance that another gyroscope would fail before then.[19]

Sometimes even careful design, testing *and* early experience leaves critical problems hidden until a substantial track record has been built up. The De Havilland Comet was the first commercial jet aircraft. In May 1953, a year after the inauguration of jetliner service, a Comet was destroyed on takeoff from Calcutta during a severe thunderstorm. The weather was blamed. Eight months later, a second Comet exploded soon after takeoff from Rome, Italy, in clear and calm weather conditions. The Comets were withdrawn from commercial service for ten weeks, then reinstated even though investigators were still unable to find any flaw in the planes. In April 1954, a third Comet exploded in mid air. Only when one of the remaining Comets was then tested to destruction was it determined that the plane had a critical flaw. Repeating the normal cycle of pressurizing and depressurizing the cabin again and again caused a fatigue crack to develop in the corner of one of the windows that soon tore the plane's metal skin apart. The Comet's designers had been confident that such a problem would not develop until many more flights than the plane was capable of making during its estimated service life. They were wrong. Only in the trial and error of continuing operation was their tragic mistake exposed.[20]

Backup Systems and Redundant Design

Reliability can usually be improved by creating alternative routes that allow a system to keep working by going around failed components. When these alternate routes remain unused until there is a failure, they are called backup systems. For example, hospitals typically have their own backup generators to keep critical equipment and facilities operating when normal power supplies are disrupted. Emergency life vests on airliners are designed to inflate automatically when a tab is pulled, but they have a backup system—tubes through which a passenger can blow to inflate them if the automatic system fails.

Alternate routes used during normal operation can also operate as backups when failures occur. For example, calls can be routed over the telephone network from point A to point B over many possible pathways. In normal times, this allows the system load to be distributed efficiently. But the same design also allows calls to go through even when part of the system fails, by routing them around failed components.

"Voting" systems are another means of using redundancy to achieve reliability. "Triple modular redundancy" (TMR) is sometimes used in the design of fault-tolerant computers. Three components (or "modules") of identical design are polled and their outputs compared. If one disagrees with the other two, the system assumes the disagreeing module is faulty, and acts on the output of the two that agree. In this way, the system can continue to operate properly even if one of the modules fails.[21]

Backup systems and redundant design can make the system as a whole more reliable than any of its parts.[22] Still, backup systems themselves can also fail. In 1976, the failure of both the main audio amplifier and its backup left Gerald Ford and Jimmy Carter speechless for 27 minutes before an estimated audience of 90 million viewers during the first presidential campaign debate in 16 years.[23] Three separate safety devices designed to prevent chemical leaks all failed during the Bhopal disaster in 1984.[24] Many backup systems failed during the nuclear power plant accident at Three Mile Island on March 28, 1979, and the much more serious accident at Chernobyl on April 26, 1986. In October 1980, when technicians entered the containment building at New York's Indian Point nuclear power plant, they discovered areas flooded with nine feet of cold, brackish water that had leaked into the building from the Hudson River. A safety device had failed to detect the flooding because it was designed to detect only hot water. Two sump pumps designed as a backup should have triggered automatically and removed the water, but both failed—one because of blown fuses, the other because of a stuck mechanism.[25]

Boeing 747 jetliners have three sophisticated navigational systems. Yet on December 20, 1989, a navigational system failure led a Thai Airways 747 carrying 391 people to mistakenly reverse its course over the northern Pacific and begin flying east instead of west. The plane flew 600 miles off its flight path before it was notified of the problem by air traffic controllers. When they finally convinced the pilot that he was going the wrong way, he reported that all of the navigational devices had failed.[26]

Adding backup systems or redundancies tends to make a system design more complex, creating potential reliability problems that offset at least some of the advantages of having those backups or redundancies. One of the nine Ranger spacecraft flights intended to survey the moon before the Apollo mission failed *because* of extra systems designed into it to prevent failure. To be sure that the mission's TV cameras would come on when the time came to take pictures of the moon's surface, redundant power supplies and triggering circuits were provided. A testing device was included to assure that those systems would work properly. But the testing device short-circuited and drained all the power supplies before the spacecraft reached the moon.[27]

Common-Mode Failure and Sensitivity

When several components of a system depend on the same part, the failure of that part can disable all of them at the same time. This is known as a "common mode" failure. For example, if a hospital's backup generator feeds power into the same line in the hospital that usually carries electricity from the power company, a fire that destroyed that line would simultaneously cut the hospital off from the outside utility and make the backup generator useless.

At 4:25 A.M. on March 20, 1978, an operator replacing a burned-out light bulb on the main control panel at the Rancho Seco nuclear power plant near Sacramento dropped the bulb. This trivial event led to a common-mode failure that almost triggered disaster. The dropped bulb caused a short circuit that interrupted power to key instruments in the control room, including those controlling the main feedwater system. The instrument failures not only caused the main feedwater system to malfunction, but also cut off information the operators needed to know what to do. Equipment designed to control the reactor automatically didn't take proper corrective action because it also depended on the malfunctioning instruments. Worse yet, the instruments sent false signals to the plant's master control system, which then caused a rapid surge in pressure in the reactor's core, combined with falling temperatures.[28] In an older reactor, this is very dangerous.

The resistance to fracture of the steels from which pressure vessels are made depends on the metal's temperature. If it falls below the "reference temperature," the metal becomes very brittle and prone to break. Given enough time, neutron irradiation from the reactor's core can raise the reference temperature high enough so that rapid cooling of the reactor vessel may bring the metal close to this critical threshold. A sharp increase in pressure could then cause any pre-existing cracks in the vessel to grow quickly, producing a potentially catastrophic fracture. If the Rancho Seco power plant had been operating at full power for 10 to 15 years instead of 2 or 3, the vessel might have cracked.[29] With no emergency system left to cool the core, that could have led to a core meltdown and a nightmarish nuclear power plant accident.

Just after 4:00 PM on July 19, 1989, a United Airlines DC-10 jumbo jet carrying nearly 300 passengers and crew crashed short of the runway at Sioux City, Iowa, and burst into flames, killing 112 people. The problem was a loss of control due to failure of all three of the plane's hydraulic systems. The failure of any one would make it harder to fly the plane. With two gone, "the plane is like a drunk elephant," but it can still be flown.[30] In the United accident, an explosion in the rear engine showered the tail with shrapnel. All three hydraulic systems run through the tail section of the plane, and so all three of the hydraulic lines were severed at once. With no shut-off valve available, hydraulic fluid began to leak from the damaged lines, causing the pilot to lose control.[31]

On January 9, 1995, construction crews at Newark Airport using an 80 foot pile driver to pound 60-foot steel beams into the ground drove one beam through a foot-thick concrete wall of a conduit 6 feet under ground and severed three high-voltage cables serving the airport's terminal buildings. Hundreds of flights were cancelled and tens of thousands of people had to scramble to rearrange travel plans, as the airport was forced to shut down for nearly 24 hours. Local power company officials said that if one cable or even two had been knocked out, there still would have been enough power to keep the airport operating. If the main power cable and auxiliary power cables ran through separate conduits rather than lying side by side in the same conduit, this expensive and disruptive common-mode failure would not have occurred.[32]

Unless every part of a system has an alternative to every other part on which it depends, common-mode failures can undo some or all of the advantages of backup systems and redundancy. As long as there are any unique common connections, there can be common-mode failures that render the system vulnerable. But duplicating every part of every system is simply not workable. In a hospital, that would involve duplicating every power line, every piece of equipment, even to the point of having a spare hospital available.

High-performance technical systems are often more sensitive, as well as more complex. Greater sensitivity also predisposes systems to reliability problems. The high-performance aircraft of today are much more sensitive to variations in fuel, collisions with birds, and the quality of materials used to manufacture them than were the planes of 50 years ago. And for all their disadvantages, electronic devices that relied on vacuum tubes were much less sensitive to voltage surges and other disruptions of current than modern solid-state electronics.

More-sensitive devices are more easily overloaded, and thus more prone to failure. They are also more likely to react to irrelevant and transient stimuli. A highly sensitive smoke alarm will go off because of a bit of dust or a burned steak. False alarms make a system less reliable. They are failures in and of themselves, and if they are commonplace, operators will be too likely to assume that the next real alarm is also false.

Highly sensitive, complex interactive systems can also behave unpredictably, undergoing sudden explosive change after periods of apparent stability. When the Dow Jones average plummeted by 508 points at the New York Stock

Exchange on October 19, 1987, losing 22 percent of its value in one day, many were quick to point an accusing finger at computerized trading practices. Programmed trading by computer, it was argued, had made the market less stable by triggering buying and selling of large blocks of stock in a matter of seconds to take advantage of small movements in prices. A stock market of program traders approximates the key assumptions underlying the theory of nonlinear game dynamics (including rivalry). When systems like this are modeled on a computer, strange behaviors result. The system may be calm for a while and seem to be stable, then suddenly and unpredictably go into sharp nonlinear oscillations, with both undershooting and overshooting.[33]

DESIGN ERROR

Engineering design results in a product or process that never existed before in that precise form. Mathematical verification of concepts, computer simulation, and laboratory testing of prototypes are all important and useful tools for uncovering design errors. But until the product or process works properly under real-world conditions, it has not really been put to the test.

In 1995, after 14 years of work and 6 years of test flights, the B-2 bomber still had not passed most of its basic tests, despite an astronomical price tag of more than $2 billion a plane. The design may have looked fine on the drawing board, but it wasn't doing so well in the real world. Among other things, the B-2 was having a lot of trouble with rain. GAO auditors reported, "Air Force officials told us the B-2 radar cannot distinguish rain from other obstacles."[34] Two years later, they reported that the plane "must be sheltered or exposed only to the most benign environments—low humidity, no precipitation, moderate temperatures."[35] Not, on the whole, the kind of conditions military aircraft typically encounter. The B-2 was first used in combat in March 1999, during the NATO air campaign against Yugoslavia. Since they were too delicate to be based anywhere that didn't have special facilities to shelter and support them, two B-2s were flown out of their home base in Missouri, refueled several times in the air each so that they could drop a few bombs and then hurry back to Missouri, where they could be properly sheltered and cared for.[36]

Designers of the space shuttle booster rockets did not equip them with sensors that could warn of trouble because they believed the boosters were, in the words of NASA's top administrator, "not susceptible to failure. . . . We designed them that way."[37] After many successful launches, the explosion of the right-side booster of the space shuttle *Challenger* in 1986 proved that they were very wrong. That same year, a design flaw that had made the RBMK-1000 reactor unstable at low power from the beginning finally led to disaster, as two explosions at Chernobyl released "hundreds of times more radiation than was produced by the atomic bombings of Hiroshima and Nagasaki."[38]

Sometimes a design fails to perform as desired because the designers are caught in a web of conflicting or ambiguous design goals. The designer of a bridge knows that using higher-grade steel or thicker concrete supports will increase the load the bridge is able to bear. Yet given projected traffic, a tight construction schedule and a tight budget, the designer may intentionally choose a less sturdy, less expensive design that can still bear the projected load. If someday a key support gives way and the bridge collapses under much heavier traffic than had been expected, it is likely to be labelled a design error. But whose error is it: the engineer who could have chosen a stronger design, the person who underestimated future traffic, or the government officials who insisted the bridge be built quickly and at relatively low first cost?

Designers always try to anticipate what might go wrong when their design is put to the test in the real world, so they can prevent problems from developing. But there are so many ways things can go wrong that even the best designers can never think of them all. In June 1995, launch of the space shuttle *Discovery* had to be indefinitely postponed because a flock of "lovesick" male woodpeckers intent on courting pecked at least six dozen holes (some as big as four inches wide) in the insulation surrounding the external fuel tanks.[39] That would have been a hard problem to foresee. The odds are good that if one of the shuttle's designers had raised the possibility that passionate woodpeckers might someday attack the fuel tank insulation en masse, the rest of the design team would have laughed out loud.

Complexity, Interactions and Design Error

Failure to understand or pay attention to the way components of a complex system interact can be disastrous. The Northern California earthquake of October 17, 1989, brought down a mile and a quarter stretch of the elevated Nimitz Freeway in Oakland, killing and injuring dozens of motorists. Reinforcing cables installed on columns supporting the two-tiered, elevated roadway as part of the state's earthquake-proofing program may actually have made the damage worse. The quake sent rolling shock waves down the highway, and when some of the columns and cables supporting the roadbed collapsed, they pulled adjoining sections down one after another, like dominoes.[40]

On January 4, 1990, the number three engine fell off a Northwest Airlines Boeing 727. Investigators didn't find anything wrong with the design or construction of the engine, the way it was attached to the fuselage, or the fuselage itself. Instead, they reported that the loss of the engine was the result of a peculiar interaction. Water leaking from a rear lavatory was turned into ice by the cold outside air. The ice built up and then broke loose, striking the engine and causing it to shear off. In 1974, a National Airlines 727, and in 1985, an American Airlines 727 had lost the same engine in flight, for the same reason.[41] Designers just had not anticipated that a water leak in a lavatory could threaten the integrity of the aircraft's engines.

Even the designers may not fully comprehend the workings of complicated systems. It is impossible to enumerate, let alone to pay attention to, all of the ways things can go wrong. After-the-fact investigations often determine that failure was due to a simple oversight or elementary error that causes us to shake our heads and wonder how the designers could have been so incompetent. But mistakes are much easier to find when a failure has focused our attention on one particular part of a complex design.

One of the worst structural disasters in the history of the United States occurred on the evening of July 17, 1981, when two crowded suspended walkways at the Hyatt Regency Hotel in Kansas City collapsed and fell onto the even more crowded floor of the lobby below. More than a hundred people were killed and nearly two hundred others were injured. When investigators finally pinpointed the problem, technical drawings focusing on a critical flaw were published on the front page of the *Kansas City Star,* as well as in technical journals. An ambiguity in a single design detail had led the builder to modify the way that the walkways were connected to the rods on which they were suspended from the ceiling. That change made them barely able to support their own weight, let alone crowds of people dancing on them. Yes, the problem should have been caught during design or construction, when it could have been easily solved. But the fatal flaw was much easier to see once the collapse forced investigators to carefully examine how the walkways were supported. At that point, the critical detail was no longer lost in the myriad of other details of the building's innovative design.[42] Unless a great deal of attention is paid to interactions, knitting together the best-designed components can still produce a seriously flawed system design. Before computers, thorough analysis of complex designs was so difficult and time consuming that good designers placed a high value on simplicity. When computers became available, designers gained confidence that they could now thoroughly evaluate the workings of even very complicated designs. This degree of confidence may have been unwarranted. After all, a computer cannot analyze a design, it can only analyze a numerical model of a design. Any significant errors made in translating an engineer's design into a computer model render the computer's analysis inaccurate. So do any flaws in the software used to analyze the numerical models.

The piping systems of nuclear power plants are so complex, it is hard to imagine designing them without the use of computers. Yet one of the computer programs used to analyze stresses in the piping system was reportedly using an incorrect value for pi (the ratio of the circumference to the diameter of a circle). According to civil engineer Henry Petroski, in another "an incorrect sign was discovered in one of the instructions to the computer. Stresses that should have been added were subtracted . . . leading it to report values that were lower than they would have been during an earthquake. Since the computer results had been employed to declare several nuclear power plants earthquake proof, all those plants had to be rechecked. . . . This took months to do."[43] Had a serious earthquake occurred in the interim, the real world might have more quickly uncovered the error—with disastrous results.

Writing the programs that model engineering designs, and writing the software the computer uses to analyze these models, are themselves design processes that involve complex, interactive systems. The same cautions that apply to designing any other complex, interactive system apply here as well. A computer cannot hope to accurately appraise a design's performance in the real world unless it is given realistic specifications of system components and the way they interact. That is not an easy thing to do. Abstract numerical models are much easier to build if idealized conditions are assumed. For example, it is much easier to model the performance of an aircraft's wing in flight if it can be assumed that the leading edge is machined precisely, the materials from which the wing is made are flawless, the welds are perfect and uniform, and so on. Taking into account all of the complications that arise when these idealized assumptions are violated—and violated in irregular ways at that—makes building the model enormously more difficult, if not impossible.

The problem of spherical aberration that crippled the Hubble Space Telescope was due to an error in the curvature of its primary and/or secondary mirror of between 1/50 to 1/100 of the width of a human hair.[44] Yet the error still might have been detected if the mirrors had ever been tested together. Each was extensively tested separately, but their combined performance as an optical system was only evaluated by computer simulation.[45] The simulation couldn't have detected an error in curvature unless that error was built into the computer model. That could have been done only if the engineers knew the flaw was there. If they had known that, they wouldn't have needed the computer to tell them about it.

No computer can provide the right answers if it is not asked the right questions. Computers are extremely fast, but in many ways very stupid. They have no "common sense." They have no "feel" for the design, no way of knowing whether anything important is being overlooked. They do what they have been told to do; they respond only to what they have been asked. It is up to the designers and users of a program that analyzes a model to ask the correct questions.

In January 1978, the roof of the Civic Center in Hartford, Connecticut, collapsed under tons of snow and ice only a few hours after thousands had attended a basketball game there. The roof was designed as a space frame, supported by a complicated arrangement of metal rods. After the collapse, it was discovered that the main cause of failure was insufficient bracing in the rods at the top of the truss structure. The bars were bending under the unexpectedly heavy weight of snow and ice, and when the rods that were bent the most finally folded, the part of the roof's weight that they were bearing was shifted to adjoining rods. The unusually heavy load those rods now had to bear caused them to fold, setting up a kind of progressive collapse of the support structure which brought down the roof. A computer simulation finally solved the problem of why and how the accident had happened, but only after investigators had directly asked the right question of a program capable of answering that question. The original designers had used an unduly simplified computer model and had apparently not asked it all the right questions. But their analysis had given them such confidence in their design that when workers pointed out that the new roof was sagging, the designers assured them that nothing was wrong.[46]

Computers are very seductive tools for designers. They take much of the tedium out of the calculations required for routine design. They allow designers to reach more easily into unexplored territory. But as with most things that are seductive, there are unseen dangers involved. Exploring new domains of complexity and sophistication in design means leaving behind the possibility of understanding a design well enough to "feel" when something is wrong or problematic. It is not clear whether or not this will increase the frequency of design error, but it is almost certain to increase the severity of errors that do occur. Undue confidence and opaque designs will make it difficult for designers to catch some catastrophic errors before the real world makes them obvious.

The Pressure for New Design

If we were content to use the same designs year after year in the same operating environment, design error would be much less common. "Tried and true" designs are true because they have been repeatedly tried. Using the same design over many years allows evolutionary correction of flaws that come to light, and more complete comprehension of how the design is likely to be affected by minor variations. As long as new products, structures and systems are replicas of old and operating conditions remain the same, there is less and less scope for catastrophic error as time goes by. But that is not the world in which we live.

In our world, there is constant pressure to look for designs that work better, are more cost effective, more aesthetically pleasing and so on. Design change is driven by our creativity, our need for challenge, our confidence that better is possible, and our fascination with novelty. That means that the technical context within which all of the systems we design must operate is changing constantly. The social context may be changing as well, on its own or directly because of technological change. Automobile technology, for example, greatly increased suburbanization, changing the pattern of land use, our use of time (increased commuting), even the degree of our social interactions with neighbors. It also increased our flexibility of travel, became a major new source of death and injury, and sharply increased environmental pollution and the rate of depletion of nonrenewable resources. The environmental impacts alone tightened the constraints imposed on other technologies. Automotive pollution and resource depletion affected the design of other energy-using systems by raising the priority attached to reducing their own polluting emissions and increasing their fuel efficiency. Thus, the development and diffusion of new designs changes the context within which the design process takes place, which reinforces the need for new designs.

Reaching beyond existing designs brings with it a higher likelihood of error. In military systems, the pressure for new designs is intense, because even a small performance advantage is believed critical in combat. It is therefore not surprising that the designers of weapons and related systems make more than their share of significant design errors. Even when they try to "play it safe" by avoiding radical changes in a proven design, the constant pressure to improve performance opens the door to serious error. The Trident II missile was to be a submarine-launched ballistic missile (SLBM) with greater range and accuracy than Trident I. The first Trident II test-launched at sea exploded four seconds into its flight. The second test went all right, but the third test missile also exploded. The nozzles on the missile's first stage failed. They were damaged by water turbulence as the missile rode the bubble of compressed gas that propels it through 30 to 40 feet of water to the point where it breaks the surface of the sea and its engines can fire. The Navy has been launching SLBMs this way for decades. Trident I had passed this test. But Trident II was much longer and nearly twice as heavy. Its designers expected that it would create more turbulence in the water, but miscalculated in extrapolating previous experience. According to Rear Admiral Kenneth C. Malley, chief of the Navy's ballistic missile program, engineers using computer simulations seriously underestimated both the effect of water jets and how much pressure there would be on the missile as it surged upward through the sea.[47]

Decades earlier the designers of the De Havilland Comet jet airliner made a similarly fundamental miscalculation. Metal fatigue created in the skin of the plane when the cabin was repeatedly pressurized and depressurized was much greater than expected. Aircraft designers of the day were quite familiar with the problem of metal fatigue. But De Havilland was pushing into uncharted waters and, despite extra precautions, made a fatal error. Using "well-established methods," the designers thought that "a cabin that would survive undamaged a test to double its working pressure . . . would not fail in service under the action of fatigue."[48] As it turned out, they were very wrong.

Proponents of relatively new complex technical systems are frequently over-optimistic in projecting their experience with early successes to second- and third-generation versions. Over-optimism comes easily as the enthusiasm that surrounds an exciting new technology combines with a rapid rate of progress in its early stages of development. But later-generation systems are often more sophisticated and very different in scale. Being too ready to extrapolate well beyond previous experience is asking for trouble. This problem has been endemic in the trouble-plagued nuclear power industry. The first commercial plant was ordered in 1963, and only five years later orders were being taken for plants six times as large as the largest then in operation. There had only been 35 years of experience with reactors the size of Unit 2 at Three Mile Island when the partial meltdown occurred. That is very little experience for a technological system so big and complex.[49]

Thirty-five years is forever compared to the operating experience we have with many complex military systems. Design changes are so frequent, introduction of new technologies so common that extrapolation from previous experience is particularly tricky. New military technical systems are frequently not thoroughly tested under realistic operating conditions. It is not surprising that they often don't behave the way we expect them to at critical moments. Even when they are tried out under special test conditions, performance aberrations are sometimes overlooked in the pressure to get the new system "on line." During flight tests beginning in 1996, one of the wings on the Navy's $70 million F/A-18 Super Hornet fighter would sometimes suddenly and unpredictably dip when the plane was doing normal combat maneuvers. Engineers and pilots struggled without success to figure out what was causing this unpredictable "wing drop," which could prove fatal in combat. Though the flaw had still not been fixed, the Pentagon authorized purchase of the first 12 production-model F/A-18s in March 1997.[50]

Acts of God and Assumptions of People

The fruits of engineering design are real products that must be able to withstand the stresses, loads, temperatures, pressures, etc. imposed by their operating environments. Engineers must therefore build assumptions about that environment into the design process. Unfortunately, there is often no way of knowing all of its key characteristics precisely in advance. Consider the design of a highway bridge. It is possible to calculate gravitational forces on the bridge with great accuracy, and to know the load-bearing capabilities, tensile strength and other relevant characteristics of the materials used to construct the bridge (provided they are standard materials). Calculating wind stresses is less straightforward, though still not that difficult under "normal conditions." But it is much harder to calculate the strength and duration of the maximum wind stress the bridge will have to bear during the worst storms it will experience in its lifetime. Or the greatest stress it will have to bear as a result of flooding or earthquake. We simply do not know enough about meteorological or geological phenomena to be able to accurately predict these occasional, idiosyncratic but critical operating conditions. For that matter, we don't always do that good a job projecting future traffic loads either.

The subtle effects of slow-acting phenomena like corrosion can also interact with the design in ways that are both difficult to foresee and potentially catastrophic. In 1967, after 38 years of service, the Point Pleasant Bridge, spanning the Ohio River between West Virginia and Ohio, suddenly collapsed. Seventy-five vehicles were on the bridge, and 46 people were killed. The bridge was suspended from two giant chains made of links 50 feet long, rather than the more standard round wire cables. The design made thorough inspection of the links in the chain difficult, at the same time it encouraged greater than normal corrosion. Over the years, undetected corrosion created cracks that eventually weakened one link to the point where it broke. That shifted the load on the rest of the supports and triggered a rapid progressive collapse of the bridge.[51] Like corrosion, the embrittlement of nuclear reactor vessels (discussed earlier) is also a slow-acting, subtle process that threatens structural strength. Since we have far less experience with embrittlement than with corrosion, it is easier to see why its effects have been dangerously underestimated by some reactor designers.

Because making assumptions about operating conditions is risky but unavoidable, it is common practice to design for "worst case" conditions. That way, any errors made are less likely to cause the design to fail. But what is the worst case? Is it, for example, the worst earthquake that has ever been recorded in the area in which a bridge is being built? Or is it the worst earthquake that has ever been recorded in any geologically similar area? Or perhaps the worst earthquake that has ever been recorded anywhere?

As the assumptions escalate, so does the cost and difficulty of building the bridge. Does it make sense to bear the cost for making all bridges able to withstand the same maximum earthshaking, knowing that few if any of them will ever experience such a severe test? The definition of "worst case" is therefore not purely technical. It almost inevitably involves a tradeoff between risk, performance and cost. Even if the most extreme assumptions are made, there is still no guarantee that more-severe conditions than had been thought credible (such as a worse earthquake than anyone had predicted) won't someday occur. During the great Kobe earthquake of 1995, at least 30,000 buildings were damaged or destroyed, 275,000 people were left homeless and the death toll passed 4,000.[52] Japanese earthquake engineers, among the best in the world, were shocked by the extent of the damage. But ground motions in the quake were twice as large as had been expected. In the words of an American structural engineering expert, the Japanese structures "will perform well during an earthquake that behaves according to their design criteria. But . . . [this] quake did not cooperate with the Japanese building codes."[53]

Engineers also try to insure proper performance by building safety factors into their designs. The safety factor is the demand on a component or system just great enough to make it fail, divided by the demand that the system is actually expected to face. If a beam able to bear a maximum load of 10,000 pounds is used to bear an actual load of 2,000 pounds the safety factor is five; if an air traffic control system able to handle no more than 60 flights an hour is used at an airport where it is expected to handle 40 flights an hour, the safety factor is 1.5. Safety factors are the allowed margin of error.

If we know how a component or system performs, and we have an established probability distribution for the demands it faces, we can calculate the factor of safety that will provide any given degree of confidence that the design will not fail. But where the component or system design is innovative and the demands it may face are unknown or subject to unpredictable variation, there is no science by which it is possible to calculate exactly what the safety factors should be. Just as in worst-case analysis, we are back to projecting, estimating, guessing how much is enough. Unfortunately, that is the situation in constantly evolving, complex high-tech systems. When the design must face unpredictable environments *and* rivals actively trying to make it fail—as is the case in military systems—the problem of preventing failure is that much more difficult.

Peculiar confluences of circumstances can also defeat a design. Engineers examining the remains of the sections of the Nimitz Freeway destroyed in the Northern California earthquake of 1989 found evidence of just such a possibility. The frequency with which the ground shook might have matched the resonant frequency of the highway. In other words, after the first jolt, the highway began to sway back and forth. By coincidence, the subsequent shocks from the earthquake may have been timed to give the highway additional shoves just as it reached the peak of its swing. Like pushing a child's swing down just after it reaches its highest point, the reinforcing motion caused the highway to sway more and more until it collapsed.[54] It would have been hard for engineers to foresee this odd coincidence when the highway was being designed.

On July 13, 1977, New York City suffered one of the worst power failures in its history. It began when lightning struck a transmission tower north of the city and short-circuited two transmission lines. Transmission towers are designed to ground most strikes. This time, the grounding was ineffective. Circuit breakers tripped, as they were supposed to, to isolate the power surge. But they failed to close again after it passed. A remarkable series of failures of switches and circuit breakers then occurred, resulting in the loss of three major transmission lines and the utility's most heavily loaded generator—all from one lightning strike. Then another lightning bolt hit another transmission tower, short-circuiting two more lines. Further failures ensued, compounded by errors made by operators in the utility's control room. The problems snowballed. An automatic load-shedding mechanism began disconnecting customers as it was designed to do, but it also caused an unexpected surge in voltage that knocked another major generator out of service. And that was that. Almost exactly one hour after the first lightning strike, New York City went dark.

"How could the . . . automatic load-shedding system . . . produce such unexpected, and disastrous, results? Largely because . . . [the utility's] engineers never dreamed their system would be reduced to such a small island. So they never bothered to analyze what would happen to system voltages after automatic load shedding on an isolated system."[55] In other words, as in the Kobe quake, the real situation exceeded the worst-case scenario engineers imagined likely enough to be worth considering. After all, two towers both with faulty grounding struck by lightning within 20 minutes, an astonishing series of equipment failures, multiple operator errors and other serious control-room problems—at some point the whole thing does begin to sound wildly implausible. But of course, this bizarre, implausible scenario is exactly what happened.

In the United States, big earthquakes are much less common in the East than in the West, so those who design most structures built in the East are not required to include severe earthquakes in their worst-case scenarios and typically do not do so. Yet the most powerful earthquake ever known to hit the United States occurred in the eastern half of the country, at New Madrid, Missouri, near the Tennessee-Kentucky border in 1811. It was later estimated to have had a magnitude of about 8.7 on the Richter scale, and was one of three quakes in that area in 1811-12, all stronger than magnitude 8.0.[56] The Richter scale is logarithmic (base 10). Thus, those nineteenth century eastern quakes were more than ten times as powerful as the magnitude 6.9 earthquake that brought down part of the Nimitz Freeway and did so much damage to San Francisco in the fall of 1989. (The New Madrid quake was nearly 100 times as strong.) They temporarily forced the Mississippi River to run backward, permanently altered its course, and were felt as far away as Washington, Boston and Quebec.[57]

All along the eastern seaboard there are geological structures similar to those responsible for a 7.0 earthquake that devastated Charleston, South Carolina, in the late nineteenth century. Milder quakes of magnitude 5.0 are not all that rare in the East. Such a quake hit New York City in 1884. Seismologists have estimated that there is about a 50-50 chance of a much stronger 6.3 quake on the New Madrid fault by the year 2000.[58] A study of New York City's vulnerability to earthquake found that a magnitude 6.0 temblor centered within five miles of City Hall would do about $25 billion worth of damage; even a quake more than three times as far away could cause an estimated $11 billion in direct damage to buildings. Estimates of damage in Northern California from the 6.9 quake in 1989 ran from $4 billion to $10 billion.[59] So a New York City–area earthquake about one-tenth as powerful as the California quake could cause up to six times as much property damage.

The reason is partly geological: the earth's crust is older, colder and more brittle in the eastern United States. But it is also because designers of structures in New York do not typically include severe groundshaking in their assumptions. By contrast, designers of structures in California have been compelled to take earthquakes into account. The modern skyscrapers in San Francisco swayed during the 1989 quake, but sustained little or no damage. Virtually every structure that suffered major damage there had been built before stringent earthquake-resistance requirements were incorporated in building codes over the last 15 to 20 years.[60] The assumptions about operating environment made by designers really do make a striking difference in how products perform.

Five large nuclear reactors used to produce plutonium and tritium for American nuclear weapons were designed and built without strong steel or reinforced-concrete "containments."[61] The last line of defense against the accidental release of dangerous radioactive materials, containments are built as a matter of course around civilian nuclear power reactors in the United States (and most other developed nations). The containment surrounding the Three Mile Island reactor prevented a large release of radioactivity such as the one that occurred at Chernobyl where there was no containment. Why were America's nuclear weapons production reactors designed and operated without this key safety feature? Ignorance may be a partial explanation. All of these reactors are "old" in terms of the nuclear business, dating back to the 1950s. The dangers of radiation were much less well understood then, and exposure to radioactive materials was often treated much too cavalierly. For example, it was during the 1950s that American soldiers were ordered to crouch in ditches during nuclear bomb tests in the atmosphere and then made to march or drive right through the point of detonation. But the 1950s was also the era of McCarthyism and of intense Cold War fears and hatreds. It is likely that the pressure to get bomb production moving, to keep ahead of the "godless Communists," also played an important role. Technical matters are not the only considerations that enter into the designers definition of worst case.

There are many sources of error inherent in the process of designing complex technical systems. With great care, the use of fault-tolerant design strategies and thorough testing, it is possible to keep such flaws to a minimum. But even the most talented and careful designers, backed up by the most extensive testing programs cannot completely eliminate design errors serious enough to cause catastrophic technical failures. This is especially true where complicated, innovative or rapidly changing technologies are involved. Many dangerous technologies are of just this kind.

MANUFACTURING AND TECHNICAL FAILURE

Even the best designs for technical systems remain only interesting ideas until they are made real by manufacturing. The process of fabricating major system components and assembling the systems themselves creates ample opportunity for error. Flawed manufacturing can translate the most perfect designs into faulty products. The more complex the system, the more sensitive and responsive it must be, and the more critical its function, the easier it is to introduce potential sources of failure during manufacture. Subcomponents and subassemblies must be checked and rechecked at every step of the way. Still serious errors persist.

The nuclear power industry provides innumerable examples of how easy it is for slips to occur during manufacturing. On October 5, 1966, there was a potentially devastating meltdown at the Enrico Fermi Atomic Power Plant, only 30 miles from Detroit. In August 1967, investigators discovered a piece of crushed metal at the bottom of the reactor vessel that they believed had blocked the coolant nozzles and played a key role in the accident. In 1968, it was finally determined that the piece of metal was one of five triangular pieces of zirconium installed as an afterthought by the designer for safety reasons. They did not even appear in the blueprints. This particular shield had not been properly attached.[62] Only a few weeks after the accident at Three Mile Island (March 1979), the Nuclear Regulatory Commission reported that they "had identified thirty-five nuclear power plants with 'significant differences' between the way they were designed and the way they were built."[63]

The multibillion-dollar nuclear power plant at Diablo Canyon in California sits close to an active fault. During construction in 1977, the utility hired a seismic-engineering firm to calculate the stresses different parts of the plant would have to withstand in an earthquake. A little more than a week before the plant was due to open, a young engineer working for the utility that owned the plant discovered a shocking error. The utility had sent the diagrams of the wrong reactor to its seismic consultants! Guided by the faulty stress calculations that resulted, the utility reinforced parts of the plant that did not need reinforcing, while vulnerable parts were reinforced too little, if at all. More than a hundred other flaws in the reactor's construction were subsequently discovered.[64]

In an attempt to stop the continuing release of radiation after the accident at Chernobyl, the Soviets built what amounted to an after-the-fact containment around the burned-out reactor—a ten-story concrete and steel "sarcophagus" with walls some 20 feet thick. Designed to last 30 years, it was constructed so quickly and under such dangerously radioactive conditions that the quality of work was poor. Only ten years later, the metal had rusted and the concrete was riddled with cracks. The whole structure was in serious need of repair.[65]

By mid 1990, the U.S. Air Force had over 1,700 nuclear warhead–carrying air-launched cruise missiles in its arsenal. These 3,000 pound, 21-foot-long, state-of-the-art missiles are designed to be carried under the wings of high-flying strategic bombers. When launched, they drop down close to the ground to avoid radars as they fly toward their targets. High-speed, ground-hugging flight requires a highly accurate navigation system to keep the missile on its preset path. Northrop manufactured the guidance system, which utilized a series of gyroscopes surrounded by a viscous fluid known as DC-200 (produced by Dow Chemical Corp.). Previously secret Pentagon and corporate documents released in late July 1990 raised doubts as to whether the guidance system, and thus the missile itself, was reliable. Apparently, prolonged exposure to extreme cold caused the fluid to interfere with the spinning of the gyros. A military-wide standard requires that the missiles must be able to function at minus 65 degrees Fahrenheit, a common temperature outside aircraft flying at or above the normal cruising altitudes of long-range commercial airliners (34,000 to 37,000 feet). An internal 1987 Northrop report stated flatly, "DC-200 does not meet the -65 ° F requirement and never did." It was corroborated by tests performed by Boeing (the missiles' prime contractor) in early 1989, in which six of nine gyroscopes failed after being kept at -65 ° F for up to two hours; only when the temperature rose to minus 40 degrees would DC-200 thaw enough to allow every gyro to spin freely.[66] The *Wall Street Journal* maintained, "The Air Force and Northrop Corporation . . . have gone to great lengths to mask the problem. . . . [I]nstead of fixing the part, the Air Force simply decided to make the test less stringent."[67]

It was not until three and a half months after the Hubble Space Telescope was launched in April 1990 that NASA finally determined the cause of the perplexing spherical aberration (curvature error) problem that had made it incapable of performing the full range of tasks for which it had been designed. When the Hubble mirror had arrived for final polishing at Perkin-Elmer's Danbury, Connecticut, plant back in 1979, it was tested with a newly developed, superaccurate tester to assure that the mirror's optical properties met NASA's exacting standards. The tester showed that the mirror had a small degree (one-half wavelength) of spherical aberration, well within acceptable limits for that stage of manufacture. The Perkin-Elmer team then began the final polishing process (which continued until 1981), polishing out the deviation their new tester had found. The only problem was that there was an undiscovered one millimeter error in the structure of the tester. By using it to monitor the polishing process, Perkin-Elmer had distorted rather than perfected the mirror's surface during final polishing, creating the spherical aberration that was later to produce such headaches in the orbiting telescope.

Interestingly, the mirror had been checked with a testing device of more standard design before it was shipped to Danbury. That device had *not* shown the degree of spherical aberration that the newly developed tester had (incorrectly) detected. The company's scientists had the results of the earlier test, but were sure that the more sophisticated tester was correct. They did not bother to conduct further tests or investigate the discrepancy.[68] *Science* reported that "astronomers experienced in making ground-based telescopes say they are appalled that NASA and Perkin-Elmer would rely on one single test. . . . [T]here are any number of simple and inexpensive experiments that could have seen the spherical aberration that now exists in Hubble."[69] In the excitement of meeting the kinds of technological challenges involved in designing and building complex, state-of-the-art systems, mundane matters, such as "simple and inexpensive" checks during the manufacturing process, are easy to overlook. When we have our eyes on the stars, it is all too easy to trip over our own feet.

COMPONENT FLAWS AND MATERIALS FAILURE

It is impossible to make high-quality, reliable products out of poor-quality, unreliable parts or seriously flawed materials. Semiconductor chips have become almost a raw material to the electronics industry. Their performance and reliability is the bedrock on which the performance and reliability of modern electronic equipment is built. In the latter part of 1984, officials at Texas Instruments (the largest chip manufacturer in the United States at the time) disclosed that millions of integrated circuits it had manufactured might not have been tested according to specification. The chips had been built into more than

270 major weapons systems by 80 different contractors. The attendant publicity—and a Department of Defense investigation—led officials at Signetics Corporation (the nation's sixth-largest microchip manufacturer) to audit their own chip-testing procedures. They concluded that as many as 800 different types of microcircuits they had supplied to military contractors might not have been tested properly. At least 60 different types of microchips sold to the Pentagon by that bulwark of the computer industry, IBM, were also determined to have "confirmed problems."[70] In the spring of 1985, the Pentagon's inquiry found that irregularities in testing military-bound microchips were pervasive in the electronics industry. The director of the industrial productivity office at the Department of Defense put it this way: "What we found was that it was common practice for the microcircuit makers to say 'Yeah, we'll do the tests,' and then for them never to conduct them."[71]

The fact that microchips are not properly tested does not mean that they are faulty. What it does mean is that the reliability of those components, and therefore of every product that contains them, cannot be assured. Because disassembly and retesting costs would have been high, reports at the time indicated that there was very little, if any, retesting of the suspect microchips that had already been built into weapons systems. But the fact that such a basic part of so many military systems might be unreliable also has its costs. If these systems fail at critical moments, the consequences can be disastrous. On June 3, 1980, the failure of a single, 46-cent microchip generated a major false warning that the United States was under land- and sea-based nuclear attack by Soviet missiles. Three days later, the same faulty chip did it again.[72]

Early in the summer of 1994, Intel Corporation, by then the standard-setting computer chip manufacturer, discovered a flaw in its much touted and widely used Pentium chip.[73] The chip could cause computers in which it was embedded to give wrong results in certain division problems that used the chip's floating-point processor.[74] Intel waited until November to publicly disclose the problem, provoking an avalanche of angry messages on the Internet from engineers and scientists disturbed by what they considered to be the company's cavalier attitude. A computer that gives the wrong results "silently" (that is, without any indication that anything is wrong) is no small thing. It is not just annoying or misleading, it is potentially dangerous. It does not take a great deal of imagination to see how a computer that gives the wrong results because of a flawed processor could cause a lot of damage if it were used to design, analyze, control or operate a dangerous-technology system. The June 1980 false warning of nuclear attack is only one of many frightening possibilities.

In September 1989, the Pentagon was forced to delay deployment of new rockets for Air Force fighters and replace components in rockets carried by Navy fighters because of defects in circuit boards costing $12 each. The boards, manufactured by Asher Engineering, were built into "stator switches" that help arm the warhead before the missile is fired. According to Congressman John Dingell of Michigan, "In our first raid on Libya, we used both HARM and Harpoon missiles which contain Asher stator switches. . . . During that raid, at least 25 percent of the HARM's and Harpoons did not detonate." Since those missiles were never recovered, there is no way to know whether the substandard switches were the reason for the warheads' failure to explode.[75]

Metallurgical defects are also a major potential source of systems failure. They seem to have played a key role in the July 19, 1989, crash of United Airlines Flight 232 near Sioux City, Iowa, discussed earlier. Apparently, a flaw in a 270-pound cast-titanium-alloy disk in the rear engine grew into a crack that broke the disk apart, shattering the plane's tail section. Metallurgists working for the National Transportation Safety Board found a tiny cavity in the metal that grew into the fatal crack. The cavity was large enough to be "readily visible with the unaided eye," raising questions as to why it was not detected either at the factory or during routine maintenance.[76] It was also discovered that the manufacturer had mistakenly given two disks made at the same time the same serial number. One had failed to pass inspection, and one was destroyed. Investigators thought that the good disk might have been destroyed, and the faulty one installed in the DC-10. The company managed to convince them that that was not true.[77]

Flaws in even the simplest of components can cause very complex technical systems to fail. On April 28, 1989, ABC News reported that "every year in this country, companies buy some $200 billion of nuts and bolts . . . and put them in everything from jet planes to children's amusement rides. . . . We now know that billions of bad bolts have come into this country." Peterbilt Trucks issued a recall because of a number of its customers reported that the steering mechanism on their vehicles would suddenly stop working, causing a virtually total loss of control. Defective bolts were found. They were brittle because they had not been properly heat treated during manufacture. According to ABC, some bolt distributors had become aware of the problem, but few said anything about it to anyone, including their customers. ABC reported, "Twice in the past year and a half, bolts holding jet engines on commercial airliners broke in flight, and the engines then fell off the airplanes. . . . The State of Louisiana noticed that the bolts that hold the Calcasieu River Bridge together were breaking off. It temporarily closed the bridge and replaced the bolts."[78]

Of course, bolt manufacturers also supply the U.S. military. Pentagon officials reassured ABC in writing that they were not aware of any "death or injury attributable to substandard fasteners installed in military equipment." But Army documents ABC obtained showed that defective or broken nuts and bolts were involved in 11 aircraft (mostly helicopter) accidents over the previous decade in which 16 people had died. Over a thousand M-60 tanks were temporarily taken out of service because of defective bolts.[79] ABC News also reported that NASA had spent millions of dollars removing suspect bolts from key systems, like the space shuttle engines. There were reports that bad bolts had been supplied for the Air Force's MX missile.[80]

THE CRITICALITY OF MAINTENANCE

There is no more mundane issue in high-technology systems than maintenance. Yet without proper maintenance, the best-designed and most carefully built system can slowly turn into a useless piece of high-tech junk. The "if it ain't broke, don't fix it" attitude is a prescription for endless, expensive trouble. Complex, sensitive systems often require extensive and painstaking preventive maintenance, not just after-the-fact repair.

More than half a decade after planning for its $30 billion space station began, NASA uncovered a serious problem with the project's design. In January 1990, Richard Kohrs, the head of the space station program told a gathering of contractors, "This program has too much EVA [extra vehicular activity, that is, space walks] . . . they're talking about 1,700 man-hours of EVA a year just for maintenance. . . . If that's true, we don't have the right design." A few months later, a special NASA team (working with estimates of failure rates derived mainly from NASA agencies and contractors) projected that more like 2,200 hours of space walks each year would actually be needed to maintain the station's 6,000 parts.[81] NASA subsequently boosted the maintenance estimate further to 3276 hours per year—about 9 astronaut-hours per day (including preparation time).[82] Space walks are dangerous. There are radiation risks and possibilities of injury from fast-moving space debris or micrometeorites. They are also expensive and time consuming. From the beginning of the American space program to 1990, astronauts had only accumulated about 400 hours of EVA. The NASA team argued that the enormous amount of maintenance EVA required each year would divert so much time from key construction tasks that it might never be possible to complete the station.[83]

It is clear enough that the problems of space station maintenance are not merely theoretical. The USSR orbited the core module for its much simpler *Mir* space station in the mid 1980s. By 1990, construction was two years behind schedule, at least in part because Soviet astronauts had to spend an inordinate amount of time maintaining and repairing the 80-ton, 100-foot-long orbiting laboratory.[84] In June 1997, a collision between *Mir* and an unoccupied cargo vessel punctured part of the space station and knocked out much of its power supply. *Mir* limped along throughout that summer, with repeated power outages, computer failures and other problems focusing the attention of ground controllers and its occupants more on maintenance and repair than on its mission.[85]

In April 1988, the mechanics responsible for maintaining Aloha Airlines's fleet were routinely inspecting one of the airline's Boeing 737s. They failed to note that a section of the upper fuselage was starting to come loose, and that the overlapping metal skins in that section were beginning to develop fatigue cracks around the rivets. On April 28, in flight, the cracks suddenly began to grow, connecting to each other and literally ripping the top off the body of the plane. A flight attendant was killed, but the pilot was able to bring a plane full of very frightened passengers down for an otherwise safe landing.[86]

Boeing's 737 jet airliner has a long record of effective service. But it wasn't designed to last forever. It was supposed to fly for 20 years, 51,000 flight hours or 75,000 takeoffs and landings. The Aloha Airlines plane had taken off and landed nearly 90,000 times—20 percent beyond its design life. By mid 1990, almost 20 percent of the 737s in use across all airlines were more than 20 years old. Airline officials argued that careful maintenance procedures, along with upgrades to the planes, could keep them flying well beyond their original design life.[87] In May 1998, the FAA issued an emergency order grounding dozens of older Boeing 737s because of a possible maintenance problem involving their fuel pump wiring.[88] The wiring on some 35 of the planes inspected in the first few days after the FAA found the problem showed some wear, and in 9 or more aircraft the insulation was worn at least halfway through.[89] Worn insulation can lead to sparks, and sparks and jet fuel are a deadly explosive combination.

The 1979 crash of a DC-10 on takeoff from Chicago's O'Hare Airport was traced to a tear in the pylon connecting one of the aircraft's engines to its wing. Rough handling that resulted from shortcut procedures used during routine maintenance was apparently the culprit.[90] The 1989 explosion of the United Airlines DC-10 near Sioux City, Iowa, discussed earlier was also attributed to a maintenance problem: flawed inspection that failed to detect a visible cavity in the rear engine's titanium-alloy disk. And faulty maintenance—poorly done repair work—was cited as the primary culprit in the worst single aircraft disaster in history, the death of 520 people in the crash of a Japan Airlines 747 northwest of Tokyo in August 1985.[91]

Nuclear power plants are designed to "fail safe." Any major problem, including a loss of power to the controls, is supposed to trigger an automatic shutdown, or "scram," of the reactor. Industry analysts have argued that the odds of a failure of this system are no more than one in a million reactor years. Yet on February 22, 1983, the Salem-1 reactor failed in just this way, refusing to halt the fission reaction in its core when ordered to scram by a safety control system. Three days later, the "one in a million" event happened again—at the same reactor.[92]

A key problem lay in a huge pair of circuit breakers, known as DB-50s (manufactured by Westinghouse) in the circuit supplying power to the mechanism that raises and lowers the core control rods. When the power is flowing and the breakers are closed, the rods can be held up out of the core to speed the fission reaction. But when the automatic system orders the reactor to scram, the DB-50s break the circuit, and gravity pulls the rods down into the core, shutting down the reaction. Investigators of the incidents at Salem-1 found that a UV coil inside the DB-50s had failed. As early as 1971, Westinghouse had issued technical bulletins warning of problems with the UV coil, and in 1974 had sent out letters emphasizing the importance of properly cleaning and lubrication of the coils twice a year. The utility did not heed the warnings. "Maintenance of the breakers at Salem was poor. . . . They never got the critical attention they deserved. . . . [T]here was *no* maintenance of the UV coils between their installation in the 1970s and August 1982, when they began to fail repeatedly."[93]

At the Maine Yankee nuclear power plant, high-pressure radioactive water is pumped through metal tubes 3/4 inch in diameter and 1/20 inch thick after being heated by the reactor core. Heat conducted through the walls of the tubes turns "clean" water into "clean" steam that drives the turbine, generating electricity. Proper inspection and maintenance of the tubes is critical, since any cracking or rupturing could allow the radioactive water from the reactor to leak into the otherwise "clean" steam and possibly escape to the environment. In early 1995, it was disclosed that about 60 percent of the plant's 17,000 tubes had severe cracks. Furthermore, the reactor had been operating in that dangerous condition for years.[94]

NRC Commissioner James Asseltine expressed grave concern that weaknesses in preventive maintenance, equipment reliability problems and other related difficulties are pervasive in nuclear industry. In his view, "The bottom line is that, given the present level of safety . . . we can expect to see a core meltdown accident within the next twenty years, and it is possible that such an accident could result in off-site releases of radiation which are as large as, or larger than, the releases estimated to have occurred at Chernobyl."[95]

Maintenance cannot be an afterthought in the kind of sophisticated, complex technological systems that a modern military expects to work well even in difficult operating conditions. Given the speed of modern warfare, equipment that fails often because it is poorly maintained or because its design is so inherently complex that it cannot be properly maintained is worse than useless. It can lead to military tactics and strategies that amount to fantasies, because they are built around equipment that won't perform as advertised—if it works at all—in the real world of combat.

Air Force analyst F. C. Spinney's appalling data on the reliability of fighter planes (given in Table 9-1) make it clear that this is not just a theoretical concern. These are not even data for planes in combat. Focusing on the F-15, Spinney makes the point that there is a difference between the way maintenance problems look "on the drawing board" and the way things work out in the real world. The fighter has built-in test equipment on board that lets the pilot or flight-line crew chief know that there has been a failure in a specific "line replaceable unit" (LRU). The LRU is then removed and taken to an "Avionics Intermediate Shop" (AIS) to be repaired. Meanwhile, another LRU is plugged into the plane and it is ready to fly. This approach is used to simplify flight-line maintenance. But according to Spinney, "the maintenance task is aggravated by long test times. . . . To hook up an LRU to the computer . . . can be a time-consuming task . . . sometimes taking up to 30 minutes. The computer then checks out the LRU—again a time-consuming task, averaging about three hours, but sometimes taking as long as eight hours. Since the computer is limited to hooking up and checking one LRU at a time, no other LRUs can be checked out during this period."[96] And after all that, the computer can't find any problem with the LRU 25 to 40 percent of the time. The whole maintenance process was thus useless.[97]

Maintenance, lackluster and pedestrian as it may seem, requires the closest attention. From aircraft to spacecraft to nuclear power plants, there is persuasive evidence that improper maintenance can lead to dangerous failures of technical systems. Far from being a mere footnote in the age of high technology, it is critically important to the performance of the most sophisticated technical systems.

The nature of technical systems themselves and the nature of their interactions with the fallible humans who design, build and maintain them guarantee that it is not possible to eliminate all causes of failure—even potentially catastrophic failure—of complex and critical technical systems. There is nothing about dangerous-technology systems that makes them an exception to this rule.

There are those who believe that it is possible to prevent failure of the most complex dangerous technologies by automating humans out of the system and putting computers in control. Computers are surrounded with an almost magical aura of perfection, or at least perfectibility, in the minds of many people. We sometimes think—or hope— that they can help us overcome the imperfection that is so much a part of our human nature. After all, they can bring commercial aircraft safely to the ground with remarkable efficiency and nuclear warheads to their targets with remarkable accuracy. In the next chapter, we take a closer look at these marvels of modern technology and try to understand why they are anything but a route to solving the problems of either technical failure or human error.

NOTES

PROLOGUE

1. Wald, Matthew L., "Nuclear Waste Tanks at Hanford Could Explode," *New York Times* (July 31, 1990).
2. Bukharin, Oleg and Potter, William C., "Potatoes Were Guarded Better," *Bulletin of the Atomic Scientists* (May-June 1995), p. 48.
3. Abrams, Herbert, "Human Reliability and Safety in the Handling of Nuclear Weapons," Center for International Security and Arms Control, Stanford University (unpublished, 1990), pp. 2-4.

CHAPTER ONE

1. The pioneering work of Amartya Sen is of special interest here. See, for example, "Starvation and Exchange Entitlement: A General Approach and Its Application to the Great Bengal Famine," *Cambridge Journal of Economics* (1, 1977); and *Poverty and Famines: An Essay on Entitlement and Deprivation* (Oxford: Clarendon Press, 1981).
2. Sivard, R. L. et al., *World Military and Social Expenditures, 1993* (Washington, D.C.: World Priorities, 1993), p. 21. Overall, the twentieth century has seen more than 250 wars that have taken the lives of more than 100 million people (Sivard, R. L. et al., *World Military and Social Expenditures, 1996,* Washington, D.C.: World Priorities, 1996, p. 7).
3. A number of interesting scientific analyses of some of the likely ecological consequences of nuclear war have been published since the mid 1970s. These include: National Research Council, *Long-Term Worldwide Effects of Multiple Nuclear-Weapons Detonations* (Washington, D.C.: National Academy of Sciences, 1975); Ehrlich, P. R., Sagan, C., Kennedy, D. and Roberts, W.O., *The Cold and the Dark: The World After Nuclear War* (New York: W.W. Norton, 1984); Harwell, M.A., *Nuclear Winter: The Human and Environmental Consequences of Nuclear War* (New York: Springer-Verlag, 1984); and National Research Research Council, *The Effects on the Atmosphere of a Major Nuclear Exchange* (Washington, D.C.: National Academy of Sciences, 1985).
4. In 1998, sugar cubes containing anthrax bacilli confiscated from a German courier in 1917 (apparently intended for germ warfare use in World War I) were found in a museum in Norway. Stored without any special precautions, the anthrax was revived, still viable and virulent, after 80 years. "Norway's 1918 Lump of Sugar Yields Clues on Anthrax in War," *New York Times* (June 25, 1998).
5. Acquired Immune Deficiency Syndrome (AIDS) is caused by a number of related viruses of an unusual type. They are called "retroviruses" because they work backwards. Whereas most viruses interfere with the DNA (deoxyribonucleic acid) of an infected cell directly and indirectly affect the cell's RNA (ribonucleic acid), retroviruses affect the RNA directly. The first human retrovirus implicated as a cause of AIDS was HIV-1 (human immunodeficiency virus-1). Since that time an HIV-2 and possibly HIV-3 have been discovered. The AIDS viruses have a number of peculiarities that make them particularly resistant to attack by the body's immune system, and make the search for an effective treatment or vaccine extremely difficult. See, for example: Marx, J.L., "The AIDS Virus—Well-Known But a Mystery," *Science* (April 24, 1987), pp. 390-392; Edwards, D.D., "New Virus, Growth Factor Found for AIDS," *Science News* (June 6, 1987), p. 356; and Barnes, D.M., "AIDS: Statistics But Few Answers," *Science* (June 12, 1987), pp. 1423-1425.
6. In a sense, biologists are today where physicists were in the early part of this century. Their research having led them to the discovery of the basic forces of the physical universe locked within the nucleus of the atom, physicists collaborated to use that knowledge to create the most destructive weapon in

human history. It was not the imperative of science that led them to use this remarkable knowledge in that way, but a political decision taken under the urgings of what was thought to be military necessity. Biologists today have uncovered the basic forces of the biological universe locked within the nucleus of the living cell. It is certain that some will again argue for the military necessity of using that knowledge to create horrendous weapons. Let us hope the biologists have learned something from the experience of the physicists, that those whose work is centered on the physical understanding of life will not allow themselves to be coerced or convinced to create instead the means of mass destruction.

While it is clear that stockpiles of chemical weapons of mass destruction exist, it is not clear whether there are comparable stockpiles of biologicals.

7. Barnaby, F., "Environmental Warfare," *Bulletin of the Atomic Scientists* (May 1976), pp. 37-43; also Westing, A.H., *Weapons of Mass Destruction and the Environment* (London: Taylor & Francis and the Stockholm International Peace Research Institute, 1977), chap. 3, pp. 49-63.
8. Ehrlich, et. al., op. cit.
9. Westing, A.H., *Ecological Consequences of the Second Indochina War* (Stockholm: Almqvist & Wiksell and the Stockholm International Peace Research Institute, 1976).
10. Van Dorn, W.G., LeMehaute, B. and Hwang, L., *Handbook of Explosion-Generated Water Waves*, Tetra Tech Report No. TC-130 (Pasadena, California: Tetra Tech, Inc., October 1968), prepared for the Office of Naval Research (Contract No. N00014-68-C-0227).
11. Larsen, C.A., "Ethnic Weapons," *Military Review* (published monthly by the U.S. Army Command and General Staff College, Fort Leavenworth, Kansas) (November 1970), pp. 3-11. An unexplained, oblique reference to the possibility of this type of weapon appeared almost 30 years later in an article in the *New York Times*, with the alarming title "Iranians, Bioweapons in Mind, Lure Needy Ex-Soviet Scientists" (December 8, 1998; by Judith Miller and William J. Broad). Such developments, we are reassured are "years away."
12. What is not widely appreciated is that the majority of high-level nuclear waste generated since the beginning of the nuclear era is from weapons production, not from civilian nuclear power plants.
13. Diamond, S., "Union Carbide's Inquiry Indicates Errors Led to India Plant Disaster," *New York Times* (March 21, 1985).
14. Sullivan, W., "Health Crisis Could Last Years, Experts Say," *New York Times* (December 7, 1984).
15. Burns, John F., "India Sets Three Nuclear Blasts, Defying Worldwide Ban; Tests Bring Sharp Outcry," *New York Times* (May 12, 1998) and "Indians Conduct 2 More Atom Tests Despite Sanctions," *New York Times* (May 14, 1998). For more details, see Albright, David, "The Shots Heard 'Round the World," *Bulletin of the Atomic Scientists* (July-August 1998).
16. Burns, John F., "Pakistan, Answering India, Carries Out Nuclear Tests; Clinton's Appeal Rejected," *New York Times* (May 29, 1998). See also, Albright, David, "Pakistan: The Other Shoe Drops," *Bulletin of the Atomic Scientists* (July-August 1998).
17. Gilmartin, Patricia A., "U.S. Officials Assess Status of Former Soviet Weapons Programs," *Aviation Week and Space Technology* (January 20, 1992), p. 27.
18. Miller and Broad, op. cit.
19. Taylor, Theodore B., "Worldwide Nuclear Abolition," in Nuclear Age Peace Foundation, *Waging Peace Bulletin* (Summer 1996), p. 3.
20. These include Bulgaria, Burma (Myanmar), China, Czech Republic, Egypt, France, India, Iran, Iraq, Israel, Libya, North Korea, Pakistan, Romania, Russia, Saudi Arabia, Slovakia, South Africa, South Korea, Syria, Taiwan, United States, Vietnam and Yugoslavia (Serbia). Hogendoorn, E.J., "A Chemical Weapons Atlas," *Bulletin of the Atomic Scientists* (September-October 1997).
21. Tucker, Jonathan B., "The Future of Biological Warfare," in Wander, W. Thomas and Arnett, Eric H., *The Proliferation of Advanced Weaponry: Technology, Motivations and Responses* (Washington, D.C.: American Association for the Advancement of Science, 1992), p. 57.
22. Ibid., p. 53.
23. Ibid., p. 54, citing Fairhall, David, "Eleven Countries 'Defying Ban on Germ Weapons,'" *London Guardian* (September 5, 1991).
24. Wander, W. Thomas, "The Proliferation of Ballistic Missiles: Motives, Technologies and Threats," in Wander and and Arnett, op. cit., p. 77; see also Spector, Leonard S., McDonough, Mark G. and Medeiros, Evan S., *Tracking Nuclear Proliferation* (Washington, D.C.: Carnegie Endowment for International Peace, 1995), pp. 185-187.
25. WuDunn, Sheryl, "North Korea Fires Missile Over Japanese Territory," *New York Times* (September 1, 1998).
26. Lorber, Azriel, "Tactical Missiles: Anyone Can Play," *Bulletin of the Atomic Scientists* (March 19 pp. 39-40.

CHAPTER TWO

1. McFadden, Robert D., "Blast Hits Trade Center, Bomb Suspected, 7 Killed, Thousands Flee Smoke in Towers: Many Are Trapped for Hours in Darkness and Confusion," *New York Times* (February 27, 1993); and Bernstein, Richard, "Trade Center Bombers Get Prison Terms of 240 Years," *New York Times* (May 25, 1994).
2. Kifner, John, "At Least 21 Are Dead, Scores Are Missing After Car Bomb Attack in Oklahoma City Wrecks 9-Story Federal Office Building: 17 Victims Were Children in 2d-Floor Day Care Center," *New York Times* (April 20, 1995); and Treaster, Joseph B., "The Tools of a Terrorist: Everywhere for Anyone," *New York Times* (April 20, 1995).
3. A similar, simple definition of terrorism can be found in the Rand Corporation's body of work on terrorism. See, for example, Cordes, Bonnie, Hoffman, Bruce, Jenkins, Brian M., Kellen, Konrad, Moran, Sue and Sater, William, *Trends in International Terrorism, 1982 and 1983* (Santa Monica, California: Rand Corporation, August 1984), p. 1.
4. "Some Poisoned Israeli Oranges Discovered in Europe," *New York Times* (February 2, 1978). In a letter sent to the West German Ministry of Health, a group calling itself "Arab Liberation Army—Palestine Commando" claimed responsibility for poisoning the oranges.
5. "Medical Sciences," *1984 Yearbook of Science and the Future* (Chicago: Encyclopaedia Britannica, Inc., 1984), p. 353. It is unclear whether the Tylenol poisonings were the work of someone with a grudge against the company or someone intending to extort money.
6. U.S. Department of Defense, *Terrorist Group Profiles* (Washington, D.C.: U.S. Government Printing Office, November 1988), p. 25.
7. Klanwatch Project, *False Patriots: The Threat of Anti-Government Extremists* (Montgomery, Alabama: Southern Poverty Law Center, 1996).
8. The so-called Reign of Terror was carried out by the infamous Maximilien Robespierre's Jacobin government between the summer of 1793 and the summer of 1794.
9. Darnton, John, "Ethiopia Uses Terror to Control Capital," *New York Times* (February 10, 1978).
10. According to the testimony, the campaign included cigarettes infected with anthrax, candies spiked with botulism, sugar containing salmonella and whiskey laced with the herbicide paraquat. See Daley, Suzanne, "In Support of Apartheid: Poison Whisky and Sterilization," *New York Times* (June 11, 1998).
11. Burns, John F., "A Network of Islamic Terrorism Traced to a Pakistan University," *New York Times* (March 20, 1995).
12. Ibid. See also Wren, Christopher S., "U.S. Jury Convicts 3 in a Conspiracy to Bomb Airliners," *New York Times* (September 6, 1996) and Weisler, Benjamin, "Mastermind Gets Life for Bombing of Trade Center," *New York Times* (January 9, 1998).
13. McFadden, Robert D., "FBI Seizes 8, Citing a Plot to Bomb New York Targets and Kill Political Figures," *New York Times* (June 25, 1993).
14. Burns, op. cit.
15. Hoffman, Bruce, deLeon, Peter, Cordes, Bonnie, Moran, Sue Ellen and Tompkins, Thomas C., *A Reassessment of Potential Adversaries to [sic] U.S. Nuclear Programs* (Santa Monica, California: Rand Corporation, March 1986), p. 5.
16. "Aum Paid ¥4 Billion to Foreign Companies," *Japan Times* (July 2, 1995). Members of the Aum Shinrikyo sect also reportedly visited the Russian nuclear research center at Obninsk in 1994 seeking nuclear materials. Obninsk is the same nuclear research institute that U.S. investigators believed to be the source of the small amount of weapons-grade nuclear material smuggled into Germany in 1994; see Katz, Gregory, "Uranium Smuggling Case Confirms Security Fears," *Dallas Morning News* (May 26, 1996).
17. This money is to be spread across all ten "closed cities" in the Russian nuclear weapons complex to help start commercial ventures. Gordon, Michael R., "Russia and U.S. Plan to Guard Atom Secrets," *New York Times* (September 23, 1998).
18. Kilborn, Peter T., "British Group's Sale of Bacteria Stirs Fear of Use by Terrorists," *New York Times* (February 11, 1977).
19. WuDunn, Sheryl, "Elusive Germ Sows Panic in Japan," *New York Times* (August 23, 1996).
20. Klanwatch Project, op. cit., p. 31.
21. Ibid., p. 25. See also Purdum, Todd S., "Two Charged with Possessing Toxin Thought to Be Anthrax," *New York Times* (February 20, 1998).

22. Ambrosino, Michael J., executive producer, "The Plutonium Connection" (Boston: WGBH-TV, NOVA #214, first transmission PBS, March 9, 1975), transcript, p. 8; see also Burnham, David, "B Asks Curb on Plutonium Use to Prevent Building of Homemade Bomb," *New York Times* (February 27, 1975).
23. *Newsday* (October 10, 1976).
24. Ostrow, Ronald J., "Backpack A-Bomb Possible, FBI Says," *Los Angeles Times* (April 26, 1979).
25. Morland, Howard, "The H-Bomb Secret: To Know How Is to Ask Why," *The Progressive* (November 1979), pp. 14-23.
26. Carmody, Dierdre, "U.S. Hunting for Copies of Classified Data on Bomb," *New York Times* (May 18, 1979).
27. Willrich, Mason and Taylor, Theodore B., *Nuclear Theft: Risks and Safeguards* (Cambridge, Massachusetts: Ballinger Publishing Company, 1974), pp. 20-21.
28. Burnham, op. cit.
29. Harper, George, "A Do-It-Yourself A-Bomb," *New Scientist* (March 27, 1980), p. 998.
30. Taylor, Theodore B., "Nuclear Power and Nuclear Weapons," Global Security Study No. 22 (Santa Barbara, California: Nuclear Age Peace Foundation, July 1996), p. 2.
31. Gillette, Robert, "Impure Plutonium Used in '62 A-Test," *Los Angeles Times* (September 16, 1977).
32. Gillette, Robert, "Proves Civilian Plants Can Be Atomic Arsenals," *Los Angeles Times* (September 14, 1977).
33. "The critical mass of metallic uranium at 10% enrichment, with a good neutron reflector [like beryllium] is about 1000 kilograms . . . a sphere . . . about a foot and a half in diameter. At 20% enrichment, the critical mass drops to about 250 kilograms . . . and at 50% enrichment, it is fifty kilograms." Willrich and Taylor, op. cit., p. 17.
34. In 1993, 4.5 kilograms of enriched reactor fuel was stolen from a Russian Navy base at Kola Bay. See Bukharin, Oleg and Potter, William, "'Potatoes Were Guarded Better,'" *Bulletin of the Atomic Scientists* (May-June 1995), p. 46.
35. Waller, Douglas, "Nuclear Ninjas: A New Kind of SWAT Team Hunts Atomic Terrorists," *Time* (January 8, 1996), pp. 39-41.
36. "Germ Warfare: New Threat from Terrorists," *Science News* (May 18, 1996), p. 311.
37. Clifford, Frank, "U.S. Drops Anti-Terrorist Tests at Nuclear Plants: Shrinking Budget Is Cited," *Los Angeles Times* (November 3, 1998).
38. Gordon, Michael R., "Russia Struggles in Long Race to Prevent an Atomic Theft," *New York Times* (April 20, 1996).
39. Ibid.
40. Spector, Leonard S., "Clandestine Nuclear Trade and the Threat of Nuclear Terrorism" in Leventhal, Paul and Alexander, Yonah, editors, *Preventing Nuclear Terrorism* (Lexington, Massachusetts: Lexington Books, 1987), p. 80.
41. Waller, op. cit. pp. 39-41.
42. Cockburn, Andrew, "Can We Stop A Bomb Smuggler?" *Parade* (November 3, 1985), p. 12.
43. Associated Press, "FBI Arrests Two in Plot to Steal Nuclear Sub," *Washington Post* (October 5, 1978).
44. From the computerized chronology of terrorist incidents at Rand Corporation, as cited in "Appendix: Nuclear-Related Terrorist Activities by Political Terrorists," in Leventhal and Alexander, op. cit., p. 125.
45. Associated Press, "Plutonium in NYC Water Probed," *Dallas Morning News* (July 28, 1985).
46. Katz, Gregory, "Uranium Smuggling Case Confirms Security Fears," *Dallas Morning News* (May 26, 1996).
47. Gates, Mahlon, E., "The Nuclear Emergency Search Team," Levanthal and Alexander, op. cit., pp. 397-402; also, Waller, op. cit., pp. 39-42.
48. Emshwiller, John R., "In Atom Bomb Scare, Federal NEST Team Flies to the Rescue," *Wall Street Journal* (October 21, 1980).
49. Operations Branch, Division of Fuel Safety and Safeguards, Office of Nuclear Material Safety and Safeguards, *Safeguards Summary Event List (SSEL)* (Washington D.C.: U.S. Nuclear Regulatory Commission, NUREG-0525, vol. 2, Rev. 3; July 1995).
50. Wald, Matthew L., "Doubts Raised on New Rules to Protect Nuclear Reactors," *New York Times* (February 11, 1994).
51. Shenon, Philip, "Saudi Truck Bomb at a U.S. Complex Kills 11, Hurts 150," *New York Times* (June 26, 1996).

52. "Weekly Information Report to the NRC Commissioners" (April 20, 1984), enclosure E, p. 3, as cited in Hirsch, Daniel, "The Truck Bomb and Insider Threats to Nuclear Facilities," in Leventhal and Alexander, op. cit., p. 209.
53. Hirsch, Daniel, "The Truck Bomb and Insider Threats to Nuclear Facilities," in Leventhal and Alexander, op. cit., p. 210.
54. Schlessinger, James R., quoted from transcript of "Meet the Press" in a *Senator Mike Gravel Newsletter* (October 31, 1973) by Krieger, David, "Terrorists and Nuclear Technology," *Bulletin of the Atomic Scientists* (June 1975), p. 32.
55. Associated Press, "Information on How to Sabotage Nuclear Plant Available to Public," *Atlanta Journal and Constitution* (November 25, 1979).
56. Fainberg, A. and Bieber, A.M., Brookhaven National Laboratory *Barrier Penetration Database*, prepared under Contract No. E-1-76-C-02-0016 to the Division of Operating Reactors, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission (NUREG/CR-0181, published July 1978).
57. Meyer, Christina, Duncan, Jennifer and Hoffman, Bruce, *Force-on-Force Attacks: Their Implications for the Defense of U.S. Nuclear Facilities* (Santa Monica, California: Rand Corporation, 1993).
58. Hoffman, Bruce, Meyer, Christina, Schwarz, Benjamin and Duncan, Jennifer, *Insider Crime: The Threat to Nuclear Facilities and Programs* (Santa Monica, California: Rand Corporation, February 1990), p. 33.
59. Ibid., p. 41.
60. Kellen, Konrad, "The Potential for Nuclear Terrorism: A Discussion" in Leventhal and Alexander, op. cit., p. 109. Note that some of these groups continue to be active, while the activities of others have waned.
61. Ibid.
62. Kristof, Nicholas D., "At Trial in Tokyo, Guru Says Aim Was to Give 'Ultimate Joy,'" *New York Times* (April 25, 1996).
63. Klanwatch Project, op. cit., pp. 58-68. See also Intelligence Project, Southern Poverty Law Center, *Intelligence Report* (Spring 1998), pp. 6-28.
64. Ibid., p. 8.
65. Ibid., p. 17.
66. Hoffman, Bruce, *Terrorism in the United States* (Santa Monica, California: Rand Corporation, January 1986), p. 51.

CHAPTER THREE

1. U.S. Department of Energy, *Plutonium: The First 50 Years* (Washington, D.C.: February 1996), p. 52.
2. Marshall, Eliot, "Nuclear Fuel Accounts Books in Bad Shape," *Science* (January 9, 1981), pp. 147-148.
3. U.S. Department of Energy, op. cit., p. 52.
4. Special AEC Safeguards Study Group report as excerpted in U.S. Senate, *The Congressional Record: Proceedings and Debates of the 93rd Congress, Second Session* (Washington, D.C.: April 30. 1974), p. S 6625.
5. Bolt, Richard, "Plutonium for All: Leaks in Global Safeguards," *Bulletin of the Atomic Scientists* (December 1988), pp. 14-17.
6. Total cumulative acquisitions of plutonium from all sources amounted to 111,400 kilograms. Total cumulative inventory difference (ID) was given as 2,800 kilograms. The ID's for the seven major DoE facilities were: Hanford, Washington = +1,265.6 kg; Rocky Flats, Colorado = +1,191.8 kg; Savannah River, South Carolina = + 232.0 kg; Los Alamos National Laboratory, New Mexico = +47.5 kg; Lawrence Livermore National Laboratory, California = +5.5 kg; Idaho National Engineering Laboratory = -5.6 kg; and Argonne National Laboratory West, Idaho = -3.4 kg. (a positive ID means that there was more shown on the books than a physical inventory could locate, while a negative ID means that there was less on the books than a physical inventory revealed.) U.S. Department of Energy, op. cit., pp. 22 and 54.
7. The total size of the combined plutonium inventories of the Departments of Energy and Defense (before adjustment for removals) is given as 111.4 metric tons (1 metric ton = 1,000 kilograms). Of this, some 2.8 metric tons was in the "inventory differences" category. Therefore, the ID was 2.5 percent of the inventory (2.8/111.4). Ibid., pp. 22 and 52-54.

8. Ibid., p. 52.
9. Holden, Constance, "NRC Shuts Down Submarine Fuel Plant," *Science* (October 5, 1979), p. 30.
10. U.S. Department of Energy, op. cit., p. 22.
11. Some estimates of world plutonium stocks are as high as 1,100 metric tons, nearly five times the size of world inventories used in these calculations. (See Williams, Phil and Woessner, Paul, "The Real Threat of Nuclear Smuggling," *Bulletin of the Atomic Scientists* (January 1996), p. 41.)
12. In Langham, W.H., "Physiology and Toxicology of Plutonium-239 and Its Industrial Medical Control," *Health Physics* 2 (1959), p. 179, it is assumed that humans would respond to plutonium as experimental animals do. On a weight-adjusted basis, this implies that a dose of 20 mg in systemic circulation would be lethal to half the exposed humans within 30 days. Using Langham's 10 percent lung absorption rate, 200 mg would have to be inhaled.
13. Halloran, Richard, "Defense Department Fights to Curb Big Losses in Arms and Supplies," *New York Times* (February 12, 1987).
14. Mohr, Charles, "Military Faulted as Unaware of Equipment Losses," *New York Times* (March 14, 1986).
15. Halloran, op. cit.
16. Army Audit Agency, *Training Ammunition Management* (January 16, 1986).
17. U.S. General Accounting Office, *Inventory Management: Problems in Accountability and Security of DOD Supply Inventories,* (Washington, D.C.: May 1986), pp. 16-18.
18. Ibid.
19. Ibid., pp. 30-32.
20. Ibid., p. 37.
21. Ibid., p. 43.
22. Ibid., pp. 53-56.
23. Ibid., p. 1.
24. Halloran, op. cit.
25. U.S. General Accounting Office, op. cit., p. 16.
26. News story broadcast on WNBC-TV (New York City: September 28, 1978, 7:25 P.M.).
27. U.S. General Accounting Office, *Inventory Management: Vulnerability of Sensitive Defense Material to Theft* (September 1997), pp. 1, 2 and 5.
28. Ibid., p. 59. These "inventory adjustments" involve a wide variety of ordinary goods and materials, not just weapons and explosives. Even the weapons and explosives they do include are conventional, mostly small arms and ammunition.
29. Arkin, William M., Norris, Robert S. and Handler, Joshua, *Taking Stock: Worldwide Nuclear Deployments 1998* (Washington, D.C.: Natural Resources Defense Council, 1998), p. 1. See also Center for Defense Information (Washington, D.C.), *Defense Monitor* (September-October 1995), p. 1.
30. Vartabedian, Ralph, "Nuclear Bomb Records Are Lost, U.S. Says," *New York Times* (October 24, 1997).
31. Martin, David, "Mystery of Israel's Bomb," *Newsweek* (January 9, 1978), pp. 26-27.
32. Burnham, David, "Computer Safety of U.S. Is Faulted," *New York Times* (February 26, 1986).
33. Burns, John F., "China Reveals Major Scandal Among Top Island Officials," *New York Times* (August 1, 1985).
34. Ingram, Timothy H., "Nuclear Hijacking: Now Within the Grasp of Any Bright Lunatic," *Washington Monthly* (January 1973), p. 22.
35. Sawicki, Michael, "Fort Bliss Sends Rockets to Mexico in Procedural Error," *Dallas Times-Herald* (January 30, 1987).
36. The following discussion of security conditions at Tooele Army Depot is based on the written and oral congressional testimony of Dale Van Atta, including a series of articles he did for the *Deseret News* of Salt Lake City that were reprinted along with his testimony. The reprinted articles by Dale Van Atta in the *Deseret News* included "World's Death Stored at TAD, and Security is Substandard" (1978); "Charges Loom in Nerve Gas Inventory Quirk" (January 16, 1978); "'Don't Talk to Deseret News'-- Keep Mum TAD Workers Told" (February 6, 1978); "Anyone Free to Fly Over TAD Cache" (February 14, 1978); "Security at TAD Broken 30 Times in Decade" (February 17, 1978); and "FAA Restricts Flights Over TAD" (February 20, 1978). See *Military Construction Appropriations for 1979*, Hearings before the Subcommittee on Military Construction Appropriations of the Committee on Appropriations, House of Representatives, 95th Congress, 2nd Session (Washington, D.C.: U.S. Government Printing Office, 1978), pp. 179-209.
37. Ibid., p. 177.

38. Ibid., pp. 177 and 188.
39. Ibid., pp. 176 and 187-188.
40. Ibid., pp. 177-178 and 182.
41. Ibid., pp. 177-178 and 182-184.
42. Ibid., p. 182.
43. Ibid., p. 176.
44. Ibid., pp. 176-177 and 189.
45. Zorpette, Glenn, "Hanford's Nuclear Wasteland," *Scientific American* (May 1996), p. 91.
46. Ibid.
47. Long, Clarence, "Views of the Honorable Clarence D. Long, Submitted to Accompany Fiscal 1975 Military Construction Appropriations" (September 24, 1974), pp. 2-3.
48. Ibid., p. 4.
49. Pastore, John, "Security Review of Certain NATO Installations," *Congressional Record—Senate* (April 30, 1975), pp. S.7184-S.7188.
50. United Press International (September 27, 1974).
51. Albright, Joseph, "Prepared Statement," *Military Construction Appropriations for 1979,* Hearings Before the Subcommittee on Military Construction Appropriations of the Committee on Appropriations, U.S. House of Representatives, 95th Congress, Second Session (Washington, D.C.: U.S. Government Printing Office, 1978), pp. 139-140.
52. Ibid., p. 142.
53. "The Nation," *Los Angeles Times* (December 6, 1978).
54. "Uranium-Laden Truck Deserted," *Dallas Morning News* (September 14, 1980).
55. Cox News Service, "Mock Raiders Break Security at Bomb Plant," *The West Palm Beach Post* (September 15, 1982).
56. Lubasch, Arnold, "8 Charged With Arms Plots Including Plan for $2 Billion Sale to Iran," *New York Times* (July 28, 1983).
57. Hirsch, Daniel, "The Truck Bomb and Insider Threats to Nuclear Facilities," in Leventhal, Paul and Alexander, Yonah, editors, *Preventing Nuclear Terrorism* (Lexington, Massachusetts: Lexington Books, 1987), p. 218.
58. Keller, Bill, "Security at U.S. Bases in Philippines Is Called Lax," *New York Times* (September 12, 1985).
59. Drummond, Bob, "Weapons Plant Fails 'Terrorist Test,'" *Dallas Times-Herald* (February 12, 1987).
60. Ibid.
61. Frantz, Douglas and O'Shea, James, "Arms Smugglers Corral Navy Parts," *Chicago Tribune* (August 17, 1986).
62. Associated Press, "Civilian Crews Transport N-Missiles Across Atlantic," *Dallas Morning News* (September 22, 1986).
63. U.S. General Accounting Office, *Army Inventory Management: Inventory and Physical Security Problems Continue* (Washington, D.C.: October 1987), pp. 36-37.
64. Lightbody, Andy and Poyer, Joe, *The Complete Book of U.S. Fighting Power* (Lincolnwood, Illinois: Beekman House, 1990), p. 290.
65. "2 in Security Police Accused of Stealing Jet Fighter Engines," *New York Times* (July 12, 1989).
66. Reuters News Service, "Seven Indicted for Thefts from Army Base" (October 3, 1996, 5:47 A.M.), Yahoo! Reuters Headlines, http:///www.yahoo.com/headlines/961003/news/stories/military_1.html.
67. Johnston, David, "Marines Accused of Weapons Trafficking," *New York Times* (October 17, 1997).
68. "Guards Charge Security Is Lax at Indian Point," *New York Times* (October 17, 1979).
69. "Reporter Cracks Three Mile Island's 'Security,'" *West Palm Beach Post* (February 3, 1980).
70. Fialka, John J., "Internal Threat: Soviets Begin Moving Nuclear Warheads Out of Volatile Republics," *Wall Street Journal* (June 22, 1990).
71. Bukharin, Oleg and Potter, William, "'Potatoes Were Guarded Better,'" *Bulletin of the Atomic Scientists* (May-June 1995), p. 49.
72. Ibid.
73. Ibid., p. 46.
74. Ibid., p. 48.
75. Ibid.
76. Associated Press, "A Power Struggle in Russia's Military," *Dallas Morning News* (September 23, 1995).
77. Ibid.
78. Specter, Michael, "Occupation of a Nuclear Plant Signals Russian Labor's Anger," *New York Times* (December 7, 1996).

79. Cockburn, Andrew and Leslie, producers, Steve Croft, reporting, *60 Minutes,* CBS Television News (September 7, 1997).
80. Berkhout, Frans, Diakov, Anatoly, Feiveson, Harold, Miller, Marvin and von Hippel, Frank, "Plutonium: True Separation Anxiety," *Bulletin of the Atomic Scientists* (November 1992), p. 29.
81. Wald, Matthew L., "U.S. Privatization Move Threatens Agreement to Buy Enriched Unranium from Russia," *New York Times* (August 5, 1998). See also Passell, Peter, "Profit Motive Clouding Effort to Buy Up A-Bomb Material," *New York Times* (August 28, 1996).
82. Wald, op. cit.
83. Panofsky, Wolfgang K.H., "No Quick Fix for Plutonium Threat," *Bulletin of the Atomic Scientists* (January-February 1996), p. 3; and Berkhout etal., op. cit., p. 29.
84. Timothy Ingram, op. cit., p. 24. Though he would not give any details, the former chief of safeguards at the AEC at the time confirmed the general character of these reports.
85. "Mystery of Israel's Bomb," *Newsweek* (January 9, 1978), p. 26; Burnham, David, "Nuclear Plant Got U.S. Contracts Despite Many Security Violations," *New York Times* (July 4, 1977); and Burnham, David, "U.S. Documents Support Belief Israel Got Missing Uranium for Arms," *New York Times* (November 6, 1977).
86. "The Uranium Trade: All Roads Lead to Khartoum's Black Market," *Africa Report* (January-February 1988), p. 6. (The title of the British television documentary cited in the *Africa Report* article is "Dispatches: The Plutonium Black Market.")
87. Ibid.
88. Maceda, Jim, *NBC Nightly News,* NBC-TV, (June 30, 1992), transcript, p. 6.
89. Zimmermann, Tim and Cooperman, Alan, "Special Report: Its Regional Mafias Are Strong, Its Nuclear Wealth Vast; In Russia, the Former Are Vigorously Pursuing the Latter, and that Means Trouble," *U.S. News and World Report* (October 23, 1995), pp. 56-67.
90. Hibbs, Mark, "Plutonium, Politics and Panic," *Bulletin of the Atomic Scientists* (November-December 1994), p. 25-26; and Williams and Woessner, op. cit., p. 43.
91. Perlez, Jane, "Tracing a Nuclear Risk: Stolen Enriched Uranium," *New York Times* (February 15, 1995); Gordon, Michael R., "Czech Cache of Nuclear Material Being Tested for Bomb Potential," *New York Times* (December 21, 1994); and Williams and Woessner, op. cit., p. 43.
92. Perlez, Jane, "Radioactive Material Seized in Slovakia; 9 Under Arrest," *New York Times* (April 2 1995).
93. Lee, Rensselaer, "Smuggling Update," *Bulletin of the Atomic Scientists* (May-June 1997), p. 55.
94. Ibid.
95. Goldstein, Steve, "A Nightmare Scenario Catches a Second Wind," *Philadelphia Inquirer* (January 10, 1999).
96. Ibid.
97. Williams and Woessner, op. cit., p. 42.
98. The report further claimed that Russian civilian nuclear research institutes did not even do physical checks of their inventories of nuclear materials, they only kept book records. Whitney, Craig R., "Smuggling of Radioactive Material Said to Double in Year," *New York Times* (February 18, 1995).
99. Lee, op. cit., p. 52.

CHAPTER FOUR

1. For an interesting sociological analysis of this phenomenon, see Perrow, Charles, *Normal Accidents: Living with High-Risk Technologies* (New York: Basic Books, 1984).
2. For a theoretical macroeconomic analysis of the long-term costs of using economic resources for military purposes, see Dumas, Lloyd J., *The Overburdened Economy: Uncovering the Causes of Chronic Unemployment, Inflation and National Decline* (Berkeley, California: University of California Press, 1986).
3. The most common design for a nuclear weapon, the so-called implosion design, wraps wedges of conventional explosive around a spherical nuclear core in which the atoms are not densely enough packed at normal pressure to sustain a runaway chain reaction. The atomic nuclei are too far apart for the neutrons released from the splitting of one nucleus to have a high enough probability of striking another nucleus and causing it to split apart, releasing energy and more neutrons. Sometimes the neutrons from the splitting of one nucleus strike and split another, but too many miss to cause an

explosive chain reaction. By directing the force of the conventional explosives inward, the implosion design causes a strong enough shock wave to pass through the nuclear core to temporarily overcome the weak electron forces that normally determine the spacing of the atoms. The nuclei are thus forced much closer together, raising the probability that the neutrons flying out of a splitting nucleus will strike and split another nucleus. A runaway nuclear fission chain reaction occurs, producing a devastating nuclear explosion. If the shock wave is not precisely uniform from every direction or the nuclear core is not spherical, the device will not work.

4. The uranium isotope U-235 is much more readily fissionable and thus much more efficient for nuclear weapons purposes than the isotope U-238. However, naturally occuring uranium consists mainly of the isotope U-238 (about 99.3 percent) with a very small percentage (about 0.7 percent) of the isotope U-235. Thus the core of uranium-based nuclear weapons is made of "highly enriched uranium," which has been processed to greatly increase the ratio of U-235 to U-238. See Glasstone, Samuel and Dolan, Philip J., editors, *The Effects of Nuclear Weapons* (Washington, D.C.: U.S. Department of Defense and U.S. Department of Energy, 1977), p. 5.
5. International Labor Office, "Toxicity Classification of Radionuclides," *Guidelines for the Radiation Protection of Workers in Industry (Ionizing Radiations)*, Occupational Safety and Health Series 62 (Geneva: International Labor Office, 1989).
6. Sax, N. Irving et al., *Dangerous Properties of Industrial Materials* (New York: Van Nostrand Reinhold Company, 1984), p. 2247.
7. The following discussion of the physical and biophysical characteristics of alpha, beta and gamma radiation draws heavily on detailed correspondence and conversation between the author and Dr. Warren F. Davis, physicist and founder of Davis Associates, Inc., West Newton, Massachusetts (summer 1995). Some additional information was provided in conversation with Dr. Georgia C. Davis, biological physicist, Francis Bitter Magnetic Laboratory, MIT (November 12, 1988).
8. The slowing alpha (or beta) particle may even be "captured" by the atom, which then gains all of the particle's remaining energy. This can cause enormous disruption.
9. Alpha particles are helium nuclei and beta particles are electrons. Alpha particles are thus much more massive.
10. Because gamma rays have no mass, they must always travel at the speed of light. This is a consequence of Einstein's special theory of relativity. Einstein showed that it would take infinite energy to accelerate a particle with mass to the speed of light. Consequently, any particle that is already moving at the speed of light must have zero mass. On the other hand, a particle of zero mass cannot be decelerated to a speed even infinitesimally less than the speed of light, since that would require extracting an infinite amount of energy from the particle. Therefore, any particle of zero mass must always be moving precisely at the speed of light. Gamma rays therefore exhibit their loss of energy not by slowing down, but by reduced frequency (color or wavelength).
11. This difference is particularly relevant in cancer radiation therapy. Beams of massive particles (such as protons or pions) can be tuned to have the correct initial energy so that they release most of their energy at the depth of a tumor, thereby destroying the tumor with minimal damage to surrounding tissues. Because massless particles (such as cobalt gamma radiation and X-rays) deposit energy uniformly along the beam, a different approach is necessary to use them to preferentially damage tumors. They are used to irradiate the tumor from many different angles, producing most of the damage at their geometric point of intersection.
12. See Richmond, C.R., "Current Status of Information Obtained from Plutonium-Contaminated People," *Radiation Research* (New York: Academic Press, 1974) and Morgan, Karl Z., "Suggested Reduction of Permissible Exposure to Plutonium and other Transuranic Elements," *American Industrial Hygiene Association Journal* (1975). Note that the physical half-life of plutonium is 24,000 years.
13. See Langham, W.H., "Physiology and Toxicology of Plutonium-239 and its Industrial Medical Control," *Health Physics* 2 (1959), p. 179.
14. Ibid. It is assumed that humans would respond to plutonium as experimental animals do. On a weight-adjusted basis, this implies that a dose of as little as 20 mg in systemic circulation would be lethal to half the exposed humans within 30 days. Using the lung absorption rate of plutonium of 10 percent given by Langham, this would mean that a total dose of 200 mg would have to be inhaled in order for 20 mg to get into systemic circulation.
15. The following calculation is based on the data presented in Edsal, John T., "Toxicity of Plutonium and Some Other Actinides," *Bulletin of the Atomic Scientists* (September 1976), pp. 28-30. In experiments carried out on dogs, at doses of as little as 100-1000 nanocuries per gram of lung tissue, most died from pulmonary fibrosis within 1-2 years. (1 nanocurie = 37 radioactive disintegrations per

second; for plutonium, this means that 37 alpha particles are shot off per second). Given an average weight of a human lung of 300-380 grams (source: Dallas Medical Examiner's Office), there is about 760 grams of lung tissue in an average person. Assuming that every gram of lung tissue is dosed with 100-1000 nanocuries, a total dosage of 76,000-760,000 nanocuries should certainly be lethal. For plutonium-239, one nanocurie equals 16.3 nanograms (billionths of a gram). Therefore, 76,000 nanocuries equal 1.2 milligrams (76,000 nc X 16.3 ng/nc = 1,238,800 ng = 1.2 mg); and 760,000 nanocuries equal 12.4 milligrams (760,000 nc X 16.3 ng/nc = 12,388,000 ng = 12.4 mg).

16. Craig, Paul P. and Jungerman, John A., *Nuclear Arms Race: Technology and Society* (New York: McGraw-Hill, 1986), p. 304.
17. Depending on the particular type and design of a nuclear weapon, there will be varying amounts of plutonium (or highly enriched uranium) in its nuclear core. The more sophisticated the design, the smaller the amount of nuclear material required to produce a blast of a given size. Less sophisticated weapons and/or weapons designed to produce larger explosions will contain more nuclear material
18. Harris, Robert and Paxman, Jeremy, *A Higher Form of Killing: The Secret Story of Chemical and Biological Warfare* (New York: Hill and Wang, 1982), p. 54; see also Bodin, F. and Cheinisse, F., *Poisons* (New York: McGraw-Hill, 1970), pp. 129-130; and Harris, William H. and Levey, Judith S., editors, *The New Columbia Encyclopedia* (New York and London: Columbia University Press, 1975), pp. 1910 and 2426.
19. Shenon, Philip, *New York Times*, "Gulf War Illness May Be Related to Gas Exposure" (June 22, 1996); "Czechs Say They Warned U.S. of Chemical Weapons in Gulf" (October 19,1996); "U.S. Jets Pounded Iraqi Arms Depot Storing Nerve Gas" (October 3, 1996); and "Pentagon Says It Knew of Chemical Arms Risk" (February 26, 1997).
20. Shenon, Philip, *New York Times*, "U.S. Jets Pounded Iraqi Arms Depot Storing Nerve Gas" (October 3, 1996); and "Pentagon Says It Knew of Chemical Arms Risk" (February 26, 1997).
21. Shenon, Philip, "New Study Raises Estimate of Troops Exposed to Gas," *New York Times* (July 24, 1997).
22. The catapult they used, called a *trebuchet*, was an even older technology. The Chinese invented it more than 1,500 years earlier.
23. Chevedden, Paul E., Eigenbrod, Les, Foley, Vernard and Sodel, Werner, "The Trebuchet," *Scientific American* (July 1995), p. 68.
24. Harris, William H. and Levey, Judith S., editors, *The New Columbia Encyclopedia*, (New York and London: Columbia University Press, 1975), p. 2161.
25. Kristof, Nicholas D., "Japan Confronting Gruesome War Atrocity: Unmasking Horror," *New York Times* (March 17, 1995). In one of the more bizarre episodes of World War II, the Japanese began to launch huge balloons containing conventional explosives at the American heartland in 1944. Carried by prevailing winds, 200 or so landed in western states. Some Japanese generals wanted to load the balloons with plague- or anthrax-carrying germ warfare agents. Ironically, that plan was vetoed by the infamous general Hideki Tojo, whom the United States later executed as a war criminal.
26. Ibid. See also Tyler, Patrick E., "China Villagers Recall Horrors of Germ Attack," *New York Times* (February 4, 1997).
27. Ibid.
28. Cole, Leonard A., "The Specter of Biological Weapons," *Scientific American* (December 1996), p. 62.
29. "'Emerging Viruses' in Films and Best Sellers," *New York Times* (May 12, 1995).
30. Cohen, Jon, "AIDS Virus Traced to Chimp Subspecies," *Science* (February 5, 1999), pp. 772-773. See also Le Guenno, Bernard, "Emerging Viruses," *Scientific American* (October 1995), pp. 58-59.
31. Preston, R., *The Hot Zone* (New York: Random House, 1994); and *Outbreak* (Los Angeles: Warner Brothers Studios, 1995).
32. Altman, Lawrence K., "Deadly Virus Is Identified in the Outbreak in Zaire," and contiguous boxed story "A Closer Look: The Ebola Virus," *New York Times* (May 11, 1995).
33. Altman, Lawrence K., "Deadly Disease Attributed to New Virus," *New York Times* (April 7, 1995).
34. Nowak, Rachel, "Cause of Fatal Outbreak in Horses and Humans Traced," *Science* (April 7, 1995), p. 32.
35. Altman, op. cit. (April 7, 1995).
36. Reuters News Service, "List Reveals Pentagon Hid 14 N-Accidents," *Dallas Morning News* (December 22, 1980).
37. Associated Press, "U.S.: 32 Nuclear Weapons Accidents Since 1952," *West Palm Beach Post* (December 23, 1980).
38. Hansen, Chuck, "1,000 More Accidents Declassified," *Bulletin of the Atomic Scientists* (June 19[illegible]), p. 9.

39. Weiner, Tim, "Safety Officer Says Military Hid Crashes," *New York Times* (June 24, 1995).
40. The sources of those accidents cited in the discussion that follows that are not specifically noted here can be found in Tables 4-1 and 4-2.
41. Admiral Gene La Rocque, "Proliferation of Nuclear Weapons," Hearings; Subcommittee on Military Applications, Joint Committee on Atomic Energy, 1974.
42. More than 40 years after this terrible accident, new details continue to emerge. See, for example, Stone, Richard, "Retracing Mayak's Radioactive Cloud," *Science* (January 9, 1999).
43. Lapp, Ralph, *Kill and Overkill* (New York, Basic Books, 1962), p. 127; and Larus, J., *Nuclear Weapons Safety and the Common Defense* (Columbus, Ohio: Ohio State University Press, 1967), pp. 93-99.
44. Decontamination required removal of 1,750 tons of radioactive soil and vegetation. By some reports, the material was returned to the United States and buried at sea off the coast of the Carolinas.
45. Sanger, David E., *New York Times*, "U.S.-Japan Ties Worsen on News that Warhead Was Lost in 1965" (May 9, 1989); and "U.S. Says the Bomb Lost Close to Japan Scattered Radiation" (May 16, 1989).
46. Broad, William J., "Russians Fear Leak from Sunken Nuclear Sub, but U.S. Disagrees," *New York Times* (May 21, 1993). See also Spaasky, Igor, "Apathy Above, Terror Below," *New York Times* (June 3, 1993).
47. Broad, William J., "Soviet Sub Sunk in '86 Leaks Radioactivity Into the Atlantic," *New York Times* (February 8, 1994).
48. Ibid.
49. Arkin, William M. and Handler, Joshua, *Neptune Papers No. 3: Naval Accidents 1945-1988* (Washington, D.C.: Greenpeace/Institute for Policy Studies, June 1989), p. 3; Table 5, "Nuclear Reactors Lost in the Oceans," p. 98; and Table 6, "Accidents Involving Nuclear Powered Ships and Submarines," p. 99. See also Eriksen, Viking O., *Sunken Nuclear Submarines* (Oslo: Norwegian University Press, 1990).
50. In August 1989, the Chinese government finally admitted that nuclear accidents in China between 1980 and 1985 had killed 20 people and injured 1200 more. They did not specify the number of accidents and gave little information about the type, claiming only that they resulted from the careless handling of nuclear waste and other radioactive materials. However, since there were no nuclear power plants operating in China at that time, the main source of nuclear waste must have been the military production of their nuclear weapons. See Associated Press, "China Admits Nuclear Accident Deaths," *Dallas Morning News* (August 6, 1989).
51. The Soviets did not admit that the epidemic was the result of an accident until 1991. Questions remain as to whether the biological warfare program that gave rise to this accident remains in operation despite Boris Yeltsin's order to abandon it in 1992. Miller, Judith and Broad, William J., "Germ Weapons in the Soviet Past or in the New Russia's Future," *New York Times* (December 28, 1998). Tucker, Jonathan B., "The Future of Biological Warfare," in Wander, W.T. and Arnett, E.H., editors, *The Proliferation of Advanced Weaponry* (Washington, D.C., American Association for the Advancement of Science, 1992), pp. 59-60. See also Leitenberg, Milton, "Anthrax in Sverdlovsk: New Pieces to the Puzzle," *Arms Control Today* (April 1992). Early reports of this accident include, "1000 Are Said to Die in Soviet Accident," *New York Times* (July 16, 1980); Gwertzman, Bernard, "Soviet Mishap Tied to Germ-War Plant," *New York Times* (March 19,1980) and Gwertzman, Bernard, "Moscow Tells U.S. Infected Meat Caused Outbreak of Anthrax," *New York Times* (March 21, 1980).
52. Clines, Francis X., "Disaster Zone Urged in Soviet Nuclear Explosion," *New York Times* (September 29, 1990); see also Associated Press, "Soviet Region Seeks Kremlin Aid after Nuclear Fuel Blast," *Dallas Morning News* (September 29, 1990).
53. Associated Press, "Suit Discloses '57 Denver Fire Emitted Radioactive Material," *New York Times* (September 9, 1981).
54. Treaster, Joseph B., "Army Discloses Three New Cover-Ups," *New York Times* (September 20, 1975).
55. These tests typically involved bacteria such as *Bacillus subtilis* and *Serratia marcescens*. See Cole, Leonard A., *Clouds of Secrecy: The Army's Germ Warfare Tests over Populated Areas* (Totowa, New Jersey: Rowman and Littlefield, 1988). See also Schmeck, Harold M., "Army Tells of U.S. Germ War Tests; Safety of Simulated Agents at Issue," *New York Times* (March 9, 1977); Altman, Lawrence K., "Type of Germ Army Used in Test Caused Infection Four Days Later," *New York Times* (March 13, 1977); Horrock, Nicholas M., "Senators Are Told of Test of a Gas Attack in Subway," *New York Times* (September 19, 1975).
56. Schneider, Keith, "U.S. Secretly Fixes Dangerous Defects in Atomic Warheads," *New York Times* (May 24, 1990).
57. Ibid.

58. Schneider, Keith, "Interest Rises in Studies of Atomic Shells," *New York Times* (May 28, 1990).
59. Schneider, Keith, "Nuclear Missiles on Some Bombers To Be Withdrawn," *New York Times* (June 9, 1990); see also Schneider, Keith, "Interest Rises in Studies of Atomic Shells," *New York Times* (May 28,1990).
60. "Plutonium Fallout Theory Revealed Here," *Japan Times* (29 October 1969); and Associated Press, "Satellite Fallout Said Not Harmful," *Japan Times* (12 April 1970).
61. Aftergood, Steven, "Nuclear Space Mishaps and Star Wars," *Bulletin of the Atomic Scientists* (October 1986), p. 40.
62. Ibid.
63. Teltsch, Kathleen, "Canada to Continue Search for Fragments of Satellite that Fell," *New York Times* (July 6, 1978); and "Follow-Up on the News: 'Hot' Spy in the Cold," *New York Times* (April 26, 1981)
64. Broad, William J., "Despite Danger, Superpowers Favor Use of Nuclear Satellites," *New York Times* (January 25, 1983).
65. Broad, William J., "Soviet Nuclear-Powered Satellite Expected to Hit Earth in Summer," *New York Times* (May 14, 1988); and Broad, William J., "New Plans on Reactors in Space Raise Fears of Debris," *New York Times* (October 18, 1988). See also Leslie, Connie and Hager, Mary, "Lost Among the Stars: A Falling Satellite Raises Global Fears," *Newsweek* (August 29, 1988).
66. Purdum, Tod S., "Russian Mars Craft Falls Short and Crashes Back to Earth," *New York Times* (November 18, 1996); and Gordon, Michael R., "Mystery of Russian Spacecraft: Where Did It Fall to Earth?" *New York Times* (November 19, 1996).
67. "Challenger Disaster," *Dallas Observer* (August 27, 1987); see also *Nation* (February 22, 1986).
68. Ibid.
69. Major Mike Morgan, deputy director of the Space Control Center, U.S. Space Command, Cheyenne, Wyoming, in interview by Derek McGinty, *All Things Considered,* National Public Radio (August 13, 1997).
70. Broad, William J., "New Plans on Reactors in Space Raise Fears of Debris," *New York Times* (October 18, 1988).
71. Wald, Matthew L., "Nuclear Waste Tanks at Hanford Could Explode," *New York Times* (July 31, 1990).
72. Wald, Matthew L., "4 Decades of Bungling at Bomb Plant," *New York Times* (January 25, 1992).
73. *Morning Report,* National Public Radio (May 15, 1997: 9:00 A.M.), broadcast on KERA-90.1FM in Dallas.
74. Pollack, Andrew, "After Accident, Japan Rethinks Its Nuclear Hopes," *New York Times* (March 25, 1997).
75. By contrast, the terrorist bombings of the World Trade Center in New York and the Murrah Federal Building in Oklahoma City each used less than three tons of ammonium nitrate.
76. "Fifty Years Later, Texas Town Recalls Horrors of Deadly Blast," *New York Times* (April 16, 1997)
77. Cushman, John H., "Chemicals on Rails: A Growing Peril," *New York Times* (August 2, 1989).

CHAPTER FIVE

1. Anderson, Harry with Mazmazumdar, Sudip and Foote, Donna, "Rajiv Gandhi Stumbles: Has India's Young Leader Become 'Directionless'?" *Newsweek* (February 23, 1987), p. 38.
2. Ford, Daniel, *The Button: America's Nuclear Warning System—Does It Work?* (New York: Simon and Shuster, 1985), pp. 52-53.
3. Ibid., pp. 25 and 52.
4. Editorial, *New York Times* (April 22, 1958), p. 10.
5. Von Hippel, Frank, "De-Alerting," *Bulletin of the Atomic Scientists* (May/June 1997), p. 35.
6. Ibid. Von Hippel was assistant director for national security in the White House Office of Science and Technology Policy from 1993 to 1994. See also Hall, Brian, "Overkill Is Not Dead," *New York Times Magazine* (March 15, 1998); and Arkin, William M. and Kristensen, Hans, "Dangerous Directions," *Bulletin of the Atomic Scientists* (March-April 1998).
7. Blair, Bruce, *The Logic of Accidental Nuclear War* (Washington, D.C.: Brookings Institution, 1993), p. 255.
8. Unless specifically noted, the incidents discussed in this section are discussed in Chapter 4 or Appendix.

9. Keith Schneider wrote a series of articles on this issue in the *New York Times,* including "U.S. Secretly Fixes Dangerous Defects in Atomic Warheads" (May 24, 1990); "Interest Rises in Studies of Atomic Shells" (May 28, 1990); and "Nuclear Missiles on Some Bombers To Be Withdrawn" (June 9, 1990).
10. Sagan, Scott, *The Limits of Safety: Organizations, Accidents and Nuclear Weapons* (Princeton, New Jersey: Princeton University Press, 1993), pp. 181-183.
11. What makes this scenario particularly interesting is that it does not assume that any of the warning or communications systems fail to function properly.
12. Wall, Don, "The Secret Arsenal," *Evening News,* WFAA-TV, Dallas, Texas (November 2, 1995).
13. For a more detailed description, see Ford, op. cit., pp. 118-119.
14. The following brief discussion is drawn from Blair, op. cit., pp. 188-191. For a detailed description of the warning systems, see also Ford, op. cit., Bracken, Paul, *The Command and Control of Nuclear Forces* (New Haven, Connecticut: Yale University Press, 1983); and Blair, Bruce, *Strategic Command and Control: Redefining the Nuclear Threat* (Washington, D.C.: Brookings Institution, 1985).
15. Nelan, Bruce W., "Nuclear Disarray," *Time Magazine* (May 19, 1997), pp. 46-47; and Blair, Bruce G., Feiveson, Harold A. and von Hippel, Frank N., "Taking Nuclear Weapons Off Hair-Trigger Alert," *Scientific American* (November 1997), pp. 74-76.
16. Ibid.
17. Center for Defense Information, *Defense Monitor* 15 (no. 7, 1986), p. 6. NORAD officials have said that the figures for the years prior to 1977 are "unavailable". These data were classified beginning in 1985 by the Reagan administration, though it is hard to imagine any legitimate security reason why these data could not be made public. As far as I have been able to determine, they are still classified.
18. Major Mike Morgan, deputy director of the Space Control Center, U.S. Space Command, in interview by Derek McGinty, *All Things Considered,* National Public Radio (August 13, 1997).
19. Blair, op. cit. (1993), pp. 192-193.
20. Ibid., p. 193.
21. Public reports of this incident did not appear until late November, and surfaced first in the British press (Frayn, Michael, "Miscellany," *The Manchester Guardian,* November 28, 1960). It was not until the first week in December that reports surfaced in the United States, after which the story was quickly swept under the rug. Various versions appeared: "Moon Stirs Scare of Missile Attack," *New York Times* (December 8, 1960, where the story was relegated to p. 71); "Canadian Is Praised Over Missile Scare," *New York Times* (December 23, 1960); and "A Nuclear Warning Disregarded on Pearl Harbor Day" (referring to the date of the first Associated Press dispatch of the story in the United States) *I.F. Stone's Weekly* (December 19, 1960). Additional accounts were published in the *Washington Star* (December 7, 1960); *Washington Post* (December 8, 1960); and *Boston Traveller* (December 12, 1960).
22. Sagan, op. cit., pp. 99-100.
23. Ibid., pp. 146-148.
24. This explanation is less likely if Penkovsky was also the source of information about the location of the drop. If he were trying to trick the Soviets into triggering a nuclear attack, the odds of succeeding would have been better if they knew nothing about the drop, or at least did not know its true location. On the other hand, the KGB had been on to Penkovsky for some time before his arrest and may have learned about the drop location another way.
25. Malnak, Lewis D., sworn affidavit (Washington, D.C.: January 10, 1974). Malnak was the president of a company that undertook a project for the Special Communications Project Office of the Navy, which interfaced with the SECT program. (It is unclear whether this second incident involved another SECT buoy from the same sub or a buoy from a different sub.)
26. Sagan, op. cit., p. 238.
27. Sulzberger, A.O., "Error Alerts U.S. Forces to a False Missile Attack," *New York Times* (November 11, 1979); Halloran, Richard, "U.S. Aides Recount Moments of False Missile Alert," *New York Times* (December 16, 1979).
28. Hart, Gary and Goldwater, Barry, "Recent False Alerts from the Nation's Missile Attack Warning System," *Report to the Committee on Armed Services of the United States Senate: October 9, 1980* (Washington, D.C.: U.S. Government Printing Office, 1980), pp. 5-6.
29. Halloran, Richard, "Computer Error Falsely Indicates A Soviet Attack," *New York Times* (June 6, 1980); Burt, Richard, "False Nuclear Alarms Spur Urgent Effort to Find Flaws," *New York Times* (June 13, 1980). See also Sagan, op. cit., p. 231.
30. Ford, op. cit., p. 78. See also footnotes 23 and 24.
31. Ford, op. cit., p. 79; Sagan, op. cit., p. 232.
32. Hart and Goldwater, op. cit., p. 7.
33. Ford, op. cit., p. 79.

34. Asakura, Toshio, "Soviet War Message Reported: Sent Shortly After Reagan Bomb Joke," *Sacramento Bee* (October 3, 1984).
35. Bracken, op. cit., pp. 65-66.
36. Halloran, Richard, "Computer Error Falsely Indicates a Soviet Attack," *New York Times* (June 6, 1980).
37. Beecher, William, "Cuban MiG Flight to Florida Spurs Review of Air Defense Procedures," *New York Times* (October 7, 1969).
38. "Soviet Plane From Cuba Flies Over a U.S. Force," World News Briefs, *New York Times* (April 23, 1977).
39. Kifner, John, "U.S. Officer Says Frigate Defenses Were Turned Off," *New York Times* (May 20, 1987); Kifner, John, "Captain of Stark Says Ship Failed to Detect Missiles," *New York Times* (May 21, 1987); Cushman, John, "Blind Spot Left Stark Vulnerable, U.S. Officials Say," *New York Times* (June 1, 1987).
40. Barringer, Felicity, "Lone West German Flies Unhindered to the Kremlin," and Reuters News Service, "Pilot Said to Have Passion for Flying," *New York Times* (May 30, 1987); Taubman, Philip, "Moscow Frees Young German Pilot," *New York Times* (August 4, 1988).
41. That might not be the case, though, if the nations tricked into war were themselves minor nuclear powers. Suppose, for example, a nuclear-capable country outside the Middle East triggered a catalytic war between, say, Iran and Israel in order to promote its own agenda.
42. The goal of designers is to make PALs difficult and time consuming to defeat, but it is generally understood that they cannot be made infallible. As one analyst put it, "Although no PAL can be certified as tamper-proof, a designer can hope to achieve a degree of tamper resistance, which is generally measured by the period of time it would take a skilled but unauthorized person with some knowledge of the PAL's design to defeat it." Zimmerman, Peter D., "Navy Says No PALs for Us," *Bulletin of the Atomic Scientists* (November 1989), p. 38.
43. Blair, op. cit. (1993), p. 50. (note that the order of some of this quote has been rearranged).
44. Gillert, Doug, "Through the Looking Glass," *Airman* (October 1987), p. 13.
45. For a simple discussion of these controls, see Ford, op. cit., p. 151-152.
46. The source of this information is Daniel Ellsberg, who was closely involved with American nuclear war planning at the Pentagon in the 1960s, as noted in Bracken, op. cit., pp. 198-199.
47. Blair, op. cit., (1993) p. 50.
48. Halloran, Richard, "U.S. Downs Iran Airliner Mistaken for F-14; 290 Reported Dead; A Tragedy, Reagan Says," *New York Times* (July 4, 1988).
49. Engleberg Stephen, "Failures Seen in Safeguards on Erroneous Attacks," *New York Times* (July 4, 1988); Gordon, Michael, "Questions Persist on Airbus Disaster," *New York Times* (July 5, 1988); "U.S. Pushes Inquiry on Downing of Jet: Questions Mount"; Halloran, Richard, "Team Goes to Gulf," and Johnson, Julie, "No Shift in Policy," *New York Times* (July 5, 1988); Hess, John, "Iranian Airliner," *New York Observer* (July 18, 1988); Aspin, Les, "Witness to Iran Flight 655," *New York Times* (November 18, 1988).
50. Shribman, David, "Korean Jetliner: What Is Known and What Isn't," *New York Times* (September 8, 1983).
51. Shribman, David, "U.S. Experts Say Soviet Didn't See Jet Was Civilian," *New York Times* (October 7, 1983).
52. Ibid., and "Korean Jetliner: What Is Known and What Isn't," *New York Times* (September 8, 1983); Pearson, David, "KAL 007: What the U.S. Knew and When We Knew It," *Nation* (April 18-25, 1984), pp. 105-124; Weisman, Steven R., "U.S. Says Spy Plane Was in the Area of Korean Airliner," *New York Times* (September 5, 1983); Polman, Dick, "Challenging the U.S. on Flight 007," *Philadelphia Inquirer* (October 18, 1984); Gwertzman, Bernard, "A New U.S. Transcript Indicates Soviet Pilot Fired 'Canon Bursts,'" *New York Times* (September 12, 1983). See also Hersh, Seymour M., *The Target Is Destroyed: What Really Happened to Flight 007 & What America Knew About It* (New York: Vintage, 1987).
53. Weisman, op. cit.; Erlanger, Steven, "Similarities with KAL Flight Are Rejected by U.S. Admiral," *New York Times* (July 4, 1988).
54. Gordon, Michael R., "U.S. Helicopters Given No Warning by Attacking Jets," *New York Times* (April 16, 1994); see also "F-15 Pilot Says Radar Plane Did Not Warn Him," *New York Times* (June 6, 1995).
55. Lietenberg, Milton, "The Case of the Stranded Sub," *Bulletin of the Atomic Scientists* (March 1982), pp. 10-13.
56. Stevenson, Richard, "Russian Submarines, or 'Ghosts' of the Cold War," *New York Times* (March 8, 1993).

57. Simon, Scott and Haydon, Simon reporting, "Swedish Government Makes an Embarrassing Discovery," *Weekend Edition/Saturday*, National Public Radio (Washington, D.C.: February 18, 1995).
58. Ford, op. cit., p. 87.
59. Ibid., p. 88.
60. Ibid., pp. 20-21.
61. Kaplan, Richard, executive producer and Koppel, Ted, anchor, "Surprise Attack: Choosing a Response," *Nightline* (New York: ABC News, Show #1169, November 14, 1985), pp. 5-6.
62. Ford, op. cit., p. 136.
63. Ibid., pp. 91-92.
64. "Pentagon Warning System Can't Handle Pressure, Says GAO," *Electronic Design* (April 12, 1980), p. 59.
65. "Warning System 'Fragile': Bad Computer Military Jinx," *West Palm Beach Post* (March 10, 1980).
66. Ford, op. cit., pp. 188-189.
67. The exercise was run in late November 1980. "Simulated Mobilization for War Produces Major Problems," *New York Times* (December 22, 1980).
68. Hudson, Richard, "Molink Is Always Ready," *New York Times* Magazine (August 26, 1973).
69. "National Warning Plan Fails," *Sacromento Bee* (February 18, 1984).
70. Keller, Bill, "Pentagon Test on News Coverage Hurt by Communications Lapses," *New York Times* (April 27, 1985).
71. *Sacramento Bee* (November 19, 1989).
72. "Norway Military Mail Sent to East Germans," *New York Times* (July 30, 1975).
73. "Coordination Plans of Military Services Attacked," *New York Times* (March 22, 1984).
74. "Army Phones Need $30 Million Repair," *New York Times* (March 2, 1985).
75. U.S. House of Representatives, Armed Services Investigating Subcommittee, Committee on Armed Services, *Review of Department of Defense World-Wide Communications* (Washington, D.C.: U.S. Government Printing Office, 1971).
76. U.S. House, Armed Services Investigating Subcommittee, op. cit., p. 6.
77. Ibid., pp. 6-11.
78. "Israeli Payment to Close the Book on '67 Attack on U.S. Navy Vessel," *New York Times* (December 19, 1980); See also "C.I.A. Papers Cite Israeli's in Attack on U.S. Navy Ship," *New York Times* (September 19, 1977).
79. U.S. House, Armed Services Investigating Subcommittee, op. cit., p. 14.
80. Ford, op. cit., pp. 173-174, and Ball, Desmond, "Can Nuclear War Be Controlled?" *Adelphi Papers* (London: International Institute for Strategic Studies, No. 169), pp. 12-13; see also "Resistance Met: All 39 From Vessel Safe—U.S. Jets Hit Cambodian Base," *New York Times* (May 15, 1975).
81. Center for Defense Information, *Defense Monitor* 15 (no. 7, 1986), p. 3. See also Sagan, op. cit., p. 64.
82. Blair, op. cit. (1993), p. 225. Bayesian analysis is a probabilistic technique for calculating the extent to which additional information causes one to revise earlier estimates of the likelihood of an event.
83. Rusten, Lynn and Stern, Paul C., *Crisis Management in the Nuclear Age,* Committee on International Security and Arms Control of the National Academy of Sciences, and Committee on Contributions of Behavioral and Social Science to the Prevention of Nuclear War of the National Research Council (Washington, D.C.: National Academy Press, 1987), p. 26.
84. Bernstein, B.J., "The Week We Almost Went to War," *Bulletin of the Atomic Scientists* (February 1976), p. 17.
85. Kennedy, John F., "Presidential Address to the Nation" (October 22, 1962), reprinted in Kennedy, Robert F., *Thirteen Days: A Memoir of the Cuban Missile Crisis* (New York: W.W. Norton, 1969), p. 168.
86. Ellsberg, Daniel, "The Day Castro Almost Started World War III," *New York Times* (October 31, 1987).
87. Ibid.
88. Paul, Derek, Intrilligator, Michael and Smoker, Paul, editors, *Accidental Nuclear War: Proceedings of the 18th Pugwash Workshop on Nuclear Forces* (Toronto: Samuel Stevens and Company and University of Toronto Press, 1990), pp. 43-51.
89. Sagan, op. cit., p. 95.
90. Ibid., p. 96.
91. Ibid., pp. 79-80.
92. Ibid., pp. 136-137.
93. Kennedy, Robert, op. cit., p. 111.
94. Hall, Brian, "Overkill Is Not Dead," *New York Times Magazine* (March 15, 1998), p. 84.

95. Stein, Janice G., "The Challenge of the Persian Gulf Crisis," *Peace and Security* (Canadian Institute for Peace and Security: Winter 1990-91), pp. 4-5.
96. Blair, Feiveson and von Hippel, op. cit., p. 80.
97. Blair, Bruce, "Russia's Doomsday Machine," and Broad, William J., "Russia Has a Nuclear 'Doomsday' Machine," *New York Times* (October 8, 1993).

CHAPTER SIX

1. U.S. General Accounting Office, "Human Factors: FAA's Guidance and Oversight of Pilot Crew Resource Management Training Can Be Improved" (November 1997: GAO/RCED-98-7), p. 2.
2. Wald, Matthew L., "Crew of Airliner Received Warning Just Before Guam Crash," *New York Times* (March 24, 1998).
3. U.S. General Accounting Office, "Military Aircraft Safety: Serious Accidents Remain at Historically Low Levels" (March 1998: GAO/NSIAD-98-95BR), p. 2.
4. Lochbaum, David, *The Good, The Bad and the Ugly: A Report on Safety in America's Nuclear Power Industry,* Union of Concerned Scientists (June 1998), p. v.
5. Bureau of the Census, U.S. Department of Commerce, *Statistical Abstract of the United States, 1998,* Table 249, p. 157. These data were converted assuming alcohol content of 3.5 percent for beer, 12 percent for wine and 40 percent for distilled spirits.
6. Cushman, J. H., "Three Pilots Dismissed in Alcohol Abuse," *New York Times* (March 17, 1990).
7. Weiner, E., "Drunken Flying Persists Despite Treatment Effort," *New York Times* (July 14, 1990).
8. Newhall, D., acting assistant secretary of defense for health affairs, "Memorandum to the Assistant Secretaries of the Army, Navy and Air Force (M&RA), Subject: Error in 'Heavy Drinkers' Category in the 1982, 1985, and 1988 Worldwide Survey of Substance Abuse and Health Behaviors Among Military Personnel" (15 August 1989).
9. Bray, R.M., et al., *1995 Department of Defense Survey of Health-Related Behaviors Among Military Personnel* (Research Triangle Institute, December 1995). Note that because the corrections were distributed some time after the 1988 report was issued, the figures cited here may differ from those given in the text of the original reports of the 1982, 1985 and 1988 surveys.
10. Bray, op. cit., Table 3, "Substance Abuse Summary for Total DoD, 1980-1995."
11. Ibid.
12. Sociologists use the term "total institution" to refer to an organizational setting in which the institution encompasses all aspects of the "inmate's" life. Examples include prisons, mental institutions and the military.
13. Bray, R.M. et.al., *1988 Worldwide Survey of Substance Abuse and Health Behaviors Among Military Personnel* (Research Triangle Institute: December 1988), p. 17.
14. To their credit, the surveyors do, in fact, mention this problem. "Many individuals question the validity of self-reported data on alcohol and drug use, claiming that survey respondents will give socially desirable rather than truthful answers." They go on to argue that their method provides "useful and meaningful data," while at the same time recognizing that "self-reports may sometimes underestimate the extent of substance abuse." They cite a 1979 study of alcohol problems among Air Force personnel which tried to look at this question by cross-checking available records. That study found some categories of answers seemed to be accurate, but it also found, "Air Force beverage sales data . . . suggested that self-reports underestimate actual prevalence of alcohol use by as much as 20 percent." Ibid., pp. 21-22.
15. Treml, Vladimir G., "Drinking and Alcohol Abuse in the USSR in the 1980's," in Jones, A., Connor, W.D. and Powell, D.E., editors, *Soviet Social Problems* (Boulder, Colorado: Westview Press, 1991), p. 121.
16. Treml, Vladimir G., "Soviet and Russian Statistics on Alcohol Consumption and Abuse," in Bobadilla, J.L., Costello, C.A. and Mitchell, F., editors, *Premature Death in the New Independent States* (Washington, D.C.: National Academy Press, 1997), pp. 222-224.
17. Treml, op. cit. (1991), p. 121.
18. This pattern is all the more striking considering the cost of alcohol in the USSR at the time, particularly after the price increases that accompanied the antidrinking campaign. Treml estimates that the average industrial worker in Western Europe or the U.S. had to work roughly 2-3 hours to earn enough money

to buy a liter of vodka, while the average Soviet industrial worker had to work 19 hours. Ibid., pp. 125 and 131.

19. 19.Gabriel, R.A., *The New Red Legions: An Attitudinal Portrait of the Soviet Soldier* (Westport, Connecticut: Greenwood Press, 1980), p. 153.
20. Ibid., p. 154.
21. Ibid., pp. 156-157.
22. "The Red Army," *World,* WGBH-TV (Boston) (May 6, 1981), transcript, p. 21.
23. For a discussion of the problems of conversion in the former Soviet Union, see Oden, Michael, "Turning Swords into Washing Machines: Converting Russian Military Firms to Consumer Durable Production" and Ullmann, John, "Conversion Problems in the Changing Economies," in Dumas, L.J., editor, *The Socio-Economics of Conversion: From War to Peace* (Armonk, New York: M.E. Sharpe, 1995).
24. Brinkley, J., "Vast Undreamed of Drug Use Feared," *New York Times* (November 23, 1984).
25. Crowe, A., "Teen Cocaine Use Triples Since 1975," *New York Times* (March 21, 1985).
26. Treaster, J.B., "Cocaine Use Found on the Way Down Among U.S. Youths," *New York Times* (January 25, 1991).
27. Goodwin, M. and Chass, M., "Baseball and Cocaine: A Deepening Problem," *New York Times* (August 19, 1985).
28. Kerr, P. , "17 Employees of Wall Street Firms Are Arrested on Cocaine Charges," *New York Times* (April 17, 1987).
29. LSD (d-lysergic acid diethylamide) was first synthesized at the research laboratories of the Sandoz drug company in Basel, Switzerland.
30. Despite the strength of the drug, it is extremely difficult if not impossible to become physically addicted to LSD. The body builds up resistance to its effects in 2-3 days. Resistance fades just as quickly. See Grinspoon, L. and Bakalar, J.B., *Psychedelic Drugs Reconsidered* (New York: Basic Books, 1979), p. 11.
31. Ibid., pp. 12-13 and 158.
32. Ibid.
33. Ibid., p. 13-14.
34. Ibid., p. 159.
35. Ibid., p. 160.
36. Ibid., pp. 14-35.
37. Of course, illegal drugs also have a variety of interaction and side effects that can magnify their already troubling effects on reliability and performance. Smoking marijuana is probably the single most common trigger of LSD flashbacks. The stimulant methamphetamine, the use of which had penetrated deep into the American heartland by 1996, has dangerous and relatively frequent side effects that include paranoia and extremely violent behavior. See Johnson, Dirk, "Good People Go Bad in Iowa," *New York Times* (February 22, 1996).
38. Angel, J.E., publisher, *Physicians Desk Reference* (Oradell, New Jersey: Medical Economics Company, 1983), pp. 629-630, 1622, 1702, 1771 and 2075-2076.
39. Griffith, H.W., *Complete Guide to Prescription and Non-Prescription Drugs* (The Body Press, 1990), pp. 116, 236, 336 and 790.
40. Ibid., pp. 156, 514 and 856.
41. Strange as it seems, in Chapter 11 we will see that even extremely rare events occur more often than one might think.
42. U.S. Department of Commerce, Bureau of the Census, *Statistical Abstract of the United States, 1998* (Washington, D.C.: U.S. Government Printing Office, 1998), Table 571, p. 359.
43. Bray, op. cit., Table 10.4, p. 209.
44. If it were suspected that a particular individual had recently taken LSD, a sophisticated gas chromatography mass spectroscopy test could be done on an isolate of his/her urine. That test, costing perhaps a few hundred dollars, would probably pick up evidence of the LSD use, though it is not likely to yield indisputable proof. Trying to screen tens of thousands of people this way each day would rapidly become prohibitively expensive. And the test would have to be repeated every day, because it would turn up negative if the person had used LSD even as recently as the day before. Source: Shulgin, A.T., private correspondence with the author (27 April and 10 May 1991). Dr. Shulgin is a biochemist who has authored more than 150 scientific works in chemistry, pharmacology and botany, and is recognized as an expert on the chemistry and pharmacology of psychedelics.
45. Ibid.
46. Barinaga, M., "Drug Use a Problem at U.S. Weapons Laboratory?" *Nature* (June 23, 1988), p. 696.
47. Kramer, J. M., "Drug Abuse in the USSR," in Jones, A., Connor, W.D. and Powell, D.E., editors, *Soviet Social Problems* (Boulder, Colorado: Westview Press, 1991), p. 94.

48. Ibid., pp. 94-96.
49. Ibid., p. 99.
50. Ibid., pp. 100-101.
51. Ibid., p. 103.
52. Ibid., p. 104.
53. In 1981, for example, in a television interview a U.S. State Department spokesperson reported on problems in the Soviet army: "We didn't find instances of drug abuse being what they really worried about, but now in Afghanistan the troops seem to have been able to get the drugs that they couldn't get before and this is becoming a problem that concerns Soviet military leaders." "The Red Army," op. cit., p. 22.
54. Schmeck, H.M., "Almost One in Five May Have Mental Disorder," *New York Times* (October 3, 1984), p. 1.
55. Bower, B., "Mental Disorders Outpace Treatment," *Science News* (February 27, 1993).
56. Hinsie, L.E. and Campbell, R.J., *Psychiatric Dictionary* (New York: Oxford University Press, 1970), pp. 200 and 221.
57. Ross, C.A., Joshi, S. and Currie, R., "Dissociative Experiences in the General Population," *American Journal of Psychiatry* (November 11, 1990), pp. 1550 and 1552.
58. Goleman, Daniel, "Severe Trauma May Damage the Brain as Well as the Psyche," *New York Times* (August 1, 1995).
59. Bower, B., "Trauma Disorder High, New Survey Finds," *Science News* (December 23 and 30, 1995).
60. Plag, J.A., Arthur, R.J. and Goffman, J.M., "Dimensions of Psychiatric Illness Among First-Term Enlistees in the United States Navy," *Military Medicine* 135 (1970), pp. 665-673.
61. Department of the Army, "Disposition and Incidence Rates, Active Duty Army Personnel, Psychiatric Cases, Worldwide, CY1980-1984 and CY1985-1989," U.S. Army Patient Administration Systems and Biostatistics Activity (Washington, D.C.: 1985, 1990).
62. Department of the Navy, "Distribution of Psychiatric Diagnoses in the U.S. Navy (1980-1989)," Naval Medical Data Services Center (Bethesda, Maryland: 1990).
63. Abrams, H. L., "Human Reliability and Safety in the Handling of Nuclear Weapons" (Stanford, California: Center for International Security and Arms Control, Stanford University, 1990, unpublished), p. 5.
64. Bray et al., op. cit., 1995, Table 29.
65. "3 Atom Guards Called Unstable: Major Suspended," *New York Times* (August 18, 1969).
66. "Three at Key SAC Post Are Arrested on Drug Charges," *International Herald Tribune* (March 29, 1971).
67. Dobish, A.P. , "U.S. Missile Unit Used Drugs Regularly, GI Says Eased Boredom of Missile Base," *Milwaukee Journal* (December 16, 1974).
68. Abrams, H.L., "Human Instability and Nuclear Weapons," *Bulletin of the Atomic Scientists* (January-February 1987), p. 34.
69. Earley, P. , *Family of Spies: Inside the John Walker Spy Ring* (New York: Bantam, 1988), p. 358. See also Abrams, H. L., "Sources of Human Instability in the Handling of Nuclear Weapons," in *The Medical Implications of Nuclear War*, Institute of Medicine, National Academy of Sciences (Washington, D.C.: National Academy Press, 1986), p. 512.
70. Abrams, Herbert L., "Human Reliability and Safety in the Handling of Nuclear Weapons," *Science and Global Security* 2 (1991), pp. 325-327.
71. Ibid. See also Associated Press, "Man Pleads Guilty to Two Murders," *Seattle Post-Intelligencer* (June 20, 1990).
72. Abrams, op. cit. See also "Courts," *Seattle Post-Intelligencer* (October 5, 1993).
73. Luongo, Kenneth L. and Bunn, Matthew, "Some Horror Stories Since July," *Boston Globe* (December 29, 1998).
74. Ibid.

CHAPTER SEVEN

1. Cornell, Charles E., "Minimizing Human Errors," *Space/Aeronautics* (March 1968), p. 72.
2. "Stray Flights Often Human Error," *Dallas Times-Herald* (September 20, 1983).
3. Flournoy, Craig, "2 of 3 Air Crashes Tied to Pilot Error," *Dallas Morning News* (August 25, 1985).

4. Wald, Matthew L., "American Airlines Ruled Guilty in '95 Cali Crash," *New York Times* (September 12, 1997); Mercer, Pamela, "Inquiry into Colombia Air Crash Points Strongly to Error by Pilot," *New York Times* (December 29, 1995).
5. Wald, Matthew L., "Peru Crash Is Attributed to Maintenance Error," *New York Times* (November 16, 1996).
6. Gordon, Michael R., "Astronaut Error Adds New Anxiety on Space Station," *New York Times* (July 18, 1997).
7. Eichenwald, Kurt, "Death and Deficiency in Kidney Treatment," *New York Times* (December 4, 1995).
8. Altman, Lawrence K., "State Issues Scathing Report on Error at Sloan-Kettering," *New York Times* (November 16, 1995).
9. Norris, Floyd, "Salomon's Error Went Right to the Floor," *New York Times* (March 27, 1992).
10. "Report Criticizes Scientific Testing at FBI Crime Lab," *New York Times* (April 16, 1997); see also "FBI Practices Faulted in Oklahoma Bomb Inquiry," *New York Times* (January 31, 1997).
11. "Bounty Hunters Kill Couple in Case of Mistaken Identity," *New York Times* (September 2, 1997).
12. Gruson, Lindsey, "Reactor Shows Industry's People Problem," *New York Times* (April 3, 1987).
13. Ingraham, Larry H., "'The Nam' and 'The World': Heroin Use by U.S. Army Enlisted Men Serving in Vietnam," *Psychiatry* 37 (May 1974), p. 121.
14. Private communication.
15. Frankenhaeuser, Marianne, "To Err is Human: Psychological and Biological Effects of Human Functioning," in *Nuclear War by Mistake: Inevitable or Preventable?,* report from an international conference in Stockholm, Sweden, February 15-16, 1985 (Stockholm: Spangbergs Tryckerier AB, 1985), p. 45.
16. "Why Planes Crash," NOVA #1403, WGBH-TV (Boston: WGBH Transcripts, 1987), pp. 10-13.
17. Flournoy, op. cit.
18. Reason, James, "The Psychopathology of Everyday Slips: Accidents Happen When Habit Goes Haywire," *The Sciences* (October 1984), p. 48.
19. The pilot escaped unharmed. Ibid., pp. 45 and 49.
20. Ibid.
21. Bower, B., "Emotional Stress Linked to Common Cold," *Science News* (August 31, 1991), p. 132.
22. Fackelmann, K. A., "Stress Puts Squeeze on Clogged Vessels," *Science News* (November 16, 1991), p. 309.
23. Vaughan, Christopher, "The Depression-Stress Link," *Science News* (September 3, 1988), p. 155.
24. Bower, B., "Stress Hormone May Speed up Brain Aging," *Science News* (April 25, 1998); Goleman, Daniel, "Severe Trauma May Damage the Brain as Well as the Psyche," *New York Times* (August 1, 1995).
25. Slaby, Andrew E., *Aftershock: Surviving the Delayed Effects of Trauma, Crisis and Loss* (New York: Villard Books, 1989), p. 33.
26. Heron, Kim, "The Long Road Back," *New York Times Magazine* (March 6, 1988).
27. Slaby, op. cit., p. 77.
28. Grady, Denise, "War Memories May Harm Health," *New York Times* (December 16, 1997).
29. Official figures at the time indicated a much lower rate of psychiatric casualties in the 1973 war because those who were both physically and psychologically wounded were counted only as physical casualties. More important, official figures also excluded those whose psychological symptoms did not appear until sometime later. Shipler, David K., "Other Israeli Wounded: Mentally Scarred in War," *New York Times* (January 8, 1983).
30. The study by Naomi Breslau and her colleagues, reported in *Archives of General Psychiatry* (March 1991), is discussed in Bower, B., "Trauma Disorder Strikes Many Young Adults," *Science News* (March 30, 1991), p. 198.
31. Bower, op. cit. The first three ranked disorders are phobias, severe depression and dependency on drugs or alcohol.
32. Bower, B., "Emotional Trauma Haunts Korean POWs," *Science News* (February 2, 1991), p. 68.
33. Slaby, op. cit., p. xiv.
34. Ibid., p. 71.
35. Since the lower military ranks are heavily populated with young adults from urban areas, there may be a real stress-related reliability problem in the lower ranks. Since traumatic stress can have a very long reach and many career officers have experienced the trauma of battle and/or captivity, there may also be a real stress-related reliability problem in the higher ranks.

36. Moore-Ede, Martin C., Sulzman, Frank M. and Fuller, Charles A., *The Clocks that Time Us: Physiology of the Circadian Timing System* (Cambridge: Harvard University Press, 1982), p. 1.
37. In the absence of environmental time cues, the free-running sleep-wake cycle for humans is typically about 25 hours. When people are isolated for long periods, the cycle tends to change, drifting to as long as 30-50 hours. There appear to be two major distinct circadian pacemakers in human beings that are coupled to each other. Together they coordinate the various daily cycles. In the absence of external information, the pacemakers eventually seem to uncouple, desynchronizing the body's biological clock. The two pacemakers each seem to control the patterns of different stages of sleep: for example, one controls REM (dream) sleep, while the other controls slow-wave sleep (deep sleep). Thus, decoupling the pacemakers can cause disruptions in the normal sequence of sleep stages and so can degrade the quality of sleep (that is, the degree of rest and refreshment it produces). Ibid., pp. 207 and 298-301.
38. Monk, T.H. and Aplin, L.C., "Spring and Autumn Daylight Savings Time Changes: Studies in Adjustment in Sleep Timings, Mood and Efficiency," *Ergonomics* 23 (1980), pp. 167-178.
39. Given enough time, typically a few days to a week, an out-of-phase biological clock will reset itself, as environmental *zeitgebers* (literally "time givers"; signals such as light and temperature variations) get the circadian rhythms back in phase with the external world. Resynchronization can be accelerated by intentionally manipulating *zeitgebers*. Certain aspects of diet, such as specific patterns of carbohydrate versus protein intake, proper timing of meals and variation of meal size can speed readjustment. So can controlled exposure to bright light. See Ehret, C.F., "New Approaches to Chronohygiene for the Shiftworker in the Nuclear Power Industry," in Reinberg et al., editors, *Advances in the Biological Sciences, Volume 30: Night and Shift Work—Biological and Social Aspects* (Oxford: Pergamon Press, 1981), pp. 267-268.

    The hormone melatonin, secreted by the pineal gland, plays such a key role in controlling circadian rhythms that it has become popular for travelers to take melatonin pills to beat jet lag. Recent research suggests, however, that melatonin supplements may not be as safe as originally thought. They might "numb" the brain's suprachiasmic nucleus, which contains the circadian clock. Barinaga, Marcia, "How Jet-Lag Hormone Does Double Duty in the Brain," *Science* (July 25, 1997), p. 480. It is also possible that excess melatonin could damage the retina of the eye, which may also contain another key circadian clock. Morell, Virginia, "A 24-Hour Circadian Clock Is Found in the Mammalian Retina," *Science* (April 19, 1995), p. 349.
40. Tilley, A.J., Wilkinson, R.T., Warren, P. S.G., Watson, B. and Drud, M., "The Sleep and Performance of Shift Workers," *Human Factors* 24 (no. 6, 1982), p. 630.
41. Moore-Ede, Martin C., Czeisler, Charles A. and Richardson, Gary S., "Circadian Timekeeping in Health and Disease: Part 2: Clinical Implications of Circadian Rhythmicity," *The New England Journal of Medicine* 309 (no. 9, September 1, 1983), p. 534.
42. Tilley, op. cit., pp. 629-631.
43. Ibid., p. 634.
44. Ibid., p. 638-639.
45. Moore-Ede, Czeisler and Richardson, op. cit., p. 531.
46. Ehret, C.F., op. cit., pp. 263-264.
47. Wald, Matthew L., "Sleepy Truckers Linked to Many Deaths," *New York Times* (January 19, 1995); and Wald, Matthew L., "Truckers Need More Sleep, a Study Shows," *New York Times* (September 11, 1997).
48. Moore-Ede, Sulzman, and Fuller, op. cit., pp. 332-333.
49. Ibid., pp. 333-334.
50. Ibid., p. 336.
51. By itself, this association does not imply either that disruptions of the biological clock necessarily trigger mental disorders or that those who suffer from mental illness always experience circadian disruptions.
52. Ibid., p. 369.
53. Ibid., p. 372.
54. Post, Jerrold M., "The Seasons of a Leader's Life: Influences of the Life Cycle on Political Behavior," *Journal of the International Society of Political Psychology* 2 (Fall-Winter 1980, no. 314), p. 42.
55. Abrams, Herbert L., "The Age Factor in the Election of 1996 and Beyond," Stanford University School of Medicine and Center for International Security and Arms Control (unpublished).
56. Post, op. cit., pp. 44-47.
57. Ibid., p. 45.
58. Ibid., p. 46.

59. L'Etang, Hugh, *The Pathology of Leadership* (London: William Heineman Medical Books Ltd., 1969), p. 84.
60. Ibid., pp. 87 and 90.
61. Ibid., p. 149.
62. Ibid., p. 150.
63. Ibid., p. 155.
64. Ibid., p. 179.
65. Ibid., pp. 181-183.
66. Kunz, Jeffrey R.M. and Finkel, Asher J., editors, *American Medical Association: Family Medical Guide* (New York: Random House, 1987), p. 535.
67. L'Etang, op. cit., pp. 184-188.
68. Woodward, Bob and Bernstein, Carl, *The Final Days* (New York: Simon and Shuster, 1976), pp. 404 and 423.
69. Ibid., p. 424.
70. Abrams, Herbert L., "The Vulnerable President and the Twenty-Fifth Amendment, with Observations on Guidelines, a Health Commission, and the Role of the President's Physician," *Wake Forest Law Review* (Fall 1995).
71. For a thorough documentation of the medical events and political implications of the disabling attempted assassination of Ronald Reagan, see Abrams, Herbert L., *The President Has Been Shot: Confusion, Disability and the 25th Amendment in the Aftermath of the Attempted Assassination of Ronald Reagan* (New York: Norton, 1992).
72. Abrams, Herbert L., "The Power Vacuum," *Stanford Magazine* (March 1992), pp. 51-52.
73. Ibid., p. 53.
74. Ibid.
75. "Memory and Aging," "Is It Alzheimer's: Warning Signs You Should Know" and "If You Think Someone You Know Has Alzheimer's," Alzheimer's Association (919 North Michigan Ave., Chicago, Illinois 60611).
76. Abrams, Herbert L., "Disabled Leaders, Cognition and Crisis Decision Making," in Paul, Derek, Intrilligator, Michael D. and Smoker, Paul, editors, *Accidental Nuclear War: Proceedings of the Eighteenth Pugwash Workshop on Nuclear Forces* (Toronto: Samuel Stevens, 1990), pp. 137-138.
77. Abrams, op. cit., "Age Factor," p. 3.
78. Ibid., pp. 139-140.
79. Ibid.

CHAPTER EIGHT

1. Azar, Beth, "Teams That Wear Blinders Are Often the Cause of Tragic Errors," *American Psychological Association Monitor* (September 1994), p. 23.
2. Holsti, Ole R. and George, Alexander L., "The Effects of Stress on the Performance of Foreign Policy-Makers," in Cotter, Cornelius P. , editor, *Political Science Annual: An International Review* 6 (1975), p. 294.
3. Halperin, Morton H., *Bureaucratic Politics and Foreign Policy* (Washington, D.C.: Brookings Institution, 1974), pp. 235-279.
4. Thomson, James, "How Could Vietnam Happen?" *Atlantic* (1968), pp. 47-53; and Halberstam, David, *The Best and the Brightest* (New York: Random House, 1972).
5. Schmitt, Eric, "How U.S. Immigration Officials Deceived a Group of Lawmakers," *New York Times* (June 29, 1996).
6. Argyris, Chris, "Single-Loop and Double-Loop Models in Research on Decisionmaking," *Administrative Science Quarterly* (September 1976), pp. 366-367.
7. Holsti and George, op. cit., pp. 293-295.
8. Schlesinger, Arthur Jr., *The Imperial Presidency* (Boston: Houghton-Mifflin, 1973).
9. Eberhardt, J., "Challenger Disaster: Rooted in History," *Science News* (June 14, 1986), p. 372.
10. Wald, Mathew L., "Energy Chief Says Top Aides Lack Skills to Run U.S. Bomb Complex," *New York Times* (June 28, 1989).
11. Ibid.
12. Schneider, Keith, "U.S. Takes Blame in Atom Plant Abuses," *New York Times* (March 27, 1992).

13. Ibid.
14. Marshall, Eliot, "Savannah River Blues," *Science* (October 21, 1988), p. 363.
15. Ibid., p. 364.
16. Ibid., pp. 363-364.
17. Spotts, Peter, "Nuclear Watchdog Agency Shows Signs of Losing Bite," *Christian Science Monitor* (June 6, 1996).
18. U.S. General Accounting Office, *Nuclear Regulation: Preventing Problem Plants Requires More Effective NRC Action* (May 1997: GAO/RCED-97-145).
19. Wayne, Leslie, "Getting Bad News at the Top," *New York Times* (February 28, 1986).
20. Ibid.
21. Shenon, Philip, "Pentagon Reveals It Lost Most Logs on Chemical Arms," *New York Times* (February 28, 1997).
22. Wye, Ted (a pseudonym), "Will They Fire in the Hole?" *Family,* supplement of *Air Force Magazine* (November 17, 1971).
23. Violation of strict rules against fraternization between the ranks were part of the legal charges leveled against drill instructors and other military officers during the flood of sexual harrassment and rape complaints lodged by women in all branches of the armed forces during the 1990s.
24. Kilborn, Peter T., "Sex Abuse Cases Stun Pentagon, But the Problem Has Deep Roots," *New York Times* (February 10, 1997).
25. A majority of the servicewomen responding to a 1996 Pentagon poll said that they had been sexually harassed. Many said their attempts to complain had resulted in "ridicule, retaliation or indifference." Later that year, the Army set up a telephone "hot line" to facilitate and destigmatize reporting sexual harassment complaints. In the first 12 weeks alone, they logged almost 7,000 calls, nearly 1,100 of which they considered legitimate enough to follow up. See Kilborn, Peter T., "Sex Abuse Cases Stun Pentagon, But the Problem Has Deep Roots," *New York Times* (February 10, 1997).
26. Holsti and George, op. cit., p. 295.
27. MacNamara, Robert S., "One Minute to Doomsday," *New York Times* (October 14, 1992).
28. Kennedy, Robert F., *Thirteen Days: A Memoir of the Cuban Missile Crisis* (New York: Norton, 1969), pp. 94-95.
29. Burlatsky, Fedor, "Castro Wanted a Nuclear Strike," *New York Times* (October 23, 1992).
30. Wilson, Richard, "A Visit to Chernobyl," *Science* (June 26, 1987), pp. 1636-1640.
31. Ibid., p. 1639.
32. Daniels, Arlene K., "The Captive Professional: Bureaucratic Limitations in the Practice of Military Psychiatry," *Journal of Health and Social Behavior* 10 (1969), pp. 256-257.
33. Ibid., pp. 255-265.
34. Ibid., p. 263.
35. Bem, D.J., "The Concept of Risk in the Study of Human Behavior," in Carney, R.E., editor, *Risk Taking Behavior* (Springfield, Illinois: Thomas, 1971).
36. Janis, Irving L., *Victims of Groupthink: A Psychological Study of Foreign-Policy Decisions and Fiascoes* (Boston: Houghton-Mifflin, 1972), p. 9.
37. Johnston, David and Revkin, Andrew C., "Report Finds FBI Lab Slipping From Pinnacle of Crime Fighting," *New York Times* (January 29, 1997).
38. Janis, op.cit., pp. 197-198.
39. Ibid., p. 67.
40. Ibid., p. 78.
41. Ibid.
42. Ibid., p. 88. It is interesting to note that this is yet another example of the common tendency discussed earlier to jump from the conclusion that an event has a low probability to the operating assumption that it will not happen, that is, that it is impossible.
43. Ibid., p. 89.
44. Ibid., p. 91.
45. Ibid., pp. 138-166.
46. Most of the following discussion of the Manson case draws heavily on the most comprehensive account of this murder case available, written by Vincent Bugliosi, chief prosecutor at the subsequent trial. See Bugliosi, Vincent with Gentry, Curt, *Helter Skelter: The True Story of the Manson Murders* (New York W.W. Norton, 1974).
47. Ibid., p. 245.
48. Much of this discussion is drawn from two primary sources: "The Death of Representative Leo Ryan, People's Temple, and Jonestown: Understanding a Tragedy," *Hearing before the Committee on*

Foreign Affairs, House of Representatives (96th Congress, 1st Session, May 15, 1979); and "The Cult of Death," special report, *Newsweek* (December 4, 1978), pp. 38-81.

49. Axthelm, Pete et al., "The Emperor Jones," *Newsweek* (December 4, 1978), p. 55.
50. Committee on Foreign Affairs, op. cit., p. 15.
51. Everbach, Tracy, "Agents Had Trained for Months for Raid" and Hancock, Lee, "Question's Arise on Media's Role in Raid," *Dallas Morning News* (March 1, 1993).
52. Loe, Victoria, "Howell's Revelation: Wounded Sect Leader, in a Rambling Interview, Says that He Is Christ," and "A Look at Vernon Howell," *Dallas Morning News* (March 1, 1993).
53. Ibid.
54. Ibid.
55. Ibid.
56. England, Mark and McCormick, Darlene, "Waco's Paper's Report Called Cult 'Dangerous,'" *Dallas Morning News* (March 1, 1993).
57. Ibid.
58. The discussion of the Heaven's Gate cult in this section is based largely on information drawn from the following articles published in the *New York Times:* Purdum, Todd S., "Tapes Left by 39 in Cult Suicide Suggest Comet Was Sign to Die" (March 28, 1997); Niebuhr, Gustav, "On the Furthest Fringes of Millennialism" (March 28, 1997); Bruni, Frank, "Leader Believed in Space Aliens and Apocalypse" (March 28, 1997); Heaven's Gate, "Our Position Against Suicide," reprinted as "Looking Forward to Trip Going to the Next Level" (March 28, 1997); Ayres, B. Drummond, "Families Learning of 39 Cultists Who Died Willingly" (March 29, 1997); Bruni, Frank, "A Cult's 2-Decade Odyssey of Regimentation" (March 29, 1997); Steinberg, Jacques, "The Leader: From Religious Family to Reins of U.F.O. Cult" (March 29, 1997); Goldberg, Carey, "The Compound: Heaven's Gate Fit In With New Mexico's Offbeat Style" (March 31, 1997); Ayres, B. Drummond, "Cult Members Wrote a Script to Put Their Life and Times on the Big Screen" (April 1, 1997); Purdum, Todd, S. "Last 2 Names Released in Mass Suicide of Cult Members" (April 1, 1997); Brooke, James, "Former Cultists Tell of Believers Now Adrift" (April 2, 1997); Bearak, Barry, "Eyes on Glory: Pied Pipers of Heaven's Gate" (April 28, 1997); and Purdum, Todd S., "Ex-Cultist Kills Himself, and 2nd Is Hospitalized" (May 7, 1997).
59. Steinberg, Jacques, "The Leader: From Religious Family to Reins of U.F.O. Cult," *New York Times* (March 29, 1997).
60. Niebuhr, Gustav, "On the Furthest Fringes of Millennialism," *New York Times* (March 28, 1997).
61. Heaven's Gate, "Our Position Against Suicide," reprinted as "Looking Forward to Trip Going to the Next Level," *New York Times* (March 28, 1997).
62. Lifton, Robert Jay, *Thought Reform and the Psychology of Totalism: A Study of "Brainwashing" in China* (New York: W.W.Norton, 1961).
63. This and much of the discussion on cults that follows draws heavily from Conway, Flo and Siegelmen, Jim, *Snapping:America's Epidemic of Sudden Personality Change* (New York: Dell Publishing, 1979).
64. Conway and Siegelman, op. cit., p. 225.
65. Ibid., pp. 22 and 27.
66. On October 30, 1980, and again on November 6, 1980, ABC-TV News aired a two-part story focused on Lifespring on *20/20.* The discussion that follows draws heavily from both parts of that program.
67. Ibid., October 30, 1980, transcript, p. 15.
68. Ibid., transcript, pp. 9 and 6, respectively.
69. Ibid., transcript, pp. 16-17.
70. Ibid., November 6, 1980, transcript, pp. 14-15.
71. Ibid., transcript, p. 16.
72. Ibid.
73. Poe, James, *The Bedford Incident,* (based on the novel by Mark Rascovich), produced by James B. Harris and Richard Widmark (Columbia Pictures: Bedford Productions Limited, 1965).

CHAPTER NINE

1. Suppose Machine A has three key parts and all of them must work right for the machine to do its job. For simplicity, assume the probability of failure of any part is independent of the failure of any other part. If each part is 95 percent reliable (that is, has only a 5 percent chance of failure), Machine A will

be 86 percent reliable (95 percent x 95 percent x 95 percent)—it will have a 14 percent chance of failure. Now suppose we change the design so that it now has five key parts, each still 95 percent reliable. Even though every part is just as reliable as before, the new Machine A would now be only 77 percent reliable (95 percent x 95 percent x 95 percent x 95 percent x 95 percent)—its probability of failure would *increase* from 14 percent to 23 percent. The added complexity has caused the machine to become less reliable.

2. Suppose Machine A is redesigned. Machine B is much more complex, having 20 key parts. Assume each part must still work properly for the machine to work. Even if each part of the new machine is only 1/5 as likely to fail as before (that is, 99 percent reliable), the machine as a whole will still be less reliable. The more complex Machine B has an 18 percent chance of failure (82 percent reliability) compared to the 14 percent chance of failure (86 percent reliability) of the original, simpler Machine A. Even though each part of the original machine was *less* reliable, its simpler design made the whole machine *more* reliable.
3. Suppose Machine C has three parts, each 95 percent reliable. Unlike Machine A, it has two failure modes: if one part fails, the machine's performance degrades, but it still keeps working; if two or three parts fail, the machine stops working. Machine C might be an electrical generator designed for hospital use so it can still provide enough power for minimal lighting, key life-support equipment and other critical functions, even though one part fails. But if more than one part fails, the generator stops working. If the probability of failure of any part does not influence the probability of failure of any other part, there will be a 13.5 percent chance that Machine C will havea partial failure, and less than a 1 percent chance that it will fail completely.

   Suppose Machine D is just like C, except that the failure of one part results in a much higher strain on the remaining parts, reducing their reliability. This might result from designing the generator to provide a higher-than-emergency level of power when one part fails by having the others bear a greater load. Say that as soon as any part fails, the reliability of the remaining parts drops from 95 percent to 75 percent because of the increased load. There will still be a 13.5 percent chance of partial failure, but the chance of complete failure will soar from less than 1 percent to 6 percent.
4. Broad, William J., "Fragmenting Space Debris Could Put Satellites at Risk," *New York Times* (May 17, 1994).
5. Peterson, Ivars, "A Digital Matter of Life and Death," *Science News* (March 12, 1988), p. 171.
6. Spinney, Franklin C., *Defense Facts of Life,* (Washington, D.C.: December 5, 1980), unpublished Department of Defense staff paper, unreviewed by the Department and therefore not an official document.
7. Wilford, John N., "Air Control Technology Refined to Meet Hazards," *New York Times* (January 2[illegible], 1980).
8. Sims, Calvin, "Disruption of Phone Service Is Laid to Computer Program," *New York Times* (January 17, 1990).
9. Ibid.
10. Markoff, John, "Superhuman Failure: AT&T's Trouble Shows Computers Defy Understanding Even in Collapse," *New York Times* (January 17, 1990).
11. For an interesting if somewhat overlong discussion of these so-called "revenge effects" of technology see Tenner, Edward, *Why Things Bite Back* (New York: Vintage Books, 1997).
12. Markoff, op.cit.
13. Ibid.
14. Ibid.
15. Perrow, Charles, *Normal Accidents: Living with High-Risk Technologies* (New York: Basic Books, 1984), p. 83.
16. Waldrop, M. Mitchell, "Hubble Managers Start to Survey the Damage," *Science* (July 6, 1990), and "Astronomers Survey Hubble Damage," *Science* (July 13, 1990).
17. Cowen, Ron, "The Big Fix: NASA Attempts to Repair the Hubble Space Telescope," *Science News* (November 6, 1993), pp. 296-298.
18. Cowen, Ron, "Hubble Finally Gets a Heavenly View," *Science News* (January 22, 1994), p. 52.
19. Cowen, Ron, "Trying to Avoid Hubble Trouble," *Science News* (March 27, 1999), p. 203.
20. Petroski, Henry, *To Engineer Is Human: The Role of Failure in Successful Design* (New York: St. Martin's Press, 1985), pp. 176-179.
21. Randell, B., Lee, P. A. and Treleaven, P. C., "Reliability Issues in Computing System Design," Association for Computing Machinery, *Computing Surveys* 10 (no. 2, June 1978), p. 135. In the case of crucial decisions with great consequences, there are two ways to strengthen TMR. One can require that all three modules agree in order for the system to take action, or the modules can be designed to

receive inputs from different, isolated systems. Unfortunately, insisting on unanimity not only destroys fault tolerance, it also biases the system against reacting. Requiring the modules to agree while receiving inputs from different sources reduces the likelihood of failure through improper action, but may increase the likelihood of failure through inaction.

22. For example, suppose Machine E has two key parts, each of which is 95 percent reliable. Assume that the probability of failure of either part does not influence the probability of failure of the other. If both parts must work for the machine to work, Machine E will then be 90 percent reliable (95 percent x 95 percent)—much less reliable than either of its parts. But, if it were designed with a third 95 percent reliable part which could serve as a backup system for either of the other two, Machine E would be 99 percent reliable—much more reliable than any of its parts.
23. Wooten, James T., "Sound of Debate Is Off Air for 27 Minutes," *New York Times* (September 24, 1976).
24. Diamond, Stuart, "The Bhopal Disaster: How It Happened," *New York Times* (January 28,1985).
25. Perrow, op. cit., p. 45.
26. The airline later reported that only two of the three inertial navigation systems had failed, but the crew could not determine which of the devices was working properly. Weiner, Eric, "Jetliner, in Flight to Tokyo, Lands in Alaska After a 600-Mile Error," *New York Times* (December 23, 1989).
27. Perrow, op. cit., p. 260.
28. Ford, Daniel, "Three Mile Island: II—The Paper Trail," *The New Yorker* (April 13, 1981), pp. 52-53.
29. *New York Times* (September 26, 1981).
30. According to John Galipault, president of the Aviation Safety Institute, as quoted in Barron, James, "Tail Fan May Have Come Apart, Crippling DC-10," *New York Times*, (July 21, 1989).
31. Weiner, Eric, "DC-10 Jets to Get Hydraulic Device," *New York Times* (September 16, 1989).
32. See Hanley, Robert, "Newark Airport Is Closed as Crew Cuts Power Lines" and "Blackout at Airport Shows Need for a Backup System," *New York Times* (January 10 and 11, 1995, respectively).
33. Waldrop, M. Mitchell, "Computers Amplify Black Monday," *Science* (October 30, 1987), p. 604.
34. Weiner, Tim, "B-2, After 14 Years, Is Still Failing Basic Tests," *New York Times* (July 15, 1995).
35. Shenon, Philip, "B-2 Gets a Bath To Prove That It 'Does Not Melt,'" *New York Times* (September 13, 1997).
36. Clark, Christopher, "B-2 Bomber Makes Combat Debut," WashingtonPost.com (March 25, 1999: 2:39 A.M. EST).
37. Wilford, John N., "NASA Considered Shuttle Boosters Immune to Failure," *New York Times* (Febraury 3, 1986).
38. Shcherbak, Yuri M., "Ten Years of the Chornobyl Era," *Scientific American* (April 1996), p. 45.
39. Wilford, John N., "Space Shuttle Is Grounded By Lovesick Woodpeckers," *New York Times* (June 3, 1995).
40. Bishop, Katherine, "Experts Ask If California Sowed Seeds of Road Collapse in Quake," *New York Times* (October 21, 1990).
41. Weiner, Eric, "Jet Lands After an Engine Drops Off," *New York Times* (January 5, 1990).
42. Petroski, op. cit., pp. 85-90.
43. Ibid., p. 197.
44. Waldrop, op. cit.,1990.
45. Eberhart, J., "Solving Hubble's Double Trouble," *Science News* (July 4, 1990).
46. Petroski, op. cit., p. 198-199.
47. Rosenthal, Andrew, "Design Flaw Seen as Failure Cause in Trident II Tests," *New York Times* (August 17, 1989).
48. Petroski, op. cit., p. 179.
49. Perrow, op. cit., p. 34.
50. Eisman, Dale, "Super Hornet Critics Charge that Navy Hid Flaws to Get Funding," *The Virginian-Pilot* (Norfolk, Virginia) (February 2, 1998).
51. Petroski, op. cit., pp. 94-95.
52. Pollack, Andrew, "Japan Quake Toll Moves Past 4,000, Highest Since 1923," *New York Times* (January 20, 1995).
53. Blakeslee, Sandra, "Brute Strength Couldn't Save Kobe Structures," *New York Times* (January 25, 1995).
54. Browne, Malcolm W., "Doomed Highway May Have Pulsed to the Rhythm of the Deadly Quake," *New York Times* (October 23, 1989).
55. "Investigators Agree N.Y. Blackout of 1977 Could Have Been Avoided," *Science* (September 15, 1978).

56. Stevens, William K., "Eastern Quakes: Real Risks, Few Precautions," *New York Times* (October [illegible] 1989).
57. Hancock, Lee, "Chances Are 50-50 for Major Quake by Decade's End," *Dallas Morning News* (July 22, 1990).
58. Ibid.
59. Stevens, op. cit.
60. Goldberger, Paul, "Why the Skyscrapers Just Swayed," *New York Times* (October 19, 1989).
61. Albright, David, Paine, Christopher and von Hippel, Frank, "The Danger of Military Reactors," *Bulletin of the Atomic Scientists* (October 1986), p. 44.
62. Fuller, John G., *We Almost Lost Detroit* (New York: Reader's Digest Books, 1975), pp. 102 and 21[illegible]-220.
63. Perrow, op. cit., p. 36.
64. Ibid., p. 37.
65. Shcherbak, op. cit., p. 48.
66. Wartzman, Rick and Pasztor, Andy, "Doubts Are Raised About the Reliability of the Cruise Missile," *Wall Street Journal* (July 27, 1990.
67. Ibid.
68. Waldrop, M. Mitchell, "Hubble: the Case of the Single-Point Failure," *Science* (August 17, 1990), p. 735.
69. Ibid., p. 736.
70. Smith, R. Jeffrey, "Pentagon Hit by New Microchip Troubles," *Science* (November 23, 1984).
71. Sanger, David E., "Chip Testing Problems Abound, Pentagon Says," *New York Times* (April 16, 1985)
72. Hart, Gary and Goldwater, Barry, "Recent False Alerts from the Nation's Missile Attack Warning System," Report to the Committee on Armed Services, United States Senate (October 9, 1980).
73. "Pentium Flaw Has Some Scientists Steamed," *Wall Street Journal* (November 25, 1994),
74. For example, if X is divided by Y, then the result is multiplied by Y, the answer should again be X. If this answer is then subtracted from X, the result should be zero. The particular values of X and Y used do not matter. But performing this sequence of operations with the flawed Intel Pentium when X = 4195835.0 and Y = 3145727.0 gives an answer of 256.
75. Rosenthal, Andrew, "Defects in $12 Circuit Board Stall Deployment of New Fighter Missile," *New York Times* (September 15, 1989).
76. Cushman, John Jr., "Findings Suggest Jet's Flaw Was Visible Before Crash," *New York Times* (November 1, 1989).
77. Cushman, John Jr., "Metallurgical Mystery in Crash that Killed 112," *New York Times* (November 3, 1989).
78. "Built to Break," ABC Television News, *20/20* #917, (April 28, 1989).
79. Ibid.
80. Ibid.
81. Broad, William J., "Major Flaw Found in Space Station Planned by NASA," *New York Times* (March 19, 1990). See also Broad, William J., "NASA Is Faulted Over Space Station," *New York Times* (March 21, 1990).
82. "Space Base Heads Back to Drawing Board," *Science News* (July 28 1990), p. 53.
83. Broad, op. cit., March 21, 1990.
84. Broad, op. cit., March 19,1990.
85. Gordon, Michael R., "Russian Space Station Damaged in Collision With a Cargo Vessel," *New York Times* (June 26, 1997). See also in the *New York Times:* Specter, Michael, "Mir Computer Failure Sends Space Station Out of Control" (August 19, 1997); Gordon, Michael R., "Mir Shadow Falls on Russian Role in Space" (August 2, 1997) and "Russian and American Astronauts Start Hazardous Space Walk to Inspect Mir Damage" (September 6, 1997).
86. Nather, David, "Safety Issues Plague Aging Airline Fleets," *Dallas Morning News* (July 22, 1990).
87. Ibid.
88. Wald, Matthew L., "Agency Grounds Scores of 737's to Check Wiring," *New York Times* (May 11, 1998).
89. Wald, Matthew L., "Checks of 737's Show More Damaged Wiring," *New York Times* (May 12, 1998).
90. Petroski, op. cit., pp. 95-96.
91. Nather, David, "Safety Issues Plague Aging Airline Fleets," *Dallas Morning News* (July 22, 1990).
92. Marshall, Eliot, "The Salem Case: A Failure of Nuclear Logic," *Science* (April 15, 1983), pp. 280-281.
93. Ibid., p. 281.

94. Pollard, Robert, "Showing their Age," *Nucleus* (Union of Concerned Scientists, Summer 1995), p. 7. Pollard is a senior nuclear safety engineer.
95. Utroska, Daniel, "Holes in the U.S. Nuclear Safety Net," *Bulletin of the Atomic Scientists* (July-August 1987), p. 40.
96. Spinney, op. cit., pp. 46-48.
97. Ibid.

CHAPTER TEN

1. Associated Press, "Pilot's Wrong Keystroke Led to Crash, Airline Says," *New York Times* (August 24, 1996).
2. See, for example, Ornstein, S. M., "Deadly Bloopers," unpublished paper (June 16, 1986), p. 5.
3. Ibid., p. 7.
4. Salpukas, A., "Computer Chaos for Air Travelers," *New York Times* (May 13, 1989).
5. Broad, William J., "New Computer Failure Imperils U.S. Shuttle Astronomy Mission," *New York Times* (December 9, 1990).
6. Clark, D., "Some Scientists Are Angry Over Flaw in Pentium Chip, and Intel's Response," *Wall Street Journal* (November 25, 1994).
7. Communication to the author from an Intel employee in the fall of 1997.
8. Gilpin, K.N., "Stray Rodent Halts NASDAQ Computers," *New York Times* (December 10, 1988).
9. Ibid.
10. Ornstein, op. cit., p. 12.
11. Heath, James R., Keukes, Philip J., Snider, Gregory S. and Williams, R. Stanley, "A Defect-Tolerant Computer Architecture: Opportunities for Nanotechnology," *Science* (June 12, 1998), p. 1716.
12. For further discussion of TMR in this context, see Randell, B., Lee, P. A. and Treleaven, P. C., "Reliability Issues in Computing System Design," Association for Computing Machinery, *Computing Surveys* 10 (no. 2, June 1978), p. 129.
13. Ornstein, op. cit., pp. 9-10.
14. Waldrop, op. cit., March 23, 1984, p. 1280.
15. Ornstein, op. cit., p. 10.
16. Peterson, I., "Phone Glitches and Other Computer Faults," *Science News* (July 6, 1991).
17. Broder, John M. and Zuckerman, Laurence, "Computers Are the Future But Remain Unready for It," *New York Times* (April 7, 1997).
18. Peterson, Ivar, "Year-2000 Chip Danger Looms Large," *Science News* (January 2, 1999), p. 4.
19. Ibid. See also General Accounting Office, Accounting and Information Management Division, *Year 2000 Computing Crisis: An Assessment Guide* (February 1997).
20. Parnas, D.L., "Software Aspects of Strategic Defense Systems," *American Scientist* (September-October 1985), pp. 433 and 436.
21. Ornstein, op. cit., p. 10.
22. Brooks, op. cit., p. 121.
23. Ibid., chapter 11, footnote 5.
24. Ibid, p. 122.
25. Parnas, op. cit., p. 433.
26. Ornstein, op. cit., p. 11.
27. See, for example, "Software for Reliable Networks," *Scientific American* (May 1996).
28. Glanz, James, "Chain of Errors Hauled Probe into Spin," *Science News* (July 24, 1998), p. 449. SOHO is an acronym for Solar and Heliospheric Observatory.
29. Waldrop, M.M., "The Necessity of Knowledge," *Science* (March 23, 1984), p. 1280.
30. In 1927, Werner Heisenberg stated the "uncertainty principle," which holds that it is impossible to specify simultaneously with infinite precision both the linear momentum and the corresponding position of a subatomic particle or photon (a "packet" of energy). The effect of the principle is to change the interpretation of some of the laws of physics from statements of absolute certainty to statements of relative probabilities. That there is some inherent inaccuracy, some essential "unknowability" at the root of the physical universe, has interesting and profound philosophical implications.
31. Peterson, Ivars, "The Soul of a Chess Machine," *Science News* (March 30, 1996), p. 201.

32. Pollack, A., "Pentagon Sought Smart Truck But Found Something Else," *New York Times* (May 30, 1989).
33. Ibid.
34. The best and most comprehensive exposition I have seen of the distinction between what computers do and what the human mind does when it thinks is Theodore Roszak, *The Cult of Information: A Neo-Luddite Treatise on High-Tech, Artificial Intelligence, and the True Art of Thinking* (Berkeley: University of California Press, 1994).
35. In 1996, a computer program "designed to reason" rather than solve a particular problem developed "a major mathematical proof that would have been called creative if a human thought of it". The feat accomplished by the researchers at the Argonne National Laboratories that wrote the program is impressive and interesting, but is very far from proving that the functioning of the human mind can be effectively duplicated by electronic means. See Kolata, Gina, "With Major Math Proof, Brute Computers Show Flash of Reasoning Power," *New York Times* (December 10, 1996).
36. Ornstein, op. cit., p. 38.
37. Parnas, op. cit., p. 438.
38. Cohen, F., "Computer Viruses: Theory and Experiments," *Computers and Security* (February 1987), p. 24.
39. Ibid., p. 29.
40. Markoff, John, "A New Method of Internet Sabotage Is Spreading," *New York Times* (September 19, 1996).
41. Elmer-De-Witt, P. , "Invasion of the Data Snatchers," *Time,* September 26, 1988, p. 67.
42. Marshall, E., "The Scourge of Computer Viruses," *Science,* April 8,1988, p. 133.
43. Elmer-De-Witt, op. cit., pp. 65-66.
44. Dewdney, A.K., "Computer Recreations: In the Game called Core War Hostile Programs Engage in a Battle of Bits," *Scientific American* (May 1984), p. 14.
45. Ibid., p. 18.
46. Cohen, op. cit., p. 31.
47. Markoff, J., "Top Secret, and Vulnerable," *New York Times* (September 25, 1988).
48. Elmer-De-Witt, op. cit., p. 62.
49. The author has not attempted to compile a comprehensive list. However, the instances described in the text are intended to illustrate a variety of different types and sources of attack. In addition to these, there were reported attacks on the National Aeronautics and Space Administration's semipublic "Space Physics Analysis Network" by "hackers" belonging to a group called the Hamburg Chaos Computer Club in West Germany (Highland, H.J., "Case History of A Virus Attack," *Computers & Security,* February 1988,p. 3); on Apple computers at Dallas-based EDS corporation, Boeing, ARCO, NASA, the Internal Revenue Service and the U.S. House of Representatives by a malicious virus called Scores believed to have been written by a disgruntled Apple employee (Elmer-De-Witt, op. cit., pp. 63-64); and on Amiga microcomputers produced by Commodore Corporation by a malicious virus somewhat similar to Scores (Highland, H.J., "Computer Viruses: A Post Mortem," *Computers and Security,* April 1988, p. 120).
50. Higher-security military communications were split off from Arpanet into a second network called Milnet in 1983.
51. Markoff, J., "'Virus' in Military Computers Disrupts Systems Nationwide," *New York Times* (November 4, 1988).
52. Shoch, J.F. and Hupp, J.A., "The 'Worm' Programs—Early Experience with a Distributed Computation," *Communications of the ACM* 25 (no. 3, March 1982), p. 172.
53. Markoff, J., "Invasion of Computer: 'Back Door' Left Ajar," *New York Times* (November 4, 1988).
54. 54 Holden, C., "The Worm's Aftermath," *Science* (November 25, 1988), pp. 1121-1122.
55. Markoff, J., op. cit.
56. Markoff, J., "'Virus' in Military Computers Disrupts System Nationwide," *New York Times* (November 4, 1988).
57. Elmer-De-Witt, op. cit., p. 65. During the mid to late 1990s, hoax virus messages were repeatedly spread widely over the Internet. They warned users that if they opened certain e-mail messages their computers would become instantly infected. One such hoax involved a message headed AOL4FREE.COM, another, Good Times. In order for a virus to infect a computer, the machine must load an executable program. Reading an e-mail message alone does not load a program, although opening an e-mail attachment can.
58. Markoff, John, "Computer System Intruder Plucks Passwords and Avoids Detection," *New York Times* (March 19,1990).

59. Markoff, John, "Data Network Is Found Open to New Threat," *New York Times* (January 23, 1995).
60. Markoff, John, "New Netscape Software Flaw Is Discovered," *New York Times* (May 18, 1996).
61. Lohr, Steve, "A Virus Got You Down? Who You Gonna Call?" *New York Times* (August 12, 1996).
62. Cohen, F., "On the Implications of Computer Viruses and Methods of Defense," *Computers and Security* (April 1988), p. 167.
63. Elmer-De-Witt, op. cit., p. 67.
64. Davis, F.G.F., and Gantenbein, R.E., "Recovering from a Virus Attack," *Journal of Systems and Software* (no. 7, 1987), pp. 255-256.
65. Glath, R.M., "A Practical Guide to Curing a Virus," *Texas Computing* (November 11, 1988), p. 14. See also Davis and Gantenbein, op. cit.; and Gibson, S., "Tech Talk: What Were Simple Viruses May Fast Become a Plague," *Infoworld* (May 2,1988).
66. Cohen, op. cit., February 1987, p. 28.
67. Marshall, E., "The Scourge of Computer Viruses," *Science* (April 8, 1988), p. 134.
68. Cohen, op. cit., February 1987, p. 30.
69. Davis and Gantenbein, op. cit., p. 254.
70. Ibid., p. 256.
71. Cohen, op. cit., April 1988, p. 168.
72. Ibid., p. 168.
73. Gibson, S., "Tech Talk: Effective and Inexpensive Methods for Controlling Software Viruses," *Infoworld* (May 9, 1988), p. 51.
74. "EPA Gets Computer Virus," *News and Observer* (Raleigh, North Carolina) (August 6, 1988).
75. For an interesting nontechnical discussion of how this type of security works, see "Special Report: Computer Security and the Internet," *Scientific American* (October 1998), pp. 95-115.
76. Weiss, P., "Lock-on-a-Chip May Close Hackers Out," *Science News* (November 14, 1998), p. 309.
77. Lewis, Peter H., "Threat to Corporate Computers Is Often the Enemy Within," *New York Times* (March 2, 1998).
78. "Could a Virus Infect Military Computers?" *U.S. News & World Report* (November 14, 1988), p. 13.
79. Markoff, John, "Secure Digital Transactions Just Got a Little Less Secure," *New York Times* (November 11, 1995).
80. Peterson, Ivar, "Power Cracking of Cash Card Codes," *Science News* (June 20, 1998), p. 388; see also Wayner, Peter, "Code Breaker Cracks Smart Cards' Digital Safe," *New York Times* (June 22, 1998).
81. Markoff, John, "Researchers Crack Code in Cell Phones," *New York Times* (April 14, 1998).
82. "'Hackers' Score a New Pentagon Hit," *U.S. News & World Report* (July 29, 1985), p. 7.
83. Ford, Daniel, *The Button: America's Nuclear Warning System—Does It Work?* (New York: Simon and Shuster, 1985), p. 79.
84. Ibid.
85. Easterbrook, G., "Divad," *Atlantic Monthly* (October 1982), p. 37.
86. Ibid., p. 34.
87. Ibid.
88. Dumas, L.J., "The Economics of Warfare," in Barnaby, F., editor, *Future War: Armed Conflict in the Next Decade* (London: Michael Joseph, 1984), pp. 133-134.
89. "Simulated Mobilization for War Produces Major Problems," *New York Times* (December 20, 1980).
90. Ibid.
91. Doherty, R., "Shuttle Security Lapse," *Electronic Engineering Times* (June 6, 1988)
92. Private communication with an informed source at IBM. Fred Cohen has argued that this program was not technically a virus (in Cohen, op. cit., April 1988, p. 170).
93. Wines, M., "Some Point Out Chinks in US Computer Armor," *New York Times* (November 6, 1988), p. 30.
94. Sandza, R., "Spying Through Computers: The Defense Department's Computer System Is Vulnerable," *Newsweek* (June 10, 1985), p. 39.
95. General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks,* (Washington, D.C.: May 1996), pp. 2-4.
96. Shenon, Philip, "Defense Dept. Computers Face a Hacker Threat, Report Says," *New York Times* (May 23, 1996).
97. Markoff, J., "'Virus' in Military Computers Disrupts Systems Nationwide," *New York Times* (November 4, 1988).
98. The Brain, Lehigh, Flu-Shot 4, Hebrew University and Fort Worth viruses all destroyed data in the systems they infected. For descriptions of these viruses, see Elmer-De-Witt, op. cit.; and Highland, H.J., "Computer Viruses: A Post Mortem," *Computers and Security* (April 1988).

99. "'Hackers' Score a New Pentagon Hit," op. cit., p. 7.
100. Elmer-De-Witt, P. , "A Bold Raid on Computer Security," *Time,* (May 2, 1988), p. 58.
101. Wines, op. cit., p. 30.
102. Cohen, op. cit., February 1987, p. 23.

CHAPTER ELEVEN

1. The likelihood of any event is mathematically measured by its "probability," expressed as a number ranging from zero (the event is impossible) to one (the event is certain). This can be thought of as reflecting the fraction of trials of repeated performance of the chance experience that result in that particular outcome. For example, the probability of randomly drawing a king from an ordinary deck of 52 playing cards is .077. This may be interpreted as meaning that if the random drawing of a card (with replacement after each draw) were repeated, a king would be drawn about 77 times for every 1,000 draws.
2. Contingency theorists of organizational structure see the desire to reduce or eliminate risk as a driving force in determining the shape and behavior of formal organizations. See Tausky, C., *Work Organizations: Major Theoretical Perspectives* (Itaska, Illinois: Peacock Publishers, 2nd edition, 1980), pp. 61 and 64-82. Experts in child development admonish parents not to keep changing the rules they expect their children to follow because of the anxiety and confusion generated by the unpredictability that constantly changing rules create. See Hetherington, E.M. and Parke, R.D., *Child Psychology: A Contemporary Viewpoint* (New York: McGraw-Hill, Second Edition, 1979), pp. 434-436.
3. Fromm, E., "Paranoia and Policy," *New York Times* (December 11, 1975).
4. In 1939, B.F. Skinner analyzed the question of whether or not Shakespeare intentionally used alliteration in his sonnets. He compared the frequency with which certain sounds appear in the English language with the frequency with which they are repeated in a given line of the sonnets. His conclusion was that, although Shakespeare may have used alliteration purposefully, chance was capable of explaining the observed degree of alliteration all by itself. "So far as this aspect of poetry is concerned, Shakespeare might as well have drawn his words out of a hat". See Skinner, B. F., "The Alliteration in Shakespeare's Sonnets: A Study in Literary Behavior," *The Psychological Record* 3 (no. 15), p. 191.
5. McElheny, V.K., "Improbable Strikes by Lightning Tripped Its System, Con Ed Says," *New York Times* (July 15, 1977). See also Sullivan, W., "Con Ed Delay Cited As A Possible Cause," *New York Times* (July 16, 1977).
6. "Investigators Agree New York Blackout of 1977 Could Have been Avoided," *Science* (September 15, 1978), pp. 994-996.
7. McFadden, R.D., "'Disaster Status Given New York and Westchester to Speed Loans; Services Resume After Blackout," *New York Times,* (July 16, 1977).
8. Tomasson, R.E.,"Meteorite Crashes Into House in Connecticut," *New York Times* (November 10, 1982).
9. Ibid. See also, Clarke, R.S., Jarosewich, E. and Noonan, A.F., "Preliminary Data on Eight Observed-Fall Chondritic Meteorites," in G.S. Switzer, editor, *Smithsonian: Contributions to the Earth Sciences* (no. 14, 1975), p. 69.
10. *International Herald Tribune* (October 31, 1968).
11. Anderson, D., "Four! A Hole-In-One Record at Open," *New York Times* (June 17, 1989).
12. "Doctors Say Gun Wound to Brain Eliminated A Man's Mental Illness," *New York Times* (February 25, 1988).
13. McFadden, R.D., "Odds-Defying Jersey Woman Hits Lottery Jackpot 2nd Time," *New York Times* (February 14, 1986).
14. Boffey, P. M., "Fifth US Rocket Failure Is Acknowledged by NASA," *New York Times* (May 10, 1986).
15. As noted in Chapter 4, *Challenger's* next scheduled mission was to be on May 16, when it was due to carry a Centaur rocket in its cargo bay, topped by a satellite powered by plutonium. The Department of Energy (DoE) has been investigating "deep space disposal . . . for concentrated separated fission products from nuclear waste" at least since the late 1970s. Any economically feasible approach to space disposal would have to involve much larger quantities of highly toxic nuclear waste per launch than are likely to have been on the *Challenger's* next payload. How was the waste to be reliably lofted into space? According to DoE, "*NASA's space shuttle* could be used to lift the concentrated waste package" (emphasis added). See Cary, P. , "Challenger Was to Carry Plutonium Next," *Miami Herald* (March

6, 1986); and "Can Nuclear Wastes Be Launched into Space?" a one-page flyer issued by the Office of Nuclear Waste Isolation, Department of Energy (505 King Ave, Columbus, Ohio 43201). For further information, see also "Draft Environmental Impact Statement, Management of Commercially Generated Radioactive Waste," U.S. Department of Energy (Washington: April 1979), vol.1.

16. Manfredi, A.F. and DiMaggio, C., "Effect of U.S. Space Launch Vehicle Problems on the SDI Decision Timeline" (Washington, D.C.: Congressional Research Service, 86-783 SPR, July 17, 1986), p. 1.
17. Boffey, op. cit.
18. Manfredi and Di Maggio, op. cit., p. 1.
19. "Navy Accidents: What Has Gone Wrong," *New York Times* (November 15, 1989), p. 15.
20. Associated Press, "Hospital Fumes That Hurt 6 Are Tied to Nerve Gas," *New York Times* (November 5, 1994).
21. Diaconis, P. and Mosteller, F., "Methods for Studying Coincidences," *Journal of the American Statistical Association* (December 1989), p. 859.
22. Ibid.
23. Ibid.
24. Ibid., p. 858. Diaconis and Mosteller give a formula for calculating the approximate number of people (N) that need to be in the room to have a 50-50 chance that at least two of them will have a birthday within k days of each other:

    $N = 1.2\,[365/(2k+1)]^{1/2}$
25. Morgan, K.Z., "Radiation-Induced Health Effects," letter to *Science* (January 28, 1977), p. 346.
26. Perrow, C., *Normal Accidents* (New York: Basic Books, 1984), pp. 137-9. See also National Transportation Safety Board, document AAR-82-3, April 6, 1982, pp. 14-17.
27. Lipkin, R., "Risky Business of Assessing Danger—Part I," *Insight* (May 23, 1988), p. 12.
28. Fischhoff, B., Slovic, P. and Lichtenstein, S., "Fault Trees: Sensitivity of Estimated Failure Probabilities to Problem Representation," *Journal of Experimental Psychology: Human Perception and Performance* 4 (no. 2, 1978), pp. 330-344.
29. Ibid., p. 334.
30. Ibid., p. 335.
31. Ibid., p. 340.
32. Ibid., p. 342.
33. Clarke., L., "The Origins of Nuclear Power: A Case of Institutional Conflict," *Social Problems* 32 (1985), pp. 474-487.
34. Clarke, L., "Politics and Bias in Risk Assessment," *Social Science Journal* 25 (no. 2, 1988), pp. 158-159.
35. Ibid., p. 159. See also Primack, J., "Nuclear Reactor Safety: An Introduction to the Issues," *Bulletin of the Atomic Scientists* (September 1975), p. 16.
36. U.S. Atomic Energy Commission, *Reactor Safety Study: An Assessment of Accident Risks in United States Commercial Nuclear Power Plants* (Washington, D.C.: U.S. Nuclear Regulatory Commission, 1975); Ford, D.F., "A Reporter at Large: The Cult of the Atom—Part II," *New Yorker* (November 1, 1982), p. 58.
37. Clarke, op. cit., 1988, p. 159.
38. Slovic, P. , Fischhoff, B. and Lichtenstein, S., "Facts and Fears: Understanding Perceived Risk," in Schwing, R.C. and Albers, W.A. editors, *Societal Risk Assessment: How Safe Is Enough?* (New York: Plenum Press, 1980), p. 195.
39. Slovic, P. , "Perceptions of Risk," *Science* (April 17, 1987), p. 283.
40. Ibid., p. 281.
41. Ibid.
42. Plous, S., "Biases in the Assimilation of Technological Breakdowns: Do Accidents Make Us Safer?" *Journal of Applied Social Psychology* (1991, 21, 13), p. 1058.
43. Weatherwax, R.K., "Virtues and Limitations of Risk Analysis," *Bulletin of the Atomic Scientists* (September 1975), p. 31.
44. Fischhoff, B., "Cost Benefit Analysis and the Art of Motorcycle Maintenance," *Policy Sciences* (no. 8, 1977), pp. 181-183.
45. National Research Council, National Academy of Sciences, *Long-Term Worldwide Effects of Multiple Nuclear-Weapons Detonations* (Washington, D.C.: National Academy of Sciences, 1975).
46. Slovic, Fischhoff and Lichtenstein, op. cit., 1980, p. 185.
47. Fischhoff, B., Slovic, P. , and Lichtenstein, S., "Knowing with Certainty: The Appropriateness of Extreme Confidence," *Journal of Experimental Psychology: Human Perception and Performance* 3 (no. 4, 1977), p. 555.

48. Ibid., p. 557.
49. Ibid., p. 558.
50. Ibid., p. 554 and 561.
51. Slovic, Fischhoff and Lichtenstein, 1980, op. cit., p. 187.
52. Lichtenstein, S., Fischhoff, B., and Phillips, L.D., "Calibration of Probabilities: the State of the Art to 1980," in Kahneman, D., Slovic, P. and Tversky, A., editors, *Judgement Under Uncertainty: Heuristics and Biases* (Cambridge: Cambridge University Press, 1982), pp. 315-318.
53. Hynes, M. and Vanmarcke, E., "Reliability of Embankment Performance Predictions," *Proceedings of the ASCE Engineering Mechanics Division Specialty Conference* (Waterloo, Ontario: University of Waterloo Press, 1976), pp. 31-33.
54. Slovic, Fischhoff and Lichtenstein, op. cit., 1980, p. 187.
55. Ibid., p. 185.
56. Lichtenstein, Fischhoff and Phillips, op. cit., p. 333. See also Plous, S., "Thinking the Unthinkable: The Effects of Anchoring on Likelihood Estimates of Nuclear War," *Journal of Applied Social Psychology* (1989, 19, 1), pp. 67-91.
57. Ibid.
58. Slovic, Fischhoff and Lichtenstein, op. cit., 1980, p. 188.
59. Bazelon, D.L., "Risk and Responsibility," *Science* (July 20, 1979), p. 279.

CHAPTER TWELVE

1. Canberra Commission, *Report on the Elimination of Nuclear Weapons,* p. 2. At this writing, the full report is only generally available on the World Wide Web at the address: http//www.dfat.gov.au/dfat/cc/cchome.html.
2. Ibid., pp. 2 and 1.
3. Diamond, J., "Air Force General Calls for End to Atomic Arms," *Boston Globe* (July 16, 1994), as cited in Forrow, Lachlan and Sidel, Victor W., "Medicine and Nuclear War," *Journal of the American Medical Association* (August 5, 1998), p. 459.
4. ECAAR Newsletter, volume 9, nos.1 and 2 (May-June 1996), p. 4.
5. Butler, Lee, "A Voice of Reason," *Bulletin of the Atomic Scientists* (May-June 1998), pp. 59 and 61.
6. Epstein, William, *The Last Chance: Nuclear Proliferation and Arms Control* (New York: The Free Press, 1976), appendix 4, p. 319.
7. Weiner, Tim, "Iraq Spies on UN So It Can Predict Arms Inspections," *New York Times* (November 25, 1997).
8. Office of Technology Assessment, Congress of the United States, *Environmental Monitoring for Nuclear Safeguards* (Washington, D.C.: U.S. Government Printing Office, September 1995), pp. 1 and 5-6.
9. Skindrud, E., "Bomb Testers Beware: Trace Gases Linger," *Science News* (August 10, 1996).
10. Annan, Kofi, "The Unpaid Bill That's Crippling the UN," *New York Times* (March 9, 1998).
11. Because biological and chemical weapons of mass destruction are much simpler, cheaper and easier to create, it is harder to achieve this degree of assurance with them than it is with nuclear weapons. But at least in the case of prohibiting the buildup of national arsenals, there is no reason to believe it cannot be done. Terrorist manufacture of one or a few of these weapons, on the other hand, is much harder to prevent.
12. One of the more interesting and potentially effective proposals for verifying disarmament is "inspection by the people," developed by Seymour Melman and his colleagues more than 40 years ago. Based on the principle that "a common feature of any organized production effort to evade a disarmament inspection system . . . is the participation of a large number of people," inspection by the people would give substantial rewards to anyone with knowledge of illicit activities that revealed them to international authorities, along with safe passage out of the country and protection against future retaliation. See Seymour Melman, editor, *Inspection for Disarmament* (New York: Columbia University Press, 1958), p. 38.
13. A number of other processes can also be used to destroy chemical weapons. In a study for the U.S. Army, the National Research Council (of the National Academy of Sciences and National Academy of Engineering) compared three other nonincineration options with chemical neutralization: chemical oxidation using electricity and silver compounds; exposure to high-temperature hydrogen and steam;

and a process involving a high-temperature molten metal bath. National Research Council, *Review and Evaluation of Alternative Chemical Disposal Technologies* (Washington, D.C.: National Academy Press, 1996).

14. The Johnston Atoll Chemical Agent Disposal System (JACADS), as the incinerator is known, released VX or GB nerve gas to the environment once in December 1990, once in March 1994, twice in March 1995 and once on the first day of April 1995. Information on the last two of these nerve gas releases is available in Program Manager of Chemical Demilitarization, U.S. Department of Defense, *JACADS 1995 Annual Report of RCRA [Resource Conservation and Recovery Act] Noncompliances* (February 25, 1996). The earlier releases were mentioned in Environmental Protection Agency (Region 9), *Report of JACADS Operational Problems* (August 1994). Information on the explosions and other operational problems at JACADS can be found in Mitre Corporation, *Summary Evaluation of the JACADS Operational Verification Testing* (May 1993). Documents concerning the problems at JACADS have been closely followed by the Chemical Weapons Working Group of the Kentucky Environmental Foundation (P. O. Box 467, Berea, Kentucky 40403).
15. Brooke, James, "Incineration of Poison Gas Loses Support," *New York Times* (February 7, 1997).
16. Brooke, James, "So Far So Good as Chemical Weapons Are Burned in Utah, Officials Say," *New York Times* (April 13, 1998).
17. National Research Council, *Review and Evaluation of Alternative Chemical Disposal Technologies* (Washington, D.C.: National Academy Press, 1996).
18. Chepesiuk, Ron, "A Sea of Trouble," *Bulletin of the Atomic Scientists* (September-October 1997).
19. Weiner, Tim, "Soviet Defector Warns of Biological Weapons," *New York Times* (February 25, 1998).
20. Alibek, Ken, "Russia's Deadly Expertise," *New York Times* (March 27, 1998).
21. U.S. General Accounting Office, *Department of Energy: Problems and Progress in Managing Plutonium* (GAO/RCED-98-68), p. 4.
22. As of 1996, access to these bunkers was obstructed by very large concrete blocks placed in front of each bunker's steel entry door. A huge crane powerful enough to move these concrete blocks aside was stored in a guarded area nearby. Conversation with Professor William J. Weida of Colorado College (formerly of the U.S. Air Force Academy), author of an extensive study of the nuclear weapons production complex (February 17, 1996).
23. Wald, Matthew L., "Energy Dept. Announces Dual Plan for Disposal of Plutonium," *New York Times* (January 15, 1997).
24. Weapons-grade plutonium is normally about 93 percent Pu-239, 6 percent Pu-240 and 0.5 percent Pu-241, while typical reactor-grade plutonium is only about 64 percent Pu-239, with 24 percent Pu-240 and 11.5 percent Pu-241. Although neither Pu-240 or Pu-241 is nearly as suitable for weapons purposes as Pu-239, is it a mistake to believe that reactor-grade plutonium could not be used to make a powerful nuclear weapon. The critical mass for reactor-grade plutonium is 6.6 kilograms, only 40 percent more than for weapons-grade. See Chow, Brian G. and Solomon, Kenneth A., *Limiting the Spread of Weapon-Usable Fissile Materials* (Santa Monica, California: National Defense Research Institute, RAND Corporation, 1993), pp. 62-63.
25. Ibid.
26. William J. Weida, "MOX Use and Subsidies" (January 28, 1997, unpublished), p. 4. Weida's calculations are based on Office of Fissile Materials Disposition, Department of Energy, *Technical Summary Report for Surplus Weapons-Usable Plutonium Disposition* (Washington, D.C.: DOE/MD-003, 1996) and Revision 1 of that document (issued October 10, 1996). As of early 1997, the Department of Energy was still not being clear about how many reactors would be required to burn all the plutonium coming out of dismantled weapons. It will take at least one, and maybe a few.

    An earlier and apparently less comprehensive estimate by the National Defense Research Institute (RAND) put the cost of the MOX option at between $7,600 and $18,000 per kilogram of weapons-grade plutonium used. For 50 metric tons, the cost would thus be $380 to $900 million. This study found underground disposal to be a safer and cheaper alternative. (Chow and Solomon, op. cit., p. 66.)
27. Toevs, James and Beard, Carl A., "Gallium in Weapons-Grade Plutonium and MOX Fuel Fabrication," Los Alamos National Laboratories document LA-UR-96-4674 (1996).
28. Wald, Matthew L., "Factory Is Set to Process Dangerous Nuclear Waste," *New York Times* (March 13, 1996).
29. For an interesting summary debate between advocates of the two-track approach and advocates of vitrification only, see Moore, Mike, "Plutonium: the Disposal Decision," Holdren, John P. , "Work with Russia" and Lyman, Edwin S. and Leventhal, Paul, "Bury the Stuff," *Bulletin of the Atomic Scientists* (March-April 1997).

30. Hall, Brian, "Overkill Is Not Dead," *New York Times Magazine* (March 15, 1998).
31. Myers, Steven Lee, "Pentagon Ready to Shrink Arsenal of Nuclear Bombs," *New York Times* (November 23, 1998).
32. "First Nuclear Triggers in 40 Years to Be Made," *Palm Beach Post* (April 5, 1998); see also Carlson, Scott and Mello, Greg, "DOE Poised to Throw Money into Pits at LANL," *The Nuclear Examiner* (November 1997), p. 2.
33. Wald, Matthew L., "U.S. to Put a Civilian Reactor to Military Use," *New York Times* (August 11, 1997).
34. Ibid., p. 44.
35. Ibid.
36. Ibid., pp. 42 and 44.
37. For a more complete discussion, see, for example, Fischer, Dietrich, *Preventing War in the Nuclear Age* (Totowa, New Jersey: Rowman and Allanheld, 1984), pp. 47-62.
38. Political scientist Gene Sharp has argued persuasively for a completely nonmilitary form he calls "civilian-based defense." See, for example, Sharp, Gene, *Civilian-Based Defense: A Post-Military Weapons System* (Princeton University Press, 1990). Dietrich Fischer has also made major contributions to the debate over nonoffensive defense. For an especially clear exposition, see Fischer, Dietrich, *Preventing War in the Nuclear Age* (Rowman and Allenheld, 1984).
39. Hufbauer, Gary C., Schott, Jeffrey J. and Elliott, Kimberly, A., *Economic Sanctions Reconsidered: History and Current Policy* (Washington, D.C.: Institute for International Economics, 1990).
40. Ibid., pp. 94-105.
41. For a more detailed analysis of this proposal and the reasoning behind it, see Dumas, L.J., "A Proposal for a New United Nations Council on Economic Sanctions," in Cortright, David and Lopez, George, editors, *Economic Sanctions: Panacea or Peacebuilding in a Post–Cold War World* (Boulder, Colorado: Westview Press, 1995), pp. 187-200.
42. Elsewhere, I have analyzed some of the principles and institutions that could make international economic relations more successful as a means to this end. See Dumas, Lloyd J., "Economics and Alternative Security: Toward a Peacekeeping International Economy," in Weston, Burns, editor, *Alternative Security: Living Without Nuclear Deterrence* (Boulder, Colorado: Westview Press, 1990), pp. 137-175.
43. Boulding, Kenneth, *Stable Peace* (Austin: University of Texas Press, 1978).
44. For a more comprehensive analysis, see Dumas, op.cit., 1990.
45. Sivard, Ruth L., *World Military and Social Expenditures, 1993* (Washington, D.C.: World Priorities, 1993), pp. 20-21. For total wars and war-related deaths from 1900 through 1995, see Sivard, Ruth L., *World Military and Social Expenditures, 1996* (Washington, D.C.: World Priorities, 1996), pp. 17-19.
46. Though these limits of liability have been increased over the years, they remain a small fraction of estimated damages. For example, in 1982, the Sandia National Laboratories prepared a study for the Nuclear Regulatory Commission (NRC), called *Calculation of Reactor Accident Consequences (CRAC2) for U.S. Nuclear Power Plants (Health Effects and Costs).* The NRC transmitted the CRAC2 study results to Congress later that year. These included estimates of potential damages of $135 billion for a major accident at the Salem Nuclear Plant, Unit 1 reactor (New Jersey), $158 billion for Diablo Canyon, Unit 2 reactor (California), $186 billion for San Onofre, Unit 2 reactor (California) and $314 billion for Indian Point, Unit 3 reactor (New York). Six years later, the 1988 update of Price-Anderson raised the liability limit to $7 billion, only 2 to 5 percent of these damage estimates.
47. Solar power can use the heat of the sun directly, generate electricity with sunlight via solar cells, or even be used to liberate hydrogen that can be cleanly burned from water; geothermal energy make use of the earth's internal heat; biomass conversion turns plant or animal waste into clean burning methane gas; turbines that generate electricity can be driven by waterfalls (hydropower), the force of the incoming and outgoing tides (tidal power), or the wind (windpower); and energy can be extracted from the sea by making use of ocean thermal gradients, the differences in temperature between different layers of seawater.
48. Dumas, L.J., *The Conservation Response: Strategies for the Design and Operation of Energy-Using Systems* (Lexington, Massachusetts: D.C. Heath and Company, 1976).
49. It is theoretically possible to transmute plutonium, uranium and other dangerous radioactive substances into more benign elements by bombarding them with subatomic particles in particle accelerators. The technology to do this in a practical and economically feasible way with large quantities

of radioactive material is nowhere near at hand. While it would be useful to pursue research in this area, whether or not this can be done must be regarded as a speculative matter for the foreseeable future.

50. Some of the more dangerous radionuclides, like strontium-90 and cesium-137 decay to very low levels within a few centuries. Others, like plutonium-239, americium-241 and neptunium-237 take many thousands to millions of years to become essentially harmless. For an interesting, brief discussion of this issue, see Whipple, Chris G., "Living with High-Level Radioactive Waste," *Scientific American* (June 1996), p. 78.
51. Brooke, James, "Underground Haven, Or a Nuclear Hazard?" *New York Times* (February 6, 1997).
52. Wald, Matthew L., "Admitting Error at a Weapons Plant," *New York Times* (March 23, 1998); Zorpette, Glenn, "Hanford's Nuclear Wasteland," *Scientific American* (May 1996), pp. 88-97.
53. U.S. General Accounting Office, *Nuclear Waste: Management and Technical Problems Continue to Delay Characterizing Hanford's Tank Waste* (Washington, D.C.: January 1996), pp. 1-2, 4 and 16.
54. Ibid., p. 8.
55. Hoffman, David, "Rotting Nuclear Subs Pose Threat in Russia: Moscow Lacks Funds for Disposal," *Washington Post* (November 16, 1998).
56. Warf, James C. and Plotkin, Sheldon C., "Disposal of High Level Nuclear Waste," Global Security Study no. 23 (Santa Barbara, California: Nuclear Age Peace Foundation, September 1996), p. 6.
57. Hollister, Charles D. and Nadis, Steven, "Burial of Radioactive Waste Under the Seabed," *Scientific American* (January 1998), pp. 61-62.
58. Ibid., pp. 62-65.
59. Whipple, Chris G., "Can Nuclear Waste Be Stored Safely at Yucca Mountain?" *Scientific American* (June 1996), pp. 72-76.
60. U.S. General Accounting Office, *Nuclear Waste: Impediments to Completing the Yucca Mountain Repository Project* (Washington, D.C.: January 1997), p. 4.
61. Wald, Matthew L., "Doubt Cast on Prime Site as Nuclear Waste Dump," *New York Times* (June 20, 1997).
62. Wernicke, Brian, et al., "Anomalous Strain Accumulation in the Yucca Mountain Area, Nevada"; and Kerr, Richard A., "A Hint of Unrest at Yucca Mountain," *Science* (March 27, 1998), pp. 2096-2100 and pp. 2040-2041, respectively.
63. Kerr, Richard A., "Yucca Mountain Panel Says DoE lacks Data," *Science* (February 26, 1999).
64. James Brooke, op. cit.
65. For a particularly interesting and erudite analysis of the problems with the WIPP site, see Citizens for Alternatives to Radioactive Dumping, "Greetings from WIPP, the Hot Spot: Everything You Always Wanted to Know About WIPP" (1997: CARD, 144 Harvard SE, Albuquerque, NM 87106).
66. Associated Press, "Nation's First Nuclear Waste Depository Opens" (March 26, 1999).
67. Lawler, Andrew, "Researchers Vie for Role in Nuclear-Waste Cleanup," *Science* (March 21, 1997).
68. The F/A-18 is estimated to cost $73 million per plane. See Eisman, Dale, "Pentagon Commits $2 billion to Super Hornet Program, Declares 'Wing-Drop' Problem Resolved," *The Virginian-Pilot* (Norfolk, Virginia) (April 6, 1998).
69. One interesting alternative is bioremediation, though much careful study is necessary before living organisms can be seriously considered as agents for degrading nuclear waste. See Travis, John, "Meet the Superbug: Radiation-Resistant Bacteria May Clean Up the Nation's Worst Waste Sites," *Science News* (December 12, 1998).
70. Environmental Protection Agency, "National Priorities List: Final and Proposed [General Superfund and Federal Facilities] Sites" (December 1996), p. 22. This unpublished list was sent to the author by the EPA Region 6 Office (Dallas, Texas) in March 1997.

    According to EPA Headquarters in Washington, an "operable unit" is a component of the cleanup process, such as groundwater treatment or land cleanup. There have been an average of 1.8 operable units per site. (Correspondence and telephone conversations between the author and Program Analyst Ed Ziomkoski at the Program Analysis and Research Management Center of U.S. EPA, March 27 and April 4, 1997).
71. Correspondence and telephone conversations between the author and Program Analyst Ed Ziomkoski at the Program Analysis and Research Management Center of U.S. EPA; March 27 and April 4, 1997.
72. Federal Facilities Profile, OSWER Directive 9200.3-14-1C, Exhibit D.1, pp. D-2 and D-3, sent to the author by Reneé P. Wynn, Federal Facilities Restoration and Reuse Office, U.S. Environmental Protection Agency, Washington, D.C. (April 11, 1997).
73. Guerrero, Peter F., "Superfund: Times to Assess and Clean Up Hazardous Waste Sites Exceed Program Goals," Testimony before the Subcommittee on National Economic Growth, Natural Resources and

Regulatory Affairs of the Committee on Government Reform and Oversight, U.S. House of Representatives (Washington, D.C.: February 13, 1997), p. 1. See also U.S. General Accounting Office, *Superfund: Times to Complete the Assessment and Cleanup of Hazardous Waste Sites* (Washington, D.C.: March 1997).

74. U.S. General Accounting Office, *Superfund: EPA Could Further Ensure the Safe Operation of On-Site Incinerators* (Washington, D.C.: March 1997).

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

In the Matter of

DUKE ENERGY CORPORATION

McGuire Nuclear Station, Units 1 and 2;
Catawba Nuclear Station, Units 1 and 2

Docket Nos. 50-369/370/413/414-LR

November 14, 2001

NOTICE OF APPEARANCE for Donald J. Moniak

Notice is hereby given that **Louis Zeller** enters an appearance as a representative of the **Blue Ridge Environmental Defense League** (BREDL). In accordance with 10 C.F.R. § 2.713(b), the following information is provided:

Louis Zeller
Name: ~~Donald J. Moniak~~ (Don Moniak)
Address: P.O Box 88 Glendale Springs NC 28629
Telephone Number: 336-982-2691
Fax Number: (336) 982-2954
E-mail Address: BREDL@skybest.com

Name of Group Representing: Blue Ridge Environmental Defense League
Address: P.O Box 88 Glendale Springs NC 28629
Executive Director: Ms. Janet Zeller
Telephone Number: 336-982-2691

Please note that single electronic and mail filings will suffice for service of documents to both Mr. Zeller and Ms. Zeller.

Sincerely,

Donald J. Moniak
Community Organizer, SRS Project Coordinator
Blue Ridge Environmental Defense League

November 30, 2001

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

BEFORE THE ATOMIC SAFETY LICENSING BOARD

In the Matter of	)	
	)	
DUKE ENERGY CORPORATION	)	Docket Nos. 50-369, 370, 413 and 414
	)	
(McGuire Nuclear Station,	)	
Units 1 and 2, and	)	
Catawba Nuclear Station	)	
Units 1 and 2)	)	

CERTIFICATE OF SERVICE

I hereby certify that copies of the following documents

- Blue Ridge Environmental Defense League (BREDL) Submittal of Contentions in the Matter of the Renewal of Licenses for Duke Energy Corporation (DUKE) McGuire Nuclear Stations 1 and 2 [McGUIRE] and Catawba Nuclear Stations 1 and 2 [CATAWBA], and Support for NIRS Motion to Suspend Proceeding.

- Notice of Appearance for Mr. Louis Zeller
- *Exhibits 1, 2, and 3*

In the above-captioned proceeding have been served on the following by deposit via next day U.S. Postal Service on the 30th day of November, 2001, as well as by e-mail on the 29th with the exception of Exhibit 1 which was sent by FAX to representatives from each party*, Exhibit 2 which was sent by email to representatives of each party*, Exhibit 3 which is only being sent via Federal Express, and the Notice of Appearance which was emailed the 30th. In addition, a CD-ROM of all source documents cited in contentions for factual basis and that are electronically available is being enclosed in the packet.

Ann Marshall Young, Chair*
Administrative Judge
Atomic Safety and Licensing Board
U.S. Nuclear Regulatory Commission
Mail Stop: T-3F23
Washington, D.C. 20555
(E-mail: AMY@nrc.gov)

Charles N. Kelber*
Administrative Judge
Atomic Safety and Licensing Board
U.S. Nuclear Regulatory Commission
Mail Stop: T-3F23
Washington, D.C. 20555
(E-mail: CNK@nrc.gov)

Office of Commission Appellate Adjudication
U.S. Nuclear Regulatory Commission
Mail Stop: O-16C1
Washington, D.C. 20555

Paul Gunter
Nuclear Information and Resource Service
1424 16th St. N.
Washington, D.C. 20026
(E-mail: pgunter@nirs.org)

Lester S. Rubenstein
Administrative Judge
Atomic Safety and Licensing Board
4760 East Country Villa Drive
Tucson, AZ 85718
(E-mail: Lesrrr@msn.com)

Office of the Secretary (two copies)
ATTN: Docketing and Service
U.S. Nuclear Regulatory Commission
Mail Stop: O-16C1
Washington, D.C. 20555
(E-mail: HEARINGDOCKET@nrc.gov)

Janet Marsh Zeller
Executive Director
Blue Ridge Environmental Defense League
P.O. Box 88
Glendale Springs, NC 28629
(E-mail: BREDL@skybest.com)

Mary Olson
Nuclear Information and Resource Service
Southeast Office,
P.O Box 7586
Asheville, NC 28802
(E-mail: donmoniak@earthlink.net)

David A. Repka, Esq.
Anne W. Cottingham, Esq.
Winston & Strawn
1400 L Street, N.W.
Washington, D.C. 20005-3502
(E-mail: drepka@winston.com
acotting@winston.com)

Susan L. Uttal, Esq.
Antonio Fernandez, Esq.
Mail Stop - O-15 D21
Office of the General Counsel
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001(E-mail:
slu@nrc.gov; axf2@nrc.gov)

Lisa F. Vaughn, Esq.
Legal Dept. (PBO5E)
Duke Energy Corporation
422 So. Church St.
Charlotte, NC 28201-1006
(E-mail: lfVaughn@duke-energy.com)

Donald J. Moniak (Don Moniak)
Blue Ridge Environmental Defense League
PO Box 3487
Aiken, SC 29802-3487

This 30th Day of November, 2001