Yale University Press / New Haven and London

Secret Agencies

U.S. INTELLIGENCE IN A HOSTILE WORLD

Loch K. Johnson

There are many elements that go into every important decision.
In the first place, you must try to grapple with the facts.
What is the actual situation?
Secretary of State Dean Rusk to Eric Goldman (January 12, 1964)

CONTENTS

PREFACE

This book examines how, and how well, the intelligence agencies of the United States have been used by government officials since the end of World War Two to guard and advance the global interests of the nation. My purpose is to help inform the American people about the hidden side of their government. For democracy relies on a knowledgeable citizenry to provide general guidance to those few individuals who make foreign policy decisions on their behalf.

America's secret agencies engage in three primary missions. First and foremost, they are expected to gather and interpret information from around the world (referred to by intelligence officers as collection and analysis). Second, the agencies are expected to protect U.S. government secrets from espionage by other governments (counterintelligence). Third, from time to time they have been directed to oppose the nation's adversaries through the use of aggressive clandestine operations abroad (covert action). Throughout the Cold War (1945–91) the Soviet Union was the nemesis of American foreign policy and hence the number-one target of the intelligence agencies. The containment of Soviet-inspired communism was the preeminent objective that shaped Amer-

ica's relations with the rest of the world and provided the raison d'être for the secret agencies.

In an earlier study, *A Season of Inquiry* (1985), I wrote about the beginning of a new era for American intelligence ushered in by a series of spy scandals. In the benchmark year 1975 government investigators had accused the secret agencies of conducting espionage against American citizens, the very people they had been created to protect. Probes by the executive and legislative branches chronicled a long list of Orwellian excesses: spying on civil rights activists and Vietnam War dissenters, plotting the assassination of foreign leaders, and running unsavory clandestine operations meant to undermine or destroy regimes considered anathema to the interests of the United States—even democracies (Chile is only the most well-known case).

In the light of this jarring breach of trust, U.S. intelligence agencies would no longer enjoy the same breadth of discretion in the conduct of covert operations around the globe as they had had before. Henceforth officials within the executive branch—and, in a dramatic expansion of supervision, the legislative branch as well—would attempt to hold the nation's spymasters to a higher standard of accountability. *A Season of Inquiry* traced the debates about the future of intelligence that took place during the "Year of Intelligence," as some officers of the Central Intelligence Agency (CIA) remember 1975, or—for the more embittered—the time of the "Intelligence Wars." Scandal had forced both the president and the Congress to grapple with the dilemma of how to tighten control over the secret agencies without stifling their initiative and morale in the struggle against America's external enemies. A unique experiment in intelligence accountability had begun.

My second study of intelligence, *America's Secret Power* (1989), examined the effectiveness of the new accountability during its first decade, including the performance of neophyte House and Senate intelligence oversight committees, the stringent approval and reporting requirements for sensitive operations, and the new Intelligence Oversight Board (IOB) set up in the executive office of the president. The verdict: even after ten years, the new relationships remained rough-hewn—and they had failed altogether to prevent the Iran-contra affair of 1986–87. Nevertheless, the new methods of democratic control had worked most of the time, and clearly they represented a vast improvement over the open-ended authority granted the secret agencies throughout the earlier era of tolerant neglect (1945–74).

America's Secret Power explored a number of problems that continued to disturb the balance between accountability and effectiveness for the baker's dozen departments and agencies that make up the so-called intelligence com-

munity (IC). Seven major "sins of intelligence" emerged from the study, the most damning of which was the failure to provide policymakers with objective information. The book identified a variety of pathologies that weakened the core intelligence mission of information collection and interpretation. It also explored the elaborate relationships that had evolved since the end of World War Two between the secret side of government and other American institutions, particularly the media and the universities.

In the same year *America's Secret Power* was published, history offered up one of its rare sea-changes in world affairs. In November 1989 the Berlin Wall was brought down suddenly, and the Soviet Union soon came tumbling after. In a quick succession of astounding and exhilarating events, the Cold War was over. These events, culminating in a splintering of the Soviet empire in 1991 into its constituent republics and once-captive nations, brought to the forefront troubling questions about U.S. intelligence capabilities. How could the secret agencies have failed to anticipate the dissolution of America's deadliest international rival? What would happen to the clandestine service now that the Cold War was over?

The present book carries forward my research into the netherworld of intelligence, further unfolding topics taken up earlier and setting out in new directions as well—among them the debate over whether the United States should engage in a more aggressive use of economic espionage against allies and enemies alike. I consider a range of ethical questions surrounding the use of covert operations, while continuing to follow the thread of intelligence accountability that weaved through the companion volumes. I offer an updated appraisal at the close of a second decade in this noble—and often shaky—experiment meant to bring some semblance of democracy into the darkest corners of American government.

I begin by examining what is meant by "intelligence," why nations with global interests consider it important to have secret agencies, and how the use of intelligence is beset with existential vexations (chapter 1). Chapter 2 brings a broad historical overview of America's secret operations abroad from the Cold War to the present. The purpose of this chapter is to indicate how the emphasis placed on the different intelligence missions by the government has fluctuated over the years. The moral implications of clandestine operations are assessed in chapter 3, where I offer a set of guidelines for a more ethical approach to the use of secret power.

The question of intelligence accountability, a central concern for any probe into the interstices between secrecy and democracy, is taken up in chapter 4 with a close look at how well overseers have monitored the intelligence agen-

cies through Congressional hearings. Chapter 5 contrasts the U.S. approach to intelligence with that of other countries.

The issue of intelligence and economic security is the focus of chapter 6. The key question here is: Should this nation's secret agencies aid the American business community in its struggle for success in the global marketplace against adroit foreign competitors like Japan and Germany? The book concludes in chapter 7 with an evaluation of how well America's intelligence agencies fared during the Cold War against the USSR, a totalitarian state bristling with nuclear weapons and endowed with powerful secret services of its own. Have the American people been well served in their quest for peace and security in a world marred by violence, intrigue, and uncertainty? Do the billions of taxpayer dollars spent on intelligence over the past fifty years add up to a wise investment or a foolish waste of money?

The methodology in this and my other books has been straightforward: study everything of a serious nature that has been written on the subject—a steadily burgeoning literature of government documents, periodicals, and scholarly treatises—and interview as many intelligence professionals and outside experts as possible.[1] The interviews have been with men and women at all levels of the secret agencies and with their overseers in the executive and legislative branches, as well as with a wide range of academic specialists from the United States and abroad.

A unifying theme binds together this corpus of research. The information provided to policymakers by the intelligence community often contributes vitally to the making of sound decisions, giving the secret agencies a role of unquestionable importance to the nation's well-being. Yet the evidence clearly reveals that, at the same time, the intelligence agencies have the capacity not only to safeguard democracy but to subvert it as well. Moreover, the information they have provided to the nation's leaders has at times been wrong, as a result of errors in judgment or bias in reporting—or because many things about the world are simply unknowable. Thus the intelligence agencies indeed warrant the support of Americans, but they also require a close watchfulness—even wariness.

This book has benefited greatly from discussions with intelligence officers and overseers, most of whom have requested anonymity for professional reasons. I thank them profusely for their patience and generosity. Some of the thoughtful people with whom I have spoken can be openly thanked, though, beginning with Les Aspin, the former secretary of defense and chairman of the Commission on the Roles and Capabilities of Intelligence. He was a wonderful source of encouragement for this project; he read and commented on por-

tions of the manuscript as I went along, and was especially helpful with chapter 7. His premature death in 1995 was a tragedy for the country and for the many of us who valued his friendship and keen analytic mind.

Others I am pleased and able to thank openly include James A. Barry, David D. Gries, Arthur S. Hulnick, Carol Minor, Kay Oliver, Hayden B. Peake, Donald P. Steury, and Michael A. Turner of the CIA's Center for the Study of Intelligence and its Office of Academic Affairs; Harold P. Ford, Joseph S. Nye, Jr., and Gregory F. Treverton, all formerly with the National Intelligence Council; Douglas J. MacEachin, formerly deputy director of intelligence at the CIA; George J. Tenet, a former senior intelligence official on the National Security Council (NSC) and presently the deputy director of central intelligence; the late James J. Angleton, chief of CIA counterintelligence; John T. Elliff, Senator Wyche Fowler, Richard H. Giza, Thomas K. Latimer, Senator Sam Nunn, and Paula L. Scalingi, former legislative overseers; Carol Rindskopf, former general counsel of the CIA; Frederick P. Hitz, the CIA's inspector general; Dean Rusk, former secretary of state; former intelligence officers George Carver, Dr. Ray S. Cline, Jack Davis, and Walter Pfortzheimer; and each of the directors of Central Intelligence from 1966 to 1995—Richard Helms, James R. Schlesinger, William E. Colby, George Bush, Adm. Stansfield Turner, William J. Casey, William H. Webster, Robert M. Gates, and R. James Woolsey—who kindly subjected themselves to the author's questioning.

I also want to express my appreciation to several scholars, friends, private analysts, and reporters who have allowed me to bend their ears on the topics in this book, often guiding me in a better direction than the one I was traveling: Christopher Andrew, Richard K. Betts, Steven Emerson, Louis Fisher, Randall Fort, John Lewis Gaddis, Roy Godson, Allen E. Goodman, Michael Handel, Glenn P. Hastedt, John Hollister Hedley, Karl F. Inderfurth, Rhodri Jeffreys-Jones, Robert Jervis, Frederick M. Kaiser, Anne Karalekas, William M. Leary, Mark M. Lowenthal, Fred F. Manget, Ernest R. May, Harvey Nelsen, Jay Peterzell, John Prados, Harry Howe Ransom (esteemed mentor), Jeffrey T. Richelson, Harry Sepp, Frank John Smist, Jr., Robert David Steele, Stafford T. Thomas, Richard R. Valcourt, Wesley K. Wark, H. Bradford Westerfield (who generously and with great insight read an early draft of the manuscript), and David Wise. No doubt they will object to some of the conclusions I have reached in these pages; but perhaps they will see their good influence here and there, too. The annotations throughout this volume are further testimony of my debt to the individuals mentioned here, along with a much wider group of intelligence specialists.

I would like to express my deep gratitude, as well, for the support I have re-

ceived from the University of Georgia. My interview trips to Washington, D.C., were made possible by funding from Thomas P. Lauth, the head of the Department of Political Science; Wyatt W. Anderson, dean of the College of Arts and Sciences; and Robert L. Anderson, the associate vice president for research. I am grateful as well to Rick Dunn and Amy Fletcher, doctoral candidates at the university, for their research assistance; to Chuck Grench, Otto Bohlmann, Susan Laity, and Richard Miller of Yale University Press for their guidance and encouragement; and to the following journals and publishers for permitting me to draw on materials I have previously published: Frank Cass, Simon & Schuster, the University of Oklahoma Press, St. Martin's Press, the *American Intelligence Journal*, the *American Journal of International Law, Foreign Policy*, the *Journal of Strategic Studies*, and the *International Journal of Intelligence and Counterintelligence*.

Above all, I want to thank my wife, Leena, and my daughter, Kristin, for the cheerful tolerance they have displayed toward the research trips that took me away from the hearth and the long hours spent huddled before the pale screen of a word processor at home. Their unwavering love and devotion have sustained me through the solitude and frustrations that accompany the writing of a book.

ABBREVIATIONS AND ACRONYMS

ABM	anti-ballistic missile
ACIS	Arms Control Intelligence Staff
AFIO	Association of Former Intelligence Officers
AG	Attorney General
AWACS	Airborne Warning and Control System
BMD	ballistic missile defense
BNL	Banca Nazionale del Lavoro
CA	covert action
CAS	Covert Action Staff (CIA)
CE	counterespionage
CHAOS	codename for CIA domestic spying operation
CI	counterintelligence
CIA	Central Intelligence Agency
CINC	commander in chief
CIO	Central Imagery Office
CISPES	an FBI counterintelligence program
C/CATF	chief/Central American Task Force
CMS	Community Management Staff
CNN	Cable News Network

COINTELPRO	Counterintelligence Program (FBI)
COMINT	communications intelligence
COMIREX	Committee on Imagery Requirements and Exploitation
CORONA	codename for first U.S. spy satellite system
COS	chief of station (CIA)
CPSU	Communist Party of the Soviet Union
CRS	Congressional Research Service (Library of Congress)
DA	Directorate of Administration (CIA)
DAS	deputy assistant secretary
DCIA	Director of the Central Intelligence Agency
DCI	Director of Central Intelligence
DDA	Deputy Director for Administration (CIA)
DDCIA	Deputy Director of the Central Intelligence Agency
DDI	Deputy Director for Intelligence (CIA)
DDO	Deputy Director for Operations (CIA)
DDS&T	Deputy Director for Science and Technology (CIA)
DEA	Drug Enforcement Administration
DECA	Developing Espionage and CI Awareness (FBI)
DEIB	*Daily Economic Intelligence Brief*
DGSE	French Intelligence Service
DI	Directorate of Intelligence (CIA)
DIA	Defense Intelligence Agency
DID	*Defense Intelligence Daily*
DINSUM	Defense Intelligence Summary
DO	Directorate of Operations (CIA)
DOD	Department of Defense
DS&T	Directorate of Science and Technology (CIA)
ELINT	electronic intelligence
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service (CIA)
FOIA	Freedom of Information Act
GAO	General Accounting Office (Congress)
GATT	General Agreement on Tariffs and Trade
GEO	geosynchronous orbit
GNP	Gross National Product
GRU	Soviet military intelligence
HEO	high-elliptical orbit
HPSCI	House Permanent Select Committee on Intelligence
HUMINT	human intelligence (espionage)
IA	Intelligence Assessment
IC	intelligence community
ICBM	intercontinental ballistic missile
IG	Inspector General
IIM	Interagency Intelligence Memorandum

IMF	International Monetary Fund
INR	Bureau of Intelligence and Research (State Dept.)
INTELINK	an intelligence community computer information system
IOB	Intelligence Oversight Board (White House)
IRS	Internal Revenue Service
ISC	Intelligence and Security Committee (Britain)
JCS	Joint Chiefs of Staff
ITT	International Telephone and Telegraph Corporation
JCS	Joint Chiefs of Staff
JETRO	Japan's external trading organization
KGB	Soviet secret police and foreign intelligence service
KH	Keyhole (satellite)
LEO	low-elliptical orbit
MASINT	measurement and signature intelligence
MIRV	multiple independent reentry vehicle
MITI	a Japanese economic planning group
MRBM	medium-range ballistic missile
MRC	major regional conflict
MVD	Soviet Ministry of Internal Affairs
NAFTA	North American Free Trade Agreement
NATO	North Atlantic Treaty Organization
NEC	National Economic Council (White House)
NEO	noncombatant evacuation operation
NFIP	National Foreign Intelligence Program
NIA	National Imagery Agency (proposed)
NIC	National Intelligence Council
NID	*National Intelligence Daily*
NIE	National Intelligence Estimate
NIO	National Intelligence Officer
NISC	National Intelligence Study Center
NOC	non-official cover
NPC	nonproliferation center
NPIC	National Photographic Interpretation Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council (White House)
NSCID	National Security Council Intelligence Directive
NTM	National Technical Means
OEOB	Old Executive Office Building
OMB	Office of Management and Budget
OOTW	operations other than war
OPA	Office of Public Affairs (CIA)
OPC	Office of Policy Coordination (CIA)
OPEC	Organization of Petroleum Exporting Countries

op sec	operational security
ORD	Office of Research and Development (CIA)
ORR	Office of Research and Reports (SOVA predecessor)
OSINT	open-source intelligence
OSS	Office of Strategic Services
OSWR	Office of Special Weapons Research
OTA	Office of Technology Assessment (Congress)
OTR	Office of Training (CIA)
PAC	Political Action Committee
PDB	*President's Daily Brief*
PDD	Presidential Decision Directive
PFIAB	President's Foreign Intelligence Advisory Board
PHOINT	photographic intelligence (imagery)
PLA	People's Liberation Army (China)
PLO	Palestine Liberation Organization
PM	paramilitary
PRC	People's Republic of China
RADINT	radar intelligence
ROSE	Rich Open Source Environment—CIA computer software
SA	Special Activities Division, DO/CIA
SAC	Strategic Air Command
SAM	surface-to-air missile
SHAMROCK	codename for NSA domestic wiretap
SIGINT	signals intelligence (special intelligence)
SIRC	Security Intelligence Review Committee (Canada)
SIS	Strategic Intelligence Service (Britain)
SLBM	submarine-launched ballistic missile
SMO	support to military operations
SNIE	Special National Intelligence Estimate
SOG	Special Operations Group (paramilitary covert action)
SOVA	Office of Soviet Analysis (CIA)
SSCI	Senate Select Committee on Intelligence
SVRR	Russian intelligence service
TECHINT	technical intelligence
TELINT	telemetry intelligence
UAV	unmanned aerial vehicle
UN	United Nations
USC	United States Code (statutory identification system)
USG	United States Government
USIB	United States Intelligence Board
USTR	United States Trade Representative
VC	Viet Cong (pro-Communist faction in Vietnam War)
WMD	weapons of mass destruction

SECRET AGENCIES

CHAPTER 1

THE MEANINGS AND METHODS OF INTELLIGENCE

In a full-page magazine advertisement that offered financial counseling for the perplexed consumer, a New York bank presented readers with a drawing of a man in a rowboat. Blithely oaring his way along a sparkling river, he seemed completely unaware of the gathering currents about to sweep him over a waterfall. The copy advised, "Moving ahead without looking ahead could prove to be the greatest risk of all."

As with boating in unfamiliar waters, steering a nation through the treacherous tides of history can also be a perilous enterprise. Responsible leaders in every nation seek knowledge—and, ideally, foreknowledge—of the world around them. For with a better understanding of global affairs, they are apt to protect and advance more effectively the vital interests of their citizens.

THE FOUR MEANINGS OF INTELLIGENCE

A prudent awareness of the dangers and opportunities that confront a nation can be achieved only through painstaking collection of information about key events, circumstances, and personalities worldwide. This gathering of infor-

mation, followed by its careful sifting, lies at the heart of "intelligence" as that term is applied to affairs of state.

More formally, professional intelligence officers define strategic intelligence as the "knowledge and foreknowledge of the world around us—the prelude to Presidential decision and action."[1] At this global level the objective is to acquire an understanding of the potential risks and gains confronting the nation from all compass points. At the more restricted level of tactical intelligence the focus turns to an assessment of likely outcomes in specific battlefields or theaters of war—what military commanders refer to as "situation awareness."

From this point of view (and it is by far the most common usage) intelligence is *information*, a tangible product collected and interpreted in order to achieve a sharper image of political and military conditions worldwide. A typical intelligence question at the strategic level would be, "If a coup toppled the Russian president, who would be among the field of leading contenders to replace him, and what political and military views do they have?" Or at the tactical level, one can imagine General H. Norman Schwarzkopf demanding during the Persian Gulf War in 1991, "I want the precise location of Iraq's Republican Guard—and I want it now!" To prevail in battle, a nation must have data on the enemy's terrain, roads, airfields, ports, waterways, and bridges. "Can that bridge support a tank?" "Is the runway long enough for a C-47?" "Is the beach firm enough to support an amphibious landing?" "Is aviation fuel available on the island?" Even the types of local parasites cannot be overlooked if troops are to be properly inoculated against infectious diseases.

What makes intelligence different from other forms of information are the strands of secret material woven into it. As Abram N. Shulsky emphasizes, intelligence often entails "information some other party is trying to deny":[2] agent dossiers locked in Kremlin safes; telephone conversations between Beijing commanders and artillery units of the People's Liberation Army (PLA) on maneuvers near Changchun; the flight plans of cocaine-filled Caravelle jets from Colombia headed for landing strips in Mexico along the Texas border.

Still, much of the information gathered and analyzed by American intelligence agencies is drawn from open sources in the public domain, such as Iranian television broadcasts, Japanese economic reports, or editorials in *Rossiiskaya Gazeta* and the hundreds of other new Russian newspapers. Allen Dulles, the chief of intelligence from 1953 to 1961, testified before the Senate Armed Services Committee on April 25, 1947, that about 80 percent of intelligence analysis is based on the public record—although CIA old-timers hasten

to add that he was including in this figure information gathered by diplomats and military attaches.

Whatever the precise mix of covert and overt information in intelligence reporting during the Cold War, both are necessary ingredients for good analysis. The overt information provides a context for the covert—a way of putting the clandestine "nuggets" into perspective. Yet classified studies (some by reputable outside scholars on contract) that have looked at the "added value" of clandestine reporting conclude that policymakers really do gain information from the secret agencies beyond what can be found in the *New York Times,* the *Economist,* or *Foreign Policy*.[3]

Nonetheless, many policymakers prefer the public literature, because it is written in a felicitous style and, since it is unclassified, can be talked about openly. Few, though, are prepared to relinquish their access to the *President's Daily Brief* or *PDB* (if they are lucky enough to be one of the thirteen policy elites to receive it), the *National Intelligence Daily* (*NID*), the *Defense Intelligence Digest* (*DID*), or the many other publications prepared by the intelligence agencies.

Policymakers understand that intelligence sources offer unique access to data on terrorist activities or enemy weapons systems, for instance, via worldwide coverage by agents in almost every capital and via surveillance satellites. Most important, decisionmakers know they can talk back to these "newspapers," asking intelligence officers to follow up with tailored oral briefings or written reports. In a word, intelligence is responsive to their needs.

During the Cold War much of the information sought by policymakers was secret ("denied") and had to be acquired through clandestine means. Espionage thus became a defining feature of intelligence-as-information. Even if the bulk of what was reported by intelligence officers came from open sources, it reached far beyond the policymaker's usual brief sampling of the daily Washington newspapers and the *New York Times*.

Since the end of the Cold War the intelligence agencies have tended to concentrate on the secret pieces of the global puzzle. Sensitive to the charge (however wrong) that it adds little to what the newspapers report, the intelligence community has made a concerted effort to demonstrate the value added from its clandestine tradecraft. The overt/covert mix also depends on the subject. With respect to terrorism, counternarcotics, and proliferation—or "hard targets" like North Korea or Iran—the overwhelming percentage (75 to 90) of all the material in intelligence reports is likely to come from clandestine sources. In contrast, political and economic subjects are often well reported in the pub-

lic media, and the secret agencies turn to these sources too for a reliable context in which to place their covert findings (anywhere from 10 to 40 percent of the total).

One intelligence analyst has observed that roughly 60 percent of the sources used by his technical branch of the CIA are open, including scientific journals, computer databases, newspaper articles, and reports from the CIA's Foreign Broadcast Information Service (FBIS), which translates thousands of foreign periodicals and newspapers into English. Another 25 percent is based on insider information, that is, hard-to-find "gray literature" (such as technical-conference proceedings), diplomatic reporting, contract studies, and surveys financed by the intelligence agencies. Only 15 percent of its information comes from mechanical and human espionage—though, it should be kept in mind, this information often proves the most valuable.[4]

From another vantage point intelligence may be considered a *process*: a series of interactive steps formally referred to as the "intelligence cycle."[5] At the beginning of the cycle officials plan what information to target around the world; then they order the information to be collected and organized—or "processed" in the narrower sense of that word—for close study (analysis) by experts.

Once the expert analysts have assessed the information, it is disseminated in the last step of the cycle to top policy officers in the executive branch and selected members of Congress with foreign policy responsibilities. An illustration of this usage of the word *intelligence* might be, "Analysts in the Directorate of Intelligence (DI), the CIA's analytic shop, play a vital intelligence role as they attempt to interpret the goals and *modus operandi* of Islamic radicals."

From a third perspective intelligence may be thought of as a set of *missions* carried out by the secret agencies. The first is collection and analysis, a shorthand phrase for the full intelligence cycle;[6] second, counterintelligence, the thwarting of secret activities directed against the United States by foreign entities (usually hostile intelligence services);[7] and third, covert action, the secret intervention into the affairs of other states[8]—sometimes called "special activities" or, for the benefit of the occasional Latin scholar who might come across the Special Activities Division (SA) crest at CIA Headquarters, "Actiones Praecipuae." An example of this usage might be, "What mix of secret intelligence operations—collection-and-analysis, counterintelligence, and covert action—might be most effective to prevent North Korea from developing an arsenal of nuclear weapons?"

Finally, the term *intelligence* is used from time to time to denote the structures or *organizations* that carry out these core missions. Intelligence in this in-

stance, refers to the actual network of officials and agencies involved in the gathering, processing, interpreting, and disseminating of information, as well as those who plan and implement counterintelligence (CI) and covert action (CA). Using this sense of the word the president might remark, "Make sure intelligence is present at the Tuesday meeting of the National Security Council." Or a battalion commander might say, "Get intelligence on the line; I need the exact coordinates of Serbian artillery near Bihac."

The establishment of intelligence as an organization in the United States has a long history, beginning with George Washington—one of the few presidents with a deep and abiding interest in the subject.[9] As general during the Revolutionary War he had his own secret code number ("711") and made use of an effective network of spies led by Paul Revere and including Nathan Hale.

Intelligence organizations have played a role in each of America's military conflicts since the Revolutionary War.[10] General Ethan Allen Hitchcock formed a highly successful spy ring in the U.S. Army during the 1840s that helped lead to victory in the war with Mexico. Allan Pinkerton assembled a talented team of spies for the Union Army during the Civil War, and Rose O'Neil Greenhow ("Rebel Rose"), a resourceful agent for the South, contributed to the Confederate success at the first Battle of Bull Run. The outbreak of war in Europe in 1914 stirred some modest efforts in Washington to create a more sophisticated secret service for the nation, but only with the onset of World War Two did this objective receive the full attention of President Franklin D. Roosevelt. In June 1942 he ordered the formation of a new intelligence agency, called the Office of Strategic Services (OSS), which vigorously pursued each of the intelligence missions against the Axis powers.[11]

Still, as the former secretary of state Dean Rusk remembers, the U.S. intelligence services during World War Two remained bare-boned. "When I was assigned to G-2 [Army Intelligence] in 1941, well over a year after the war had started in Europe," he once told a Senate subcommittee, "I was asked to take charge of a new section that had been organized to cover everything from Afghanistan right through southern Asia, southeast Asia, Australia, and the Pacific. . . . Because we had no intelligence organization that had been giving attention to that area up to that time, the materials available to me when I reported for duty consisted of a tourist handbook on India and Ceylon, a 1924 military attache's report from London on the Indian Army, and a drawer full of clippings from the *New York Times* that had been gathered since World War One. That was literally the resources of G-2 on that vast part of the world a year after the war in Europe had started."[12]

At the end of the war President Harry S Truman turned toward the task of

modernizing the government's intelligence organization. The attack by the Japanese air force at Pearl Harbor on December 7, 1941, had caught the U.S. Navy by surprise and caused extensive destruction to the Pacific fleet. This "day of infamy," in President Roosevelt's phrase, is still considered the most disastrous intelligence failure in American history.

Until the attack the U.S. military was unaware that the Japanese possessed a new type of aerial torpedo that could navigate the relatively shallow waters of Pearl Harbor. Nor did government officials have reliable information about the likely targets of a Japanese air attack; conventional wisdom at the time pointed to the Philippines as the probable site. Moreover, the fragments of information obtained by U.S. military intelligence that did point to Hawaii were never adequately analyzed and coordinated within the government; the president and other high officials were never given access, for example, to decoded intercepts of Japanese military communications that indicated that Pearl Harbor could be in jeopardy.[13]

With the establishment of the CIA by way of the National Security Act of 1947, President Truman hoped to improve the capabilities of the United States to anticipate security dangers. His objective was to upgrade the collection, analysis, and—especially—the interagency coordination and dissemination of information useful to policymakers as they dealt with world affairs. Above all, the goal was to have no more Pearl Harbors. At the time Truman gave little thought to counterintelligence or covert action; indeed, mention of these missions was omitted altogether from the National Security Act, although they would soon take on a life of their own as U.S.-Soviet hostilities deepened.

The Cold War sired and nourished strapping espionage bureaucracies in both the United States and the Soviet Union. Today, America's spy empire—the intelligence community—consists of thirteen major and several minor secret agencies. According to various newspaper accounts, the IC employs over 150,000 people and, in recent times, has spent some $28–30 billion a year.[14]

Beneath the president and the National Security Council (NSC) in the intelligence chain-of-command stands the director of Central Intelligence or DCI. This chief intelligence officer is in charge—titularly at least—of the entire secret government. (Appendix A provides a list of the seventeen men who have served in this position since 1947.) The DCI simultaneously heads "the Agency," as the CIA is called by insiders, and in this capacity is referred to as the DCIA (director of the CIA).[15]

The CIA is the best known of the secret agencies. Its headquarters are in the Washington, D.C., suburb of Langley, Virginia, in a campus-like setting along the banks of the Potomac River—known sarcastically by some intelligence of-

ficers outside the CIA as "Langley Farms."[16] The DCI has his main office on its seventh floor, but he also occupies a suite on the third floor of the Old Executive Office Building, or OEOB, next to the White House. The CIA is mainly responsible for the analysis of strategic information and has also been granted control over the planning and conduct of covert action. (Counterintelligence is a responsibility shared by all the intelligence agencies, in coordination with a new—and still inchoate—National Counterintelligence Center, established in 1994 in the wake of the Aldrich Ames spy scandal.) The CIA's organizational chart (as of 1995) is presented in figure 1.1.

The CIA's major companion agencies include the National Security Agency (NSA), located at Fort Meade, Maryland, responsible for codebreaking and electronic eavesdropping; the National Reconnaissance Office (NRO), with quarters in newly constructed buildings near Dulles Airport in the Virginia countryside and chartered to coordinate the development and management of surveillance satellites; the Central Imagery Office (CIO), in the Department of Defense (DOD), which supervises the photographic side of foreign surveillance; the Defense Intelligence Agency (DIA), also in the DOD and in charge of military intelligence analysis; and the four military intelligence services, each gathering tactical intelligence from all corners of the globe. Each of these entities is under the command of the secretary of defense (as well as the DCI—a sure prescription for blurred lines of authority) and as a result are considered the nation's military intelligence agencies.[17]

On the civilian side of intelligence stand (along with the CIA): the Bureau of Intelligence and Research (INR), at the Department of State; the FBI's intelligence units, housed within the Department of Justice; the Department of the Treasury, home of the Secret Service and the Internal Revenue Service, both of which have an intelligence component; and the Department of Energy's intelligence corps, which (among other duties) tracks the flow of fissionable materials around the globe.[18] Together, these military and civilian agencies comprise the largest organization for the production of information in the history of civilization (see figure 1.2).[19]

AN ENCOMPASSING VIEW OF INTELLIGENCE

Regardless of how the term is used—as product, process, mission, or organization—intelligence is widely considered America's "first line of defense."[20] The assumption behind this perspective is that sound choices for U.S. foreign policy depend on decisionmakers having the most accurate, complete, and timely information possible about the capabilities and intentions of other na-

Figure 1.1 The Office of the DCI and the Central Intelligence Agency

Figure 1.2 The United States Intelligence Community

tions or factions. This is not an easy assignment on a vast planet where nations keep their political ambitions closely veiled and hide their development of new weapons inside heavily guarded buildings and even, as in North Korea, in deep underground caverns.

At bottom the intelligence community, with its intricate worldwide network of mechanical and human spies, has but one overmastering objective: to safeguard the United States and its international interests. This can mean anything from promoting democracy to ensuring access to foreign oil and preventing internal subversion—an important mission of the domestically oriented intelligence agencies, like the FBI. To achieve these goals, it is first necessary to acquire and understand information about the potential threats and opportunities; consequently, reliable facts and analysis are seen by many scholars and government practitioners as the sine qua non of effective decisionmaking. "Every morning I start my day with an intelligence report," President Clinton has remarked. "The intelligence I receive informs just about every foreign policy decision we make."[21]

A former secretary of state has suggested why decisionmakers often display a healthy appetite for information of all kinds, including intelligence: "The ghost that haunts the policy officer or haunts the man who makes the final decision is the question as to whether, in fact, he has in his mind all of the important elements that ought to bear upon his decision, or whether there is a missing piece that he is not aware of that could have a decisive effect if it became known."[22]

The situation in the Persian Gulf in August 1990 provides an illustration of how vital intelligence can be to policy officers. No question pressed more heavily on those in the White House and the Pentagon during that month than the exact size and strength of the Iraqi military units that were headed south to invade Kuwait. An effective American response would have to rely substantially on accurate intelligence about the troop and weapons strength of the Iraqi forces. Drawing on a combination of intelligence sources (including the order-of-battle expertise of an Iraqi military defector), the CIA and the DIA quickly provided answers.

In this instance of "competitive analysis" the two agencies disagreed dramatically on the potency of the Iraqi military. It took another two months of data scrubbing before it became clear that the DIA figures had been based on outdated information from the Iran-Iraq war and consequently were inflated. Yet even in those frustrating instances where the secret agencies disagree, the debate that ensues gives a more reliable result than if leaders were able to turn to only one agency for an answer. Out of this particular interagency disagree-

ment came a useful cross-checking of sources and methodologies which eventually produced a highly reliable order-of-battle assessment. Regrettably, a president will not always have the luxury of waiting so long before dispatching troops into battle. Nor will the United States always possess the resources—even in more robust economic times—to provide intelligence support for every possible military contingency the country may face overseas. Even the idea (endorsed by the bottom-up review conducted by Secretary of Defense Les Aspin in 1994) of fighting simultaneously two so-called major regional conflicts (MRCs)—say, in North Korea and Iraq—would stretch American intelligence support and warfighting capabilities to the limit.

Defense Secretary William J. Perry, Aspin's successor, questioned the feasibility of the 2MRC concept in public hearings. "It's an entirely implausible scenario that we'd fight two wars at once," he conceded before the Senate Defense Appropriations Subcommittee in 1994.[23] Yet demands for intelligence support for military operations (referred to as SMO in the Pentagon) extend even beyond the prospect of two major wars. Intelligence support is needed for small-scale interventions (like Haiti and Somalia) as well as "Operations Other Than War" (OOTW in Pentagonese), which include dispensing military and humanitarian aid, staging counternarcotics operations, noncombatant evacuations (NEOs), and United Nations (UN) peacekeeping operations, as well as counterterrorism operations, interdicting weapons of mass destruction (WMDs), and assisting foreign forces.

Each of these activities stands to benefit from good intelligence support; and this is only the Pentagon's list. The civilians in the government who deal with foreign affairs have their own intelligence requirements, too, from information on trade matters to support at international environmental conferences—all tugging at the same finite resources. The tension between uniforms and suits—tactical intelligence for the military field commanders and strategic intelligence for the president and the rest of the civilian part of the government—lies at the heart of the current debate over future directions for American intelligence.

The president, as the commander in chief and the highest civilian officer in the government, is caught in this cross fire between contending intelligence requirements. Added to the complexity of the rival claims on the intelligence dollar is the fact that most of the time, happily, the United States is at peace. Yet when war comes, the nation must be ready. In the first instance, the president can tilt toward the civilian side of intelligence, using the assets of the intelligence community to gather and analyze information that may head off a war. In the second instance, however, he must tilt toward success on the battlefield,

with the fewest American casualties possible. (Zero-body-bag wars is the quixotic goal of some military planners in whose heads dance visions of remote-control, penny-arcade weapons.) These are quite different postures (despite some overlap); as a result, sorting out the nation's future intelligence needs is hampered by turf battles within the bureaucracy.

Given these multiple dimensions of intelligence, how shall it be defined? If one prefers a narrow dictionary definition, the idea of intelligence as product—*secret* information—is apt to be most satisfying. As we have seen, however, this perspective leaves aside a good many activities carried out by the secret agencies. For that reason, in this book I prefer a broader perspective. Regardless of one's favorite definition, the most important point is to have an understanding of what duties the secret agencies actually perform. In this spirit, one can say that intelligence has to do with a cluster of government agencies that conduct secret activities, including counterintelligence, covert action, and, foremost, the collection and analysis of information (from a mixture of open and covert sources) for the illumination of foreign policy deliberations.

THE METHODS OF INTELLIGENCE

Human beings have always needed information to secure their livelihood and their safety—the location of the best fishing stream, the site where firewood might be gathered, when deer herds were likely to appear. During the Cold War the presence of nuclear warheads and rapid-delivery systems held out for Americans—and perhaps for all humankind—the prospect of sudden extinction. This ominous condition made accurate information about the intentions and capabilities of the well-armed adversary, the USSR, more vital than ever.

In this current "information age" we are constantly bombarded by facts, opinions, speculation, rumor, and gossip from every direction. Television carries into our homes each night unsettling images of squalor and death from around the world (not to mention our own backyard). Computers draw us into an interactive milieu where e-mail gives, and expects in return, ever more rapid exchanges of information. The cellular telephone assures that a flow of information will follow us everywhere: into the car, the mall, the meetingplace. What effect has this rising tide of information—and its secret undercurrents we call intelligence—had on decisions made in the high councils of government?

Foreign policy decisions are preceded in most cases by the gathering and interpretation of information by government officials about the costs and benefits that may accrue to their nation from various options. In prehistoric times, people were touched by only small eddies of data about the world around them:

hints of changing weather in the cloud formations, the scent of game, the sound of a twig snapping at night that warned of an intruder. In our own time, American leaders stand in the middle of a deep and rushing stream of information from across the globe—from newspapers, computers, radio, telephone, and especially television. As Ronald Steel observed in 1995, "We would probably not be involved in any of these areas [Somalia, Rwanda, the Balkans] were it not for the power of television to bring the most horrifying images into the American living room."[24]

The form of some information that comes to the president and other top officials has changed little from the early days of the republic: whispers from the First Lady, ruminations over drinks in the Georgetown parlors, the counsel of confidants offered in the privacy of the Oval Office. Yet consider these dramatic changes: thousands of high-resolution satellite photographs arrive each day in the offices of intelligence analysts; data in the form of signals intelligence (SIGINT) pour into the receiving antennae at the NSA; live, ghastly pictures of the carnage in Rwanda and Bosnia fill the television screens in the White House and most every other house; a deluge of citizen opinion jams Internet terminals throughout the government, including the warrens of the Old Executive Office Building, where NSC staffers prepare their influential option papers on foreign affairs. The advance of technology has produced a downpour of information that falls relentlessly on intelligence officers and policymakers alike.

Information Collection

Sophisticated spy machines, designed for the purposes of broader and faster information collection, have exercised a fascination on those in public office. Over the years since 1947 the managers of the secret agencies have successfully promoted a steadily rising investment for technical intelligence, or TECHINT.

By definition TECHINT refers chiefly to IMINT and SIGINT. IMINT is the acronym for imagery intelligence, also called photographic intelligence (PHOTINT), electro-optical intelligence, or, in plain English, photography. SIGINT, also known as "special intelligence," encompasses the interception and analysis of communications intelligence (COMINT)—say, two drug dealers talking to one another via cellular telephones in Colombia—and electronic intelligence (ELINT), such as the electronic signals associated with radar jamming.[25]

Foreign radios, satellites, cellular telephones, and land-line and fiber-optic communications all are inviting targets for SIGINT collectors hoping to learn the intentions of adversaries. Electronic eavesdropping can be the key to avert-

ing war. For example, it could tip off the attack plans of a belligerent nation that might be countered by stepped-up diplomacy or a show of military strength. It may also save the lives of individual Americans abroad. Recently a U.S. ambassador was forced to plan an evacuation because of a civil war that was spreading through the country in which he was stationed. A SIGINT intercept disclosed that a team of assassins had learned of the proposed evacuation route and intended to slay the ambassador, his wife, and children. Warned of the trap, the ambassador and his family took a different route to the airport and escaped.

Another of the technical "ints" is MASINT, which stands for measurement and signature intelligence. MASINT exploits the physical properties of foreign targets (an enemy missile, for example) through the use of special technical sensors. These properties might include energy emitted from a nuclear warhead, mechanical noises, or telemetry intelligence (TELINT), the collection of data emitted by weapons as they are being flight-tested, which reveals their specifications.

Prior to the advent of the U-2 spy airplane in the 1950s, the most important TECHINT efforts against the Soviet Union came from radar sites in Turkey and Iran (collecting RADINT, or radar intelligence, a form of MASINT); from EC-135 and RC-135 aircraft lumbering along the perimeter of the USSR; and from camera-laden, unmanned balloons drifting across Soviet airspace. Some of the balloons made it to Japan and the Pacific, but most crashed somewhere in the vast Soviet territory.

The U-2 is an imagery collector and the most outstanding of the early TECHINT innovations.[26] Developed in an accelerated program to obtain reliable data on the extent of the feared "bomber gap," this sleek spyplane—the so-called Black Lady of Espionage—made its debut with a flight over the Soviet Union on July 4, 1956. A series of twenty-nine additional U-2 flights deep into the USSR during the late 1950s and early 1960 (brought to a halt for six months beginning on May 1, 1960, when the Soviets shot down over Sverdlovsk a U-2 piloted by Gary Francis Powers) provided IMINT impressive enough to persuade American leaders that the Soviets had far fewer long-range bombers than initially feared. The Bison and Bear aircraft simply were nowhere to be found in the anticipated numbers on Soviet airfields.

Evidence regarding the next alarm—a "missile gap," stemming from concern over a possible acceleration of the Soviet ICBM program—remained inconclusive.[27] Following the U-2 shootdown in 1960, President Dwight D. Eisenhower had promised his Kremlin counterpart, Nikita Khrushchev, that he would curb further U-2 flights over Soviet territory, so the answer to the missile debate would require a different approach: satellite photography from the

more secure confines of space. With a new sense of urgency, the government rushed forward with its nascent satellite program.

After a frustrating concatenation of technical disasters, in 1960 the United States at last placed a reliable surveillance satellite in space (Project CORONA). The first CORONA image, taken on August 18, 1960, was disappointingly fuzzy but clear enough nonetheless to discern a Soviet airfield at Mys Shmidta. Unfortunately, most of the satellite photos taken in 1960 were dark and difficult to read; during 1961, however, the spy cameras improved greatly, and their pictures of military installations in the USSR did indeed disclose the existence of a missile gap—but one that favored the United States.

By the 1970s America had launched several types of satellites into the heavens—some as big as a Mack truck. A few relied on electro-optical technology, others on infrared sensors and radar. Some circled the planet in a low elliptical orbit (LEO), others in a high elliptical orbit (HEO), and a few remained in a stationary posture over a single nation or region (achieved by orbiting in synchrony with the earth's own spin velocity, called geosynchronous orbit or GEO). The perigees and apogees ranged from less than one hundred to more than twenty-four thousand miles in space. Together, the constellation of satellites ("platforms") offered an exciting new TECHINT blend of collection cameras and sensors that allowed several perspectives of the same target.

Harold Brown, the secretary of defense during the Carter presidency, has commented on the value of this intelligence synergism:

> Our national technical means [NTM, the accepted euphemism at the time for satellites and other TECHINT machines] enable us to assemble a detailed picture of Soviet forces, including the characteristics of individual systems, by using information from a variety of sources. . . . We regularly monitor key areas of the Soviet ICBM test ranges. We monitor missile test firings with a wide variety of sensors: cameras taking pictures of launch impact areas; infrared detectors measuring heat from the engine; radars tracking ICBMs in flight; and radios receiving Soviet telemetry signals. . . . The use of multiple sources complicates any effort to disguise or conceal a violation.[28]

The technological advances were fairly steady and remarkable from 1956 to the 1980s, though always punctuated by setbacks. By 1963 the "Keyhole" or KH cameras (a generic term for spaceborne image collectors, just as "Talent" refers to cameras aboard aircraft like the U-2) could peer from remote space into newly dug Soviet missile silos. In the 1970s the "Rhyolite" generation of satellites tracked missile telemetry with ever greater accuracy and,

joined by its cohorts "Chalet" and "Jumpseat," achieved major breakthroughs in COMINT. The infrared and radar satellites of the late 1960s and the 1970s were especially important innovations because, unlike electro-optical photography, they are able to penetrate through cloud cover and the darkness of night (relying on star glow alone to provide the necessary definition). The KH-11 imagery satellite launched in 1976 presented as a gift to incoming president Jimmy Carter one of the greatest advances of all: real-time imagery of the USSR and other foreign targets. The main points of friction now were the processing and interpretation of the images, not their delivery to earth.

Into the 1980s the TECHINT wizards in the intelligence community and their colleagues in the private sector spun out more devices for watching American adversaries more closely. The speed with which data were moved from satellite platform to earth-bound photointerpreters accelerated, new cameras provided wider swaths of coverage, and engineers produced an expanded range of camera angles for greater comprehension of such matters as a missile's dimensions. Further, the lifespan of the satellites rose from a few days to months, then years; and the number of ground stations increased to process more rapidly the stream of data from space. Failed launches that so plagued the early days of the spy satellite program became a rarity.[29]

Spy satellites have their limits, of course. Despite their sophisticated phototechnology, they do not have x-ray vision and cannot see through roofs. Moreover, nations like Russia and China have learned how to track their orbits. Foreign regimes often halt their use of sensitive communications and telemetry testing and hide their weapons as the "birds" pass overhead. The North Koreans solved this problem by locating their most sensitive weapons facilities underground. Yet the reconnaissance satellites have contributed in a major way to making the world more transparent and therefore safer from the dangerous hysteria that has frequently arisen over the possible machinations of unseen enemies.

The recruitment of human spies who can steal secrets from vaults or overhear important conversations among foreign adversaries is still a high priority for America's secret agencies. During the Cold War, however, spending on TECHINT far outdistanced spending on old-fashioned espionage (known as human intelligence or HUMINT).[30] A strong proclivity exists among those who make budget decisions for national security to focus on warheads, throw weights, missile velocities, fuel range, and the specifications of spy satellites—things measurable.

Briefings to legislators who hold the intelligence purse strings are in-

eluctably accompanied by state-of-the-art visual aids: flashy four-color slides ("grabbie graphics," a CIA specialty), videotapes, and CD-ROMs. They portray satellites outfitted with all the latest bells and whistles, and clad—like the Great Gatsby's famous motorcar—in shiny metal and glass that mirror a dozen suns as they rotate the earth.

Unlike the traditional human spy (whose identity is a tightly held secret—no pictures allowed), the spy satellite has a tangible presence. Not only can the DCI show it off with slides during closed-door hearings, he can also pass around the photographs it has produced: startlingly detailed displays of the enemy's missile sites and tank deployments; infrared tracings of "hot" radioactive material flowing through the pipelines of a weapons factory deep within the territory of a nation whose leaders claim that the facility is merely a pharmaceutical laboratory; radar impressions, taken at night or through cloud cover, of fighter aircraft bearing missiles on a remote runway. Satellite cameras neither lie nor defect to the enemy, while their human counterparts (recruited by trolling bars in foreign capitals) have been guilty on both counts. Technical intelligence is, in a word, *trusted* by collectors, analysts, and policy officers alike.

One result of this growing reliance on TECHINT has been the acquisition of more and more information collected at ever faster rates. And the intelligence agencies have worked to improve the mobility of the collection platforms and achieve greater flexibility in reorienting their instrumentation toward fresh targets at a moment's notice. The aspiration is to create a "surge capacity" that will allow the quick shifting of platforms toward whatever newly threatening targets may suddenly arise—Somalia today, Suriname tomorrow.

Once information is captured by an intelligence platform, the ability to send the data hurtling back to Washington for processing has also been tremendously accelerated. Film from the early CORONA satellites had to be catapulted from space back toward earth, then plucked out of the ether by ponderous C-119 and C-130 aircraft—which sometimes failed to snare the precious eighty-four-pound capsules as they descended by parachute toward the Pacific Ocean.[31] The data were flown home while fidgeting photointerpreters awaited the next batch of black-and-white images. Now, as a result of modern digital communications, the trip from satellite to Stateside takes only moments.

Recent technological advances have improved overt information collection too. Intelligence officers are turning increasingly toward new computer-based information search tools (like Lexis-Nexis) and the daily reporting of information from around the world by private companies (like Oxford Analytica),

along with the burgeoning use of the Internet, facsimile machines, and e-mail. Academe, business, the media, and government are busy harnessing these powerful tools of information management.[32] At the CIA, an impressive system called ROSE (Rich Open Source Environment) allows agency analysts to tap into more than two thousand full-text on-line journals, from the *African Economic Digest* to the *Yale Law Review*.

Recently a program called INTELINK, based on Internet technology, has been introduced as a means of spinning the government's secret agencies into at least a limited web of classified-information exchanges, to be supplemented eventually with access to the ROSE materials. After a number of false starts, the infrastructure for modern computer information management is growing steadily and drawing the analytic side of the secret agencies closer together than ever before. The CIA now has secure e-mail facilities to maintain contact with its stations around the world; and fax intelligence, sent over secure lines, has become a favorite means by which intelligence officers communicate with policymakers.

In spite of efforts by the intelligence agencies to keep up with technological advances in communications, close observers suggest that in some respects they have fallen behind the private business sector—and even some college dormitories—in desktop information management. Inside the State Department, for instance, the INR's e-mail system is self-contained (for security purposes). This prevents intelligence officers from sending classified e-mail to the diplomats they are supposed to support—not to mention adding to INR's sense of isolation in the building. Policy officers in the OEOB, an antiquated (if charming) structure, are similarly without secure e-mail connections to the intelligence agencies; NSC staffers must hike over to the Situation Room in the basement of the White House to read classified cable traffic. Impressive recent progress aside, the IC's communications infrastructure still has a long way to go before analysts are connected to each other, to collectors, to open-source data banks, and to the policy community in a sophisticated network of work stations.

While technology has undoubtedly made the task of information collection more efficient, human beings continue to play a vital role. The case officer engaged in HUMINT overseas must carry out the sensitive agent-recruitment operations abroad and attempt to calculate the intentions of foreign leaders.[33] For as Ephraim Kam has emphasized, an adversary's most important secrets "often exist in the mind of one man alone . . . or else they are shared by only a few top officials."[34] This kind of information is accessible, if at all, only to an in-

telligence officer with ties to someone inside the closed councils of the target government.

"No matter how good our technology, we'll always rely on human intelligence to tell us what an adversary has in mind," President Clinton has acknowledged. "We'll always need gifted, motivated case officers at the heart of the clandestine service. We'll always need good analysts to make a clean and clear picture out of the fragments of what our spies and satellites put on the table."[35] In the early days of tracking the Soviet target, when TECHINT was still in its infancy, HUMINT sources—even though good ones were rare—sometimes proved of great value. Colonel G. A. Tokaty-Tokaev, for example, defected to the United States in 1948 with useful information on the state of the Soviet ICBM program; and Colonel Oleg Penkovsky's espionage on behalf of the United States and Great Britain during the 1960s was an even greater windfall.

During the Carter administration the nation was reminded again of the importance of HUMINT when Iranian student militants took American diplomats hostage inside the U.S. embassy in Tehran. In planning a rescue operation, satellites could provide excellent eagle-eye pictures of Tehran but could not see inside the embassy or find precisely where the hostages were being kept. "We had a zillion shots of the roof of the embassy and they were magnified a hundred times," remembers one of the rescue planners. "We could tell you about the tiles; we could tell you about the grass and how many cars were parked there. Anything you wanted to know about the external aspects of the embassy we could tell you in infinite detail. We couldn't tell you shit about what was going on inside that building."[36]

The question of intelligence targeting further illustrates the cardinal role of the human being in matters of intelligence gathering. The most important targets for the intelligence community are those nations or factions that present a danger, or potential crisis, for the United States (so-called Tier 0 nations in current jargon). Yet while North Korea, Iraq, Iran, and other "rogue states" are easy enough to place into this category, will U.S. leaders have the sagacity to anticipate what other targets should be at the top of the list in the immediate—let alone the long term—future?

"When I became Secretary of Defense [in 1993], I served several months without ever giving Rwanda a thought," recalled Les Aspin. "Then, for several weeks, that's all I thought about. After that, it fell abruptly off the screen again and I never again thought about Rwanda."[37] Knowing where to position the nation's high-tech intelligence platforms is not a simple task, since countries have an annoying habit of leaping suddenly from Tier 4 (the outer fringes of the tar-

geting list) to Tier 0—Grenada, Panama, Kuwait, Yugoslavia, and Somalia, among other recent "shooting stars" or "flavors of the month," as analysts call them.

Information Processing

The next step in the intelligence cycle is called processing, which involves the refinement of freshly gathered, "raw"information into a form that is more easily studied by intelligence analysts. Coded data are "decrypted," foreign languages translated, and the focus of photographic material sharpened to provide maximum resolution of the imagery. Advances in technology have made a major contribution here too. State-of-the-art computer methods make foreign diplomatic codes more vulnerable to unraveling by cryptographers at the NSA and help sort out the elaborate calculations involved in converting radar images into digital data.

Here again technology rubs up against the human dimension of intelligence. The surveillance satellites—often described as gold-plated "vacuum cleaners" in the sky—yield far more data than the government has the resources to process. "The information coming down from these [satellites] is just going to choke you," laments the physicist Jerry Nelson. "You can't buy big enough computers to process it. You can't buy enough programmers to write the codes or to look at the results to interpret them. At some point you just get saturated."[38] Near the end of the Cold War the NSA reportedly processed only about 20 percent of the SIGINT it collected; recently another NSA official estimated that the figure has dropped to about 1 percent—although new techniques have improved (though by no means perfected) the NSA's ability to focus on the most important 1 percent.[39] Little wonder that a recent NSA director, Vice Admiral J. M. ("Mike") McConnell, was often heard declaiming, "I have three major problems: processing, processing, and processing."[40]

Another processing headache is language translation. The shortage of qualified linguists available to the secret agencies remains a serious deficiency, particularly with respect to the more exotic languages. Moreover, the technology to machine-read and translate texts reliably and quickly from foreign languages into English will not reach high levels of proficiency for decades—although it is reasonably good now for some limited tasks where the language is precise, such as translating Russian scientific texts.

Information Analysis

Technology has also aided the third crucial step in the intelligence cycle: analysis. At this stage the experts assess what the unevaluated intelligence ac-

tually means for the security of the United States. The objective is to produce fully interpreted intelligence based on a blend of covert collection products from all the secret agencies ("all-source intelligence") and open-source materials. The output of intelligence materials has been prodigious. In 1994, for example, the DI alone produced over thirty-five thousand intelligence reports of one kind or another, from oral briefings to encyclopedic studies.[41]

The written form of finished intelligence may be either an intelligence report or—the crown jewel of community-wide analysis—a full-blown National Intelligence Estimate (NIE). In both cases the focus may be on a single foreign country or a specific topic (say, Iraqi oil production).[42] In contrast, the intelligence product may also consist of short, up-to-the-minute reports known as "current intelligence." These can take the form of special intelligence reports (crisp, highly focused papers no longer than three pages), intelligence memoranda (five-to-seven pages), or, in sharply abbreviated form ("in-briefs"), one to several paragraphs in the prestigious *PDB* or one of several other intelligence "newspapers."

According to a recent unclassified CIA document, "hundreds of reports derived from SIGINT, imagery, and human sources are sent to consumers [policy officers] and other producers [fellow analysts] each day."[43] Interviews with intelligence managers conducted in 1994 indicate that a majority of the papers written by the DI are foreign leadership analyses, chiefly personality profiles of political and military elites.

For decisionmakers, the favorite product from among this extensive menu is no doubt current intelligence. "Research reports [like the lengthy NIEs] work their way from the in-box to the burn bag unread," concludes an INR analyst ruefully. Why? "Because consumers don't have time to read them," the analyst continues. "The demands today are for the quick report and the quick answer—'bumper sticker' or 'time-bite' intelligence."[44] This same analyst reports that at INR the number of extensive research papers has plummeted over the past decade from 250–300 to just fifteen a year.

Some policy officers prefer "reports" that are briefer still: the raw intelligence alone. "I would ask for some of the raw data which was behind the reports," Dean Rusk once recalled, "so I could make my own check."[45] At the NSC staff level a former senior aide has said, "When I wanted intelligence, I went straight to the Sit [Situation] Room and read the raw cable traffic coming in from overseas."[46]

Other policymakers prefer not to read any intelligence whatsoever, raw or evaluated; they rely instead on spoken communication. Commenting on the widespread use of oral intelligence briefings, Allen E. Goodman of George-

town University wryly remarks that among policymakers, "some don't read, some won't read, and some can't read."[47] About one-third of the "products" created by DI analysts are oral briefings[48]—mainly presented to policy officers in the executive branch but increasingly to members of Congress as well. Now and then the briefings are delivered on the run down the corridors of power, as VIPs rush to the next meeting, or in the back seats of limousines on the way to Washington National Airport.

The oral briefing, despite its obvious shortcomings, plays a vital part in the intelligence cycle. "Estimation is more an oral than a written process," a chairman of the National Intelligence Council (NIC) has explained. "It starts with oral contacts between NIOs [National Intelligence Officers, senior analysts in the intelligence community assigned to the NIC] and policy makers, to find out what's on the policy maker's mind. Then it can take various written forms: an NIE, a two-page update on an earlier NIE, a short NIC memo of two or three pages. And it ends in an oral process, with the NIO briefing the policy maker on the key conclusions, because they're probably not going to have read the written report."[49]

Intelligence managers value the oral briefing highly—unlike many analysts, who prefer the opportunity to work on carefully nuanced written papers that display their expertise and allow them more room to hedge. "The situation we find the best," declares a former CIA manager, "is . . . when one of our substantive officers sees the president every day for a period, however brief, to get the intelligence [to the decisionmaker] and receive his reaction to it, including tasking for the next day."[50] This way the intelligence manager knows for certain that the product has reached the intended consumer instead of the circular file, and he or she can learn immediately what information the policymaker—ideally, the president—wants next.

Gerald R. Ford and, even more so, George Bush accepted this approach, for the most part. Some presidents, though, have refused oral briefings, preferring short written summations. Richard Nixon cut off DCI Richard Helms from the Oval Office after the director had enjoyed good access during the Johnson presidency; Helms remembers Nixon as "the ultimate loner."[51] Ronald Reagan, a former screen star, showed an enthusiasm for intelligence presented on videotape. Whether current intelligence, raw intelligence, oral briefings, or intelligence "movies," the declining emphasis on in-depth research holds a danger for the future. The intellectual resources stored by the secret agencies may simply dry up. "Long-term research is putting money into the bank," says former DCI Robert M. Gates; "current analysis is taking money out of the bank."[52]

By all accounts the secret agencies provide some of the best forums in the

government for the analysis of international events. According to one experienced government official, "Intelligence analysts—essentially DI analysts—do 90 per cent of the analysis of the USG [United States Government] on foreign affairs."[53]

Further, regardless of all the help that machines have provided in manipulating data and crafting eye-catching graphic displays, the analytic process remains vitally dependent on the experience and intellectual abilities of the men and women preparing the written reports and delivering the oral briefings. Yet, does the analyst have the requisite skills to make accurate forecasts? Are the right experts available to give a full and timely response to the policymaker's request for an assessment of some foreign event? How deep-keeled is the analyst's knowledge of the country, or the circumstance, he or she is attempting to evaluate? Too few analysts have spent adequate recent time in the countries they are expected to understand. How many intelligence officers preparing reports for the NSC have lived in Somalia or Rwanda, Haiti or Iraq?

Moreover, the analytic process is replete with disputes over which of several competitive interpretations of "the facts" ought to be forwarded to the next level of the bureaucracy before going on to the White House. In the formal estimating process by which NIEs are produced, analysts have an opportunity (if their managers see fit) to register their dissent in the form of a footnote or, during the Clinton administration, in the text itself. Technology plays a role here too, as Lawrence Freedman shows. "As a profession, intelligence analysts are dedicated empiricists with a shared respect for certain types of 'hard' evidence, sufficient to force them to acknowledge it even if it contradicts strongly-held beliefs," he writes. "Such evidence is that which comes from technical collection programs, such as radar and satellites. Other evidence will have varying degrees of 'softness' and its reliability may be disputed. . . . The more estimators have to guess, speculate, infer, induce and conjecture in order to reach a conclusion, the greater the possibility of open disagreement."[54]

Most troubling is when the DCI or another manager decides to bury the work of an analyst because he finds his own interpretation of events more compelling, or because he hopes to curry favor with the White House by providing "intelligence to please." At times the DCI has been an ideologue who wants the intelligence community to shape its interpretations to match his own worldview. Robert Gates has testified that as deputy DCI he watched his boss, William J. Casey, "on issue after issue sit in meetings and present intelligence framed in terms of the policy he wanted pursued."[55]

For the most part, though, DCIs—like the analysts below them in the intelligence hierarchy—have exercised a professionalism that wards off tempta-

tions to distort intelligence. "Know the truth and the truth shall make you free" is the CIA's motto, and it is taken seriously by virtually all of the men and women who enter the analytic side of the profession. Thus, the recommendation of a well-regarded former DDCI is valid most of the time: "You have to have faith that the CIA's professionals are strong enough to make straight calls."[56]

Information Dissemination

Technology has had a major effect as well on the last phase of the intelligence cycle: the dissemination of information to the policy officer—the consumer of intelligence. Stewart A. Baker, a former intelligence official, is not alone in his conclusion that from Pearl Harbor on, "the intelligence failures that hurt the worst have not been those of collection but rather those of dissemination."[57]

To start with a positive case, Operation Desert Storm in 1991 provides a vivid example of swift and reliable intelligence support to the consumer. American surveillance satellites sensed the Iraqi anti-aircraft radar the moment it was activated and relayed that information rapidly to waiting fighter pilots and cruise-missile commanders. The word soon spread in Baghdad that it was suicidal to flip the "on" switch inside a radar facility, as moments later the person at the switch would be annihilated by American F-117 aircraft or self-propelled Tomahawk cruise missiles.

The "dissemination architecture" for intelligence during the Persian Gulf War was by no means flawless, however. In the field the military had fourteen different kinds of receiving devices for incoming intelligence, only two of which were compatible.[58] This lack of battlefield "connectivity" no doubt contributed to the frustrations later vented by General Schwarzkopf, who was unquestionably correct in this postmortem: "We just don't have an immediately responsive [imagery] intelligence capability that will give the theater commander near-real-time information that he personally needs to make a decision."[59]

In the aftermath of the Gulf War, General James R. Clapper, Jr., the talented DIA director, concentrated his attention on making improvements in the dissemination of battlefield intelligence. His objective was the "prompt delivery to all combat commanders, regardless of echelon, of the 'pictures, not reports' they tell us are essential to accomplishing their mission."[60] High-tech planners in the intelligence community foresee a time in the near future when all satellite and aircraft IMINT and SIGINT will be downlinked to vans in the backlines of the battlefield, where the processing and dissemination of data will be

carried out close to the soldiers—not back in Washington. In General Clapper's vision, "the ultimate ideal is to have a constant God's-eye view of the battlefield. Anywhere, anytime, all the time."[61] One must wonder, however, about the practicality—not to mention the expense—of staring down on Earth as if one were God.

Whatever its shortcomings, the flow of information from sensor-to-soldier during Operation Desert Storm set a new benchmark for intelligence achievement in support of the fighting men and women. Indeed, the dissemination of information to distant battlefields has proven easier in some respects than across the few miles that separate the intelligence agencies from the White House and the National Security Council.

INFORMATION AND THE POINT OF DECISION

At some point a decision must be made. Until then, technology contributes mightily to the production of the richest stream of information, laced with secrets, ever enjoyed by a nation's leaders. At the moment of decision, however, statecraft becomes paramount, and all the sophisticated technology of a modern superpower is to little avail.

As officials prepare to deliberate on foreign policy, often they are too busy to absorb new information (let alone deep analysis); or their ideological lenses may distort the information that does reach them. Sometimes the problem is mutual ignorance: the intelligence officer is unsure what the decisionmaker really wants, and the decisionmaker is unaware of what the intelligence officer has to offer. As a former government official recalls, when he was on the NSC staff in 1989–90, he "did not read a single [National Intelligence] Estimate. Not one." He explains why: "DI analysts did not have the foggiest notion of what I did, and I did not have a clue as to what they could or should do."[62] Only years later, as a participant in arms control negotiations (a CIA forte), did he discover how a close working relationship with intelligence officers could prove beneficial.

Among the hazards found at the intersection between information dissemination and decision is the trap of intelligence to please—the politicization or "cooking" of intelligence, in which the facts are slanted to suit the political needs of the current administration. As DCI, Richard Helms reportedly changed an estimate on Soviet military intentions at the urging of a Nixon administration official. He is said to have gone along with the Pentagon's position on Soviet first-strike preparations, despite contrary views among analysts within the CIA, because "an assistant to [Secretary of Defense Melvin] Laird

informed Helms that the [views of the CIA's analysts] contradicted the public position of the Secretary."[63]

As a result of intimidation, good information sometimes never even makes it to the table where decisions are made in Washington. "Nothing permeates the Cabinet Room more strongly than the smell of hierarchy," Peter Wyden remarks in his study of why DI analysts capitulated to the views of more senior government officials during deliberations over the proposed Bay of Pigs operation in 1961.[64] Policymakers in the Kennedy administration and their allies in the CIA's Operations Directorate (some of whom enjoyed the advantage of a Georgetown *bon vivant* relationship with the president) were so intent on toppling Castro that DI analysts convinced themselves that any discouraging prognostications—and they had more than a few—would not only have been fatuous but would also have been sharply resented and would have threatened their careers.

According to an expert on organizational behavior, this tendency to "*get along* with others and *go along* with the system is preferred [in all government bureaucracies]."[65] Steve Chan has discerned this conformist instinct inside the secret agencies. "Like other bureaucrats, intelligence analysts have to conform to the regime's basic views about the nature and morality of international relations if they wish to be treated as 'responsible' and 'serious,'" he writes. "Therefore, they refrain from asking the really 'tough' but crucial questions such as [during the Cold War] the aggressiveness of the Soviet Union, the morality of the Vietnam War, and the validity of the 'domino theory.'"[66]

The attempt to ensure that policy officers appreciate and understand information provided to them by the intelligence agencies, without misperceiving or otherwise distorting its meaning, presents another challenge. At times those in power will embrace intelligence only if it conveniently corresponds to their existing beliefs and ideologies, rejecting the rest. They quickly learn, observes a former INR director, "that intelligence can be used the way a drunk uses a lamppost . . . for support rather than illumination."[67]

The Eisenhower administration reportedly discouraged any assessments from the intelligence community "as to Soviet policy motivation that departed from the implicit stereotypical cold war consensus"—especially the hardline stance advocated by Secretary of State John Foster Dulles.[68] Former DDI Dr. Ray S. Cline has chronicled the unwillingness of the Johnson and Nixon administrations to accept the CIA's discouraging reports on the likelihood of an American victory in the Vietnam War.[69]

The rejection of objective intelligence became particularly controversial during the Reagan administration. The White House is said to have dismissed

the conclusions of intelligence analysts who called into question the administration's views: that Syria was merely a puppet of the Soviet Union, or that Nicaragua aggressively exported arms to Marxist guerrillas throughout Central America; that a Soviet oil pipeline to Western Europe would significantly increase the vulnerability of U.S. allies to Soviet pressure; that the shooting down of a South Korean passenger airline in 1983 was an intentional murder of civilian passengers rather than a mistake made by a Soviet fighter pilot who thought it was a spyplane; and that the assassination plot against Pope John Paul II in 1984 had been concocted in Moscow.[70]

The danger of distortion by policymakers is thought to be greatest with political intelligence. On technical matters—military weapons and other "difficult" scientific or economic subjects—the policymaker is more inclined to accept the judgment of intelligence experts. "Hardware [weapons] estimates . . . have traditionally been first in acceptance and impact," reports an intelligence official.[71]

Wishful thinking is another form of self-delusion that can cause a policy officer to ignore or distort intelligence. A senior CIA officer likes to tell of the man who bought an expensive new barometer. He took it home only to discover the needle was stuck on "Hurricane," yet there had not been a hurricane for years in his part of the country, and it was perfectly sunny outside. He shook the barometer gingerly and tapped on the facing. No movement. The man sat down at his desk and wrote a scathing letter of rebuke to the manufacturer. Then he left home on a trip. When he returned, the barometer was gone. So was his house.

Ego defense further complicates the use of intelligence. James Thomson's reflections on decisionmaking during the Vietnam War emphasize "the central fact of *human ego investment*. Men who have participated in a decision develop a stake in that decision. As they participate in further, related decisions, their stake increases."[72] Fresh intelligence assessments that call into question their basic views are unlikely to be well received by individuals in leadership roles—especially when they may have already sent thousands of soldiers to an early grave to implement their policies. Yaacov Vertzberger's analysis of India's failure to anticipate a 1962 Chinese invasion concludes similarly: "The need to prove methodically, all through the period in question, that the policy pursued had been the right one, and that the level of aspirations had been realized, made it necessary [for Indian policymakers] to ignore any information that contradicted this."[73]

Even if no distortion of information occurs, have a nation's leaders sufficient time to evaluate carefully the implications of the reports placed before them by the intelligence agencies? A profile of Secretary of Defense Caspar W.

Weinberger, who served in the Reagan administration, reported him "swamped," "overwhelmed," "left with not enough time to think forward."[74] Another study of the highest decision echelons in America during the Vietnam War found widespread "executive fatigue," which had a deadening effect on "freshness of thought, imagination, a sense of possibility and perspective. . . . The tired policy maker becomes a prisoner of his own narrowed view of the world and his own cliched rhetoric."[75] Not exactly a hospitable environment for the absorption of fresh intelligence insights.

Time's winged chariot pulls leaders toward brief forms of current intelligence, as seen in a description of the intelligence cycle offered by a former head of the NIC. "[The analyst must] mine the great lode of outside material, compress it, add the clandestine nuggets, and put it in a form that is usable to policy makers. If you can't get it to them in three pages or three minutes, they're not going to get it."[76]

Perhaps nothing so underscores the importance of the human dimension in the making of foreign policy decisions as the fragile relationship between the producer and the consumer of intelligence. Dialogue, rapport, trust—here are the girders that attempt to bridge the gap between the technology-driven intelligence cycle and the deeply human point of decision. Ambassador Robert D. Blackwill advocates this widely endorsed prescription: "The key [to the success of intelligence] is getting close enough to the individual policy maker to find out what he needs."[77]

No doubt many a fine analytic report has died in the in-box simply because the requisite bonds of trust had never been established between the worlds of the intelligence officer and the policymaker. A balance between the two can be hard to achieve, though, because in establishing rapport the intelligence officer must at the same time avoid the trap of intelligence to please—the politicization of intelligence, the unforgivable sin.

Every nation—large or small, rich or poor—faces these intelligence/decision traps. What can be done to avoid them? The answer has roots in ancient philosophy: select leaders (and intelligence officers) imbued with wisdom and a love of truth—the human virtues, which continue to lag far behind our technological achievements.

The nation's secret agencies are but one source of information competing for the ear of the policy officer.[78] Friends and confidants, television news, radio talk shows, influential newspapers, lobbying groups, opinion polls, public and private pronouncements of foreign leaders, even at times astrologers—this information stream that feeds into the government is wide and deep.

Intelligence from the secret agencies can be a dominant current in this stream, notably on matters where they enjoy special access to covert information and can proffer a unique, synergistic mix of SIGINT, IMINT, MASINT, and HUMINT. With respect to weapons proliferation, terrorism, or events inside closed regimes, the clandestine services often have more reliable intelligence (based on covert sources inside an adversary's government) than the media or academe. On other occasions the reverse may be true. "Determining the situation in Rwanda [in 1994] was best ascertained from the people on the scene," writes a former NRO director. "Analyzing its significance and its relevance in that part of the world was best accomplished by scholars and others dedicated to understanding that society and that area, not members of the current intelligence community, which was developed to address quite different cultures."[79]

The secret agencies are likely to be considered by some policymakers a national asset of the highest order, but most think of them simply as one of many tributaries feeding the information stream—sometimes helpful, sometimes not. And for a few—usually those who have never taken the time to discover the value of intelligence—the secret government will be discounted altogether, as if its bed had run dry, leaving nothing to offer that could not be found in the nation's best newspapers.