THE US INTELLIGENCE COMMUNITY

"The authoritative survey of the American cloak-and-dagger establishment."
—*Washington Post Book World*

SEVENTH EDITION

JEFFREY T. RICHELSON

THE U.S. INTELLIGENCE COMMUNITY

SEVENTH EDITION

THE U.S. INTELLIGENCE COMMUNITY

JEFFREY T. RICHELSON

Routledge
Taylor & Francis Group
New York London

First published 2016 by Westview Press

Published 2018 by Routledge
711 Third Avenue, New York, NY 10017, USA
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

Routledge is an imprint of the Taylor & Francis Group, an informa business

Library of Congress Cataloging-in-Publication Data

Richelson, Jeffrey.
The U.S. intelligence community / Jeffrey T Richelson. -- Seventh edition.
pages cm
Includes bibliographical references and index.
ISBN 978-0-8133-4918-3 (paperback) -- ISBN 978-0-8133-4919-0 (e-book) 1. Intelligence service--United States. I. Title.
JK468.I6R53 2015
327.1273--dc23

2015005759

ISBN 13: 978-0-8133-4918-3 (pbk)

CONTENTS

List of Illustrations, xi
Preface, xv

1 Intelligence 1
Intelligence Activities 2
The Intelligence Cycle 3
Varieties of Finished Intelligence 4
Targets 7
The Utility of Intelligence 9
The Intelligence Community 12
Notes 13

2 National Intelligence Organizations 18
Central Intelligence Agency 18
National Security Agency 31
Special Collection Service 37
National Reconnaissance Office 39
National Geospatial-Intelligence Agency 44
National Underwater Reconnaissance Office 49
Notes 49

3 Defense Department Intelligence: The Defense Intelligence Agency 59
History and Current Charter 59
Overview 63
Directorate for Operations 65
Directorate for Science and Technology 68
Directorate for Analysis 70
Regional Centers 73
Directorate for Intelligence 74
National Media Exploitation Center 75
Notes 75

4 Military Service Intelligence Organizations 81
Army Intelligence Organizations 82
Navy Intelligence Organizations 88
Air Force Intelligence Organizations 94
Marine Corps Intelligence Organizations 104
Coast Guard Intelligence Organizations 107
Notes 111

5 Civilian Departmental Intelligence Organizations 118
Department of State Intelligence 118
Department of Energy Intelligence 121
Department of the Treasury Intelligence 124
Department of Homeland Security Intelligence 128
Federal Bureau of Investigation 133
Drug Enforcement Administration Intelligence 140
Notes 144

6 Unified Command Intelligence Organizations 152
Africa Command 155
Central Command 156
European Command 158
Northern Command 162
Pacific Command 165
Southern Command 166
U.S. Special Operations Command 168
Strategic Command 174
Transportation Command 176
Notes 177

7 Geospatial Intelligence Collection, Processing, Exploitation, and Dissemination 184
Collection 186
Processing and Exploitation 205
Dissemination 209
Notes 212

8 Signals Intelligence and Cyber Collection 223
Targets 225
Space Collection 228
Airborne Collection 235
Ground-Based Remote Collection 241
Embassy and Consular Intercept Sites 243
Clandestine SIGINT 244
RAMPART, MUSCULAR, and PRISM 250
Surface Ships 251

Underwater Collection 252
Notes 254

9 Measurement and Signature Intelligence 266
Space Collection 267
Airborne Collection 275
Ground Collection 278
Seaborne Collection 283
Undersea Collection 285
Notes 288

10 Space Surveillance 296
Dedicated SSN Sensors 299
Collateral Sensors 303
Contributing SSN Sensors 305
Additional Space Surveillance Capabilities 308
Notes 311

11 Human Intelligence 318
Officers and Diplomats 320
Agents and Assets 323
Defectors and Émigrés 328
Detainees and POWs 332
Travelers and DOD Personnel 337
Notes 338

12 Open Sources, Site Exploitation, and Foreign Materiel Acquisition 346
Open Sources 346
Site Exploitation 355
Foreign Materiel Acquisition 359
Notes 363

13 Cooperation with Foreign Services 370
Geospatial Intelligence Cooperation 372
Signals Intelligence Cooperation 375
Measurement and Signature Intelligence Cooperation 383
Space Surveillance Cooperation 384
Human Intelligence Cooperation 386
Open Source Intelligence Cooperation 388
Counterterrorism Cooperation 389
Counternarctotics Cooperation 393
Analysis and Data Exchange 394
Notes 396

14 Analysis 406
Analysts 406
Analytical Techniques 407
Current Intelligence 408
Warning Intelligence 415
Estimates 415
Reports and Studies 418
Leadership Profiles 421
Reference Documents and Databases 422
Domestic Intelligence Analysis 426
Notes 429

15 Counterintelligence 438
The Foreign Intelligence Threat 439
Investigations 443
Collection 444
Evaluation of Defectors and Agents 450
Research, Analysis, and Production 453
Disruption and Neutralization 457
CI Functional Services 459
Notes 460

16 Covert Action 468
Afghanistan 473
GREYSTONE 474
Iran 476
Libya 479
Pakistan 479
Somalia 481
Syria 483
Yemen 484
Notes 485

17 Managing National Intelligence 492
The President, the National Security Council, and the President's Intelligence Advisory Board 493
Director of National Intelligence and Deputies 497
Committees, Boards, and Councils 499
Intelligence Community Directives 501
National Intelligence Program 502
National Intelligence Management Council 503
National Intelligence Council 508
National Counterterrorism Center 511
National Counterproliferation Center 514

National Counterintelligence and Security Center 515
Cyber Threat Intelligence Integration Center 516
Notes 517

18 Managing Defense Intelligence 523
The USD (I) 523
Military Intelligence Program 525
The Military Intelligence Board and Defense Intelligence Space Threat Committee 528
Defense Warning Council 528
Defense Open Source Council 529
JCS Reconnaissance Operations Division 529
Defense Intelligence Officers 532
DOD and Service Directives and Instructions 533
Notes 535

19 Managing Intelligence Collection, Covert Action, and Information Access 538
Managing Satellite Imaging 538
Managing SIGINT 540
Managing HUMINT 546
Managing Covert Action 549
Managing Information Access 551
Notes 563

20 Issues 568
Spying All Over the World 569
Fighting Terror 570
Bulk Collection 573
Secrecy, Transparency, and Leaks 574
Congressional Oversight 576
A Government-Wide Problem 578
Notes 581

Acronyms and Abbreviations, 585
Index, 595

LIST OF ILLUSTRATIONS

TABLES

5.1 Main Legal Attaché Offices and Areas of Responsibility 138
6.1 Description of Activities Assigned to U.S. Special Operations Command 170
7.1 Targets of U.S. Imagery Satellites, 1990–2014 192
7.2 Location of P-3C VP Squadrons 199
7.3 Joint Imagery Interpretation Keys 207
7.4 Resolution Required for Different Levels of Interpretation 208
8.1 Unmanned and Manned SCS Locations 245
8.2 Clandestine SIGINT Against Diplomatic Targets 248
9.1 MASINT Mission Areas 268
16.1 Notable Deaths Due to Drone Campaign Attacks in Pakistan 482
17.1 NSCIDs Issued on February 17, 1972 495
17.2 Intelligence Community Directives 504
17.3 Budget for NIP Programs 506
19.1 U.S. Signals Intelligence Directives 542
19.2 Exceptionally Controlled Information (ECI) Compartments and Classification Levels 556
19.3 Overhead Imagery System Code Words 560
19.4 SIGINT Satellite Code Words 560

FIGURES

1.1 The Execution of Imam Khomeini's Order (EIKO) International Financial Network 6
2.1 Organization of the Central Intelligence Agency 21
2.2 Probable Organization of the National Clandestine Service 25
2.3 Organization of the National Security Agency 35
2.4 Organization of the NSA Signals Intelligence Directorate 35
2.5 Organization of the Information Assurance Directorate 37
2.6 Organization of the Special Collection Service 39
2.7 Organization of the National Reconnaissance Office 43

2.8 Organization of the National Geospatial-Intelligence Agency 48
3.1 Organization of the Defense Intelligence Agency 64
4.1 Organization of the Deputy Chief of Staff, G-2 83
4.2 Organization of U.S. Army Intelligences and Security Command 85
4.3 Organization of the Office of Naval Intelligence 90
4.4 Organization of the Farragut Technical Analysis Center 91
4.5 Organization of the Naval Criminal Investigative Service 93
4.6 Organization of the Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance 95
4.7 Organization of the 25th Air Force 98
4.8 Organization of Air Force Technical Applications Center 102
4.9 Organization of the National Air and Space Intelligence Center 105
4.10 Organization of the Marine Corps Intelligence Department 106
4.11 Organization of Marine Corps Intelligence Activity 108
4.12 Organization of the Coast Guard Intelligence Coordination Center 110
5.1 Organization of the Bureau of Intelligence and Research, Department of State 120
5.2 Organization of the Office of Intelligence and Counterintelligence, Department of Energy 122
5.3 Organization of the Z Program, Lawrence Livermore National Laboratory 125
5.4 Organization of the Office of Terrorism and Financial Intelligence, Department of the Treasury 126
5.5 Organization of the Office of Intelligence and Analysis, Department of the Treasury 127
5.6 Ten Facts About Terrorism and Financial Intelligence (TFI) 129
5.7 Organization of the Office of Intelligence & Analysis, Department of Homeland Security 131
5.8 Organization of the National Security Branch, Federal Bureau of Investigation 136
5.9 Organization of the Drug Enforcement Administration Intelligence Division 141
6.1 Map of the Unified Command Plan 154
6.2 Organization of the Africa Command J-2 157
6.3 Organization of the Central Command Intelligence Directorate 159
6.4 Organization of the Central Command Joint Intelligence Center 160
6.5 Organization of the European Command Joint Intelligence Operations Center 161
6.6 Organization of the European Command Joint Analysis Center 163
6.7 Organization of the Northern Command Intelligence Directorate 165
6.8 Organization of the Pacific Command Intelligence Directorate/Joint Intelligence Operations Center 167
6.9 Organization of the Southern Command Intelligence, Surveillance, and Reconnaissance Directorate 169

6.10 Organization of the U.S. Special Operations Command Intelligence Directorate, 2010 172
6.11 Organization of the Joint Intelligence Center, Special Operations Command, 2010 173
6.12 Organization of Strategic Command Joint Intelligence Operations Center 175
6.13 Organization of the Transportation Command Intelligence Directorate 177
7.1 The Electromagnetic Spectrum 185
9.1 Sample Alert Report Text: Atmospheric 274
9.2 Sample Alert Report Text: CIS/PRC Underground Test Site Events 282
10.1 Number of Nations and Government Consortia Operating in Space 298
10.2 Distribution of Space Surveillance Network Sensors 309
11.1 Enhanced Interrogation Techniques 335
13.1 U.S. Third Party Allies 380
14.1 Excerpt from the *President's Daily Brief*, August 6, 2001 410
14.2 Military Leadership Profile of General Cao Gangchuan 423
15.1 Table of Contents: Iraq: Foreign Intelligence and Security Services 455
17.1 Organizational Chart of the Office of the Director of National Intelligence 499
17.2 FY 2013 Request by Program 506
17.3a Consolidated Cryptologic Program 507
17.3b National Reconnaissance Program 507
17.4 National Counterterrorism Center Organization Chart 513
17.5 Organization of the National Counterproliferation Center 515
17.6 Organization of the Office of the National Counterintelligence Executive 516
18.1 Organization of the Office of the Under Secretary of Defense for Intelligence 526
18.2 Military Intelligence Program Elements 527
18.3 SR-71 Mission Request 531
18.4 Organization of the Joint Chiefs of Staff Reconnaissance Operations Division 532
19.1 Director of Central Intelligence Directive 6/1, "The SIGINT Committee" 544
19.2 Presidential Finding on Iran 550

PHOTOS

2.1 CIA headquarters, Langley, Virginia. 20
2.2 NSA headquarters, Fort George G. Meade, Maryland. 33
2.3 NRO headquarters, Chantilly, Virginia. 41
3.1 DIA center, Bolling AFB, Washington, D.C. 63

4.1 NGIC headquarters, Charlottesville, Virginia. 87
4.2 NMIC, Suitland, Maryland. 89
5.1 FBI headquarters, Washington, D.C. 133
7.1 LACROSSE/ONYX radar imagery satellite under construction. 190
7.2 U.S. satellite photograph of Shifa Pharmaceutical Plant, Sudan. 195
7.3 P-8A Poseidon aircraft. 200
7.4 Global Hawk unmanned aerial vehicle. 204
7.5 Aerospace Data Facility–East. 211
8.1 Inside the radomes at Buckley AFB, Colorado. 234
8.2 Joint Defence Facility, Pine Gap, Australia. 234
8.3 The COMBAT SENT version of the RC-135. 238
8.4 RC-135V/W Rivet Joint aircraft. 238
9.1 An artist's rendering of an SBIRS GEO spacecraft. 272
9.2 RC-135S Cobra Ball aircraft. 276
9.3 USNS *Howard O. Lorenzen*. 284
10.1 The TEAL BLUE space surveillance site in Hawaii. 307
12.1 CIA aerial photo of Osama bin Laden's compound in Abbottabad, Pakistan. 358
12.2 T-72 tank. 361
13.1 Communications Security Establishment headquarters. 377
15.1 Vitaly Yurchenko. 452
15.2 Aldrich Ames. 452
16.1 The Predator MQ-1B. 472
16.2 MQ-9 Reaper drone. 472

PREFACE

As with past editions, this book is titled *The U.S. Intelligence Community*, although it might be more properly titled *The U.S. Intelligence Community Plus*. The home page of the Office of the Director of National Intelligence (ODNI) describes the Intelligence Community as "a coalition of 17 agencies and organizations, including the ODNI, within the Executive Branch that work both independently and collaboratively to gather and analyze the intelligence necessary to conduct foreign relations and national security activities." Such a description is highly misleading because a number of organizations that are counted as single entities—including the Defense Intelligence Agency, the 25th Air Force, and the ODNI itself—contain within them a number of entities that are, in reality, distinct organizations. In addition, there exist numerous intelligence organizations and activities that take place outside the designated Intelligence Community organizations. Thus, the U.S. Intelligence Community represents a subset of what might be referred to as the "Federal Intelligence Enterprise."

Although not all of the federal intelligence organizations and activities outside the Intelligence Community are discussed in this work, a good number are—as they have been in earlier editions. To omit them would create a misleading impression as to the nature of U.S. intelligence organization and activities. Organizations thus discussed include the intelligence components of the Unified Commands, while entities that are not part of the Intelligence Community manage a number of the strategic measurement and signature intelligence (MASINT) and space surveillance activities described.

This edition involves a number of changes in terms of organization and titles. I have reversed the order of the chapters on departmental civilian intelligence organizations and Unified Command intelligence organizations, reflecting the fact that the latter are not officially part of the Intelligence Community. I have titled Chapter 7 "Geospatial Intelligence Collection, Processing, Exploitation, and Dissemination," although the key part still involves imagery intelligence. Chapter 8 has become "Signals Intelligence and Cyber Collection," and its content reflects the fact that, in addition to intercepting data in motion, a crucial part of the National Security Agency's mission is to acquire "data at rest," a term used initially to describe the extraction of information residing in computers around the world. Parts of the chapter also reflect the significant disclosures due to Edward Snowden. In addition, the title of Chapter 12, "Open Sources, Site Exploitation, and Foreign Materiel Acquisition," reflects my decision to move discussions of emplaced sensors into the chapters covering the relevant disciplines.

The content of the book, of course, reflects both its basic structure and the developments since the sixth edition went to press in the spring of 2011. These most prominently include the raid that resulted in the demise of Osama bin Laden, the administration's release of a white paper concerning targeted killings, and the disclosures concerning U.S. and allied signals intelligence activities that have appeared in (or on the websites of) the *Intercept*, *Guardian*, *Washington Post*, *New York Times*, *Der Spiegel*, and elsewhere. For the first nineteen chapters I have tried to maintain a neutral approach in the discussion of U.S. intelligence activities—particularly as I find annoying books whose authors' would claim to be objective but whose constant, one-sided editorializing suggests that they are not.

The final chapter contains my discussion of five issues—the extent of U.S. intelligence operations around the world, the covert (and not so covert) fight against terrorist organizations, domestic surveillance by the FBI and NSA, congressional oversight, and secrecy and leaks—as well as some observations on the extent to which Intelligence Community performance with regard to transparency and civil liberties reflects not so much the unique circumstances of the intelligence world but problems in bureaucratic behavior at all levels of government.

The information in this book comes from a variety of sources: interviews; official documents, many obtained under the Freedom of Information Act (FOIA); books written by former intelligence officers, journalists, and academics; websites; trade and technical publications; and newspapers and magazines. The public literature on intelligence is vast, and I have done my best to sort the wheat from the chaff. I have also sought to incorporate the most recent information available at each stage of the production process to minimize the inevitable discrepancies between the situation described and the situation at the time of publication. In addition, I have identified sources to the maximum extent possible, while protecting the identities of those individuals who wish to remain anonymous.

A number of institutions and individuals were instrumental in providing material for this book. There are the FOIA and public affairs offices and officers who responded to my requests (although some deserve to be noted for their obstruction, which I will do in Chapter 20). In addition, a number of individuals and websites have made it easy to obtain a large number of relevant and valuable documents and articles with little effort—specifically, Matthew Aid (http://www.matthewaid.com), Steve Aftergood (http://fas.org/blogs/secrecy), John Young (http://www.cryptome.org), and those responsible for the Public Intelligence (http://www.publicintelligence.net) and Government Attic (http://www.governmentattic.org) sites.

In addition, those who provided assistance have included Matthew Aid, William Burr, Ted Molczan, and Robert Windrem, and they have my thanks. I would also like to thank the National Security Archive for its support in a variety of ways. Finally, thanks are due to Ada Fung, Krista Anderson, Carolyn Sobczak, Jennifer Kelland Fagan, and others at Westview who turned my manuscript into a book.

1

INTELLIGENCE

The U.S. government contains a substantial number of officials and organizations that require intelligence (domestic or foreign) to fulfill their responsibilities, whether those responsibilities involve making policy or implementing it. Intelligence can be defined as "the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations."[1]Those individuals and institutions that deal with national security issues have the most prominent need for such intelligence. Hence, the President and his National Security Advisor, the Vice President, the National Security Council and its staff, the Departments of State, Defense, Homeland Security, Treasury, and Justice, the Joint Chiefs of Staff (JCS) and their Joint Staff, the military services, and the general and admirals who head the nation's unified commands are the most obvious consumers of foreign and domestic intelligence.

Today, those individuals and institutions face a multitude of concerns, including the capabilities, activities, financing, and plans of al-Qaeda and its offshoots, the Islamic State in Iraq and Syria (ISIS), Hezbollah, and other terrorist groups; the threat from cyber operations (including computer network attacks and exploitation); weapons of mass destruction (WMD) programs and associated personnel in Iran, North Korea, and a number of other nations; Russian and Chinese foreign policies and military activities; internal turmoil in a number of Middle Eastern nations; and developments involving India, Pakistan, and Latin America. Other concerns involve the threat of domestic terrorism, returning jihadists, and threats to the power grid.[2]

A number of events in the new millennium have illustrated the potential value of good intelligence to U.S. officials, as well as the consequences of poor or limited intelligence: the attacks of September 11, 2001, and subsequent failed and successful terrorist attacks, the operations that resulted in the death of Osama bin Laden and failure to capture al-Shabaab personnel, the failure of U.S. forces to find WMD stockpiles in Iraq after the 2003 invasion and the insurgency that followed, the difficulties in trying to halt the North Korean and Iranian nuclear weapons programs, Iranian and North Korean missile launches, Russia's seizure of the Crimea, Syria's pursuit of nuclear weapons and the regime's actions (including the use of chemical weapons) to retain power, and the inability to rescue American journalists held by ISIS.[3]

In addition, other policymakers have a need for intelligence, even if dealing with less pressing concerns. Those with responsibilities in the areas of international economics, trade and technology transfer, energy, the environment, and public health may require foreign intelligence. The actions of foreign governments and groups can influence both the security of foreign energy resources and the stability of the dollar.

The Environmental Protection Agency (EPA) may require intelligence on environmental accidents, foreign government compliance with international environmental obligations, and the status of environmentally sensitive areas. With respect to compliance, the EPA has been interested in the disposal of nuclear wastes, illegal ocean dumping, and the smuggling of animals and animal products. The National Aeronautics and Space Administration (NASA) is concerned with foreign technology developments and foreign space programs, as well as space debris that might threaten its spacecraft—debris that might result from an antisatellite test monitored by the Intelligence Community. The Department of Agriculture has been concerned with foreign government compliance with negotiated agricultural agreements, the development of global trading blocks, agricultural production and supply, and the food requirements of countries with chronic food deficits.[4]

INTELLIGENCE ACTIVITIES

Intelligence activities fall into four categories: collection, analysis, counterintelligence, and covert action. Collection—defined as the purposeful acquisition of any information that an analyst, consumer, or operator might desire—can involve any of several overlapping forms: open source collection, human source collection and interrogation, and technical collection. Open source collection includes the acquisition of material in the public or semipublic domains. Targets of open source collection include radio and television broadcasts, newspapers, magazines, technical and scholarly journals or papers, books, unclassified government reports or other documents, open activities that defense attachés or foreign service officers can monitor, and the various components of the Internet (including social media).

Human intelligence (HUMINT), concerning military, political, or economic matters, may be obtained from recruiting a foreign national to secretly provide information (or, as has often been the case, accepting an offer to provide such information). Human source collection may also involve a straightforward interview with a willing (or semiwilling) source or the interrogation of a hostile detainee. And it may be conducted in person or in cyberspace.

Technical collection comes in a number of different forms. Geospatial collection involves the use of several different sensors (electro-optical, infrared, radar) to produce images and maps. Much of signals intelligence (SIGINT) collection has relied on the placement of antenna systems on platforms as diverse as submarines and satellites to intercept communications, foreign instrumentation signals (including missile telemetry), and radar emissions. In addition, cyber collection through computer network exploitation (accomplished either remotely or by direct access) can yield data stored in foreign computer systems. Audio surveillance or emplaced sensors can also gather signals. Measurement and signature intelligence collection represents, in effect, "all other" technical collection activities, including nonimaging infrared, seismic detection, and

acoustic collection. Such collection activities may be conducted remotely, from miles to tens of thousands of miles away, or using sensors covertly installed quite near a target.[5]

Analysis involves the integration and evaluation of collected information—that is, employing raw intelligence to produce finished intelligence. The finished intelligence product might be a simple statement of facts, an evaluation of the capabilities of another nation's military forces, a projection of the likely course of political events in a foreign country, or an analysis of the capabilities and objectives of a terrorist group.

Counterintelligence encompasses all information acquisition and all activity designed to assess foreign intelligence and security services (including those of terrorist groups) and neutralize hostile services. These activities involve human, technical, and open source collection, as well as analysis of information concerning the structure and operations of foreign services. Such collection and analysis, with respect to the technical collection activities of foreign services, can guide denial and deception operations. Counterintelligence may also involve the direct penetration and disruption of hostile intelligence organizations and their activities.

Traditionally, covert action included any operation designed to influence foreign governments, persons, or events in support of the sponsoring government's foreign policy objectives, while keeping the sponsoring government's support of the operation secret. Today, terrorist organizations are an even more important target for covert action operations; as a result there may at times be no need or ability to hide the sponsorship of certain activities—for example, the support of Northern Alliance forces seeking to overthrow the Taliban or the post-9/11 use of armed drones to kill al-Qaeda personnel. There are several distinct types of covert action: black propaganda (which purports to emanate from a source other than the true one); gray propaganda (in which the true sponsorship is not acknowledged); paramilitary or political actions designed to overthrow, undermine, or support a regime; paramilitary or political actions designed to counteract a regime's attempts to procure or develop advanced weaponry; support (aid, arms, training) of individuals or organizations (government components, opposition forces and political parties, and labor unions); economic operations; deception; and targeted killings.

THE INTELLIGENCE CYCLE

The concept of the "intelligence cycle" puts the collection and analysis activities conducted by various intelligence units into perspective—that is, it relates those activities to the requirements of the government officials who use the intelligence produced. The intelligence cycle is the theoretical sequence in which information is requested, acquired, transformed into finished intelligence, and disseminated to policymakers or implementers. The cycle consists of six steps: planning and direction, collection, processing and exploitation, analysis and production, dissemination, and evaluation.[6]

The planning and direction component involves the management of the entire intelligence effort, from the identification of the need for data to the final delivery of an intelligence product to a consumer. Requests for intelligence, based on the needs of the president, the Departments of State, Defense, Homeland Security, or Treasury, or other consumers, may initiate the process. Collection, as indicated above, involves the gathering, by a variety of means, of raw data from which finished intelligence is

produced. The next step, processing and exploitation, concerns conversion of the vast amount of information flowing into the system into a form suitable for the production of finished intelligence. This may involve the interpretation and measurement of images and signals, including identification of a nuclear reactor in an image, determination of the accuracy of a missile, or estimation of the yield of a nuclear detonation. It may also involve language translation, decryption, subject matter sorting, or data reduction. The analysis and production element entails the conversion of basic information into finished intelligence and includes the integration, evaluation, and analysis of all available data and the preparation of various intelligence products. Because the "raw intelligence" collected is often fragmentary and at times contradictory, specialists are needed to give it meaning and significance. Dissemination involves the distribution of the finished intelligence to its consumers: the policymakers and operators whose needs trigged the process. The final step includes evaluation by and feedback from consumers who receive the product.

Like any model, the outline of the intelligence cycle simplifies reality. Certain requirements become standing requirements. Thus, the Intelligence Community need not be reminded to collect information on al-Qaeda or Hezbollah activities, nuclear proliferation, Chinese or Russian nuclear forces, or developments in the Middle East. And policymakers do not specify, except in rare cases, particular items of information to be collected (which may also serve to permit them to deny that they approved specific techniques or targets). The collectors take responsibility for determining how to obtain the information necessary to satisfy the standing or consumer-initiated requirements. In addition, the collection agencies have certain internal needs to acquire information to support their continued operations—information related to counterintelligence and security and information that will be useful in potential future operations. It should be noted that decision makers, particularly in the midst of a crisis, may require only processed intelligence. Thus, in the midst of the Cuban missile crisis, the most important intelligence was purely factual reporting concerning Soviet activities in Cuba and on the high seas.

VARIETIES OF FINISHED INTELLIGENCE

Just as one can distinguish different types of intelligence activities, one can also identify the different types of intelligence they produce. The varieties of intelligence include political, military, scientific and technical, financial, economic, sociological, and medical/biometric. Political intelligence encompasses both foreign and domestic politics. Clearly, the foreign policies of other nations have an impact on the United States and might involve a number of issues: support or opposition to U.S. initiatives in dealing with Iran, North Korea, or Syria, other nations' political and economic relations with those countries, attitudes and policies concerning the Middle East, support of terrorist groups, and perceptions of U.S. leadership and policies. In addition, terrorist groups and nongovernmental organizations have policies that guide their actions with regard to the United States and its allies.

The domestic politics of other nations—whether friendly, neutral, or hostile—are also of significant concern to the United States. The resolution of domestic conflicts—whether by coup, civil war, or election—can affect the orientation of that nation in the

world, the regional balance of power, the accessibility of resources critical to the United States, or the continued presence of U.S. military or intelligence facilities. In addition, terrorist organizations also have their own internal, sometimes quite deadly, politics, with outcomes of potentially vital importance to the United States. One aspect of intelligence on domestic politics is leadership intelligence, focusing on the personalities, histories, powers, position, and preferences (policy and personal) of key officials.

Military intelligence has a variety of uses. To determine its own military requirements—whether nuclear, conventional, or special operations—the United States must have a good grasp of the capabilities and vulnerabilities of both friends and potential adversaries. The government also requires military intelligence to assess the need and impact of any military aid the United States might be asked to provide. Furthermore, it needs military intelligence to assess the balance of power between pairs of nations (e.g., India-Pakistan, North Korea–South Korea) whose interactions can affect U.S. interests. And, as with foreign and domestic political intelligence, one subset of military intelligence is military leadership intelligence, including biographic reports as well as reports on the ups and downs of military officials.[7]

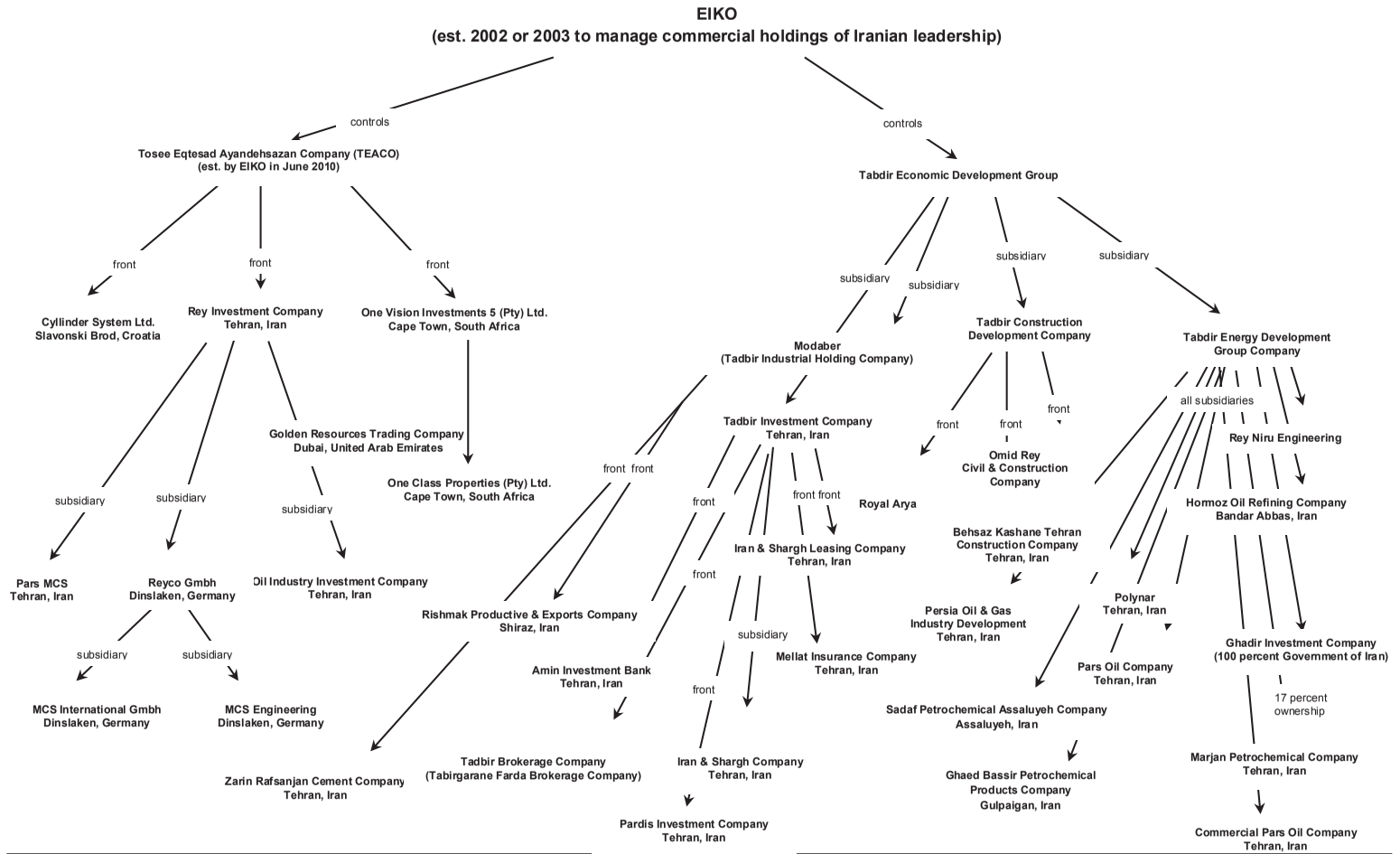
Scientific and technical intelligence includes both civilian- and military-related scientific and technical developments. A nation's ability to employ modern agricultural methods or efficiently extract energy resources may affect its stability. In many cases, technological developments in the civilian sector have military applications. Examples include information and computer technology, biotechnology, mirrors and optical systems, and lasers. Hence, intelligence concerning a nation's progress or ability to absorb foreign-produced technology in those areas is relevant to its potential military capability.

One aspect of scientific and technical capabilities, atomic energy intelligence, has been of constant concern for more than seventy years. In addition to the obvious need to determine whether various foreign nations are developing nuclear weapons, there has been a perceived need to acquire secret intelligence in support of decision making concerning applications for nuclear-technology-related exports. In 1947 the first Director of Central Intelligence noted that the United States "cannot rely on information submitted by a licensee" and that it was necessary for the United States to "determine actual use, [to] endeavor to discover secondary diversions."[8] A nation's scientific and technical expertise relevant to the production of biological or chemical weapons—the "poor man's atomic bomb"—has also been of concern to U.S. intelligence. In addition, the potential of terrorist organizations to make use of such weapons of mass destruction is a major concern to those charged with protecting the U.S. homeland and overseas possessions and facilities.[9]

Financial intelligence focuses on both the individuals and the institutions involved in the transfer of funds for the financing of organizations, activities, or facilities of interest, including terrorist groups, weapons-related technology sales, and the construction of nuclear facilities, as well as the data or communications involved in funds transfers. Such intelligence forms the basis for U.S. designations of individuals or institutions involved in activities that result in sanctions. It can serve as a deterrent or a means to prevent or disrupt terrorist activities.[10] Figure 1.1 shows the results of one product of the financial intelligence effort.

Economic intelligence is also of great importance. One component includes the strengths and vulnerabilities of national economies. Knowledge of the strengths aids

FIGURE 1.1 The Execution of Imam Khomeini's Order (EIKO) International Financial Network



Source: U.S. Department of the Treasury.

in understanding a nation's capacity for conflict, whereas knowledge of the vulnerabilities may be key in assessing threats to stability as well as the likelihood that economic sanctions will induce a change in policy. Another component is the availability and pricing of key resources, from oil to an assortment of metals and minerals. In addition, economic intelligence looks at regional and other economic organizations, national fiscal and monetary policy, and international payments mechanisms. It also concerns topics such as sanctions busting, money laundering, bribery and corruption, and economic espionage.[11]

Sociological intelligence involves group relations within a nation. Relations between groups, be they ethnic, religious, or political groups, can significantly impact a nation's stability as well as its foreign policy—as demonstrated in the last two decades by events in Iraq, Syria, Yugoslavia, Africa, and Russia.

Medical intelligence can involve both the conditions of single individuals and threats to large groups. Determining the medical and psychological condition of foreign leaders and other key foreign officials has been a responsibility of the Central Intelligence Agency (CIA) since the early days of the Cold War. In addition, the CIA and other intelligence organizations have been concerned with medical hazards (from diseases to poisonous snakes) to U.S. military personnel in foreign environments as well as with the spread of disease in foreign nations. Biometric/identity intelligence includes DNA samples, which can be used to uniquely identify individuals (whether dead or alive).[12]

TARGETS

The U.S. Intelligence Community has an impressive array of intelligence targets to monitor. These fall into three, sometimes overlapping, categories:

- Transnational targets
- Regional targets
- National targets

Transnational targets extend across regions and may require nontraditional approaches with respect to the collection and analysis of relevant intelligence, as well as to the organization of the intelligence effort. Among the most prominent transnational targets are international terrorist or criminal groups, organizations and activities that could result in WMD proliferation, and illicit arms or narcotics trafficking. Targets also include international organizations including the United Nations and, at least potentially, nongovernment organizations hostile to the United States and the West.[13]

Although individual governments undertake attempts to develop nuclear weapons, Iraq, Iran, Pakistan, and Libya not only made use of indigenous capabilities in their efforts but also relied on a significant international supplier network and the assistance of foreign governments. This contrasts sharply with the largely indigenous manner in which the Soviet Union and China developed their nuclear arsenals. Likewise, Syria's accumulation of chemical weapons depended on foreign assistance along with indigenous effort.[14]

Terrorist groups, whether located in the Middle East, Africa, or Asia, have killed, maimed, and destroyed property around the world—in New York and Washington,

D.C., in Madrid and London, in Africa and Indonesia. Furthermore, such groups, unlike states, can relocate when a host government deems their presence too burdensome at a particular location or they become the target of retaliation. Likewise, the tentacles of South American and Asian drug cartels, as well as of the Russian Mafia, extend far beyond the borders of their home territories.[15]

Other transnational concerns include developments in cyber capabilities, the state of the environment (including the impact of toxic waste dumping in the oceans), uncontrolled refugee migrations, population growth, communications technology, the spread of diseases such as HIV/AIDS, Ebola, or the avian flu, and international economic activity.[16]

The concept of regional targets recognizes that developments in a particular area of the world may stem not only from individual governments' choices but also from the interaction between governments. Clearly, a war in the Middle East, in Southwest Asia, or on the Korean Peninsula would represent the most violent of such regional targets. Regional targets, which increase the chance of war, include border clashes, arms races, and cross-national movements of weapons and troops. Thus, the criteria for U.S. arms-transfer policy have included taking into account "consistency with U.S. regional stability interests, especially when considering transfers involving power projection capability or introduction of a system which may foster increased tension or contribute to an arms race."[17]

Regional activity of interest to the U.S. Intelligence Community may extend beyond governmental activities. The Asian financial crisis of 1997 concerned U.S. officials, for it had the potential to affect internal political developments, the foreign trade activities of a number of nations, and, ultimately, the U.S. economy. The same could be said of the 2008–2009 financial crisis.

National targets, the most traditional type, include all nations whose policies may have a significant impact on the United States, from the friendliest to the most hostile, although the type of information required and the means employed to acquire it vary considerably. China is a major national target, given its impact on international trade and finance, its arms trade, its potential to help or hinder in alleviating problems with Iran, Syria, and North Korea, its cyber activities, its growing military space operations, its air and naval operations in the Pacific, its nuclear relations with Pakistan and other nations, and the ongoing transformation of the People's Liberation Army "from a mass army designed for protracted wars of attrition on its territory to one capable of fighting and winning short-duration conflicts along its periphery against high-tech adversaries."[18] Other significant national targets include, for a variety of reasons, Iran, Syria, North Korea, Yemen, and Pakistan. Items of interest are Iran's and North Korea's nuclear and missile programs, Iranian support for terrorist groups, the Syrian government's adherence to its pledge to turn over its stock of chemical weapons, the internal conflicts within and foreign policies of Iran and North Korea, terrorist activity in Yemen and the consequences of the fall of Yemen's government for U.S. counterterrorism efforts, and the stability of Pakistan's government as well as the security of its nuclear weapons.[19]

Even after the collapse of the Soviet Union and the end of the Cold War, Russia remained a significant nation of concern to U.S. national security officials, and that concern has undoubtedly increased in recent years. Topics of interest to U.S. officials

regarding Russia include Vladimir Putin's health and behavior, the personalities and views of key Russians, the prospects for Russian democracy, the state of the economy, organized crime and corruption, the security of Russian nuclear weapons, the state of Russia's armed forces, the status of its strategic weapons programs, its arms sales and technology-transfer activities, its policies toward Iran, Syria, North Korea, China, and other entities, its activities in Ukraine, and its intelligence activities targeting the United States.[20]

Director of National Intelligence James R. Clapper Jr. noted some examples of topics of concern to the U.S. Intelligence Community in 2015—undoubtedly a small subset of the full range—in a statement to the Senate Armed Services Committee. The global issues he discussed included the global cyber threat, unauthorized disclosures and foreign intelligence threats, terrorism, weapons of mass destruction proliferation, space and counterspace, transnational organized crime, economics and national resources, and human security.[21] Clapper also identified threats in the Middle East and North Africa, South Asia, Sub-Saharan Africa, East Asia, Russia and Eurasia, Latin America and the Caribbean, and Europe.[22]

THE UTILITY OF INTELLIGENCE

The utility of intelligence activity, here narrowly construed to mean collection and analysis, depends on the extent to which it aids national, departmental, and military decision makers and those who implement their policies and decisions. Two questions arise in this regard: In what ways does intelligence aid those individuals, and what attributes make intelligence useful?

With respect to the first question, intelligence can be useful to national decision makers in five distinct areas: policymaking, planning, managing conflict situations (ranging from negotiations to war), warning, and monitoring treaty compliance. In their policymaking roles, national decision makers set the basic outlines of foreign, defense, and international economic policy and decide specific actions with regard to key issues. The Rockefeller Commission's 1975 report summed up the need for intelligence: "Intelligence is information gathered for policymakers which illuminates the range of choices available to them and enables them to exercise judgment. Good intelligence will not necessarily lead to wise policy choices. But without sound intelligence, national policy decisions and actions cannot effectively respond to actual conditions and reflect the best national interests or adequately protect . . . national security."[23]

In addition to its value in policymaking and guiding decisions about alternative courses of action, intelligence is vital to planning decisions. Some planning decisions may concern the development and deployment of new weapons systems. One Air Force regulation noted, "Timely, accurate, and detailed intelligence is a vital element in establishing requirements and for planning and initiating RDT&E (Research, Development, Test, and Evaluation) efforts and continues to impact these efforts throughout the development and system life cycle." A more recent Navy instruction states, "Intelligence is key to understanding the potential current and future threat posed by foreign weapon and Information Technology (IT) system capabilities, and must be integral to U.S. system development and acquisition decisions."[24]

One incident illustrating the role of intelligence in weapons development occurred in 1968, when the U.S. Navy monitored a member of the oldest class of Soviet nuclear submarines traveling faster than thirty-four miles per hour, with apparent power to spare. That speed exceeded previous CIA estimates for the submarine and led the agency to order a full-scale revision of speed estimates for Soviet submarines. The revised estimates also provoked one of the largest programs in the history of the U.S. Navy—the production of the SSN 688-class attack submarine.[25]

At the same time, intelligence can help save substantial sums of money by avoiding unnecessary research and development and deployment programs. Several of the CIA's human assets, including Peter Popov, Adolf G. Tolkachev, and Dmitri Polyakov, provided information that saved the United States billions of dollars in research and development costs. Two former CIA officers wrote that Tolkachev "provided details on Soviet military weaponry long before it was deployed, and thus long before information on the systems could be picked up by technical collection. It sometimes changed the direction of our own research and development and, by so doing, saved the U.S. government billions of dollars."[26] In addition, The first successful U.S. photographic reconnaissance satellite system, code-named CORONA, produced information that eliminated fears of a missile gap and thus permitted the United States to cap its deployment of strategic missiles at a lower level than otherwise would have been possible. The successor program, HEXAGON, was instrumental in facilitating arms control agreements with the Soviet Union that would limit U.S. expenses on strategic weapons systems.[27]

Another set of planning decisions involves the development of war plans. In the months between the Iraqi invasion of Kuwait (August 1990) and the beginning of Operation DESERT STORM (January 1991), the United States collected a massive quantity of intelligence about Iraqi nuclear, chemical, and biological weapons programs, electrical power networks, ballistic missiles, air defense systems, ground forces, and air forces. The data collected allowed the development and implementation of a war plan based on the most up-to-date information possible. Likewise, planning for the attacks on Serbian targets in 1999 required gathering and evaluating information on air defense forces. Preparations for the invasion of Afghanistan in 2001 and Iraq in 2003, as well as the mission into Pakistan in May 2011, required significant intelligence collection and analysis efforts.[28]

Other decisions aided by intelligence include the suspension or resumption of foreign aid, the employment of trade sanctions and embargoes, and attempts to block the transfer of commodities related to nuclear or ballistic missile proliferation. Intelligence can inform decision makers of the likely effects of such actions, including the reactions of nations targeted by decisions. Thus, the Carter administration went ahead with the planned sale of planes to Saudi Arabia in part as a result of intelligence indicating that if the United States backed out of the deal, the Saudis would simply buy French planes.[29]

Several actions taken to inhibit Iran's pursuit of a nuclear weapons capability have followed acquisition of related intelligence. In 1992 the United States, based on intelligence indicating a "suspicious procurement pattern" by Iran, acted to forestall the sale of equipment that the Iranians could use to begin manufacturing nuclear weapons. Argentina halted certain sales to Iran after the United States expressed concern that

the equipment in question would allow Iran to convert natural uranium into precursor forms of highly enriched uranium. Similarly, the United States successfully lobbied the People's Republic of China to halt the sale of a large nuclear reactor that would have included a supply of enriched fuel and permitted Iran to conduct research related to the nuclear fuel cycle.[30]

In January 1998, intercepted communications between a senior Iranian official and mid-level counterparts in Beijing indicated that Iran was negotiating to purchase "a lifelong supply" of a chemical it could use to transform naturally occurring uranium into the highly enriched form required for nuclear weapons. Senior Chinese officials informed White House aides that the contract had been suspended and was under review. During the spring of 2000, U.S. intelligence agencies uncovered plans for the D. V. Efremov Institute in St. Petersburg to provide Iran with a laser facility that could be used for uranium enrichment. Once U.S. officials became aware of the proposed transaction, they urged Russian officials to cancel it because, in the words of one official, there was "no question that the turn-key facility was intended for" Iran's nuclear weapons program. During preparations for the September 2000 meeting between U.S. President Bill Clinton and President Vladimir Putin of Russia, the subject was raised again. Russian officials informed White House aides that the contract had been suspended and was under review.[31]

Intelligence is also useful in a variety of conflict situations, most prominently combat. Indeed, with the issuance of Presidential Decision Directive 35, "Intelligence Requirements," the Clinton administration designated "support to military operations," including combat operations as well as planning and exercise activities, the first priority of U.S. intelligence. Regardless of how well developed a war plan is, combat forces require intelligence on the movements and actions of enemy forces and on the impact of air and other attacks against enemy facilities and troops. Thus, even after months of extensive collection prior to Operation DESERT STORM, the United States still needed to conduct an intense intelligence collection campaign during the conflict. Similarly, the prolonged combat operations in Iraq and Afghanistan required an extensive use of intelligence resources.

Intelligence is also of value in nonmilitary conflict situations, including any in which nations have at least partially conflicting interests, such as arms control negotiations, trade negotiations, or international conferences. Intelligence can indicate how far the United States can push other parties and the extent to which it must modify its own position. In 1969 the United States intercepted Japanese communications concerning negotiations between Washington, D.C., and Tokyo regarding the reversion of Okinawa to Japanese control. It has also relied on communications intelligence during the negotiations that led to the first Strategic Arms Limitation Treaty and during the 2003 UN debate over Iraq.[32]

Intelligence can also provide warning of upcoming hostile or unfavorable military, terrorist, or other actions against the United States or an ally. Sufficient advance notice allows defenses to be prepared, responses to be considered and implemented, and preemptive diplomatic or military action taken to forestall or negate the action. In 1980, on the basis of human intelligence, President Jimmy Carter warned Soviet general secretary Leonid Brezhnev of the consequences of invading Poland. In March 1991, on the basis of communications intelligence indicating Iraq's intention to use chemical

weapons against rebel forces, the United States warned the Iraqis that it would not tolerate such an action. Intelligence has been credited with short-circuiting the plot, hatched in Yemen, to destroy two U.S. freight aircraft in flight over the United States in 2010.[33]

Intelligence is also necessary to assess whether other nations are in compliance with various international obligations. The United States wishes to know, for example, if Russia or China is complying with arms control agreements currently in force. Intelligence is also vital in detecting violations of agreements and treaties limiting nuclear proliferation and testing. In 1993 the United States was reportedly concerned with China's apparent violation of its pledge not to sell M-11 missiles to Pakistan. In 2014 intelligence on Russian testing of a new ground-launched cruise missile led to the conclusion that Moscow was "in violation of its obligations under the intermediate-range nuclear forces (INF) treaty."[34]

For maximum utility the intelligence must not only address relevant subjects but also possess the attributes of quality and timeliness. Unless intelligence assessments on a subject marshal all relevant information, the quality of the finished product may suffer. As Professor Hugh Trevor-Roper observed, "Secret intelligence is the continuation of open intelligence by other means. So long as governments conceal a part of their activities, other governments, if they wish to base their policy on full and correct information, must seek to penetrate the veil. This inevitably entails varying methods. But, however the means may vary, the end must still be the same. It is to complement the results of what for convenience we may call 'public' intelligence: that is, the intelligence derived from the rational study of public or at least available sources. Intelligence is, in fact, indivisible."[35]

In addition to resting on all relevant information, the assessment process must be objective. As former secretary of state Henry Kissinger told the U.S. Senate in 1973, "Anyone concerned with national policy must have a profound interest in making sure that intelligence guides, and does not follow, national policy."[36] Furthermore, intelligence much reach decision makers in good time for them to act decisively—either by warning a foreign government before it commits irrevocably to a particular course of diplomatic or military action or by ordering actions to undermine or negate such actions.

THE INTELLIGENCE COMMUNITY

Almost forty years ago a National Security Council study noted, "U.S. intelligence is unique in the world for its state of the art, the scope of its activities, and the extraordinary range and variety of [its] organizations and activities."[37] Its activities include the collection of information using reconnaissance satellites, aircraft, ships, ground stations, emplaced sensors, computer network exploitation, and undersea surveillance, along with traditional overt and clandestine human sources. It also acquires and exploits open sources, foreign materiel, as well as videos and documents. In addition, its personnel process and analyze the information collected using the most advanced computers and a variety of specially developed techniques for extracting a maximum of information from the data. The 2016 National Intelligence Program and Military Intelligence Program budget requests envisioned the expenditure of $53.9 and $17.9

billion, respectively, to fund the activities of the more than 100,000 members of the U.S. Intelligence Community.[38]

That community officially consists of seventeen organizations: the Office of the Director of National Intelligence; the Central Intelligence Agency; the National Security Agency; the National Reconnaissance Office; the National Geospatial-Intelligence Agency; the Defense Intelligence Agency; the Bureau of Intelligence and Research of the State Department; the intelligence elements of the five military services; the Federal Bureau of Investigation; and intelligence components of the Drug Enforcement Administration, the Department of Energy, the Department of the Treasury, and the Department of Homeland Security. Those intelligence elements can be grouped into four categories:

- National intelligence organizations
- Department of Defense intelligence
- Military service intelligence organizations
- Civilian departmental intelligence organizations

A fifth group of intelligence organizations plays a significant role in the production of intelligence: the intelligence components of the unified commands.

Notes

1. Department of Defense, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, March 14, 2013, 141.

2. Ellen Barry, "Al-Qaeda Open Branch on Indian Subcontinent," *New York Times*, September 5, 2014, A13; Mark Mazzetti, "A Terror Cell That Avoided the Spotlight," *New York Times*, September 25, 2014, A1, A12; Michael Madden, "Meet Kim Jong Un's New Nuclear Warriors," www.foreignpolicy.com, September 22, 2014, http://foreignpolicy.com/2014/09/22/meet-kim-jong-uns-new-nuclear-warriors; "Major Military Drills Underway Against Simulated Enemy in Seas of Okhostsk and Japan," *Siberian Times*, September 15, 2014, http://siberiantimes.com/other/others/news/major-military-drills-underway-against-simulated-enemy-in-seas-of-okhotsk-and-japan; Rebecca Smith, "Nation's Power Grid Vulnerable to Sabotage," *Wall Street Journal*, March 13, 2014, A1, A6; Bill Sweetman, "Russian Renaissance," *AW&ST*, November 11–18, 2013, 48–50; Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States*, 2014, 4.

3. Ken Dilanian, "A Big Surprise for the Spies?," *Los Angeles Times*, March 5, 2014, 6; Nicholas Kulish and Eric Schmitt, "'Imperfect Intelligence' Said to Hinder U.S. Raid on Militant in Somalia," *New York Times*, October 9, 2013, A10; Office of the Press Secretary, White House "U.S. Government Assessment of the Syrian Government's Use of Chemical Weapons on August 21, 2013," August 30, 2013, http://www.whitehouse.gov/the-press-office/2013/08/30/government-assessment-syrian-government-s-use-chemical-weapons-august-21; Adam Entous, Siobhan Gorman, and Jaeyeon Woo, "Portrait of New Leader Takes Shape," *Wall Street Journal*, December 20, 2011, A14.

4. Environmental Protection Agency, "EPA NSR-29 Intelligence Requirements," May 14, 1992; National Aeronautics and Space Administration, "NSR-29 Intelligence Requirements," January 17, 1992; "Space Surveillance Network NASA Support Requirements Matrix," attachment to Daniel S. Goldin, Administrator, NASA, to General Howell M. Estes III, August 27, 1997; Department of Agriculture, "NSR-29 Intelligence Requirements," January 15, 1992.

5. For a discussion of the diverse elements of technical collection, see Robert M. Clark, *The Technical Collection of Intelligence* (Washington, DC: CQ Press, 2011).

6. Office of the Director of National Intelligence, *U.S. National Intelligence: An Overview 2013*, April 9, 2013, http://www.dni.gov/index.php/newsroom/reports-and-publications/193-reports-publications-2013/835-u-s-national-intelligence-an-overview-2013-sponsored-by-the-intelligence-community-information-sharing-executive, 5–6.

7. See, for example, Choe Sang-Hun, "North Korean Leader Tightens Grip with Removal of His Top General," *New York Times*, October 11, 2013, A4; Jeremy Page, "China Party Fills Top Military Posts," *Washington Post*, November 5, 2012, A11.

8. Sidney Souers, "Atomic Energy Intelligence," Record Group (RG) 218 (Joint Chiefs of Staff), July 1, 1947, National Archives and Records Administration, College Park, Maryland.

9. See, for example, CIA, *Chemical and Biological Weapons: The Poor Man's Atomic Bomb*, December 1988; CIA, *The Chemical and Biological Weapons Threat*, March 1996. With regard to recent concerns, see Eric Schmitt and Thom Shanker, "Qaeda Trying to Harness Toxin for Bombs, U.S. Officials Fear," *New York Times*, August 13, 2011, A1, A3.

10. Department of the Treasury, TG-838, "Treasury Designates al-Qai'da Finance Section Leader," August 24, 2010; Peter Fritsch, "Small Bank in Germany Tied to Iran Nuclear Effort," *Wall Street Journal*, July 19, 2010, A1, A14; Chico Harlan, "U.S. Official Outlines Plan Targeting Firms, Banks That Help Fund North Korea," www.washingtonpost.com, August 3, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/08/02/AR2010080201697.html; Greg Miller, "Syrian Money Transfers Tracked," *Washington Post*, March 6, 2012, A1, A11; Helene Cooper, "Treasury Dept., Citing Six People as Operatives, Accuses Iran of Aiding Al Qaeda," *New York Times*, July 29, 2011, A4; Matthew Levitt, "Leveraging Financial Intelligence to Combat Transnational Threats," *Georgetown Journal of International Affairs* 12, no. 1 (Winter/Spring 2011): 34–43; Yochi Dreazen, "Inside the Treasury Department's War on Iran," www.foreignpolicy.com, November 6, 2013, http://foreignpolicy.com/2013/11/06/inside-the-treasury-departments-war-on-iran; Joby Warrick, "Islamic Charity Officials Gave Millions to al-Qaeda, U.S. Says," www.washingtonpost.com, December 22, 2013, http://www.washingtonpost.com/world/national-security/islamic-charity-officials-gave-millions-to-al-qaeda-us-says/2013/12/22/e0c53ad6-69b8-11e3-a0b9-249bbb34602c_story.html; W. J. Hennigan and Brian Bennett, "Targeting Militants' Cash," *Los Angeles Times*, September 28, 2014, A1, A4.

11. U.S. Congress, Senate Select Committee on Intelligence, *Current and Projected Threats to the United States and Its Interests Abroad* (Washington, DC: U.S. Government Printing Office, 1997), 92; Department of the Treasury, "Treasury Targets Columbian Money Laundering Network Tied to FARC," May 6, 2010.

12. Mark Landler and Choe Sang-Hun, "In Kim's Death, an Extensive Intelligence Failure," *New York Times*, December 20, 2011, A1, A12; "Spies Track Physical Illnesses of Foreign Leaders," www.voanews.com, September 20, 2011, http://www.voanews.com/content/spies-track-physical-illnesses-of-foreign-leaders-130222673/171599.html; Alyce M. Glradi, Leslie R. Pyenson, Jon Morris, and Francis X. Brickfield, "Impact of Coronary Heart Diseases on World Leaders," *Annals of Internal Medicine* 134, no. 4 (February 20, 2001): 287–290; U.S. Interests Section Havana, Subject: Cuba: How Believable Is a Fidel Castro Comeback?, www.nytimes.com, March 16, 2007, http://www.nytimes.com/interactive/2010/11/28/world/20101128-cables-viewer.html#report/cuba-07HAVANA258; David E. Sanger, "Militant in Beheading Videos Has Been Identified, F.B.I. Chief Says," *New York Times*, September 26, 2014, A11.

13. Canadian Security Intelligence Service (CSIS), *The Future of al-Qaeda: The Results of a Foresight Project* (Ottawa: CSIS, 2013); U.S. Congress, *Al Qaeda in Yemen and Somalia: A Ticking Time Bomb* (Washington, DC: U.S. Government Printing Office, 2010); Ernest Sternberg, "Purifying the World: What the New Radical Ideology Stands For," *Orbis* 54, no. 1 (Winter 2010): 61–86.

14. See David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (New York: Free Press, 2010); Gordon Corera, *Shopping for Bombs: Nuclear Proliferation, Global Insecurity and the Rise of the A. Q. Khan Network* (New York: Oxford University Press,

2006); David E. Sanger, Andrew Lehren, and Rich Gladstone, "With the World Watching, Syria Amassed Nerve Gas," *New York Times*, September 8, 2013, 1, 9; Gunther Latsch, Fidelius Schmid, and Klaus Wiegrefe, "Did German Companies Aid Syrian Chemical Weapons?" *Spiegel Online*, January 23, 2015, http://www.spiegel.de/international/germany/german-companies-suspected-of-aiding-syrian-chemical-weapons-program-a-1014722.html.

15. Barack Obama, White House, *National Strategy for Counterterrorism*, June 29, 2011, http://www.whitehouse.gov/blog/2011/06/29/national-strategy-counterterrorism; U.S. Congress, House Committee on International Relations, *The Threat from Russian Organized Crime* (Washington, DC: U.S. Government Printing Office, 1996); June S. Beittel, Congressional Research Service, *Mexico's Drug Trafficking Organizations: Source and Scope of the Violence*, April 15, 2013, https://www.fas.org/sgp/crs/row/R41576.pdf.

16. Richard Smith, "The Intelligence Community and the Environment: Capabilities and Future Missions," *Environmental Change and Security Project Report* 2 (Spring 1996): 103–108; National Geospatial-Intelligence Agency, Press Release 2015-01, "NGA, Digital Globe Human Geography Data and Satellite Imagery and International Ebola Response," January 7, 2015, https://www1.nga.mil/MediaRoom/PressReleases/Pages/2015-01.aspx.

17. Office of the Press Secretary, White House, "Criteria for Decisionmaking on U.S. Arms Exports," Washington, D.C., February 17, 1995, 1.

18. Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2008*, Department of Defense, 2009, http://www.defense.gov/pubs/pdfs/China_Military_Report_08.pdf, 1; Ken Dilanian, "Quick Strides by China's Military," *Los Angeles Times*, January 7, 2011, A1, A22; Keith Bradsher, "China Said to Bolster Missile Capabilities," *New York Times*, August 25, 2012, A5; Edward Wong and Nicola Clark, "China's Arms Industry Makes Global Trends," *New York Times*, October 21, 2013, A1, A3; Saeed Shah, "China-Pakistan Reactor Deal Spurs Concern," *Wall Street Journal*, October 16, 2013, A11; Jane Perlez and Martin Fackler, "China Patrols Air Zone over Disputed Islands," *New York Times*, November 29, 2013, A17; Bill Gertz, "China Conducts Second Flight Test of New Long-Range Missile," *Washington Free Beacon*, December 17, 2013; Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013*, 2013, http://www.defense.gov/pubs/2013_china_report_final.pdf; Shirley A. Kan, Congressional Research Service, *China and Proliferation of Weapons of Mass Destruction and Missiles: Policy Issues*, January 5, 2015, http://fas.org/sgp/crs/nuke/RL31555.pdf.

19. U.S. Congress, Senate Select Committee on Intelligence, Report 113–71, *Report of the Select Committee on Intelligence, United States Senate, Covering the Period January 5, 2011 to January 3, 2013*, 2013, https://www.fas.org/irp/congress/2013_rpt/srpt113-7.pdf, 9; David E. Sanger, "Intelligence on North Korea, and Its New Leader, Remains Elusive," *New York Times*, May 7, 2013, A6; Entous, Gorman, and Woo, "Portrait of New Leader Takes Shape"; Adam Entous, Julian E. Barnes, and Nour Malas, "Elite Syrian Unit Scatters Chemical Arms Stockpile," *Wall Street Journal*, September 13, 2013, A1, A7; Robert F. Worth, "Yemen Emerges as Base for Qaeda Attacks," *New York Times*, October 30, 2010, A6; Rick Gladstone, "Launching Site in Iran Raises Missile Worries," *New York Times*, August 9, 2013, A5; Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the Democratic People's Republic of Korea 2013*, 2013, http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf; Ken E. Gausse, *North Korean Leadership Dynamics and Decision-Making Under Kim Jong-un: A Second Year Assessment*, Center for Naval Analyses, March 2014, https://www.cna.org/sites/default/files/news/FlipBooks/NKorea_Year2_web/flipviewerxpress.html.

20. Andrew E. Kramer, "Russia Sending Missile Systems to Shield Syria," *New York Times*, June 16, 2012, A1, A8; Daniel Michaels, "Russia's New Air Power Turns Heads," *Wall Street Journal*, June 21, 2013, B8; "Russia Fields More Topol-M ICBMs," *Global Security Newswire*, December 21, 2010, http://www.nti.org/gsn/article/russia-fields-more-topol-m-icbms; David M. Herszenhorn, "Prosecutor Urges Six-Year Term for Russian Opposition Leader," *New York Times*,

July 6, 2013, A4; Jim Nichol, Congressional Research Service, *Russian, Political, Economic, and Security Issues and U.S. Interests*, September 13, 2013, https://www.fas.org/sgp/crs/row/RL33407.pdf; Maxim Pyadushkin, "Russian Resurgence," *AW&ST*, December 16, 2013, 32; Bill Gertz, "Russia Tests Multi-Warhead ICBM," www.freebeacon.com, April 14, 2014, http://freebeacon.com/national-security/russia-tests-multi-warhead-icbm; Trude Pettersen, "Russia Builds Huge Nuclear Missile Depot in Severomorsk," www.barentsobserver.com, December 13, 2013, http://barentsobserver.com/en/security/2013/12/russia-builds-huge-nuclear-missile-depot-severomorsk-13-12; Reid Standish, "Where in the World Is Vladimir Vladimirovich Putin? Not Giving Birth," www.foreignpolicy.com, March 13, 2015, http://foreignpolicy.com/2015/03/13/where-in-the-world-is-vladimir-vladimirovich-putin-not-giving-birth.

21. James R. Clapper, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, Statement for the Record before the House Permanent Select Committee on Intelligence, February 26, 2015, http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf, ii.

22. Ibid., ii–iii.

23. Commission on CIA Activities Within the United States, *Report to the President* (Washington, DC: U.S. Government Printing Office, 1975), 6.

24. Headquarters, U.S. Air Force, Assistant Chief of Staff, Intelligence, I INOI 80-1, "The Intelligence Role in Research, Development, Test and Evaluation (RDT&E)," January 18, 1985, Internet Archive, https://archive.org/stream/CIADocuments/CIA-303_djvu.txt; Chief of Naval Operations, OPNAV Instruction 3811.1E, "Subject: Threat Support to the Defense Acquisition System," January 4, 2012, 1.

25. Patrick Tyler, "The Rise and Fall of the SSN 688," *Washington Post*, September 21, 1986, A1, A18.

26. Jeffrey T. Richelson, *A Century of Spies: Intelligence in the Twentieth Century* (New York: Oxford University Press, 1995), 257–258, 269, 272, 395; David Wise, *Nightmover: How Aldrich Ames Sold the CIA to the KGB for $4.6 Million* (New York: HarperCollins, 1995), 59–66, 105–106, 124, 271, 327; Barry G. Royden, "Tolkachev, a Worthy Successor to Penkovsky," *Studies in Intelligence* 47, no. 3 (2003): 5–33; Sandra Grimes and Jeanne Vertefeuille, *Circle of Treason: A CIA Account of Traitor Aldrich Ames and the Men He Betrayed* (Annapolis, MD: Naval Institute Press, 2012), 76.

27. Dwayne A. Day, John Lodgson, and Brian Latell, eds., *Eye in the Sky: The Story of the CORONA Spy Satellites* (Washington, DC: Smithsonian Institution Press, 1998); Curtis Peebles, *The CORONA Project* (Annapolis, MD: Naval Institute Press, 1997); Frederic C. E. Oder, [deleted], and Paul E. Worthman, *The HEXAGON Story* (Washington, DC: National Reconnaissance Office, December 1992), 93, 136, 138, 174.

28. DCI Interagency Balkan Task Force, *Bosnian Serb Air Defense Forces*, June 12, 1995; Craig Whitlock and Barton Gellman, "To Hunt Osama bin Laden, Satellites Watched over Abbottabad, Pakistan, and Navy SEALs," www.washingtonpost.com, August 29, 2013, http://www.washingtonpost.com/world/national-security/to-hunt-osama-bin-laden-satellites-watched-over-abbottabad-pakistan-and-navy-seals/2013/08/29/8d32c1d6-10d5-11e3-b4cb-fd7ce041d814_story.html.

29. Zbigniew Brzezinski, *Power and Principle: Memoirs of the National Security Adviser, 1977–1981* (New York: Farrar, Straus & Giroux, 1983), 248.

30. Steve Coll, "U.S. Halted Nuclear Bid by Iran," *Washington Post*, November 17, 1992, A1, A30.

31. Barton Gellman and John Pomfret, "U.S. Action Stymied China Sale to Iran," *Washington Post*, March 13, 1998, A1, A20; Walter Pincus, "Russia: Laser Deal with Iran Blocked," *Washington Post*, September 20, 2000, A25.

32. Seymour Hersh, *The Price of Power: Kissinger in the Nixon White House* (New York: Summit, 1983), 103.

33. Benjamin Weiser, "A Question of Loyalty," *Washington Post Magazine*, December 13, 1992, 9ff.; Benjamin Weiser, *A Secret Life: The Polish Officer, His Covert Mission, and the Price He Paid to Save His Country* (New York: Public Affairs, 2004); Patrick E. Tyler, "U.S. Said to Plan Bombing of Iraqis if They Gas Rebels," *New York Times*, March 10, 1991, 1, 15; Mark Mazzetti, Robert F. Worth, and Eric Liptor, "Quick Response to Intelligence Foiled Bombers," *New York Times*, November 1, 2010, A1, A6.

34. Ann Devroy and R. Jeffrey Smith, "U.S. Evidence Suggests China Breaks Arms Pact," *Washington Post*, May 18, 1993, A9; Douglas Jehl, "China Breaking Missile Pledge, U.S. Aides Say," *New York Times*, May 6, 1993, A1, A6; John M. Goshko, "U.S. Warns China of Sanctions of Missile Exports to Pakistan," *Washington Post*, July 26, 1993, A10; "Psst . . . Want to Buy a Missile?," *Newsweek*, September 6, 1993, 28; R. Jeffrey Smith, "Ukraine Begins to Dismantle Nuclear Missiles Aimed at U.S.," *Washington Post*, July 28, 1993, A13; Department of State, *Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements Commitments*, July 2014, http://www.state.gov/documents/organization/230108.pdf, 8.

35. Hugh Trevor-Roper, *The Philby Affair: Espionage, Treason and Secret Services* (London: Kimber, 1968), 66.

36. U.S. Congress, Senate Committee on Foreign Relations, *Nomination of Henry A. Kissinger* (Washington, DC: U.S. Government Printing Office, 1973). For evidence that Kissinger did not always follow his own advice, see Hersh, *The Price of Power*, 529–560.

37. National Security Council, *Report on Presidential Review Memorandum/NSC 11: Intelligence Structure and Mission*, 1977, 1.

38. Office of the Director of National Intelligence, ODNI News Release No. 1, "DNI Releases Requested Budget Figure for FY 2016 Appropriations," February 2, 2015; Department of Defense, Release No. NR-034-15, "DOD Releases Military Intelligence Program Base Request for Fiscal Year 2016," February 2, 2015, http://www.defense.gov/releases/release.aspx?releaseid=17128.

2

NATIONAL INTELLIGENCE ORGANIZATIONS

Of the seventeen organizations that officially constitute the U.S. Intelligence Community (IC), four are national collection and/or analysis organizations: the Central Intelligence Agency (CIA), the National Security Agency (NSA), the National Reconnaissance Office (NRO), and the National Geospatial-Intelligence Agency (NGA). Collectively, these organizations' proposed budgets accounted for almost $41 billion in the fiscal year 2013 budget request (the most recent year for which budget request data are available for individual agencies). Two additional national organizations, while not among the seventeen officially listed, are the Special Collection Service (a joint CIA-NSA operation whose budget comes out of the CIA and NSA budgets) and the still-classified National Underwater Reconnaissance Office (NURO). Collectively, they account for virtually all of the National Intelligence Program budget and over 50,000 Intelligence Community employees.

CENTRAL INTELLIGENCE AGENCY

World War II resulted in the creation of the Office of Strategic Services (OSS), America's first central intelligence organization. Its functions included espionage, covert action (ranging from propaganda to sabotage), counterintelligence (CI), and intelligence analysis. The OSS represented a revolution in U.S. intelligence not only because of the varied functions performed by a single national agency but also because of the breadth of its intelligence interests and its use of scholars to produce finished intelligence.[1] In the aftermath of World War II, President Harry S. Truman ordered the OSS disbanded; it officially closed down on October 1, 1945. Its secret intelligence and counterintelligence branches were transferred to the War Department to form the Strategic Services Unit, while the Research and Analysis Branch was moved into the State Department.[2]

At virtually the same time that he ordered closure of the OSS, Truman authorized studies of the intelligence apparatus required by the United States in the postwar world. The result was the creation of the National Intelligence Authority (NIA) and its operational element, the Central Intelligence Group (CIG). Initially responsible for coordinating and synthesizing the reports produced by the military service intelligence agencies and the Federal Bureau of Investigation (FBI), the CIG was soon tasked with clandestine intelligence collection.[3]

The National Security Act of 1947, as part of a general consideration of national security needs, established the Central Intelligence Agency as an independent agency within the Executive Office of the President. The CIA replaced the CIG, and the NIA was eliminated. According to the act, the CIA was to have five functions:

1. To advise the National Security Council [NSC] in matters concerning such intelligence activities of the government departments and agencies as relate to national security.
2. To make recommendations to the National Security Council for the coordination of such intelligence activities of the departments and agencies of the government as related to national security.
3. To correlate and evaluate the intelligence relating to national security and to provide for the appropriate dissemination of such intelligence within the government, using, where appropriate, existing agencies and facilities.
4. To perform for the benefit of existing intelligence agencies such additional services of common concern as the National Security Council determines can be more effectively accomplished centrally.
5. To perform other such functions and duties related to intelligence affecting national security that the National Security Council may from time to time direct.[4]

The provisions of the act left considerable scope for interpretation. Thus, the fifth and final provision has been cited as authorization for covert action operations. In fact, the provision was intended only to authorize espionage.[5] The ultimate legal basis for covert action is presidential direction and congressional approval of funds for such programs.

Whatever the intentions of Congress in 1947, the CIA developed in accord with a maximalist interpretation of the act. Thus, the CIA became the primary U.S. government intelligence agency for intelligence analysis, clandestine human intelligence collection, and covert action. It also came to play a major role in the development of reconnaissance and other technical collection systems employed for gathering imagery, signals, and measurement and signature intelligence.

President Ronald Reagan's Executive Order 12333, still partially in effect, permits the CIA to secretly collect "significant" foreign intelligence within the United States if the collection effort does not target the domestic activities of U.S. citizens and corporations. The order also gives the CIA authority to conduct, within the United States, "special activities" or covert actions approved by the president, that are not intended to influence U.S. political processes, public opinion, or the media.[6]

The CIA's founding legislation established the position of Director of Central Intelligence (DCI), responsible for managing the activities of the entire Intelligence Community as well as running the CIA. The Intelligence Reform and Terrorism Prevention Act of 2004 eliminated the DCI position and established the position of Director of National Intelligence (DNI) to oversee and guide the activities of the Intelligence Community. The individual heading the CIA became the Director, Central Intelligence Agency (D/CIA).[7]

Headquartered in Langley, Virginia, just south of Washington, D.C., the CIA has a number of other offices scattered around the Washington, D.C., area, particularly in northern Virginia. In 1991 the CIA had approximately 20,000 employees, but

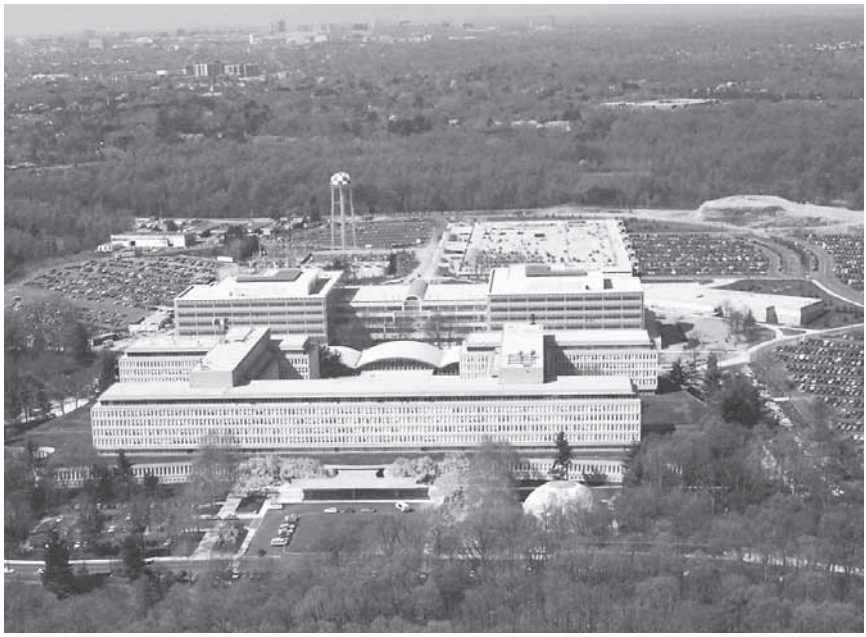


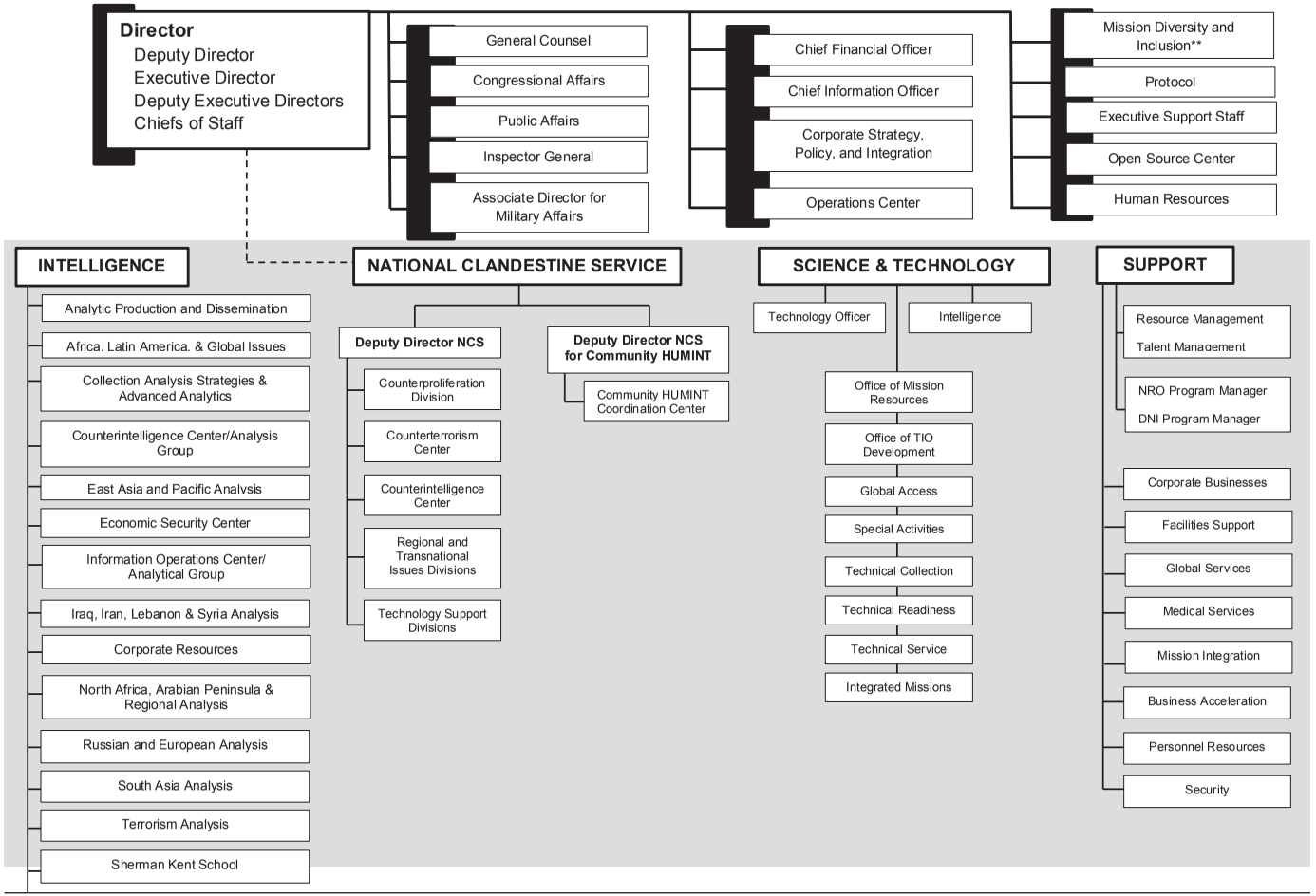
PHOTO 2.1 CIA headquarters, Langley, Virginia. *Photo credit:* CIA.

post–Cold War reductions in the 1990s and the transfer of the CIA's imagery analysts to the National Imagery and Mapping Agency (NIMA) probably reduced that number to about 16,000. In the aftermath of 9/11, the CIA expanded; by September 2011, its approximate personnel strength passed the 21,000 mark. Its requested budget for the 2013 fiscal year was $14.7 billion, approximately a fivefold increase from its 1994 budget ($3.1 billion).[8]

As Figure 2.1 indicates, in addition to the offices and staff elements that report to the CIA's director, deputy director and deputy executive directors, there were, as of March 2015, four major directorates. Two, the National Clandestine Service (NCS) and the Directorate of Science and Technology (DS&T), were fully or partially involved in intelligence collection; another, the Directorate of Intelligence (DI), was responsible for intelligence analysis; the fourth, the Directorate of Support, was responsible for a variety of support functions.

The NCS, formerly the Directorate of Operations and before that the Directorate of Plans, was responsible for clandestine collection and covert action. Established in 2005, it also absorbed the clandestine collectors of the Defense HUMINT Service (DHS), created in the mid-1990s to consolidate service human intelligence (HUMINT) activities. The NCS was headed by a director appointed to manage human intelligence and covert action operations of the CIA and to "coordinate, deconflict, and assess HUMINT operations through the IC." The NCS director had two deputies, one responsible for the daily activities of the NCS divisions and centers of the CIA and another who focused on human intelligence activities across the Intelligence Community.

FIGURE 2.1 Organization of the Central Intelligence Agency



Source: CIA.

The latter, the Deputy Director of the NCS for Community HUMINT, supervised the Community HUMINT Coordination Center, the National HUMINT Requirements Tasking Center, and a center devoted to HUMINT standards and practices.[9]

Figure 2.1 shows the structure of the NCS as presented in the unclassified 2015 CIA organizational chart. It indicates the existence of a number of "Technology Support Divisions" that probably augment the work of the DS&T's Office of Technical Service (OTS). These divisions, in turn, probably trace their origin to Deputy Director of Operations Thomas Twetten's creation, in the early 1980s, of a rival technology group with the operations division.[10]

The other components of the NCS comprised seven regional divisions, one division with a worldwide mission, and five centers. The National Resources Division (NRD), established by the 1991 merger of the Foreign Resources Division (FRD) and the National Collection Division, operated in the United States. The NRD had offices in about thirty U.S. cities. In 2005 it was reported that NRD headquarters would be relocated to Denver, Colorado, "for operational reasons."[11]

The two divisions that merged to form the NRD became its branches. The FRD was created in 1963 as the Domestic Operations Division and assigned responsibility for "clandestine operational activities of the Clandestine Services conducted within the United States against foreign targets." Today, the Foreign Resources Branch (FRB) is responsible for locating foreign nationals of special interest residing in the United States and recruiting them to serve as CIA assets when they return home (or to some other foreign location). To identify such individuals the FRD has relationships with scores of individuals in U.S. academic institutions, including faculty. These individuals do not attempt to recruit students but assist by providing background information and occasionally brokering introductions.[12] According to one report, a key element of FRB operations (which constituted nearly 30 percent of the NRD's activities) is the recruitment, while they are in the United States, of foreign scientists, engineers, and corporate officials to provide telecommunications intelligence or assist the U.S. Intelligence Community in acquiring such intelligence. The program involved is, or was, designated MXSCOPE, according to the report.[13]

The National Collection Branch (NCB), which before being known as the National Collection Division had been designated the Domestic Collection Division and the Domestic Contact Service, collected intelligence from U.S. residents who had traveled abroad, including scientists, technologists, economists, and energy experts returning from foreign locations of interest. Among those interviewed were academics; in 1982 the Domestic Collection Division was in touch with approximately nine hundred individuals on 290 campuses in the United States.[14] The chief of the NRD (and probably the NCB and FRB chiefs) could approve the use of employees or invitees of an organization within the United States to collect significant foreign intelligence at fairs, workshops, symposia, and similar types of commercial or professional meetings open to those individuals in their overt roles but closed to the general public. After 9/11 the division received additional funding, and some offices closed in the 1990s were reopened, bringing the total number of NRD offices to about thirty.[15]

The regional divisions, covering the rest of the world, were the Central Eurasian, Latin American, European, East Asian, Near East, and African divisions. Such divisions formed the core of the CIA's clandestine collection operations since the agency's

creation, directing the activities of the various CIA stations whose officers are responsible for recruiting and/or running sources as well as conducting covert action operations.[16]

One division had worldwide responsibilities. The Special Activities Division (SA) handled paramilitary activities, such as those directed against the Sandinista government in Nicaragua and the Soviet intervention in Afghanistan during the 1980s, as well as those in support of the U.S. efforts directed against al-Qaeda, at unseating the Taliban in Afghanistan, and at deposing Saddam Hussein. One component of the division was the Global Response Staff (GRS), whose members "serve[d] as armed guards for the agency's spies" and in some cases provided security for personnel from other agencies, "including National Security Agency teams deploying sensors or eavesdropping equipment in conflict zones." GRS personnel might also assess the security of potential meeting sites and even make first contact to ensure that case officers were not walking into a trap. SA's heritage included a number of earlier incarnations, including the International Activities Division, the Paramilitary, Insurgency, Narcotics Staff, the Special Activities Staff, and the Military and Special Programs Division.[17]

Two of the five NCS centers, the Counterterrorism Center (CTC) and the Counterintelligence Center (CIC), were established as "DCI Centers" during the tenures of William J. Casey (1981–1987) and William Webster (1987–1991), respectively. The objective was to give heightened status to the counterterrorism and counterintelligence missions as well as to bring together representatives of different Intelligence Community components, including analysts, involved in those missions. In 1997 a Terrorism Warning Group was established within the CTC with the mission of alerting civilian and military leaders to specific terrorist threats. As early as 1996, the CTC established a special unit with about twenty-five staff members, designated Alec Station, to track Osama bin Laden and his top aides. That unit was closed in late 2005. The CTC itself grew from about 300 to more than 1,100 analysts and operators after the terrorist attacks of September 11, 2001.[18]

A June 2005 CIA Office of the Inspector General (OIG) report was critical of the CTC's performance prior to the 9/11 attacks: "Agency officers from the top down worked hard against the al-Qa'ida and Usama Bin Ladin (UBL) targets," but "they did not always work effectively and cooperatively." There were, according to that report, "failures to implement and manage important processes, to follow through with operations, and to properly share and analyze critical data." Those judgments were in sharp contrast to an OIG report published (within classified channels) only a month before the attacks. The executive highlights section of that report began, "The DCI Counterterrorist Center (CTC) is a well-managed component that successfully carries out the Agency's counterterrorist responsibilities to collect and analyze intelligence on international terrorism and to undermine the capabilities of terrorist groups." Nearly a decade later, leading up to May 2, 2011, CTC analysts "found a courier trail that led them to bin Laden's compound in Abbottabad."*[19] In 2013 the CTC was described as the "hub of America's targeted killing operations in Pakistan, Yemen, and

*The Counterterrorist Center was renamed the Counterterrorism Center in 2005. See Mark Mazzetti, *The Way of the Knife: The CIA, a Secret Army, and a War at the Ends of the Earth* (New York: Penguin Press, 2013), 162n.

other places where presidents might choose to wage war in the future." The center's Pakistan-Afghanistan Department directed operations in Pakistan and Afghanistan. The expansion of counterterrorist operations in Yemen and Somalia led to the creation of a department to manage counterterrorist operations in those nations.[20]

The CIC consolidated the Counterintelligence Staff, the Foreign Intelligence Capabilities Unit (established in 1983 to look for attempts by foreign intelligence agencies to influence the perceptions of U.S. intelligence), elements of the administration directorate's Office of Security, and other Intelligence Community elements. The director of the CIC was given the status of Associate Deputy Director for Operations for Counterintelligence. The center "analyzes the capabilities, intentions, and activities of foreign intelligence services."*[21]

Creation of the Counterproliferation Center (CPC) was announced in August 2010. One key element of the CPC is the former NCS Counterproliferation Division (CPD) established in the mid-1990s in recognition of the transnational character of the proliferation of weapons of mass destruction. The CPD was intended to facilitate the CIA's collection of information regarding or neutralization of proliferation activities involving multiple regions of the world—such as those involving A. Q. Khan—without having to operate through several divisions. In addition to the CPD, the CPC, headed by an undercover NCS officer with deputies for operations and analysis, included elements from the DI's Weapons Intelligence, Nonproliferation, and Arms Control Center (WINPAC).[22]

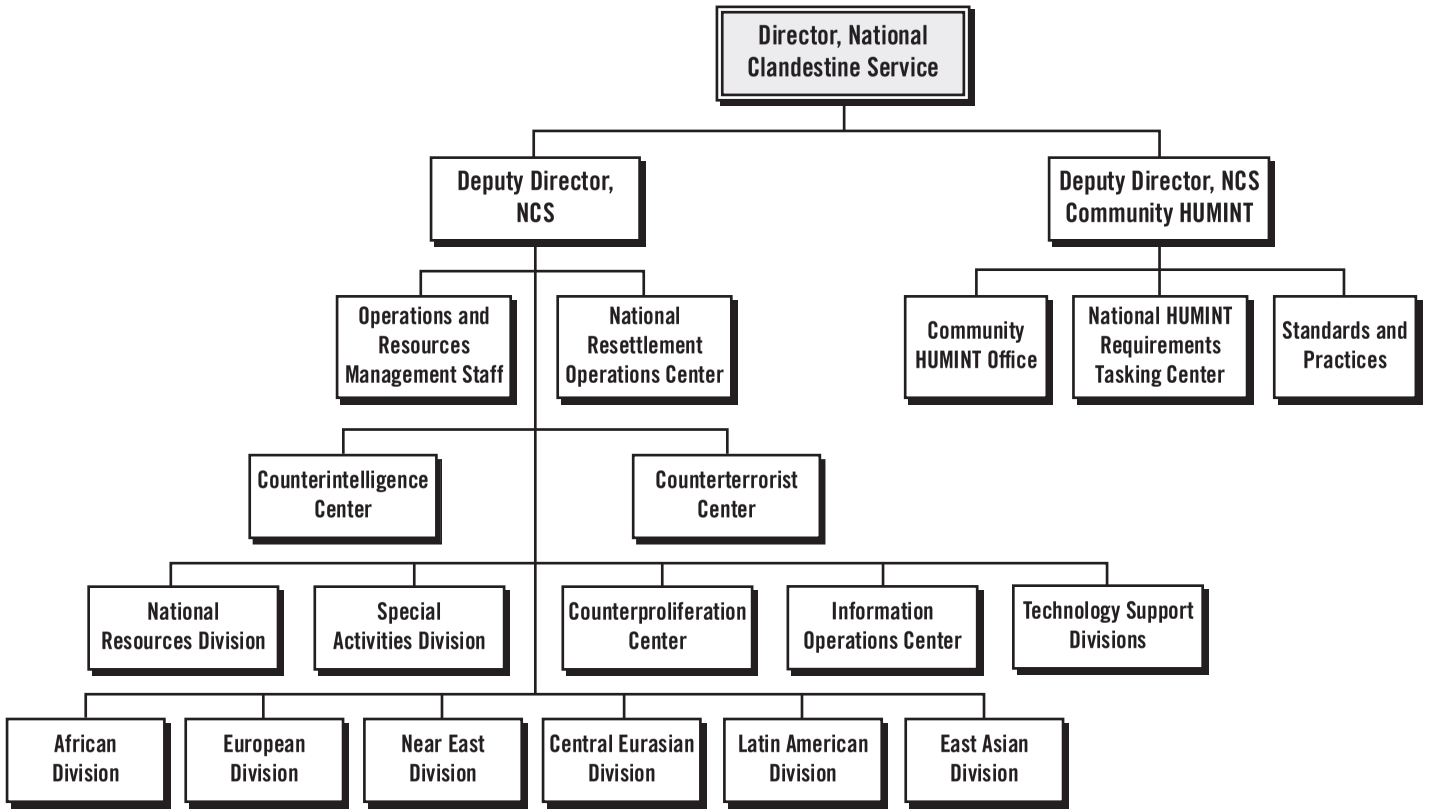
The Information Operations Center (IOC), established in the very late 1990s, absorbed some of the functions of the DS&T's Clandestine Information Technology Office, established in 1996. The office was officially described as responsible for addressing "collection capabilities within emerging information technologies," which at the time included the Internet. A fifth center within NCS was the National Resettlement Operations Center, previously known as the Defector Resettlement Center, established to remedy CIA deficiencies in handling defectors, such as those who played a role in the redefection of Vitaly Yurchenko.[23] The complete organization chart of the NCS probably looks like the one shown in Figure 2.2.

The Directorate of Science and Technology, with over 5,000 employees, was created in 1962 as the Deputy Directorate of Research and assumed responsibility for the CIA's efforts in developing and/or operating technical collection systems, particularly the U-2 and OXCART (A-12) spy planes as well as the CORONA reconnaissance satellite. It became the Deputy Directorate of Science and Technology in 1963 and the Directorate of Science and Technology in 1965.[24]

The DS&T has undergone several reorganizations and has gained and lost responsibilities over the years. In 1963 the DS&T assumed control of the Office of Scientific Intelligence, which had been in the Directorate of Intelligence. In 1976 all science and technical analysis functions reverted to the DI. In 1996 the National Photographic Interpretation Center (NPIC), transferred to the DS&T in 1973, was merged into the

*Whether the centers could truly be considered interagency centers was a matter of perspective. See Douglas E. Garthoff, *Directors of Central Intelligence as Leaders of the U.S. Intelligence Community, 1946–2005* (Washington, D.C.: Center for the Study of Intelligence, 2005), 188–189.

FIGURE 2.2 Probable Organization of the National Clandestine Service



newly created National Imagery and Mapping Agency. In 2005 the responsibility for open source collection, including the activities of the Foreign Broadcast Information Service (FBIS), was transferred from the DS&T to the Office of the Director of National Intelligence, although it is administered by the Director of the CIA.[25]

The post-9/11 impacts on the directorate have included a greater overseas presence, estimated as a 150 percent increase by October 2008. There has also been a greater emphasis on close-access collection relative to that obtained by remote sensors. In addition, "there was a big explosion after 9/11 in the need for tracking and locating technology," the Deputy Director for Science and Technology stated in 2008.[26] Figure 2.1 indicates that a number of DS&T components have been disestablished in the last few years, including the Office of Development and Engineering (OD&E), the Office of Special Communications Programs, and the Office of Systems Engineering and Analysis.

The OD&E could trace it origins directly to the Special Projects Staff established in 1963 to manage CIA reconnaissance satellite efforts, which became the Office of Special Projects in 1965 and the OD&E in 1973. It was involved in the development of major technical collection systems, such as the KH-11 imaging satellite. The office "provide[d] total systems development for major systems—from requirements definition through design engineering, and testing and evaluation, to implementation, operation and even support logistics and maintenance." Prior to the reorganization of the NRO in 1992, the office constituted the NRO's Program B; subsequent to the reorganization it was responsible for providing CIA personnel to work at the reconnaissance office.[27]

The now defunct Office of Special Communications Programs, established in 2003, served as an advocate for programs in the CIA and the wider national security community that were used to provide for the continuous worldwide transfer of data in support of intelligence activities outside the United States. The Office of Systems Engineering and Analysis had been established in 2002 to provide a more independent CIA capability in the field of reconnaissance satellite development in response to concerns that the NRO had become less imaginative and innovative.[28]

The early 2015 version of the DS&T, as shown in Figure 2.1, included eight offices: Mission Resources, Technical Intelligence Officer (TIO) Development, Global Access, Special Activities, Technical Collection, Technical Readiness, Technical Service, and Integrated Missions. The Office of TIO Development is the career development organization for the DS&T (since the term "technical intelligence officer" applies to all DS&T officers). Subsets of the TIO category include operations tradecraft, technical research, technical development, and technical analysis.[29]

A declassified CIA description characterized the Office of Global Access, established in 2003, as responding to "[deleted] requirements combining operations, analysis, and engineering to attack the most difficult technical collection challenges worldwide." The description also stated, somewhat repetitively, that the office "integrate[s] analysis, technology, and tradecraft to attack the most difficult targets, and to provide worldwide collection capability." Also established in 2003, the Office of Special Activities (OSA) provided technical, engineering, research, and analytical expertise for tactical and strategic operations. Both were created out of already existing directorate components.[30]

The Office of SIGINT Operations (OSO) and the Office of Special Projects were merged to form the Office of Technical Collection (OTC). The OSO "develop[ed], operat[ed] and maintain[ed] sophisticated equipment required to perform collection and analysis tasks." OTC personnel provided the CIA contribution to the Special Collection Service (SCS; see below). OSO and its predecessor, the Office of Electronic Intelligence (OEL), were involved in the construction of signals intelligence (SIGINT) facilities operated by China and Norway, in those nations' training of personnel, and in the maintenance of equipment at the sites. The Office of Special Projects, in its last incarnation, was involved in the development and operation of support of systems, including emplaced sensor systems, that collected measurement and signature intelligence (MASINT), SIGINT, and nuclear intelligence. According to a CIA document, the office "develop[ed] collection systems tailored to specific targets." One component of the OTC was the Clandestine MASINT Operations Coordination Center, which likely monitors the output of emplaced MASINT sensors. OTC has also worked with the U.S. Marshals Service to develop technology that can be carried on aircraft and trick cell phones into providing their unique registration information.[31]

The Office of Technical Readiness (OTR), also created in 2003 out of an already existing directorate component, provided support to DS&T technical personnel and facilities overseas, including the construction, operation, and maintenance of directorate facilities. According to its Intellipedia entry, "OTR manages all the elements entailed in field operations." In addition, it worked on the concealment of CIA devices and capabilities as an aid to tradecraft.[32]

The Office of Technical Service was the Technical Services Division of the Directorate of Operations before being transferred to the DS&T in 1973. OTS services included devising secret writing methods, bugging equipment, hidden cameras, coding and decoding devices, enhancing videos and images, and providing chemical imaging. Prior to the April 1980 mission to rescue U.S. hostages in Iran, OTS devised battery-powered landing lights that could be emplaced easily and switched on remotely from the air. After the September 1988 explosion of Pan Am Flight 103 over Lockerbie, Scotland, the OTS matched the timing device to be used in the planned Libyan terrorist operation with a part of the timing device that survived the explosion. In the early 1990s, the service implanted a beacon in a walking stick provided to Osman Ato, an arms importer and financial supporter of Somali warlord General Mohammed Farah Aidid. The beacon allowed Delta Force personnel to capture Ato as he drove through Mogadishu. In 1993 OTS developed a locating system that provided "continuous near-real-time global geolocation information for targets of special interest," the director of OTS reported. In late 2001, a six-member ordnance team from the OTS arrived in Kandahar, Afghanistan, to help dismantle explosive devices encountered by the first CIA teams deployed to the country after 9/11. The team discovered a 2,500-pound improvised explosive device (IED) and disarmed it shortly before it was to explode.[33]

The Office of Integrated Missions, established in March 2009, absorbed elements of the Office of Systems Engineering and Analysis, the In-Q-Tel Interface Center, and one other agency entity. According to a DS&T announcement, over the previous five years, those offices had "delivered new solutions to the toughest problems the Intelligence Community faces, improved the efficiency of our mission infrastructure

backbone and provide access to leading edge commercial technologies."[34] The In-Q-Tel Interface Center served as a liaison between individuals and organizations inside and outside the intelligence agency. The CIA created In-Q-Tel in late 1999 as an in-house nonprofit venture capital firm and appropriated $28.5 million in agency funds for its support. By 2012 it had funded more than 180 companies and had 87 in its current portfolio, a third of which were located in Silicon Valley.[35]

One project funded by In-Q-Tel involved a commercial search engine, named NetOwl, that relied on natural-language processing in place of key words to locate information. In-Q-Tel funding was also vital in developing the Presidential Intelligence Briefing System, used to produce the *President's Daily Brief*. Rather than having intelligence sort through hundreds of cables, the system placed the cables in a Lotus Notes database, performed a variety of search and analysis functions, and then placed the brief on a notebook computer. A third project involved enhancing a piece of software called Triangle Boy, which allowed users to examine websites anonymously.[36]

More recent In-Q-Tel projects involved support to Sonitus Medical, which was developing a tiny, wireless, two-way communications device that is covertly placed in an individual's mouth, as well as to Infinite Z, which makes holographic simulations. Fluidigm and Silver Tail Systems, also recent recipients of In-Q-Tel funding, make microchips that analyze genetic samples and detect suspicious activity on government websites, respectively. Additional recent recipients of In-Q-Tel supported have included Lens Vector, which produces technology for miniature cameras, 3VR, which produces video surveillance equipment that can analyze faces, license plates, and other images, and NetBase, which provides semantic-search capabilities that can read online posts in English, Spanish, French, German, and Portuguese. In 2012, then CIA director David Petraeus reported, "Among the analytic projects underway with In-Q-Tel startups is one that enables collection and analysis of worldwide social media feeds, along with projects that use either cloud computing or other methods to explore and analyze Big Data."[37]

The DS&T also participated in the activities of the NCS Information Operations Center.[38] The Directorate of Intelligence underwent extensive reorganization in the post–Cold War years, including between 2009 and 2013. The 1996 reorganization, the directorate's first major one since 1981, reduced the number of directorate offices from nine to six. After 2009, a number of directorate components were eliminated (with their functions absorbed by other entities), while some new offices were established and others were renamed to reflect a change in the scope of their responsibilities. Disestablished components included the Crime and Narcotics Center (CNC) and the Office of Transnational Issues (OTI). The CNC was staffed by analysts from the CIA, FBI, NSA, and the Defense, State, Treasury departments, who produced finished intelligence on narcotics trafficking and international organized crime. The CNC was established in 1989 as the DCI Counternarcotics Center; its name was changed in 1994 to reflect its additional role in gathering international organized crime intelligence.[39]

The Office of Transnational Issues examined developments in international energy, trade, and finance, as well as topics such as refugee flows, food security, and border tensions. OTI analysts also focused on money laundering, illicit finance, corruption, and sanctions violations. Other office analysts analyzed foreign denial and deception efforts as well as attempts to manipulate U.S. perceptions. Within OTI was the

Medical and Psychological Analysis Center, which produced assessments on global health issues (such as disease outbreaks) and the health of foreign leaders.[40]

As indicated in Figure 2.1, as of early 2015 six directorate offices focused on specific geographic regions. Only one of the geographic offices that existed in 2009, the Office of Russian and European Analysis, remained unchanged. The other geographic offices were Africa, Latin America, & Global Issues (which assumed the responsibilities previously assigned to OTI); East Asia and Pacific Analysis; Iraq, Iran, Lebanon, & Syria Analysis; North Africa, Arabian Peninsula, & Regional Analysis; and South Asia Analysis.

Other key elements of the directorate were the Counterintelligence Center Analysis Group, the Information Operations Center Analytical Group, the Economic Security Center (ESC), the Office of Terrorism Analysis, and the Weapons Intelligence, Nonproliferation, and Arms Control Center. The directorate also houses the Analysis Group of the NCS Counterterrorism Center. The Counterintelligence Center's Analysis Group focused on two specific types of counterintelligence threats. One type is transnational threats, including the counterintelligence component of terrorism or the threats posed to the U.S. government, intelligence operations, and U.S. government information systems by emerging or changing technologies. The second type pertains to the threat posed by foreign intelligence services. The Information Operations Center's Analytical Group evaluated foreign threats, from both state and nonstate organizations to U.S. computer systems, particularly those that support critical infrastructures.[41]

The Economic Security Center, a recent addition to the Directorate of Intelligence's analytical components, was established during David Petraeus's brief tenure (September 2011–November 2012) as CIA director. The CIA did not release any information on the center's function, but it would appear to have been responsible, inter alia, for examining the potential impact of economic and resource issues on the probability of conflict and instability. In that vein, the ESC reportedly absorbed the duties assigned to the joint DS&T-DI Center for Climate Change and National Security, disestablished in 2012, whose mission included examining the impact of desertification, rising sea levels, population shifts, and increased competition for natural resources.[42]

The Office of Terrorism Analysis was the analytic component of the NCS Counterterrorism Center. Its analysts tracked terrorists and states that sponsor terrorism and assessed terrorists' vulnerabilities, analyzing their ideologies, goals, capabilities, associates, and locations. The analysts also examined worldwide terrorist threat information and look for patterns that would allow them to warn of planned terrorist activity. In addition, they sought to identify emerging and nontraditional terrorist groups and possible collusion among terrorist groups. Finally, the office was involved in "identifying, disrupting, and preventing international financial transactions that support terrorist networks and operations."[43]

The core of the Weapons Intelligence, Nonproliferation, and Arms Control Center was established in September 1991 as the DCI Nonproliferation Center (NPC) after disclosures about Iraq's ability to produce nuclear and other weapons of mass destruction indicated that the Intelligence Community had underestimated both the diversity and progress of the program. By 1999, the NPC consisted of about two hundred intelligence analysts and clandestine operators, about a quarter to a third of whom

had come from agencies other than the CIA. The center monitored the worldwide development and acquisition of production technology, designs, components, and entire military systems in the area of nuclear, chemical, and biological weapons, as well as advanced conventional weapons.[44]

NPC also developed strategic plans to help guide the U.S. government's response to the proliferation problem and provided support to collection and law enforcement organizations. It also worked on collection platform development and produced a "gaps" study that identified deficiencies in proliferation-related collection activities. Furthermore, the NPC was authorized to review the Intelligence Community's performance on proliferation activities and to make relevant budget recommendations.[45]

WINPAC was created in March 2001 from the merger of the NPC, the DCI's Arms Control Intelligence Staff, and the OTI's Weapons Intelligence Staff. It is responsible for (1) "studying the development of the entire spectrum of threats, from weapons of mass destruction . . . to advanced conventional weapons like lasers, advanced explosives, and armor, as well as all types of missiles," and (2) providing intelligence support to U.S. nonproliferation, threat reduction, and arms control efforts.[46]

Additional Directorate of Intelligence components included the Offices of Analytic Production and Dissemination, Corporate Resources, and Collection Analysis and Strategies, as well as the Sherman Kent School for Intelligence Analysis. The Office of Collection Analysis and Strategies assists DI analysts in making use of collection systems and provided guidance for the development of future systems. Specifically, its functions include informing the president and other senior policymakers about U.S. collection capabilities and intelligence-gathering issues, running special collection efforts, evaluating the use and value of current collection capabilities, guiding the development of future collection programs, and providing twenty-four-hour collection support to the CIA's Operations Center.[47]

The offices under the Directorate of Support consisted of the Offices for Corporate Business, Facilities Support (previously Global Infrastructure), Global Services, Medical Services, Mission Integration, Business Acceleration (the new office), Personnel Resources, and Security. Of these components, the oldest was the Office of Medical Services, which has been responsible for medical examinations and immunizations for employees and dependents traveling overseas, health education, emergency health care, and psychiatric services. It also helped develop the Psychological Assessment Program to determine which individuals are best suited for the agency and is involved in psychiatric and medical intelligence production.[48]

The Office of Security had been split into separate components responsible for personnel security and physical security, but these were then reunited, giving the office responsibility for clearing personnel, investigating possible security breaches, and ensuring the security of CIA facilities. The other offices in the directorate provide a variety of functions essential to CIA operations, including provision of facilities for communications between CIA headquarters and overseas personnel, logistics, maintenance of facilities, disbursement of funds for CIA operations, determination of personnel requirements, and training and education. The directorate operated the CIA's training facilities, including the Armed Forces Experimental Training Facility at Camp Peary, Virginia, and the Harvey Point Defense Testing Activity in Hertford, North Carolina. A CIA arms depot, presumably the responsibility of the Directorate of

Support and designated the "Midwest Depot," appears to be located at the U.S. Army Camp Stanley Storage Activity in San Antonio, Texas.[49]

In early March 2015, CIA director John Brennan announced a major reorganization of the agency that would involve the renaming of several major components, the establishment of ten hybrid mission centers, and the creation of a new directorate. Specifically, the Directorate of Intelligence would become the Directorate of Analysis, while the National Clandestine Service would revert to its previous name—the Directorate of Operations. Further, both would serve largely as recruiting and training organizations. Responsibility for both analytical and operational (including liaison) activities would be shifted to the ten centers (managed by assistant directors), seven of which would be regional and three functional. The new Directorate of Digital Innovation will focus on exploiting advances in computer technology and communications.[50]

In addition to the seven regional centers, the functional centers will include expanded versions of at least two already in existence—the Counterproliferation Center and the Counterterrorism Center—and possibly, a third, the Counterintelligence Center. The Digital Innovation Directorate will absorb the Open Source Center as well as the Information Operations Center from NCS. It will also seek to assist the CIA in employing digital means of persuading targets to provide secret information. In addition, the directorate will assist CIA officers in evading detection overseas due to the use of phones, computers, or ATM cards.[51]

In explaining the creation of the centers, Brennan observed, "There was . . . great esprit de corps in those directorates, but also at times, those directorates were a bit siloed, and were stovepiped." He also observed that critical data about threats could still fall into gaps between different divisions. With regard to creation of the Directorate of Digital Innovation, he noted that "the digital world touches every aspect of our business" and that the CIA had been slow to rise to the challenge of digital espionage.[52]

The announcement left a number of questions unanswered, not just because of classification issues but because Brennan indicated that the reorganization was a work in progress that would take several months to accomplish. Questions involved how it would impact the organizational structure of the Support and Science & Technology directorates (which retained their names), what would happen to organizations within the NCS that don't fit neatly into a geographic structure (e.g., the Special Activities Division, the National Resettlement Operations Center), whether the National Resources Division would be part of a geographic center, and whether the Counterintelligence Center would become the third mission center.

NATIONAL SECURITY AGENCY

The predecessor of the National Security Agency, the Armed Forces Security Agency (AFSA), was established within the Department of Defense (DOD) under the command the Joint Chiefs of Staff on May 20, 1949. In theory, the AFSA was to direct the communications intelligence activities of the military service SIGINT units (at the time consisting of the Army Security Agency, Naval Security Group, and Air Force Security Service). In practice, the AFSA had little power since its functions were defined in terms of activities not performed by the service units.[53]

On October 24, 1952, President Harry S. Truman sent a top secret, eight-page (now declassified) memorandum titled "Communications Intelligence Activities" to the Secretaries of State and Defense; the memorandum abolished the AFSA and transferred its personnel to the newly created National Security Agency, established that day by draft National Security Council Intelligence Directive No. 9. (The draft was formally approved in December.)[54]

The NSA had its origins in a December 10, 1951, memo sent from Walter Bedell Smith to National Security Council executive secretary James B. Lay, stating that "control over, and coordination of, the collection and processing of Communications Intelligence had proved ineffective" and recommending a survey of communications intelligence activities. The resulting report, completed within six months, identified the need for a much greater degree of coordination and direction at the national level. As the change in the security agency's name indicated, the NSA's role was to extend beyond the armed forces; hence, the NSA is considered to be "within but not part of DOD."[55]

Although the agency was created in 1952 and the fact of its existence was never classified, the *U.S. Government Organization Manual* did not note it as a "separately organized agency within the Department of Defense" that "performs highly specialized technical and coordinating functions relating to national security" until 1957. But the NSA's existence was a matter of public knowledge from at least early 1954, when Washington, D.C., newspapers ran several stories concerning the construction of its new headquarters at Fort George G. Meade, Maryland. In late 1954 the NSA was again in the news when one of its employees was caught taking secret documents home.[56]

The charter for NSA is a National Security Council Intelligence Directive (NSCID). The current version, NSCID No. 6, "Signals Intelligence," which has not been updated since January 17, 1972, directs the NSA to produce SIGINT "in accordance with the objectives, requirements, and priorities established by the Director of Central Intelligence Board." The directive also authorizes the Director of NSA (DIRNSA) "to issue direct to any operating elements engaged in SIGINT operations such instructions and assignments as are required" and states that "all instructions issued by the Director under the authority provided in this paragraph shall be mandatory, subject only to appeal to the Secretary of Defense."[57]

NSCID No. 6 defines SIGINT activities as consisting of communications intelligence (COMINT) and electronic intelligence (ELINT). The directive states, "COMINT activities shall be construed to mean those activities which produce COMINT by interception and processing of foreign communications. . . . Interception comprises range estimation, transmitter operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of plain text, the fusion of those processes, and the reporting of results. COMINT and COMINT activities as defined herein shall not include (a) any intercept and processing of unencrypted written communications, press and propaganda broadcasts, or (b) censorship."[58]

When established, the NSA did not have authority over ELINT operations, which remained the responsibility of the military services, but this authority was assigned to the agency in 1958. NSCID No. 6 defines ELINT as "the collection (observation and recording) and the processing for subsequent intelligence purposes, of information derived from foreign noncommunications, electro-magnetic radiation emanating from

PHOTO 2.2 NSA headquarters, Fort George G. Meade, Maryland. *Photo credit:* NSA.

other than atomic detonation or radioactive sources. ELINT is the technical and intelligence product of ELINT activities."[59] From its inception, ELINT was primarily associated with the interception of emanations from radar systems. Telemetry intelligence (TELINT), the interception and exploitation of signals from foreign missile tests, was originally a branch of ELINT but became a separate "INT" in 1971. Subsequently, it became part of a new third component of SIGINT, foreign instrumentation signals intelligence (FISINT), which included telemetry, missile and satellite command signals, beacons, and computer-based data.

The SIGINT responsibilities of NSA and its director are specified by a 2010 DOD directive, "The National Security Service and Central Security Service." It specifies that NSA will

- Collect (including through clandestine means), process, analyze, produce, and disseminate SIGINT information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions. . . .
- Provide SIGINT support for the conduct of military operations, pursuant to tasking, priorities, and standards of timeliness assigned by the Secretary of Defense.
- Establish and operate an effective, unified organization for SIGINT activities, including executing any SIGINT-related functions the Secretary of Defense so directs.
- Develop rules, regulations, and standards governing the classification and declassification of SIGINT. . . .
- Exercise SIGINT operational control and establish policies and procedures for departments and agencies to follow when appropriately performing SIGINT activities.[60]

Computer network exploitation, an adjunct to the traditional SIGINT mission (whether involving remote collection or close access via technical surveillance), has been defined as "enabling operations and intelligence collection to gather data from target or adversary automated systems or networks." Such exploitation can be intended to produce information in support of intelligence collection or as a prelude to computer network attack, an activity delegated to the NSA in March 1997 by the Secretary of Defense.[61]

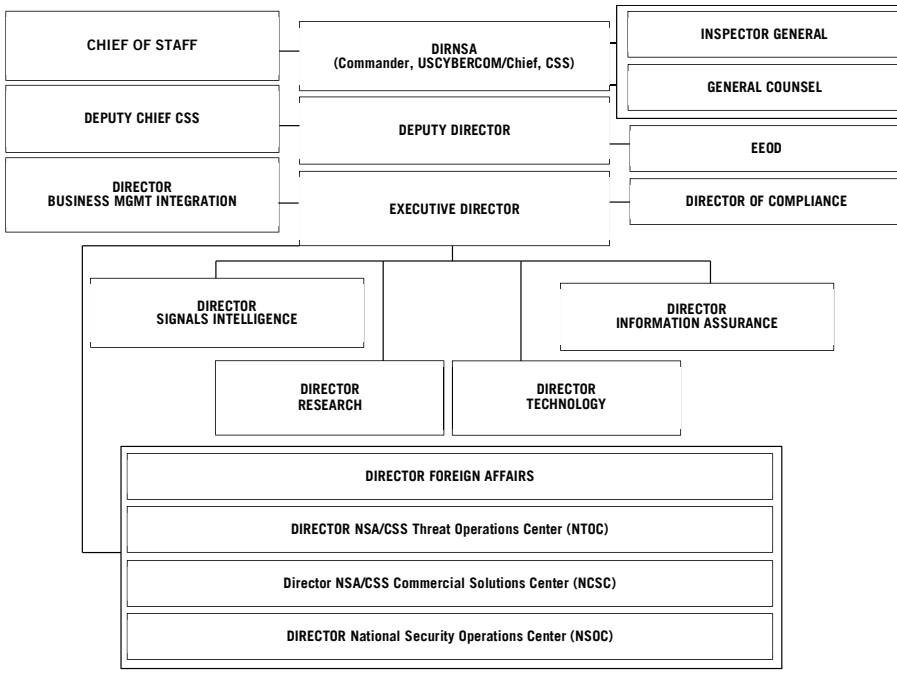
The NSA has another major mission, originally known as communications security (COMSEC), which became information security in the 1980s and is currently known as information assurance (IA). In its IA role, NSA creates, reviews, and authorizes the communications procedures of a variety of government agencies, including the State and Defense departments, the CIA, and the FBI. This role includes development of secure data and voice transmission links on satellite systems, including those for defense communications satellites. Likewise, for sensitive communications, FBI agents have used a special scrambler phone requiring a different code from the NSA each day. The agency's IA responsibilities also include securing communications security for strategic weapons systems so as to prevent unauthorized intrusion, interference, and jamming. In addition, NSA is responsible for developing the codes by which the president must identify himself in order to authorize the release of nuclear weapons. As part of its IA mission, NSA is also responsible for protecting national security data banks and computers from unauthorized access by individuals or governments.[62]

NSA headquarters at Fort George G. Meade houses from 20,000 to 24,000 employees in three buildings. The NSA's requested budget for the 2013 fiscal year was $10.8 billion. This figure does not take into account funding for the military service cryptologic elements that conduct eavesdropping operations on behalf of NSA, just as the personnel figure does not include the personnel in those units.[63]

In addition to directing the agency's activities, the NSA director is responsible for supervising the SIGINT activities of the Service Cryptologic Elements (SCEs), which consists of the Navy Fleet Cyber Command, Marine Corps support battalions, components of the Army Intelligence and Security Command, components of the 25th Air Force, and the Coast Guard Deputy Assistant Commander for Intelligence. In this role, the director serves as the head of the Central Security Service (CSS). The CSS function of the NSA, with the DIRNSA serving simultaneously as CSS chief, was established in 1971 "to provide a unified, more economical and more effective structure for executing cryptologic and related operations presently conducted under the Military Departments." There is, however, no separate CSS staff.[64]

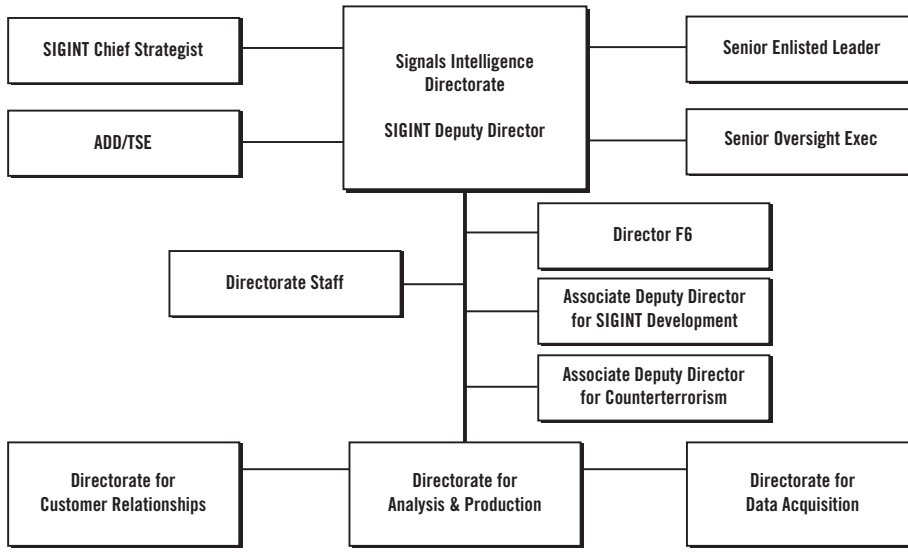
As shown in Figure 2.3, NSA consists of five directorates (Signals Intelligence, Information Assurance, Research, Technology, and Foreign Affairs) and other components, but the two that perform its fundamental functions are the Directorates of Signals Intelligence and Information Assurance (IAD). The Signals Intelligence Directorate (formerly the Directorate of Operations), whose organization chart is shown in Figure 2.4, contains three directorates that highlight the three key elements of the directorate's mission: collecting SIGINT (Directorate for Data Acquisition), analyzing data and producing reports (Directorate for Analysis and Production), and providing those reports to the appropriate individuals in NSA or in other government agencies (Directorate for Customer Relationships).

FIGURE 2.3 Organization of the National Security Agency



Source: NSA.

FIGURE 2.4 Organization of the NSA Signals Intelligence Directorate



Source: NSA.

Among the key offices of the Directorate for Data Acquisition are the Office of Tailored Access Operations, which engages in computer network exploitation; Global Access Operations, which operates a variety of remote collection operations, including satellites and satellite communications intercept stations; and Special Source Operations, which handles relations with corporate entities, including Internet service providers and telecommunications companies. Within the Directorate for Analysis and Production are a number of regional and transnational "product lines," including South Asia, Russia, counterterrorism, foreign counterintelligence, combating proliferation, and arms control.[65]

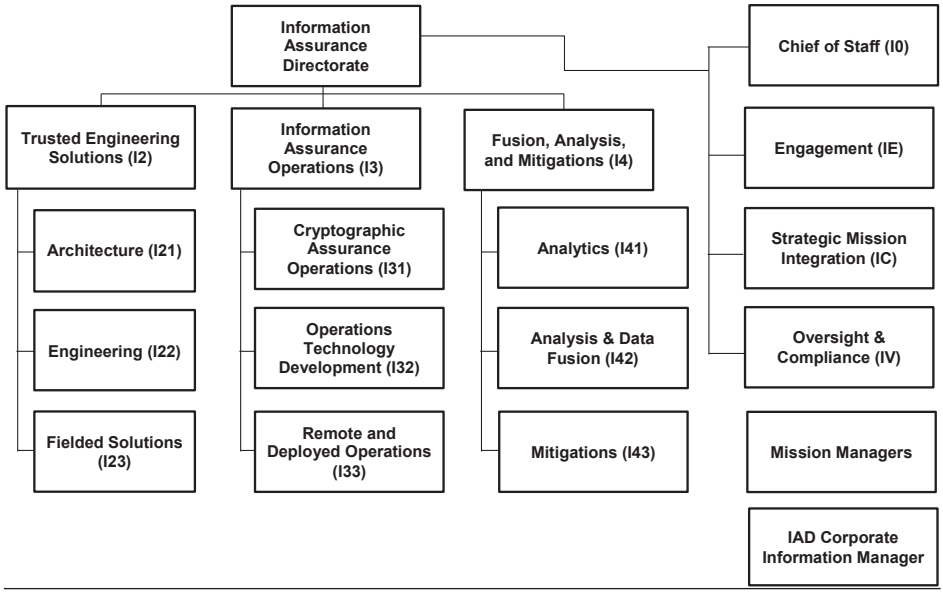
Another product line is the one for weapons and space, and a key element in that product line is the Defense Special Missile and Aerospace Center (DEFSMAC), established as the Defense Special Missile and Astronautics Center (then referred to as Defense/SMAC) via a secret April 27, 1964, DOD directive. Its current charter is Department of Defense Instruction S-5100.43 of September 24, 2008, which reflects the replacement of "Astronautics" with "Aerospace," a change made in 2002. DEFSMAC was reported to have a staff of more than 230 in 2001.[66]

According to a history of DEFSMAC, its mission is "to accomplish 24 hour surveillance of foreign missile and space activities; alert and exercise technical control of DOD intelligence collection systems directed against foreign missile and space events; provide technical support, including tip-off, to all DOD missile and space intelligence collection activities to enable mission accomplishment; and perform all source current analysis and reporting of all detected foreign missile and space events based on initial site reporting of all detected foreign missile and space events received up to 72 hours after the event."[67] According to a former NSA deputy director, "DEFSMAC is a combination of [Defense Intelligence Agency (DIA)] with its military components and the NSA. It has all the inputs from all the assets and is a warning activity. They probably have a better 'feel' for any worldwide threat to this country from missiles, aircraft or overt military activities, better and more timely, at instant fingertip availability than any group in the United States. So DEFSMAC is an input to NSA, but it also [is] an input to DIA and the CIA and the White House Situation Room and everybody else."[68] DEFSMAC receives data related to space and missile launches by Iran, North Korea, Russia, China, and other nations. In turn it notifies those who task or operate collection assets—from satellites to aircraft to ground stations—that a launch is imminent so that they can prepare to monitor the event and obtain the maximum intelligence available.[69]

The mission of the Information Assurance Directorate "involves detecting, reporting, and responding to cyber threats; making encryption codes to securely pass information between systems; and embedding IA measures directly into the emerging Global Information Grid. It includes building secure audio and video communications equipment, making tamper protection products, and providing trusted microelectronic solutions." In addition, its work "entails testing the security of customers' systems, providing OPSEC [operations security] assistance, and evaluating commercial software and hardware against nationally set standards, to better meet our nation's IA needs."[70] Figure 2.5 shows the IAD's organization chart.

Two key centers outside the Signals Intelligence and Information Assurance directorates are the National Security Operations Center (NSOC) and the NSA/CSS Threat Operations Center (NTOC). The NSOC, formerly the National SIGINT Operations

FIGURE 2.5 Organization of the Information Assurance Directorate



Source: NSA.

Center, was responsible for overseeing and directing the SIGINT coverage of any crisis event. It operated around the clock and was in instantaneous touch with every major NSA facility in the world. In the event a facility intercepted signals it deemed significant, the facility personnel filed a Critical Intelligence Communications (CRITIC) report with NSOC, which could immediately pass the message on to DIRNSA. If NSOC authorities felt that the event lacked sufficient importance, they could revoke the report's CRITIC status. As a result of the increased emphasis on information warfare, the National SIGINT Operations Center was rechristened the National Security Operations Center, which continues to perform the previous missions but now operates the Information Protect Cell and includes the Defensive Information Operations Staff.[71] The NTOC, staffed by representatives of both the Signals Intelligence and Information Assurance directorates, attempts to identify cyber threats posed by foreign nations or terrorist groups to NSA, DOD, and military service computer systems.

Among its collection facilities in the United States (discussed in Chapter 8), the NSA has a major facility located at Camp Williams, Utah, near Bluffdale. Known as the Utah Data Center or the Intelligence Community Cybersecurity Initiative Data Center, it serves as a repository for very large amounts of data gathered from domestic NSA stations, overseas listening posts, and satellite systems.[72]

SPECIAL COLLECTION SERVICE

The Special Collection Service is not one of the seventeen organizations listed as constituting the U.S. Intelligence Community since it is a joint operation of the CIA and NSA (which designates the service as "F6"). But it does have its own three-hundred-acre

headquarters complex outside Beltsville, Maryland, and a worldwide presence (discussed in Chapter 8). While the existence of the SCS is not classified, all details of its mission are, and the sign at its headquarters reads "Communications Security Support Group."[73]

At the beginning of 1976, the CIA had two entities involved in SIGINT operations: the Office of Electronic Intelligence in the Directorate of Science and Technology and Division D in the Directorate of Operations. The latter organization, originally established to serve as the funnel for COMINT into the CIA, had expanded its mission to include operations against foreign cipher personnel and embassy-based intercept operations, primarily as a means of supporting the CIA's case officers and their clandestine collection activities. Then, in February 1977, OEL and Division D were merged to form the Office of SIGINT Operations.[74]

By that time the staff director of the House Armed Services Committee, Charlie Snodgrass—who seemed, according to NSA historian Thomas Johnson, "to harbor a visceral distrust of the CIA"—had launched a study focusing on U.S. SIGINT activities. He concluded that there was too much duplication, not enough coordination, and a lack of clear lines of authority. It had been the CIA's practice to ignore the edicts issued by NSA's director, who was ostensibly the national manager for SIGINT. The study and congressional pressure forced the CIA to acknowledge the NSA as the national SIGINT authority. A memorandum of agreement—or "Peace Treaty," according to Johnson—between the two covered liaison, overhead collection, and a number of other subjects. The CIA also agreed to merge their embassy intercept operations with those of NSA (whose operations had aimed at supporting national and military decision makers).[75]

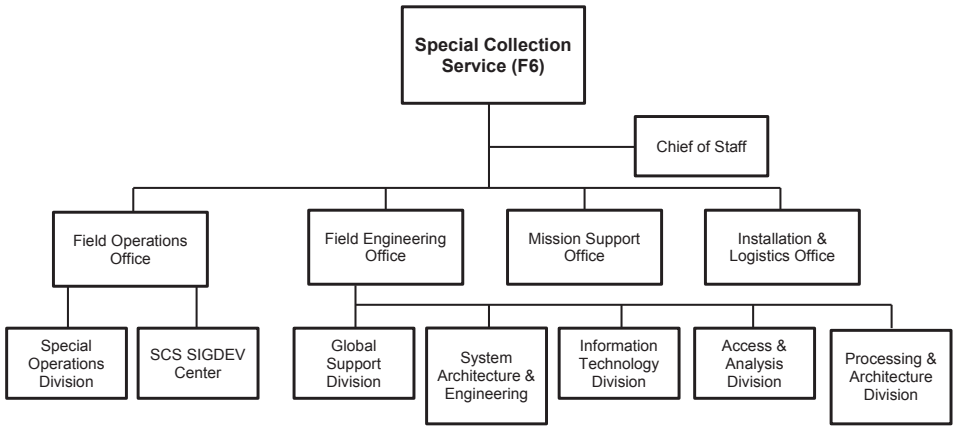
Details of the merger were worked out between the Director of NSA and the head of the CIA OSO. They agreed that a CIA official would initially head the joint enterprise, to be called the Special Collection Service, serving a two-year term. The SCS's deputy director would be selected from NSA, and an NSA official would become director after the CIA official completed his term. The director's job would continue to alternate between CIA and NSA officials, with the deputy director succeeding the director.[76]

A leaked document from 2002 described the SCS effort as involving "covert SIGINT collection abroad from official U.S. Government establishments, typically U.S. embassies and consulates" and stated, "NSA partners with the CIA in the SCS construct in which NSA employees under diplomatic cover conduct SIGINT collection."* The same document also reported, "Special Collection Sites provide considerable perishable intelligence on leadership communications largely facilitated by the site presence within a national capital."[77]

By the end of 1983, a Special Collection Element (SCE) would be present in about a third of U.S. embassies abroad. In 1988 there were SCEs at eighty-eight sites; by

*By mid-1994, individuals from the military services were being seconded to work for the SCS after cover problems had been overcome. Four Air Intelligence Agency (AIA) candidates were selected to participate in the program, designated SENSOR SILVER. (See Joyce M. Hons, Juan R. Jimenez, Gabriel G. Marshall, and Jimmy D. Ford, *History of the Air Intelligence Agency, 1 January–31 December 1994,* Volume 1 (San Antonio, TX: AIA, December 1995), 1:39.

FIGURE 2.6 Organization of the Special Collection Service



Source: NSA, SCS, Pacific STGDEV Conference, March 2011.

2002, the number had shrunk to sixty-five, a change explained by the fact that "SCS has always opened and closed sites based on productivity." The teams, which might consist of only two or three people, produced excellent intelligence, particularly if the embassy was located on high ground or near the foreign or defense ministries or other key offices in the capital. In 2010 there were ninety-six SCS sites in five categories: staffed locations (seventy-four), unmanned remote (fourteen), dormant (three), active survey (three), and technical support activity (two).[78]

According to several accounts, SCS personnel are also involved in placing antennas in nondescript locations as well as undertaking "black-bag jobs" since "sometimes . . . it's easier to simply break into a building and install a hidden microphone, whereupon intelligence can be gathered and voices recorded before encryption ever takes place."[79] Figure 2.6 shows the SCS organization chart.

NATIONAL RECONNAISSANCE OFFICE

In its May 2, 1946, report, *Preliminary Design for an Experimental World-Circling Spaceship*, the Douglas Aircraft Corporation examined the potential value of satellites for scientific and military purposes, including "observation." Almost nine years later, on March 16, 1955, the U.S. Air Force issued General Operational Requirement No. 80, officially establishing a requirement for an advanced reconnaissance satellite. Over the next five years, the U.S. reconnaissance satellite program evolved in a variety of ways. The Air Force program was first designated the Advanced Reconnaissance System, then SENTRY, and finally SAMOS.[80]

Concern about the amount of time it would take to achieve the SAMOS program's primary objective—development of a satellite that could return its imagery electronically—led to President Dwight D. Eisenhower's approval, in early February 1958, of a CIA program. Designated CORONA, it aimed to develop a satellite that would return imagery in a canister. By June 1960, continued problems with SAMOS

led Eisenhower to order a review of the program. The review culminated in an August 25, 1960, meeting in which Eisenhower accepted a recommendation for streamlined management for the SAMOS program. The new arrangement would establish a direct line of authority from the Secretary of the Air Force to the SAMOS project director, eliminating intervening levels of bureaucracy, including the Air Staff.[81]

On August 31, Secretary of the Air Force Dudley C. Sharp ordered creation of an Office of Missile and Satellite Systems within his own office to assist the secretary "in discharging his responsibility for the direction, supervision and control of the Samos project." That same day, Sharp also directed the formation of a SAMOS project office at the California headquarters of the Air Force Ballistic Missile Division as a field extension of the Office of the Secretary of the Air Force. The order stated, "The Director is responsible to and will report directly to the Secretary of the Air Force."[82]

Those orders established a new structure for the Air Force program but did not affect the management arrangements for the CIA's CORONA program. However, a number of events and individuals would lead to the creation of a national reconnaissance organization. Among them were James Killian and Edwin Land, two key presidential scientific advisors. Looking at the successful U.S. Air Force–CIA partnerships that had existed with respect to the U-2, OXCART, and CORONA programs, they pushed for permanent, institutionalized collaboration between the two organizations.[83]

Subsequent to John F. Kennedy's assumption of the presidency, Under Secretary of the Air Force Joseph Charyk drafted a proposal, at Killian and Land's request, for the establishment of a national coordinating agency for satellite reconnaissance. Sometime after mid-July, Secretary of Defense Robert McNamara asked Charyk to draft the specific documents that would put the proposal into effect. A key change between the original and final drafts was the expansion of the office's responsibility from satellite reconnaissance to overhead reconnaissance of denied areas, thus including in its set of responsibilities both satellites and selected manned and unmanned aerial systems.[84]

On September 6, 1961, an agreement signed by the acting DCI, General Charles Pearre Cabell, and Deputy Secretary of Defense Roswell Gilpatric established the National Reconnaissance Office as a joint CIA–U.S. Air Force operation. In 1962 the U.S. Navy's space reconnaissance effort, the GRAB electronic intelligence satellite, became part of the NRO framework. In keeping with the "matrix" nature of the organization, the essence of the NRO structure for the next thirty years included an NRO director (and eventually deputy director), an NRO staff (headed by an Air Force brigadier general who reported to the director), and three programs: Program A (Air Force Office of Special Projects in El Segundo); Program B (the CIA's U-2, OXCART, and satellite efforts); and Program C (Navy, originally headquartered in Washington). In early 1963, a second Air Force element, Program D, was established, initially encompassing what was then designated the R-12 (and subsequently became the SR-71, the Air Force version of the OXCART). Program D also assumed responsibility for the TAGBOARD/D-21 reconnaissance drone and a nonreconnaissance project, the interceptor version of the R-12. Program D continued as a component of the NRO until responsibility for the SR-71 was turned over to the Strategic Air Command in 1969; it was formally dissolved in 1970 or 1971.[85]

In 1992, after thirty years as an organization whose existence was classified the "fact of" the NRO's existence was declassified. DCI Robert Gates announced

PHOTO 2.3 NRO headquarters, Chantilly, Virginia. *Photo credit:* NRO.

reorganization plans before a joint public hearing of the Senate and House intelligence oversight committees. He stated that there would be "a far-reaching internal restructuring of the Intelligence Community organization responsible for designing, building, and operating our overhead reconnaissance assets."[86]

That restructuring involved replacing the alphabetic program offices with three major directorates—the Imagery Intelligence (IMINT), SIGINT, and Communication Systems Acquisition and Operations directorates—each responsible for both acquiring and supervising contract research and development as well as for purchasing and operating the relevant spacecraft and ground stations.[87]

The NRO headquarters are located in a four-tower structure in Chantilly, Virginia, near Dulles International Airport. Government personnel working for the NRO are drawn largely from the Air Force, CIA, NSA, and Navy. In 1997 the 2,753 NRO government employees consisted of 1,456 from the Air Force (53 percent), 649 from the CIA (24 percent), 412 from the NSA (15 percent), 214 from the Navy (8 percent), and 22 from other agencies such as the DIA and Army (<1 percent). In March 2006, the Government Accountability Office estimated that Air Force personnel made up approximately 57 percent of NRO employees. With the disestablishment of the Office of Development and Engineering, CIA personnel assigned to the NRO would be tied to specific DS&T mission areas. Today, NRO government employees total about 2,800, although NRO contractors account for many thousand more, either working at NRO headquarters or with NRO projects at contractor sites. Its fiscal year 2013 budget request was $10.3 billion.[88]

Just as the NRO operated for decades with its Program A-B-C structure, it also operated for decades under two charter documents: a 1964 DOD directive and a 1965

agreement between the Director of Central Intelligence and the Secretary of Defense. In 2009 Congress, via the Intelligence Authorization Act for Fiscal Year 2010, mandated that the Director of National Intelligence and Secretary of Defense produce a new charter for the NRO, updating the 1965 DCI-DOD agreement.[89]

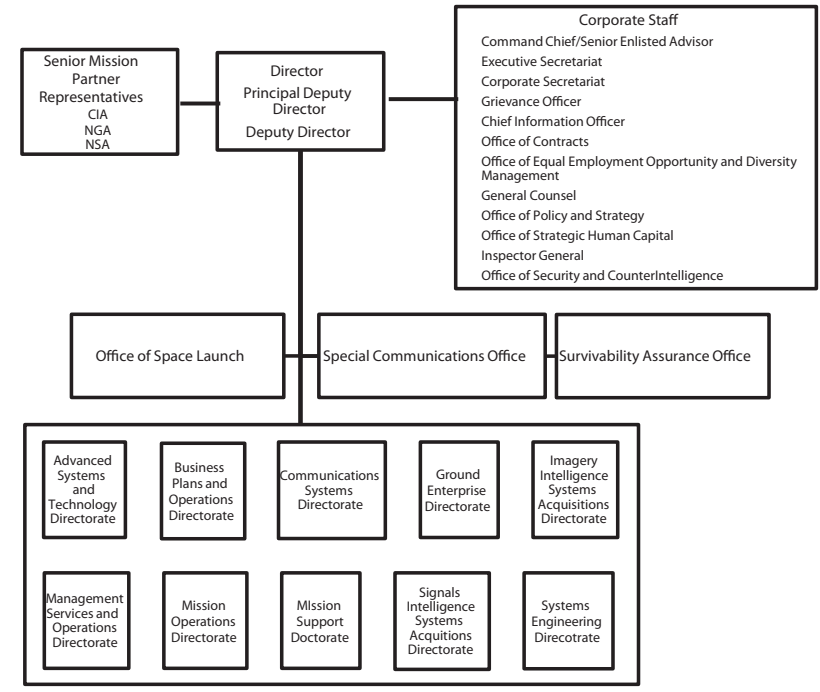
On September 21, 2010, DNI James R. Clapper Jr. and Secretary of Defense Robert Gates signed a memorandum of agreement concerning the NRO, specifying that the NRO was responsible for "research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence." The agreement also specified that the NRO director had three broad sets of responsibilities: to manage and operate NRO programs, to act as principal advisor to the Secretary of Defense and DNI on overhead reconnaissance, and to share responsibility for "leading and managing the national security space sector." The agreement also specified that the NRO director should establish and chair an Overhead Reconnaissance Advisory Group (ORAG) to serve as a principal advisor to the director on overhead reconnaissance.[90]

A more detailed DOD directive issued in June 2011 serves as the current charter for the NRO. It repeats the mission statement in the agreement and goes on to discuss organization and management, responsibilities and functions with regard to operations (including support for the military, Intelligence Community, security, and counterintelligence), creation of the ORAG, acquisition, and relationships, among other topics.[91] A key element of the directive is its definition of "overhead reconnaissance," a term that traditionally included both space and aerial reconnaissance overflights of denied areas, reflecting the NRO's involvement in developing and operating both space and aerial systems (both manned and unmanned). However, the directive defines overhead reconnaissance as "activities carried out by space-based capabilities whose principal purpose is conducting and/or enabling intelligence collection," implying that the NRO will have no role in developing aerial reconnaissance systems. The definition also specifies that overhead reconnaissance includes "associated R&D, acquisition, test and evaluation, and system operations performed on or by satellites, communications, and facilities for data processing as well as command and control of spacecraft and payloads."[92] In addition, the directive specifies that the NRO director should identify a Special Communications focal point to represent NRO interests to the DOD Special Communications Enterprise Office, a reflection of the NRO's role in data exfiltration—receiving and relaying through its satellites data acquired by emplaced sensor systems.[93]

The current structure, shown in Figure 2.7, represents a significant expansion in the number of directorates, which in turn reflects a significant change in the organization's approach to carrying out its mission. The three directorates established in 1992 and 1993 continued the cradle-to-grave approach in which a single NRO component conceived, developed, constructed, and operated satellites. Over the subsequent two plus decades, the NRO has distributed those functions over a number of directorates.

The IMINT Systems Acquisition and Operations Directorate and the SIGINT Systems Acquisition and Operations Directorate have become the Imagery Intelligence Systems Acquisition Directorate and the Signals Intelligence Systems Acquisition Directorate, indicating that they are now responsible only for the acquisition part of the space reconnaissance effort. Responsibility for operating the orbiting spacecraft

FIGURE 2.7 Organization of the National Reconnaissance Office



Source: NRO.

belongs to the Mission Operations Directorate, while handling the ground stations and processing the data they receive is the job of the Ground Enterprise Directorate. Creation of the Mission Operations Directorate reflected the desire to give customers a single point of contact for space intelligence data, regardless of the collection system that obtained it. Creation of the Ground Enterprise Directorate reflected the expectation that it would result in greater attention to the ground component of NRO operations.[94]

Three additional key NRO directorates are those for Advanced Systems & Technology (AS&TD), Systems Engineering (SED), and Mission Support (MSD). The Advanced Systems & Technology Directorate was established in 1997, as recommended by a review group, by upgrading and expanding the functions of the Office of Systems Applications, established to investigate the feasibility of small satellites for reconnaissance. The directorate's mission is to investigate and conduct research and development for systems that would differ significantly from those currently in operation.[95]

On October 15, 2006, the Office of the Deputy Director for Systems Engineering was replaced by a fifth directorate, the Directorate for Systems Integration and Engineering, created to establish standards for systems engineering, to develop and coordinate with other NRO directorates a high-level NRO architectural description, and to "review all major trade-offs analyses [and] architectural alternatives . . . prior to

their presentation outside the NRO."[96] Today, it is known as the Systems Engineering Directorate.

The origin of the Mission Support Directorate goes back to April 1990 when the position of Deputy Director for Military Support (DDMS) was established to facilitate the provision of NRO support to military commanders. In late 1996 the position of Deputy Director for National Support (DDNS) was established to balance the DDMS position. According to the DDNS mission statement, the new official was to "maintain close coordination with senior officials in all national-level departments and agencies who can represent their respective current and future space-based reconnaissance needs." The position was created in response to a frequently expressed concern about the extent of focus on supporting military operations. In 2006 the two positions were merged into the single DDMS position. Subsequently, the deputy director position was eliminated and the functions placed in a directorate.[97]

Among the offices constituting the NRO Corporate Staff is the Office of Security and Counterintelligence. In June 1992, the NRO established a Counterintelligence Staff to "increase the awareness of foreign intelligence threats to NRO programs, facilities and personnel, . . . communicating that information to NRO CI activities." Its primary functions included research and analysis; coordination within the NRO, the CI community, and investigative agencies; and operations support. In March 2006, the director of the NRO announced that the Counterintelligence Staff would be realigned within the Office of the Director of Security, whose position would become Director of NRO Security and Counterintelligence. The Director of Security and Counterintelligence reports to the Principal Deputy Director.[98]

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

In his April 1992 testimony before the House and Senate intelligence committees, DCI Robert Gates noted that the Imagery Task Force he had established upon becoming DCI had recommended the creation of a National Imagery Agency (NIA), which would absorb the CIA's National Photographic Interpretation Center as well as the Defense Mapping Agency (DMA).[99]

The task force's vision for an NIA was not as broad as that recommended by some in congressional hearings and written into proposed legislation by both the House and Senate intelligence committees. The broader vision would have created an NIA responsible for virtually the entire range of imagery functions, decisions on spacecraft and aircraft capabilities, research and development to support those decisions, tasking, collection operations, and analysis.[100] During his testimony Gates rejected the recommendations of both his task force and the congressional committees, in part because Chairman of the Joint Chiefs of Staff Colin Powell wanted to maintain DOD control of the Defense Mapping Agency. However, Gates and Secretary of Defense Richard Cheney agreed to a less dramatic fix, and a month later the Central Imagery Office (CIO) was established within the Department of Defense. The intent was to address some of the same concerns that had led to suggestions for the establishment of an NIA, including congressional frustration with a lack of coherent imagery management, imagery collection, and dissemination problems that surfaced during the Persian Gulf War, budgetary constraints, and changing requirements for the support

of military operations. Thus, the CIO was established on May 6, 1992, chartered by both Department of Defense Directive 5105.26 and Director of Central Intelligence Directive 2/9 as a DOD combat support agency.[101]

In contrast to the proposed alternative national imagery agencies, the CIO was not designed to absorb existing agencies or to take on their collection and analysis functions. Rather, its mission included tasking of national imagery systems (assuming that mission in place of the DCI Committee on Imagery Requirements and Exploitation) to ensure responsive imagery support for the Department of Defense, combatant commanders, the CIA, and other agencies and advising and evaluating the performance of imagery components. Pursuant to the provision of imagery support, the CIO was assigned the role of systems development—specifically, establishing imagery architectures and standards for interoperability of imagery dissemination systems and supporting and conducting research and development.[102]

Establishing the CIO delayed but did not prevent creation of a national imagery and mapping agency. In April 1995, DCI-designate John Deutch told the Senate Select Committee on Intelligence that, if confirmed, he would "move immediately to consolidate the management of all imagery collection, analysis, and distribution," arguing that "both effectiveness and economy can be improved by managing in a manner similar to the National Security Agency's organization for signals intelligence."[103] After his confirmation, Deutch established a National Imagery Agency Steering Group, which in turn chartered an NIA Task Force. The task force produced eleven different options for an NIA, ranging from a strengthened CIO to a highly centralized NIA, with program, budget, and management authority for all aspects of imagery. In late November 1995, Deutch and Secretary of Defense William J. Perry sent a joint letter to congressional leaders and relevant committees about their plan to establish a National Imagery and Mapping Agency as a combat support agency within the Department of Defense on October 1, 1996. Their letter noted that the proposed agency would consolidate the DMA, CIO, NPIC, DIA's imagery exploitation element, and portions of the Defense Airborne Reconnaissance Office and NRO involved in imagery exploitation and dissemination.[104]

The planned agency would leave the acquisition and operation of space systems and their ground stations to the NRO and the service intelligence organizations' imagery exploitation activities in their hands. According to the letter, the task force recommended the proposed consolidation for three basic reasons:

1. A single, streamlined and focused agency could best serve the imagery and mapping needs of a growing and diverse customer base across government;
2. The current disposition of imagery and mapping responsibilities does not allow one agency to exploit the tremendous potential of enhanced collection systems, digital processing technology and the prospective expansion in commercial imagery;
3. The revolution in information technology makes possible a symbiosis of imagery intelligence and mapping which can best be realized through more central management.[105]

Former intelligence (particularly CIA) officials and many within Congress questioned the wisdom of the plan. The primary concern was that, as a result of the transfer

of NPIC personnel from the CIA to the DOD, imagery support for national policymakers would suffer in order to support the requirements of military commanders. However, although the opposition was unable to block the creation of the new agency, the Senate Select Committee on Intelligence did persuade the Senate Armed Services Committee to amend the legislation creating the NIMA to stipulate that the DCI would retain tasking authority over national imagery systems and that the Secretary of Defense needed to obtain the DCI's concurrence before appointing the NIMA director or else note the DCI's lack of concurrence to the president. In addition, the Senate Armed Services Committee agreed to the modification of the National Security Act to state explicitly NIMA's responsibility to provide intelligence for national policymakers.*[106]

NIMA came into being as projected on October 1, 1996, incorporating all the elements mentioned in the late-November statement as well as the Office of Imagery Analysis of the CIA's Directorate of Intelligence and the Defense Dissemination Program Office. It would also eventually absorb some activities of the CIA's Office of Development and Engineering. The consolidation thus created an agency with around 9,000 personnel—about 2,000 imagery interpreters and about 7,000 individuals from the Defense Mapping Agency.[107]

Like the CIO, NIMA was chartered by both a DOD directive—5105.60 of October 11, 1996, "National Imagery and Mapping Agency (NIMA)"—and a DCI directive. To emphasize the fact that the organization "merges imagery, maps, charts and environmental data to produce . . . 'geospatial intelligence' [GEOINT]—the exploitation and analysis of imagery and geospatial information to describe, assess, and virtually depict physical features and geographically referenced activities of the earth," Director James Clapper sought to change NIMA's name to the National Geospatial-Intelligence Agency (NGA), an alteration authorized by the 2004 National Defense Authorization Bill, which took effect when President George W. Bush signed the legislation on November 24, 2003.[108]

Because of the geographical distance between the agencies absorbed by NGA, significant portions of the agency were not at first colocated but could be found at the Washington Navy Yard (NPIC's location); in Washington, D.C. (various offices of DIA); in Bethesda, Maryland (DMA headquarters and hydrographic production); in St. Louis, Missouri (DMA aerospace production); and at Fort Belvoir, Virginia (the main ground station for the NRO's electro-optical satellites). NGA began moving into new headquarters at Fort Belvoir in January 2011. When established, NIMA had about 9,000 employees, but there were plans to reduce that number to 7,500. Today, there are 16,000 NGA employees who largely work either at the Fort Belvoir or St. Louis facilities. The agency's 2013 fiscal year budget request was $4.8 billion.[109]

The current charter for NGA is a July 29, 2009, DOD directive that specifies NGA's mission, organization, and management, as well as the responsibilities and functions of the NGA director. It outlines the director's forty-two responsibilities with regard to the production of GEOINT, GEOINT architecture and standards, GEOINT systems,

*There was also some concern about the proposed merger from DMA officials, who feared that their formal inclusion in the Intelligence Community might have a negative impact on their relationships with foreign nations that provided mapping information.

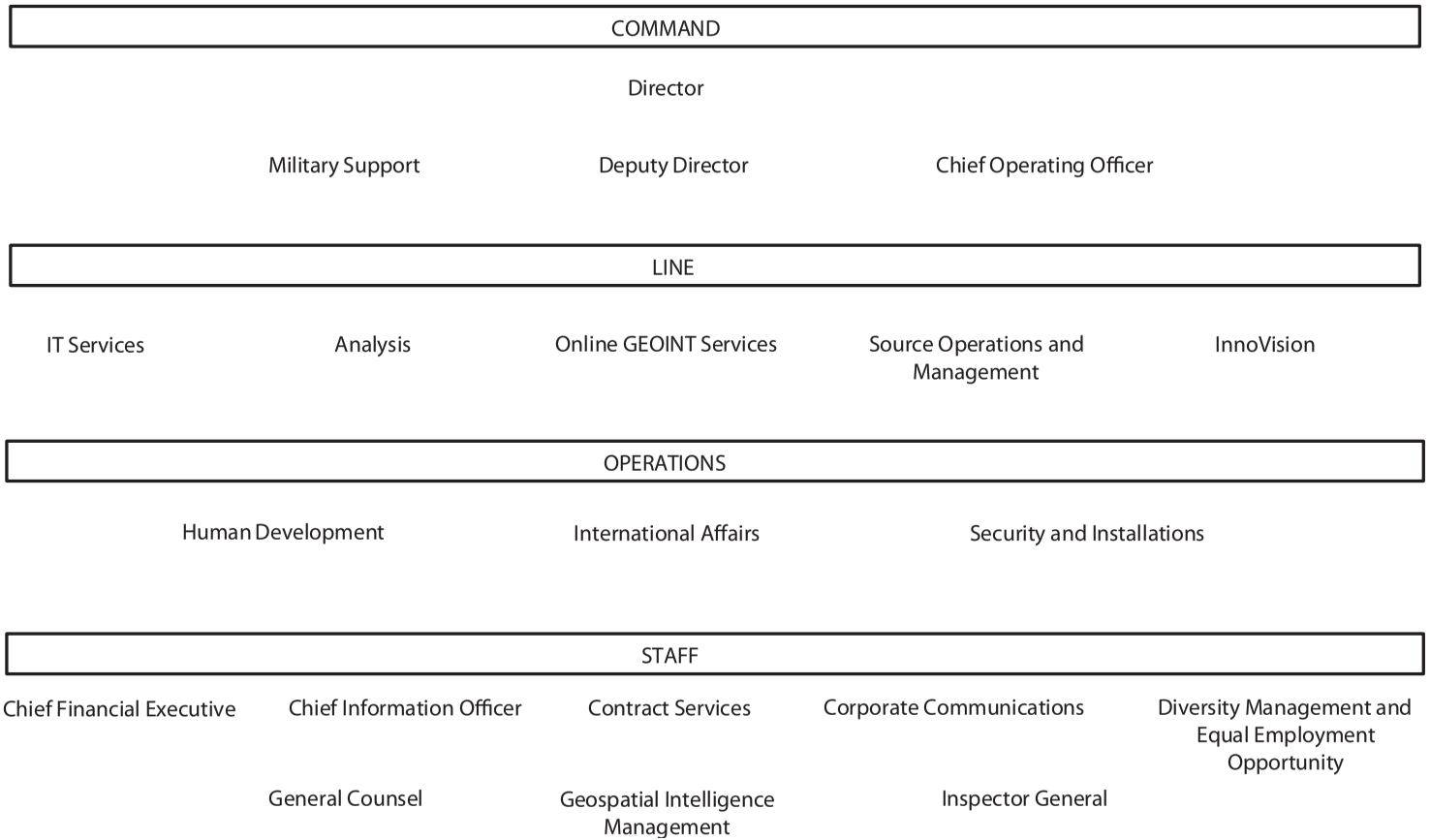
GEOINT training and education, GEOINT functional management and program management, and GEOINT international engagement. Those responsibilities include the requirements to

- Provide responsive GEOINT products, support, services, and information
- Manage GEOINT planning, collection, operations, analysis, production, and dissemination
- Establish and/or consolidate DOD geospatial data collection requirements and, as appropriate, task or coordinate collection with the DOD components to collect and provide these data
- Monitor and evaluate the performance of the DOD components having GEOINT planning, programming, tasking, collection, processing, production, exploitation, dissemination, and retention functions in meeting national and military GEOINT requirements and, to the extent authorized by the DNI, monitor the performance of other U.S. government departments having GEOINT functions
- Serve as the DOD lead for GEOINT standards and prescribe, mandate, and enforce standards and architectures related to GEOINT and GEOINT tasking, collection, processing, exploitation, and international geospatial information
- Establish end-to-end and system architectures related to GEOINT in compliance with National and Defense Information Infrastructure guidance and standards
- Develop, acquire, and field GEOINT-related systems
- Serve as the program manager for the National Geospatial-Intelligence Program within the National Intelligence Program
- Establish and maintain international GEOINT agreements and arrangements with foreign governments and international organizations.[110]

The NGA's organizational structure comprises the five directorates shown in Figure 2.8. The Analysis Directorate is home to imagery interpreters focused on particular nations and regions as well as on specific topics such as warning, global navigation, and counterproliferation. They "provide geospatial intelligence and services to policymakers, military decision makers, and tailored support to civilian federal agencies and international organizations."[111] The key function of the Source Operations & Management Directorate is carried out by its Source Operations Group. The group is responsible, like the CIO's Central Imagery Tasking Office and the Committee on Imagery Requirements and Exploitation in earlier years, for the tasking of U.S. imagery satellites: sorting through requests for imagery coverage of targets from government, military, and civilian organizations, determining which satellites to employ against specific targets, and selecting the altitude and angle from which to obtain imagery.[112]

Beyond being renamed and reorganized since its 1996 establishment, the agency has also evolved in a number of ways. The development of high-resolution commercial imagery satellites has made it possible for the NGA to procure significant quantities of imagery through commercial channels that in the past could be obtained only from the NRO's classified systems. As a result, NGA has become a significant factor in the financial health of commercial imagery firms.[113] The terrorist attacks of 9/11 led to NGA's assuming a homeland security role through the provision of detailed

FIGURE 2.8 Organization of the National Geospatial-Intelligence Agency



Source: NGA.