This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL
REPORT

Toward a Revolution in Intelligence Affairs

Deborah G. Barger

NATIONAL SECURITY RESEARCH DIVISION

This report results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by donors and by the independent research and development provisions of RAND's contracts for the operation of its U.S. Department of Defense federally funded research and development centers. This research was conducted within the RAND National Security Research Division (NSRD), a division of the RAND Corporation. NSRD conducts research and analysis for the Office of the Secretary of Defense, the Joint Staff, the Unified Commands, the defense agencies, the Department of the Navy, the U.S. intelligence community, allied foreign governments, and foundations.

Published 2005 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

FOREWORD

Intelligence is often considered to be the most secretive function in our government. Yet, during the past decade, more than a dozen public commissions and panels made recommendations on how to reform U.S. intelligence given the end of the Cold War, the changing nature of ournational security environment, the need to respond to increasing technical and analytic complexity, and a number of perceived intelligence failures, including those surrounding the tragic events of September 11, 2001. At a time when "transformation" is underway in defense and other areas of government, intelligence must keep pace or run the risk of increasing irrelevance and potential decline. And, in whatever form change comes, it must ultimately remain focused on the key goal of intelligence--outthinking and outsmarting our adversaries.

Deborah Barger is a senior intelligence officer who was and continues to be passionately interested in the topic of change in the U.S. Intelligence Community. During her year-long fellowship at the RAND Corporation, she focused intensely on possible antecedents for a "revolution in intelligence affairs" (RIA) in the areas of defense reform (i.e., the revolution in military affairs), private-sector reform, and intelligence reform and development during the period following World War II. Because of the risk that the RIA would be too easily targeted by grandstanders and pundits, Deborah worked quietly, carefully, and methodically to understand the true nature of those reforms and how they might inform an RIA. In this endeavor, she was assisted by dozens of individuals both inside and outside government, who all have an intense passion for improving the U.S. intelligence enterprise.

By design, Deborah's research provides no specific recommendations on how to change U.S. intelligence organizations, operations, or approach to technology. The reader who is looking for a "quick-fix"recommendation, such as to close a specific intelligence agency, to build a specific satellite technology, or to hire a specific group or class of analysts, will be unsatisfied with this report. What Deborah

has done, however, is to develop a framework for how the United States should consider specific changes to our intelligence enterprise, based on how those changes would improve the effectiveness of U.S. intelligence. Under an assumption that an RIA may already be under way, in part because of prior study, Deborah offers an intellectual framework by which to consider past proposals for change as well as future ones. The framework offered here provides a pathway for continuous change in intelligence, even in an increasingly complex world. The framework should help intelligence leaders and managers to do the following:

- evaluate *holistically* proposed changes to a complex system (i.e., avoid fixing one thing while inadvertently breaking another)
- evaluate proposals for change objectively and from something other than a political or bureaucratic perspective
- develop their own proposals for change, driven by rapid changes in the external environment (rather than failures)
- follow an approach that will help the Intelligence Community succeed in actually implementing needed changes, not once but continuously.

Regrettably, the limited public debate that takes place today on U.S. intelligence either focuses on fear or failure, or pits various constituencies against each other, such as the debate that has emerged on whether the Intelligence Community needs more collection or analysis. In today'scomplex world, the United States needs better and more of both, but U.S. intelligence also needs to be more creative, adaptive, and risk-taking in how it pursues those two activities. The people who are most aware of this are the men and women of the U.S. Intelligence Community, who have worked tirelessly to meet the needs of a growing number of intelligence consumers, even in the face of increased mission complexity and an unprecedented scrutiny of what they do and how they do it.

The framework offered here provides not only an intellectual foundation for change, but also an argument that real change can result

only from the emergence of many pockets of innovation rather than from any single individual or organizational entity. Since the time that she authored this report, Deborah Barger has been given official responsibility for both understanding the sources of change across the U.S. intelligence community and for instituting change. We thank her for her dedication to this research and her devotion to improving the U.S. intelligence organization.

Kevin M. O'Connell
Former Director
Intelligence Policy Center
RAND Corporation

PREFACE

As the global war on terrorism continues to expand and the post-Cold War security environment remains in flux, both the strengths and weaknesses of U.S. intelligence have been thrust into the public spotlight, leading to renewed recognition of the importance of intelligence and the need for improvements in intelligence operations.

The research presented in this report was conducted by Deborah Barger, a senior intelligence officer, during her Intelligence Community Fellowship at the RAND Corporation from September 2002 to August 2003. She advances the argument that a "Revolution in Intelligence Affairs" is needed to prepare the Intelligence Community to meet its future challenges. In this report, she presents a framework for how the United States should consider specific changes to its intelligence enterprise to improve its effectiveness. As such, this report should be of interest to intelligence professionals, students, scholars, and researchers alike.

Data for this research project was gathered through a variety of unclassified sources including books, articles, and other documents; speeches; Internet searches; workshops attended by government and non-government officials; and one-on-one interviews with numerous intelligence officials, policymakers, former military officers, intelligence consumers, retired intelligence experts, historians, academics, and intelligence scholars. The research was multidisciplinary, drawing lessons from scientific history, political science, psychology, military theory and strategy, business theory, organizational dynamics, biographical history, sociology, and change management. The data presented in this report are current as of June 2004.

This report results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by donors and by the independent research and development provisions of RAND's contracts for the operation of its U.S. Department of Defense federally funded research and development centers. This work

was done within the Intelligence Policy Center (IPC) of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis for the Office of the Secretary of Defense, the Joint Staff, the Unified Commands, the defense agencies, the Department of the Navy, the U.S. Intelligence Community, allied foreign governments, and foundations.

The views expressed in this report are solely those of the author and do not necessarily represent the views of the U.S. government.

For more information on RAND's Intelligence Policy Center, contact its acting director, Greg Treverton. He can be reached by email at Greg_Treverton@rand.org; by phone at 310-393-0411, extension 7122; or by mail at the RAND Corporation, 1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138. More information about RAND is available at www.rand.org.

CONTENTS

FIGURE

TABLES

ACKNOWLEDGMENTS

It is my hope that this initial exploration will prompt additional, more in-depth research and a livelier debate on the future of U.S. intelligence—one that will involve people from all branches of government and many segments of the private sector.

This work would not have been possible without the help and advice of dozens of people in the Intelligence Community and other parts of the federal government. Please know that I am forever indebted to each of you. I am also grateful to a number of former government officials who are now retired or in the private sector, as well as to the many folks from both the public and private sectors who participated in the two RAND-sponsored workshops on the subject of a "Revolution in Intelligence Affairs." I hope that in this work I have done some justice to your ideas. I would also like to thank several reviewers within government for their quick turnaround in confirming that this report contains no classified information.

I would especially like to thank my former colleagues at RAND—especially those in the Intelligence Policy Center—for their comments, suggestions, and advice and, in several cases, for their formal, in-depth peer reviews. In their contributions to this project, and through their patience and support throughout my fellowship at RAND, all were very generous with their time, thoughts, and suggestions.

I would also like to thank the RAND editor, Nancy DelFavero, who helped smooth the rough edges to get this report ready for publication. That said, the responsibility for judgments reflected herein is mine, as is the responsibility for any errors or omissions.

ACRONYMS

ADCI	Assistant Director of Central Intelligence
AIDS	Acquired Immune Deficiency Syndrome
ARDA	Advanced Research and Development Agency
CIA	Central Intelligence Agency
CIG	Central Intelligence Group (CIA Predecessor)
DCI	Director of Central Intelligence
DDO	Deputy Director of Operations
DIA	Defense Intelligence Agency
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
HIV	Human Immunodeficiency Virus
IC	Intelligence Community
ITIC	Intelligence Technology Integration Center
MTR	Military Technical Revolution
NATO	North Atlantic Treaty Organization
NGA	National Geospatial-Intelligence Agency (formally NIMA)
NIC	National Intelligence Council
NIMA	National Imagery and Mapping Agency
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council
OMB	Office of Management and Budget
OODA	Observe-Orient-Decide-Act
OSS	Office of Strategic Services
RIA	Revolution in Intelligence Affairs
RMA	Revolution in Military Affairs
TRADOC	The Army’s Training and Doctrine Command
UN	United Nations
USD(I)	Undersecretary of Defense for Intelligence
WMD	Weapons of Mass Destruction

1. INTRODUCTION

When I began this research project in fall 2002, much of the debate concerning U.S. intelligence was focused on how to prevent the next September 11. During the ensuing one-year research period, the "global war on terrorism" expanded and continued, conflicts in Afghanistan and Iraq waxed and waned, cracks in traditional security alliances widened and narrowed, new coalitions formed and frayed, and security strategies were reassessed and updated, all of which are testament to the constant flux that has come to characterize the post-Cold War security environment.

Along the way, some amazing contributions and some glaring weaknesses of intelligence organizations, processes, and products were thrust into the public spotlight. An investigation by an independent commission began, in addition to an internal review, multiple congressional hearings, the creation of numerous new organizations and offices that use or produce intelligence, and a spate of editorials, articles, books, and lectures on how to "fix" intelligence in the 21st century. Thus, there was no shortage of efforts to gain insight into the problems associated with U.S. intelligence today, and no dearth of competing solutions for its future design.

Inevitably, as has been the case with most of the intelligence reform movements over the past 50 years,[1] the focus during this period was on reorganization of the Intelligence Community and the political issues surrounding the authorities and responsibilities of the director of Central Intelligence. How the U.S. intelligence apparatus is structured is an important issue, but to begin and end the debate there would be to ignore the more profound questions that are arising about the future of intelligence in a rapidly changing global society.

As my research proceeded, I grew increasingly concerned that the intelligence reform movement was too constrained in its scope and

---

[1] Kindsvater, Larry C., "The Need to Reorganize the Intelligence Community: A Senior Officer's Perspective," *Studies in Intelligence*, Central Intelligence Agency, Vol. 47, No. 1, 2003, p. 33.

imagination. My fear was that the reformers would focus on redressing past errors at the expense of seizing opportunities to address the future. The danger, then, would lie in the failure to recognize either the need for, or the possibility of, new or different roles and missions for intelligence in a world far different from the one in which U.S. centralized intelligence was created. The intent of this research project was to make the case that the future of intelligence must be viewed and assessed in a broader context, that it must be addressed systemically rather than piecemeal, and that many nontraditional participants should be both welcomed and involved in the debate.

DEVELOPMENT OF THE REVOLUTION IN INTELLIGENCE AFFAIRS CONCEPT

As a career intelligence officer who witnessed firsthand the difficulties of pushing through systemwide changes in U.S. intelligence, I initially approached the subject of revolutionary change with some skepticism, and thus examined the arguments both for and against such an undertaking. Over time, I came to accept and then advance the argument that marginal organizational changes will be insufficient to prepare the Intelligence Community to meet future challenges. Rather, a more fundamental reshaping that springs from what I refer to in this report as a "Revolution in Intelligence Affairs" (RIA) is needed. This research, in my view, substantiated four related points that ultimately led to the development of the RIA concept:

- There is both a need and an opportunity for the Intelligence Community to change in ways that would change its form and function well beyond what is currently being contemplated, let alone imagined, by the various proponents of reform.
- If the Intelligence Community is to remain relevant and effective in the face of an evolving security environment, it must recognize both the need to change and seize an historic opportunity to change fundamentally.
- The prospects for meaningful change in the Intelligence Community are heightened by the record of success enjoyed by similarly complex organizations that responded to

significantly altered circumstances by adopting a revolutionary approach to change.

- Previous experiences in bureaucratic revolutions will be instructive to the Intelligence Community as it comes to terms with fundamental change, especially because those experiences illustrate the principle that successful revolutions are driven from within and invigorated by external forces.

If the need and the potential to effect fundamental change in the Intelligence Community exist, then the real question is, by what means will that be done? I argue that an RIA responds to evolving circumstances. The objective of an RIA is to establish a process for dynamic reinvention, not implement static, overarching reorganization. The purpose is to transform the Intelligence Community into an organization that continuously learns and adapts to accommodate change. This will enable the community to minimize the bureaucratic delays that lead to calls for wrenching and comprehensive overhauls.

The construct for the RIA comprises two distinct but related elements--a cultural shift that sees the Intelligence Community embrace the need to change and a procedural shift that enables the Community to objectively evaluate alternative responses to change and to incorporate them in a continuous manner. Both are necessary for the Community to successfully become an adaptive organization.

The *cultural* element involves a reshaping of the Intelligence Community's reaction to the pressure to adjust to changing circumstances. Historically, the primary cultural driver was the bureaucratic tendency to defend existing organizational boundaries and purviews. In contrast, under the RIA, the community's mindset would be characterized by the following:

- a willingness across the workforce to question the status quo and seek answers that will accommodate alternative futures
- a style of leadership that encourages constructive criticism and promotes investigation of alternative solutions

- a shared understanding of the value these efforts can contribute to the collective endeavor.

The *procedural* element involves the creation of mechanisms to bring about systematic changes to the form and the function of the Intelligence Community. The mechanisms must address the acquisition, evaluation, and implementation of change proposals. Without the means to effect physical change, the cultural dimension of the RIA will be an academic exercise. Under the RIA, the means for evaluating and incorporating change will be as follows:

- a formal doctrine to serve as a strategic foundation for institutionalizing a response to change
- a coalition of advocates to sponsor change-related efforts
- experimental designs and metrics to support objective assessment of alternative futures
- a finite list of key players with well-defined roles in the tactical execution of change-related activities.

TERMINOLOGY

This report frequently employs the terms "intelligence" and "Intelligence Community." It is important for the reader to comprehend the intended meaning of these terms. To avoid protracted arguments about which definitions to use, I chose to refer to the definitions in the National Security Act of 1947, as amended, the law that is currently the legal underpinning of most U.S. intelligence activities.

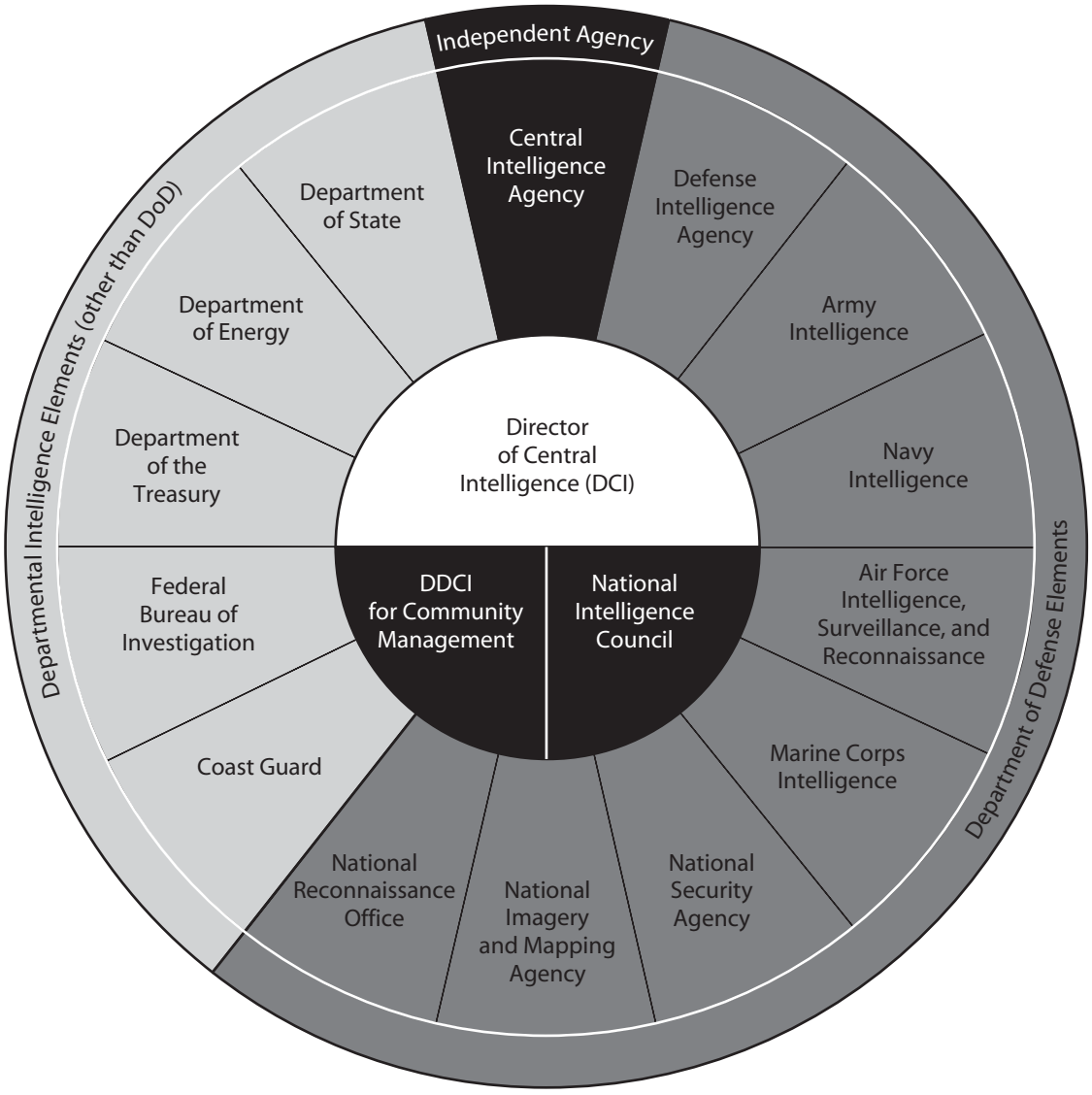
According to the Act, the term *intelligence* includes foreign intelligence and counterintelligence. The term *foreign intelligence* refers to information relating to the capabilities, intentions, or activities of foreign governments or elements thereof: foreign organizations, foreign persons, or international terrorist activities. The term *counterintelligence* refers to information gathered and activities conducted to protect against espionage, and other intelligence activities, sabotage, or assassinations conducted by or on

behalf of foreign governments or elements thereof: foreign organizations, foreign persons, or international terrorist activities.

The term *Intelligence Community* (see the following figure) includes the following:

1. Office of the Director of Central Intelligence (DCI), which shall include the Office of the Deputy Director of Central Intelligence (DDCI) [for Community Management? per the figure], the National Intelligence Council, and such other offices as the DCI may designate
2. Central Intelligence Agency
3. National Security Agency
4. Defense Intelligence Agency
5. National Imagery and Mapping Agency (recently renamed the National Geospatial-Intelligence Agency)
6. National Reconnaissance Office
7. Other offices within the Department of Defense (DoD) for the collection of specialized national intelligence through reconnaissance programs
8. Intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, the Department of the Treasury, the Department of Energy, and the Coast Guard
9. Bureau of Intelligence and Research of the Department of State
10. Such other elements of any other department or agency as may be designated by the President of the United States, or designated jointly by the Director of Central Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

The term *national intelligence* refers to intelligence, which pertains to the interests of more than one department or agency of the government, and does not refer to counterintelligence or law enforcement activities conducted by the Federal Bureau of Investigation.



RAND *TR242-S.1*

The Intelligence Community

2. THE CASE FOR CHANGE IN INTELLIGENCE AFFAIRS

"Change is hard because people overestimate the value of what they have—and underestimate the value of what they may gain by giving that up."

James Belasco and Ralph Stayer
Flight of the Buffalo (1994)

In the year following the September 11 terrorist attacks on New York and Washington, D.C., calls for intelligence reform stirred once again throughout the halls of Congress, prompting new discussions on the subject in academic institutions and think tanks. This was not a rare event. More than 20 official commissions and boards attempted "intelligence reform" since the inception of the U.S. Intelligence Community in 1947. Yet, few of these well-intentioned undertakings resulted in truly significant change. Intelligence reform is an approach that historically has not worked well because it focuses largely on fixing past mistakes and "failures." Reform looks backward to assess previous errors and then fixes things to prepare in essence for a repeat of "what was." A transformation process looks forward to consider the impact of changed circumstances and to discern opportunities to address "what could be."

Thus, if one were more interested in transformation than reform, a logical approach would be to take the evolving American national security context as a perspective from which to gauge the implications of various proposals for changing the U.S. Intelligence Community. The extent to which the larger national security context for intelligence has changed will shed light on whether marginal adjustments or a more fundamental reshaping of the Intelligence Community is needed.

Now, early in the 21st century, it also seems evident that the concept of national security--what it embraces and how it is created and maintained--is not what it was. The state of the world, both in its present form and in a potential alternative form in the future, differs

markedly from that under which the U.S. Intelligence Community was shaped. The demands on U.S. intelligence during times of crisis and war are growing and changing as the profile and pace of American engagement increase. While war-fighting requirements have recently dominated the security agenda, other applications of intelligence—e.g., to promote and preserve peace so that war is an unnecessary remedy in times of crisis—are no less a priority.

With a strategy that implies confronting dictators and disease, countering nation-states and stateless movements, contesting foreign and domestic battlefields, and controlling outer space and cyberspace, the United States is engaged and challenged across the security spectrum as never before.

This report proceeds, then, from the conviction that so much has changed in the geopolitical, social, and technological backdrop for the intelligence mission that few of the old assumptions--about why we have an intelligence apparatus, what its missions are, and what capabilities give U.S. intelligence a dominant advantage over its adversaries--apply. This chapter of the report buttresses that idea with an overview of what many view as evidence of a fundamental shift in the security environment and its impact on intelligence definitions, missions, and structures. The discussion reveals that it is not only reasonable but also critical to question whether the dated charters and designs of the country's intelligence organizations are compatible with the spectrum of challenges generated by an evolving context of national security. It also questions whether the Intelligence Community can produce results commensurate with the rapidly increasing requirements of the U.S. government and the expectations of the American people.

THE CONTEXT FOR REVOLUTION: FUNDAMENTAL CHANGES IN THE SECURITY ENVIRONMENT

A review of the threats that pose a danger to the United States today, and will continue to do so in the future, clearly shows some significant differences from the threats of the past. Based on the assumption that few observers believe current and coming dangers are no different than those that have come before, this report does not develop an exhaustive analysis of changes in the national security environment

of the 21st century. Instead, the following highlights should serve to illustrate the extent to which the security challenges have already evolved and to alert those who might overlook the implications of those challenges for intelligence and the Intelligence Community.

The Changing Nature of Threats

Threats are a constant of existence. Some threats (war and disease) persist and are seemingly endemic to the human condition. Others fade, only to have new dangers take their place. The change that is more substantial than any other aspect of the threats facing the United States is that nation-states and future peer competitors are no longer our only concern or our primary concern. The potential for weapons of mass destruction in the hands of criminal enterprises, small groups, and individuals is fundamentally changing each nation's security calculus. Nuclear weapons are a particularly dire concern, despite the efforts and hopes for their elimination. Worse, adding to the arsenal of mass destruction are biological weapons that include more effective variants of familiar pathogens and wholly new types and strains.

Elements of this arsenal are rapidly diffusing to countries and groups around the world. In his Worldwide Threat briefing to Congress in February 2003, Director of Central Intelligence (DCI) George Tenet stated, "More has changed on nuclear proliferation over the past year than on any other issue . . . in my view we have entered a new world of proliferation." Tenet said his primary concern is that "additional countries may decide to seek nuclear weapons as it becomes clear their neighbors and rivals are already doing so." Compounding the problem is the fact that knowledgeable groups and individuals can now obtain and sell weapons of mass destruction (WMD) technology and equipment that could previously be supplied only by countries with established capabilities; thus, tracking these materials becomes far more difficult.[1]

As nuclear expert Thomas Schelling said, the United States will not be able to regulate nuclear weapons in the future any better than it can

[1] Tenet, George J, "The Worldwide Threat in 2003: Evolving Dangers in a Complex World," testimony presented to Congress, February 11, 2003.

control the Saturday-night special, heroin, or pornography today. Furthermore, if terror organizations, religious movements, organized crime, and other non-national forces gain access to nuclear weapons, nuclear deterrence strategy will become obsolete, because small diffuse groups are not threatened by possible retaliation. Some argue that the possibility of this threat means that "advanced rules of restraint" will have to be devised if normal daily life is to be protected.[2] Such rules would no doubt require a strict and extensive monitoring regime with enormous implications for intelligence.

In his testimony on Capitol Hill, DCI Tenet also addressed the only other real weapon of mass destruction besides nuclear weapons—biological weapons (experts argue that chemical and radiological weapons, unlike nuclear or biological weapons, cause mass *disruption,* but not mass *destruction*). "BW [biological weapons] programs have become more technically sophisticated as a result of rapid growth in the field of biotechnology research and the wide dissemination of this knowledge," Tenet said. "Almost anyone with limited skills can create BW agents."[3] The challenge this presents for intelligence professionals, who are charged with anticipating and preventing such a threat, is obvious.

Unfortunately, the legacy of danger posed by WMD is made worse by the emergence of another new phenomenon, the rise of the "Super-Empowered Angry Man." This term describes the lone individual who with the aid of advanced technology could potentially cause as much harm to the United States and its interests as could many foreign governments.[4] An anonymous fanatic with a nuclear or biological weapon is the nightmare scenario of the future. How real is this threat, and how likely is it to become the defining threat of the coming decades? According to Thomas Friedman and others, this is the dark side of globalization. "The greatest danger that the United States faces today is from super-empowered individuals who hate America more than ever

---

2 John D. Steinbruner, *Principles of Global Security*, Washington D.C.: Brookings Institution Press, 2000, p. 5.

3 Tenet, 2003.

4 For a detailed discussion on the "super-empowered angry man," see Thomas Friedman, *The Lexus and the Olive Tree*, New York: Anchor Books, 2000, pp.401-405.

because of globalization, and who can do something about it on their own, thanks to globalization," he states.[5]

This super-empowered individual could be a terrorist, a criminal, a computer hacker, a zealot or a despot—in fact, anyone who would willingly and could capably use technology to kill Americans or otherwise act or plan against U.S. national security interests. The ability to threaten and bring about catastrophic destruction no longer resides solely in the hands of governments. This development, taken to its logical conclusion, would likely force a change in the security calculus not only of the United States but also of every nation-state that might incur the wrath of such an individual.

The Intelligence Community shares Friedman's gloomy assessment. In December 2000, the National Intelligence Council (NIC) published *Global Trends 2015,* an unclassified document that summarizes a yearlong dialogue between officials of the Intelligence Community and experts from academia, think tanks, and the corporate world. The document warns that most adversaries will recognize the information advantage and military superiority of the United States, and will try to circumvent or minimize U.S. strengths and exploit perceived weaknesses. The document states, "IT-driven globalization will significantly increase interaction among terrorists, narco-traffickers, weapons proliferators, and organized criminals, who in a networked world will have greater access to information, to technology, to finance, to sophisticated deception and denial techniques, and to each other. Such asymmetric approaches, whether undertaken by states or non-state actors, will become the dominant characteristic of most threats to the U.S. homeland."[6]

One type of super-empowered angry man, by now depressingly familiar to us all, the religious terrorist, is likely to continue as a particular danger in the future.[7] Counterterrorism expert Bruce Hoffman

---

[5] Friedman, 2000, p. 398.

[6] National Intelligence Council, *Global Trends 2015: A Dialogue About the Future with Nongovernment Experts*, December 2000, p. 14 (http://www.cia.gov/nic/NIC_globaltrend2015.html).

[7] Interview with Bruce Hoffman, terrorism expert, RAND Corporation, Washington, D.C., January 2003. This perspective on religious terrorism is explained in more detail in Lesser, Ian O. et al., *Countering the New*

argued in a recent interview, "For the religious terrorist, violence is a theological demand or imperative, justified by scripture. Religion therefore functions as a legitimizing force, specifically sanctioning wide-scale violence against an almost open-ended category of opponents." Hoffman believes that such terrorist attacks in the U.S. are likely to get worse—in terms of both frequency and lethality—over the next couple of decades.

In a speech delivered at West Point in June 2002, President George W. Bush declared, "The gravest danger to freedom lies at the crossroads of radicalism and technology." The National Security Strategy that was released later that year signaled the intention of the United States to "adapt the concept of imminent threat to the capabilities and objectives of today's adversaries." To forestall or prevent such acts, the document says, "The United States will, if necessary, act preemptively." To support preemptive options, the document states, the U.S. will require better and more integrated intelligence capabilities to provide timely, accurate information on threats, "wherever they may emerge."[8] The difficulties inherent in providing sufficient evidence of "imminent threat" have become more obvious in the aftermath of the second Gulf War. A presidential commission has been formed to address the controversy over intelligence regarding weapons of mass destruction in Iraq.

While the threats from catastrophic terrorism and the proliferation of destructive weapons technology are the top priorities of today's national security strategy, it is unlikely that we will have the luxury to focus solely on these threats five or ten years from now. Other disconcerting trends involve the following:

- **demographics**, e.g., frictions between an aging Europe and a juvenile North Africa; the mass migration of people all over the globe from rural areas to overwhelmed cities;

Terrorism, Santa Monica, Calif.: RAND Corporation, MR-989-AF, 1999, p. 20.

[8] The White House, President George W. Bush, *National Security Strategy of the United States,* September 2002, p.16 (http://www.whitehouse.gov/nsc/nss.html).

concentration of often-disenfranchised youth in urban poverty, and other such trends

- **economics**, e.g., the destabilizing effect of HIV/AIDS on developing countries; the wrenching social consequences of countries attempting to adjust their infrastructure to accommodate new fiscal and trade policies
- **politics**, e.g., a deteriorating Middle East and a maddeningly difficult North Korea; escalating regional disputes involving nuclear powers such as China, India, Pakistan, and others.

Thus, one of the most significant challenges for U.S. intelligence will be to accommodate a world of expanding threats within a budget shaped by finite domestic resources.

The Changing Nature of Peace

Presidents have often relied on intelligence as an important instrument of peace. In a speech given at the Central Intelligence Agency (CIA) headquarters in November 1959, President Eisenhower told CIA employees, "America's fundamental aspiration is the preservation of peace. To this end, we seek to develop policies and arrangements to make the peace both permanent and just. This can be done only on the basis of comprehensive and appropriate information."

As the previous discussion suggests, the new security paradigm that is unfolding does not lead to a safer world. Keeping the peace is far more problematic than anticipated at the end of the Cold War. Globalization, the Internet, and the interconnected economy, once cited as forces for integration, peace, and stability, are also creating a world of extremes.

Global Trends 2015 suggests that in the coming years, the U.S. government's efforts in peacekeeping and diplomacy will be far more complicated. For various reasons, to include the increasing influence of nongovernment organizations in world affairs, "the U.S. government will exercise a smaller and less powerful part of the overall economic and cultural influence of the United States abroad."[9] The document suggests

[9] National Intelligence Council, 2000, p. 13.

that the United States will have greater difficulty building coalitions to support its policy goals, despite the fact that the international community will often turn to Washington (if reluctantly) to lead multinational efforts in real and potential conflicts. The future role of U.S. intelligence in supporting nongovernment organizations and multinational peacekeeping efforts poses a range of formidable challenges to the status quo in the U.S. Intelligence Community.

In tomorrow's complicated mosaic for shaping the peace lies the potential for new roles for intelligence. Intelligence is essential to monitoring arms-control agreements and can be used to anticipate crises, aid diplomacy, reassure nations with heightened security concerns, support post-conflict resolutions, and monitor uneasy peace agreements. Some would argue, however, that the unremitting requirements for intelligence support to military operations dominates the security agenda to such an extent that the other purposes for intelligence—to keep the peace, mitigate strategic surprise, and help prevent conflict—have become obscured, and that strategic thinking about the myriad uses of intelligence to prevent or diffuse crises has atrophied.

The Changing Nature of Warfare

Recognition of the rapidly changing threat, new technological opportunities, and new objectives outlined by the National Security Strategy are already changing military strategy, tactics, training, and doctrine. In an article published in *Foreign Affairs* in summer 2002, Secretary of Defense Donald Rumsfeld stated that the military's challenge for the 21st century is "to defend our nation against the unknown, the uncertain, the unseen, and the unexpected." This, he said, "May seem an impossible task. It is not. But to accomplish it we must put aside comfortable ways of thinking and planning—take risks and try new things."[10] Clearly, there are major implications for U.S. intelligence in his vision.

Rumsfeld is so convinced that the transformation of intelligence is essential to the successful prosecution of future conflicts that in 2003

[10] Rumsfeld, Donald H., "Transforming the Military," *Foreign Affairs,* May-June 2002.

he created a new Undersecretary of Defense for Intelligence (USD[I]) under whom "all intelligence and intelligence-related oversight and policy guidance functions in the Office of the Secretary shall be organized." In his confirmation hearing before the Senate, the new USD(I), Dr. Steven Cambone, told the Senate Armed Services Committee that his responsibilities are to "ensure the components within the department are, to quote Title X of the U.S. Code, manned, trained, equipped--and organized--for this era of surprise."

The 2002 National Security Strategy added a sense of urgency to ongoing defense transformation efforts. It emphasized the development of new advanced remote-sensing techniques, long-range precision-strike capabilities, and transformed maneuver and expeditionary forces. It stated that innovation will rest on experimentation with new approaches in warfare, strengthening joint operations, exploiting U.S. intelligence advantages, and taking full advantage of science and technology. In emphasizing the need for transformation of intelligence capabilities, it focuses on the fact that shorter decision cycles and swifter reaction times require closer integration of intelligence and operations.

The Defense Intelligence Agency (DIA), created in the early 1960s to provide coordinated military intelligence to the secretary of defense, has the lead in providing timely and objective intelligence data and analysis to war fighters, defense policymakers, and force planners. Vice Admiral Lowell E. Jacoby, DIA director, along with Lt. General (retired) James Clapper, the director of the National Geospatial-Intelligence Agency (NGA) and Lt. General Michael V. Hayden, director of the National Security Agency (NSA), is responsible for helping the undersecretary of defense for intelligence think about change in the defense intelligence arena. Jacoby believes that bringing intelligence and operations closer together through "persistent surveillance will be revolutionary."[11] Adversaries that know that they are persistently being watched are likely to change their behavior, and may even give up without resorting to violent actions. "They can't run and hide," said Jacoby. Developing the doctrine, methods, and

[11] Jacoby, Vice Admiral Lowell E., director, DIA, interview with author, March 12, 2003.

organization for intelligence support to such "effects-based" operations will be a major challenge in the coming decades.[12] Jacoby is also a supporter of "horizontally integrating" information and activities in an effort to discover "new knowledge." He said, "If we could connect the dots better, we would have an overwhelming advantage."[13]

Both the wide-ranging possibilities—and the limitations—of intelligence were demonstrated in military engagements in Afghanistan and Iraq. Intelligence was a critical factor both before and during these conflicts, and will no doubt be critical to the success of the much-longer-term reconstruction phases following the conflicts. The task list for intelligence in such conflicts is so long that the real issue is how far such capabilities can be stretched before they break. And as defense transformation leads to force structures and "footprints" that are smaller, the reliance on intelligence will only grow larger.

The Changing National Security Strategy

In espousing new doctrine on peace and war, the 2002 National Security Strategy reflected a significant shifting of U.S. national security policy. It stated that disrupting and destroying terrorist organizations is the top national security priority (not maintaining the ability to fight two major regional conflicts simultaneously, as had previously been the case). It pointed out that "today, the world's great powers find ourselves on the same side—united by common dangers of terrorist violence and chaos" (although the war in Iraq showed that unity has its limits). It maintained that the United States increasingly shares common values with Russia and China and that the United States is committed to institutions like the United Nations (UN) and the Northern Atlantic Treaty Organization (NATO).

The National Security Strategy also acknowledged that "it has taken almost a decade for us to comprehend the true nature of this new threat" and that the United States "can no longer solely rely on a reactive posture as we have in the past." The document introduced the policy of

---

[12] *DIA Workforce of the Future, Creating the Future of the Defense Intelligence Agency*, unclassified Defense Intelligence Agency document, May 15, 2003.

[13] Jacoby, 2003.

preemptive action against those posing direct threats to the United States, and presumes that there will be evidence to establish "imminent threat" and underscore the legitimacy of action undertaken. The criticism leveled by the Congress and others regarding the intelligence on WMD preceding Operation Iraqi Freedom suggests, however, that "evidence" means different things to different people. Intelligence professionals would maintain that intelligence is largely inferential. Rarely does intelligence provide indisputable evidence.

It is worth noting that the National Security Strategy devoted a significant amount of attention to the importance of intelligence, referring to it as the "first line of defense against terrorists and the threat posed by hostile states." It will be necessary, the document further elaborates, to "transform our intelligence capabilities and build new ones to keep pace with the nature of this threat" and specifically recommended the following:

- strengthening the authority of the Director of Central Intelligence
- establishing a new framework for intelligence warning
- developing new methods of collecting information
- preventing the compromise of intelligence capabilities, and
- improving all-source analysis.[14]

The establishment of the new Undersecretary of Defense for Intelligence, the new Directorate for Information Assurance and Infrastructure Protection in the Department of Homeland Security, the new Terrorist Threat Integration Center, and several other organizations that use or integrate intelligence can be seen as the logical outcome of the new emphasis on intelligence to address both foreign and domestic terrorism, and particularly on intelligence sharing and collaboration. It remains to be seen how all of these quickly established organizations will be knitted together to transform and improve the performance of U.S. intelligence writ large.

---

[14] The White House, 2002.

Other Trends: The Changing Nature of Information

Intelligence has competition in the "knowledge" business. Raw data, as well as sophisticated analysis, on millions of topics are readily available on the World Wide Web and through other commercial supplies of information. The competition will grow and improve as the economic value of "knowledge" increases, and some observers will begin to question the "value" of intelligence capabilities when so much other information is available, especially users who have found intelligence slow, inconclusive, or hidebound by classification rules and other controls. U.S. intelligence has always enjoyed an advantage in expertise and access in some areas, but will it in the future? The competition will force everyone in the knowledge business—U.S. intelligence included—to rapidly change processes and procedures in order to stay relevant.[15]

Although constrained budgets during the 1990s forced the Intelligence Community to struggle to keep up with rapidly changing information technology, in many cases it succeeded. Advances in information technology proved to be the catalyst for numerous changes—from analytical tools to dissemination of intelligence products—over the past two decades. Developments in both information technology and communications greatly impacted the speed and ability with which intelligence can be shared, and allowed for the rapid flow of intelligence to any point on the globe.

Bruce D. Berkowitz and Allan E. Goodman, among others, argue that the Intelligence Community did not adequately adapt to the Information Revolution. They believe that among the reasons for recent intelligence shortcomings is the fact that intelligence requirements and the Intelligence Community's comparative advantage are both fluid, while its bureaucratic processes are static.[16] As a result, they say, the Intelligence Community may be locked into outmoded technologies,

---

[15] Toffler, Alvin, and Heidi Toffler, *War and Anti-War*, New York: Warner Books, 1993, pp. 188-193. The Tofflers devote an entire chapter to the impact of information technology on intelligence and a section on the impact that the changing nature of information (the "third wave" of fundamental societal change) will have on intelligence.

[16] Berkowitz, Bruce D., and Allen E. Goodman, *Best Truths: Intelligence in the Information Age*, New Haven: Yale University Press, 2000, p. 44.

collection operations, and analytical methodologies when new and possibly better ways of developing knowledge are available.

As the amount of available information (and misinformation) continues to increase, isolating information with intelligence value that is relevant, timely, *and* accurate may become even more difficult. A former vice chairman of the National Intelligence Council, Gregory F. Treverton, believes that this problem will be compounded in the future unless the Intelligence Community drops the distinction between collection and analysis. "During the Cold War, collectors could be separated from analysts, since what to look for was not a problem: Almost anything about the Soviet Union would do," Treverton said. "Now . . . the best looker is not a spymaster, much less an impersonal satellite, but rather someone trained in the substance of the subject—an analyst."[17]

The Information Revolution calls into question not only the distinction between collection and analysis, but also more fundamentally, the distinction between intelligence and information. Some even wonder whether the development of an "Information Community" would prove more useful in analyzing and synthesizing data on many future challenges (civil unrest, economic destabilization, environmental degradation, health emergencies) than an Intelligence Community (and it could certainly reduce the difficulties in sharing information among governmental and non-governmental organizations not in the U.S. national security arena, as well as multinational entities). The Intelligence Community needs to more clearly define its role in the rapidly evolving security environment, as commonly available information and knowledge improve in quality, accuracy, and timeliness.

The Pace of Technological Change

While information technology radically transformed society over the past two decades, several new areas of technology possess the potential to provide the same monumental impact over the next two decades.

---

[17] Treverton, Gregory F., *Reshaping National Intelligence for an Age of information*, Cambridge, UK: Cambridge University Press, 2003, p. 10.

Innovations in biotechnology, material science, and nanotechnology could prove to be the catalysts of tomorrow's revolutions in everything from transportation to agriculture.[18]

However, what is likely to prove to be different about the technological changes of the next two decades is the *rapidity* with which technological innovations come, who the technology leaders are, and how the technical knowledge related to these innovations is shared. All of these developments are the result of the spread of information and communications technology across the globe. According to *Global Trends 2015,* "The time between the discovery and the application of scientific advances will continue to shorten. Developments in the laboratory will reach commercial production at ever faster rates, leading to increased investments."[19] Unfortunately, information about potentially destructive technology will also spread with greater rapidity.[20] The U.S. is unlikely to be the only beneficiary of rapid technological development in the future, and, many observers argue, is unlikely to be the technology leader in many areas, such as nanotechnology, in the years to come.

Expectations of Intelligence Consumers

Three dynamics are rapidly changing what consumers[21] are expecting from intelligence: who the consumers are, what they want, and when they want it. After September 11, the list of would-be intelligence consumers grew exponentially. The type of intelligence that state, local, and tribal officials need is different from the typical intelligence product. The "decision-window" for these new consumers is not open for long, and whatever information is available should be provided to them immediately, and in a form that is useful to them. "I believe we should get more information—before news media does," complained one law-

[18] National Intelligence Council, 2000, p. 32.
[19] National Intelligence Council, 2000, p. 32.
[20] National Intelligence Council, 2000, p. 14.
[21] A *consumer* in this context is defined as an authorized person who uses intelligence or intelligence information directly in the decisionmaking process or to produce other intelligence (Central Intelligence Agency, Office of Public Affairs, *A Consumer's Guide to Intelligence,* Washington, D.C.: CIA, 1994).

enforcement official.[22] "It seems police are the last to know and the first to get a call!"

When the CIA was established in 1947, it was created primarily to serve the president of the United States. Thus, the tendency toward centralization—so that the president could turn to one spokesperson on intelligence matters rather than many—made sense. But as the intelligence apparatus grew and became more capable, the number of consumers grew, as did their expectations for what intelligence should be able to provide them. The cabinet members of the National Security Council were always consumers, but over the years the list came to include military and civilian policymakers at many levels of government and in many locations, each wanting their intelligence advisors close at hand. "Who is intelligence to serve?" is one of the thorniest questions at the heart of the debate between those demanding greater centralization and those seeking greater decentralization of intelligence.

Assimilating new consumers into the mix is difficult even if they are familiar with intelligence culture and practices, and it is especially challenging if they are new consumers unversed in the strictures regarding the protection of sources and methods. Initially, both intelligence producers and consumers regard each other with some suspicion. New users cannot be expected to be able to articulate their requirements with the same degree of specificity and sophistication as traditional users. It takes some time for both to adjust to the new relationship and for intelligence to meet the new demands.

The needs of traditional consumers are changing at the same time. Contrary to popular perception, busy policymakers are not spending all their time surfing the Net and doing their own fact-finding and analysis. Rather, according to Treverton, they are more, not less,

---

[22] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission), *Implementing the National Strategy: Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction,* Santa Monica, Calif.: RAND Corporation, December 15, 2002, p. 29 (http://www.rand.org/nsrd/terrpanel/report4rec.html).

reliant on information brokers. "The images that are sometimes evoked of policymakers surfing the Net themselves, in direct touch with their own information sources are very misleading," he says, adding that as their access to information multiplies, "their need for processing, if not analysis, goes up."[23]

There is no doubt though, that common access to vast amounts of data, as well as sophisticated analysis available through open sources, heightens intelligence consumer expectations. John Gentry, a former CIA officer, observed, "No small part of the disillusionment policymakers have had with intelligence is that they—consumers of intelligence—have inflated and unrealistic expectations of what the Intelligence Community can do."[24]

One final issue with regard to consumer expectations is the speed with which they expect their intelligence to be delivered. Advances in computer technology and communications provide the technical ability for information to be disseminated instantaneously. Intelligence consumers—especially new consumers—expect nothing less and will likely be frustrated by anything other than immediate, real-time answers to their questions. It is easy to confuse, at times, the speed with which one can provide data ("Okay, sir, here are the facts and the numbers on this issue") with the speed with which one can provide analysis ("And here's what they mean in the context of the question you're asking"). The challenge for intelligence analysts will always be to either try to meet the expectations of Internet-savvy consumers or to explain more clearly why such expectations cannot, at times, be met.

Expectations of the American Public

"One result of the inquiries into the tragedy of September 11, CIA Deputy Director for Operations (DDO) James Pavitt told the American Bar Association, "is that the American people have—I believe—a far better

---

[23] Treverton, 2003, p 10.

[24] Gentry, John A., *A Framework for Reform of the U.S. Intelligence Community*, prepared for the Brown-Aspin Commission on the Roles and Capabilities of the United States Intelligence Community, June 6, 1995 (published with the consent of John Gentry on the Federation of American Scientists [FAS] Web site, www.fas.org/irp/gentry/index/html).

sense of what their intelligence agencies can and cannot do. We have now had a chance to share, in general terms, the difficulties we face and the breakthroughs we have made."[25]

It would be difficult to argue that there was a time when the contributions of intelligence were better known, or its shortcomings more widely publicized. In addition to public Web sites maintained by various intelligence organizations, there are also many other sources on the Web—some with accurate information, others of a more questionable nature—available to those who wish to learn more. A search for books on the "CIA" in the public library yields a list of well over 100 titles. Movies, documentaries, and television shows about intelligence abound. The net result of this public information is often unrealistic expectations for what intelligence can deliver.

Intelligence scholar Walter Laquer agrees: "The crisis of intelligence is, in part, the disappointment that results from unrealistic hopes." He notes, for example, that new technologies are of great value in establishing the presence or absence of certain weapons systems, but are of no value in addressing other intelligence problems. "This is particularly true of political, as distinct from military, intelligence," he says. He also notes, moreover, that there are real crises resulting from the need to cover more ground, more countries, and many more problems. He makes a point of distinguishing these issues from the "problems besetting all big bureaucracies."[26]

The public demand for success in the war on terrorism is likely to be the greatest catalyst for revolutionary change in U.S. intelligence in the near future. The American public fully expects the Intelligence Community to anticipate and prevent any potential attack by any individual bent on killing Americans. But will the American public be willing to forego some of the rights to privacy that are held so dear in order to root out potential terrorists before they strike? The *September 11th Joint Inquiry Report* acknowledged this issue, stating, "We need to

---

[25] Pavitt, James L., CIA Deputy Director for Operations, speaking during the American Bar Association Standing Committee on Law and National Security Breakfast Program, January 23, 2003.

[26] Laquer, Walter, *A World of Secrets: The Uses and Limits of Intelligence*, New York: Basic Books, 1985, p. 9.

be honest about the fact that our homeland is very difficult to protect. For strategic warning to be effective there must be a dedicated program to address the vulnerabilities of our free and open society."[27]

This statement speaks to the tradeoffs between the right to privacy and the right to security and safety—a discussion that directly impacts the American public. At the time of this writing, the mood is swinging toward the right to security and safety. For now, the top priority is to catch terrorists and ensure that terrorist acts are prevented, and this gives U.S. intelligence and U.S. law enforcement more latitude than it did in the past. Few believe that this is a permanent state of affairs; the U.S. Patriot Act, passed shortly after September 11, has already been intensely scrutinized. As the terrorist threat waxes and wanes, so will the public's tolerance for intrusions on its privacy, but the demand for complete protection against terrorist acts will likely remain constant.

Will the Intelligence Community ever fully meet the expectations that some have of intelligence today, let alone tomorrow—i.e. prevent every terrorist strike, anticipate every surprise, *and* continue to protect individual rights to privacy? It seems apparent that U.S. intelligence is likely to be charged with more "failures" unless one of two things occurs: Either the American public comes to understand and accept the current limitations of what intelligence is, does, or can be expected to do, and expectations are adjusted accordingly, or the Intelligence Community sees this unmet challenge as an incentive to find revolutionary new ideas that will help it get closer to meeting these seemingly unrealistic demands.

THE IMPACT ON INTELLIGENCE: OUTDATED DEFINITIONS, ROLES, AND MISSIONS?

While challenging basic assumptions is necessary to begin a Revolution in Intelligence Affairs, for the purposes of this report, the following will be accepted as an underlying premise: As long as there

---

[27] U.S. Senate Select Committee on Intelligence and U.S. Permanent Select Committee on Intelligence, *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks* of *September 11, 2001*, December 2002 (http://www.gpoaccess.gov/serialset/creports/911.html).

are states, groups, or individuals who try to harm Americans or engage in activities that run counter to their interests, the U.S. government must have the means to acquire--overtly or covertly---the knowledge necessary to prevent them from doing so. To that end, the United States will need some form of official intelligence-gathering apparatus for the foreseeable future.[28] Accepting that an intelligence apparatus is and will be needed, however, does not require a prior acceptance of the current definition, roles, missions, or functions of U.S. intelligence. Those aspects of the intelligence apparatus should instead be driven by the changing security environment.

Compared with a decade ago, the security environment in which U.S. intelligence operates is significantly changed. Compared with the security environment of 1947, when the conceptual design of the Intelligence Community was formulated, the change has been monumental. Yet, in that 50-plus-year period, no one has successfully challenged the underlying premises that shape and define the Intelligence Community. According to the former executive director for Intelligence Community Affairs in the Office of the Director of Central Intelligence, Larry C. Kindsvater, during that span of time, more than 20 official commissions and executive branch studies proposed organizational and administrative adjustments to improve the operation of the Intelligence Community. Yet, Kindsvater notes, "None of the recommendations that would fundamentally alter the management or organizational structure of the Intelligence Community have been implemented."[29]

In addition to official commissions and studies, numerous academics, scholars, former intelligence officials, and interested observers generated ideas for improving intelligence.[30] Many focused on

---

[28] Several U.S. presidents have made this argument. For example, Dwight D. Eisenhower said the following during a televised report after the Paris summit of May 25, 1960: "During the period leading up to World War II, we learned from bitter experience the imperative necessity of a continuous gathering of intelligence information."

[29] Kindsvater, Larry C. "The Need to Reorganize the Intelligence Community: A Senior Officer's Perspective," *Studies in Intelligence,* Central Intelligence Agency, Vol. 47, No. 1, 2003, p. 34.

[30] See the following Web sites for a selection of unclassified reform proposals that have circulated since the end of the Cold War: Center for the Study of Intelligence (http://www.cia.gov/csi/pubs.html),

one agency or a specific intelligence discipline and offered point solutions. A few offered more sweeping reforms that ran into political, bureaucratic, financial, legal, or jurisdictional obstacles upon attempted implementation. Others reiterated recommendations from earlier proposals, while still others came to contradictory conclusions, leading to frustration on the part of both the reformers and the to-be-reformed.

Why did so few of the reform efforts succeed in effecting fundamental change? In no small part, bureaucratic resistance from the military services and the departments of state and defense initially forced the establishment in 1947 of a small, weak CIA and a Director of Central Intelligence (DCI) with limited authority. This influence continues to play a role in keeping the Congress and the president from passing reforms that would give the CIA or the DCI direct authority over the Intelligence Community.[31] Perhaps, as some would have it, there really is no "Intelligence Community," but rather an abstraction and a policy creation instead of a viable, operational entity. Therefore, there is no need for a comprehensive, Intelligence Community-wide approach to reform in the future. That argument maintains that intelligence is a support function appropriately subordinated to a specific consumer, and the organizations comprised by the Intelligence Community should not be artificially bound together in any way. A closer study of the whys and wherefores of the limited success of intelligence reform, however, suggests a combination of many factors that come into play whenever a large, mature, and fairly successful institution is faced with the possibility of dramatic change.

A biologist would say that in an ideal structure, form should follow function. Based on that logic, discussion of restructuring or reorganization should be preceded by discussions on possible changes in intelligence functions. Functions will change if they no longer support

---

Loyola University Center for Strategic Intelligence (http://www.loyola.edu/dept/politics/intel.html), and Columbia University, which has links to documents relating to intelligence reform (http://www.columbia.edu/cu/lweb/indiv/lechman/intell.html).

[31] For discussions on the bureaucratic politics at the center of the centralization/decentralization debate, see Zegart, Amy, *Flawed by Design: The Evolution of the CIA, JCS, and NSC*, Stanford, Calif.: Stanford University Press, 1999.

the intelligence mission, and the intelligence mission will change if there are fundamental changes in the larger national security environment. The previous review of changes in the external environment suggests that a point has been reached where the debate does not need to return to another battle over reorganization, but instead focus on first principles.

What is intelligence? Why does it exist? What is its role in a democratic society? What are its missions? One early definition of intelligence was offered by Sherman Kent, the "father of CIA analysis." He described intelligence as "knowledge that our highly placed civilians and military men must have to guard the national welfare."[32] In today's online, plugged-in, "24/7" world, however, this definition is somewhat problematic, since these same civilians and military personnel arrive at work with a great deal of knowledge from watching CNN, MSNBC, or some other news outlet--options not available in 1947. They can continue throughout the day to increase this knowledge by reading the Early Bird compendium of mostly print media reports and from tapping into online updates from a staggering variety of Internet sites. For intelligence producers, CIA historian Michael Warner has said, "The equation 'intelligence = information' is too vague to provide real guidance." Warner observed, "Mere data is not intelligence; thus these definitions are incomplete. Think of how many names are in the phone book, and how few of those names anyone ever seeks. It is what people do with data and information that gives them the special quality that we casually call intelligence."[33]

Others have not necessarily defined intelligence, but have tried to at least describe, bound, or characterize it. In this sense, intelligence is something more than information and something more than knowledge. It includes data that is obtained through specialized means

---

[32] Kent, Sherman, *Strategic Intelligence for American World Policy,* New Haven, Conn.: Yale University Press, 1949, p. vii.

[33] Warner, Michael, "Wanted: A Definition of Intelligence," *Studies in Intelligence,* Central Intelligence Agency, Vol. 46, No. 3, 2002, p. 17.

and provided for very specific purposes.[34] It involves experience, intuition, and judgment. It is both an activity and a product.

A better definition of intelligence will facilitate the debate on everything from new functions to new structures. Warner's proposed definition of intelligence--"secret, state activity to understand or influence foreign entities"--emphasizes the fact that intelligence is more about secrecy than information. He argues that clarification of the definition in this manner will assist scholars in their development of new intelligence theories, provide a firmer institutional footing for covert action, guide declassification policy, and help sort the various activities that should be performed in the Intelligence Community, leaving the remainder to be performed by other parts of government.

Clarification of the definition of intelligence also helps intelligence consumers and the American public to understand what intelligence does and does not do. Some believe that "intelligence" is a type of "hyperinformation," and thus should be able to provide "knowledge" on any and all security topics from the profound to the obscure. This debate—between defining intelligence narrowly as secret information obtained by secret means, and defining it more broadly as the processing of all types of information to best serve the intelligence consumer (with secret information being a "condiment")[35]—must be resolved before any consensus is reached on the future direction of intelligence. The more expansive the definition of intelligence, the larger and more inclusive of outsiders the intelligence "community" will need to be.

In addition to its definition, the description of the roles and missions of intelligence requires updating as well. After the shock of

---

[34] Berkowitz and Goodman (2000) also provide an interesting definition of intelligence: "Expertise and information on subjects the private sector will not cover adequately because it is unprofitable; Information that the private sector will not or cannot collect because it would be too technologically demanding; Information that the private sector should not, cannot, or will not collect because of legal constraints or risks; and, Tailored products providing this specialized information combined with other sources (as appropriate) to U.S. officials."

[35] Comment made during a workshop on "A Revolution in Intelligence Affairs" in Arlington, Va., January 2003.

Pearl Harbor, the peacetime intelligence apparatus that came to be known as the Intelligence Community was created primarily to provide "strategic warning"[36] of possible threats to the United States and its interests. Many within the Intelligence Community believe that preventing strategic surprise has been the overarching mission of intelligence for thousands of years, is still the mission today, and is more than likely to remain the mission of tomorrow. But while this may be the de jure mission of intelligence, the de facto mission of intelligence appears to be significantly changing. It appears that the intelligence mission may now go beyond simply warning of a potential attack—to *preventing* any type of attack that places the country at risk.

While at first blush this might seem a subtle semantic distinction, in fact it is a distinction with enormous implications. Anyone reading the newspapers before September 11 knew that al Qaeda was a threat to Americans both home and abroad. DCI Tenet stated in his testimony before the Joint Inquiry into the events of September 11 that Bin Laden and his activities came to the attention of the CIA during the Saudi's stay in Sudan from 1991-1996.[37] Al Qaeda's attack, therefore, was *not* a strategic surprise, nor was it even an operational surprise; the use of airliners as weapons was anticipated, but that did not prevent the loss of nearly 3,000 lives in what was certainly a tactical surprise. According to the final report of the Joint Inquiry on the events of September 11, "Some significant pieces of information in the vast stream of data being collected were overlooked, some were not recognized as potentially significant at the time and therefore not disseminated, and some required additional action on the part of foreign governments

---

[36] According to the Joint Military Intelligence College (JMIC) publication *Anticipating Surprise: Analysis for Strategic Warning* (JMIC: Washington, D.C., March 2002), *strategic warning* is defined as "a forecast of a probable attack or that enemy-initiated hostilities may be imminent; warning must be received early enough to permit decision-makers to undertake countermeasures . . . usually can range from a few weeks to several days."

[37] DCI testimony to U.S. Senate Select Committee on Intelligence and U.S. Permanent Select Committee on Intelligence (2001), p. 3.

before a direct connection to the hijackers could have been established."[38]

In other words, if U.S. intelligence is to help protect Americans from future attacks, more precise "tactical" warning—that a specific individual plans to strike at a specific place with a specific weapon at a specific time—is necessary. That level of precision is likely to be the new threshold for intelligence "success" in the future. Even as it shifts focus to challenges imposed by new threats, new forms of warfare, and new methods for finding peaceful solutions, it does not appear likely that the Intelligence Community will ever be able to abandon its traditional mission of warning of an impending attack by a foreign nation. Thus, the new "tactical" warning missions associated with homeland security will likely be added to the traditional strategic warning mission related to potential conflict, and to the various missions of intelligence after a crisis or conflict begins. Will the U.S. Intelligence Community be equipped to do all this and more?

Mission success—difficult though it may be to measure at times—will always be the primary determinant of the Intelligence Community's effectiveness. If the mission—even a rapidly changing mission—is not being accomplished, then that is a sure sign there is a fundamental problem. It is imperative to clarify whether the overarching mission of intelligence is substantially changing, and if, in turn, its sub-missions are changing as well. What specifically is the role of intelligence in homeland security? Where does its mission begin and end? Is it a higher priority than support to U.S. troops overseas? Is it a higher priority than support to diplomatic efforts in the Middle East?

A debate on a Revolution in Intelligence Affairs and the future of intelligence must begin with a fresh look at what truly threatens the safety and security of Americans today and then contemplation of how that threat might change throughout the coming decades. The debate should question how this changing security environment would affect intelligence charters, missions, and priorities and should consider the

---

[38] U.S. Senate Select Committee on Intelligence and U.S. Permanent Select Committee on Intelligence (2001).

implications for intelligence capabilities, functions, policies, and organizations.

3. THE ARGUMENTS FOR AND AGAINST A REVOLUTIONARY RESPONSE

"Even those who fancy themselves the most progressive will fight against other kinds of progress, for each of us is convinced that our way is the best way."

Louis L'Amour
The Lonely Men (1969)

This chapter of this report examines the implications of mismatches between a rapidly changing security environment and linear, evolutionary change in the Intelligence Community. The Intelligence Community, if it is to effectively continue as a collective body of interdependent constituents, must come to terms with any shortfalls in its functions and capabilities and any incompatibilities in its organization and structure. Changes in the nature, magnitude, and reach of the challenges imposed by the evolving security context within which the Intelligence Community operates merit a response beyond that of marginal change. Currently, serious shortfalls and incompatibilities exist and are likely to worsen in the future. Reform efforts falling short of a revolutionary response to the altered security environment will, at best, provide only localized or short-lived improvements, and at worst, condemn the Intelligence Community to anachronism.

THE IMPETUS FOR BUREAUCRATIC INCREMENTALISM

The relevant questions with regard to the future of U.S. intelligence are not whether it should change—it will change regardless of whether anyone wants it to or not—but what should be the magnitude and pace of that change. The evolutionary versus revolutionary debate is still alive and well throughout the various government bureaucracies.

In the face of a significant change in the security context in which U.S. intelligence must operate, it would seem logical to expect widespread recognition that the Intelligence Community needs to change accordingly. If this argument prevails, the Intelligence Community would

accept the need and seize the opportunity to change fundamentally in order to remain relevant and effective in the evolving security context. Yet, that is not the case today. Many observers, while recognizing some change in the security context, believe that it is not necessary to significantly alter the status quo to accommodate new requirements. Still others fear that fundamental change in the form and function of intelligence would be ill advised if not downright dangerous.

The evolutionary argument is captured well by Richard J. Harknett in his critique of the Revolution in Military Affairs (RMA), a concept that was the topic du jour in the 1990s. The RMA theorists argued that, in military organizations, technological changes created opportunities for fundamental restructurings that, in turn, could lead to convincing operational superiorities. Harknett stated, "The information-age enthusiasts insist that the United States should overturn a system it already dominates and push to radically expand America's advantage." He further said, "The normal process of evolutionary adaptation is perfectly adequate to the times and is a safer and wiser response to new technology . . . incremental change is a better—if less exciting—bet than radical transformation. The revolution can wait."[1]

Nonetheless, many believe that an RMA has already transpired, citing cases in which large bureaucratic entities brought about revolutionary change. In each case in which such a change occurred, distinct internal and external conditions were present. The primary condition was a shared recognition of a serious unmet challenge that "business as usual" could not address. In corporate America, this juxtaposition is called a "strategic inflection point," a time when a company must *fundamentally* change or risk its very existence. It is not clear, however, whether there is a consensus within the Intelligence Community that it has reached a strategic inflection point or that there is sufficient motivation to undertake the painful process of revolutionary change.

---

[1] Harknett, Richard J., and the Joint Center for International Security Studies, "The Risks of a Networked Military," *Orbis,* Winter 2000, p. 12.

Those who argue against the need for a revolutionary change in the U.S. approach to intelligence often begin by stating that there have in fact been many changes in the Intelligence Community since the end of the Cold War. These changes exist particularly in how the Intelligence Community operates and therefore are less visible. Some of these changes are the result of a change in priorities; others were driven by decreasing budgets and drastic reductions in personnel. The testimony of DCI George Tenet before the Joint Inquiry investigating the events of September 11 states, "During the 1990s, our Intelligence Community funding declined in real terms--reducing our buying power by tens of billions of dollars over the decade. We lost nearly one in four of our positions. This loss of manpower was devastating, particularly in our two most manpower-intensive activities: all-source analysis and human source collection."[2]

Tenet said, during the Joint Inquiry into the events of September 11, that to cope with declining assets the Intelligence Community was encouraged to "surge" to address each unfolding crisis--that is, redirect assets from one activity to another rather than add more people or money to address emerging intelligence challenges. The need to surge was almost constant throughout the 1990s to deal with crises ranging from Somalia to Kosovo. Moreover, the surge to address an emerging crisis was rarely temporary. The intelligence surge during the Gulf War, for example, was followed by years of round-the-clock support to Operation Southern Watch in Iraq.[3]

Demands as diverse as supporting the conflict in the Balkans, monitoring hostilities between India and Pakistan, and tracking the spread of weapons of mass destruction and the growing threat of terrorism[4] in effect forced the shrinking Intelligence Community to quickly adapt to new, and in many cases, enduring priorities. The net effect was an Intelligence Community redirected from its old Cold War

---

[2] Tenet, George, "Written Statement for the Record of the Director of Central Intelligence Before the Joint Inquiry Committee," http://www.cia.gov/cia/public_affairs/speeches/2002/dci_testimony_10172002.html, October 17, 2002, p. 22.

[3] Tenet, 2002, p. 23.

[4] Tenet, 2002, p. 23.

focus, but spread thin in many areas. Compounding the problem was the fact that during the 1990s the defense department was also reducing its tactical intelligence units and funding, thus putting an additional burden on national intelligence systems to cover tactical military intelligence gaps.[5]

Despite the normal and expected bureaucratic resistance, there were a number of organizational changes during these years as well. A new agency—the National Imagery and Mapping Agency (NIMA, since renamed the National Geospatial-Intelligence Agency, or NGA)—was created. Existing agencies, including the CIA, NSA, DIA, and the National Reconnaissance Office (NRO), reorganized not once but numerous times. Several "DCI centers" were formed to address evolving threats, such as weapons proliferation, narcotics, international crime, and counterintelligence.[6] There were changes in how the Intelligence Community operated as well. New focus was given to the toughest regional challenges. According to CIA DDO James Pavitt, "We have more reporting on the really hard targets than I can remember at any time in my nearly 30 years of agency service."[7] Other initiatives were launched to rebuild the clandestine service and the analytic corps, and to improve scientific and engineering expertise.

The National Security Act of 1947 deliberately limits the DCI's authority over the "combat support agencies" run by senior military officers. The Act ensured that he shared his authority with the Secretary of Defense. In 1997, however, the DCI's ability to manage the Intelligence Community was strengthened by new legislation that established a deputy DCI for community management and several assistant DCIs (ADCIs) responsible for intelligence collection, analysis and

---

[5] Tenet, 2002, p. 23.

[6] For a fuller description of the five agencies mentioned above, as well as the DCI centers, see Central Intelligence Agency, Office of Public Affairs, *A Consumer's Guide to Intelligence,* Washington, D.C.: CIA, 1994.

[7] Pavitt, James L., CIA Deputy Director for Operations, speaking during the American Bar Association Standing Committee on Law and National Security Breakfast Program, http://www.cia.gov/cia/public_affairs/speeches/2003/ddo_speech_01232003.html, January 23, 2003.

production, and administration.[8] As a result, a number of new communitywide processes and procedures were established, and several strategic planning documents were published under the DCI's auspices providing guidance to the entire Intelligence Community, rather than just the CIA. For the most part, however, any attempt at organizational reform during these years was left to the individual agencies.

In addition to changes generated from within, a good deal of pressure to redirect the Intelligence Community's efforts after the Cold War was exerted by the six congressional oversight committees, the Office of Management and Budget, and a new cadre of inspectors general within many of the agencies. President Clinton's National Performance Review succeeded in streamlining some intelligence processes, and a much closer partnership was forged between the Intelligence Community and analytical experts on the outside. A great deal of new technology was developed during these years, but the ability to experiment was limited because aging systems and infrastructure ate up discretionary dollars.[9]

Contrary to the notion of an Intelligence Community that has not changed since the end of the Cold War, some would describe an intelligence workforce that is now in the throes of reform "fatigue." Alvin Toffler described this effect as "future shock," or the stress and disorientation induced in individuals by subjecting them to too much change in too short a time.[10] While others would dispute this, it is an important consideration in contemplating why new reform efforts might encounter institutional lethargy, if not resistance. Some observers believe that after 13 years of nearly continuous change, U.S. intelligence is doing as well as can be expected. In the view of those observers, plans to rebuild lost capabilities are underway, and all that is necessary is the time to bring them to fruition. Many who subscribe

---

[8] The Intelligence Authorization Act of fiscal year (FY) 1997 amended the National Security Act of 1947 and established the deputy DCI for community management and three assistant DCIs: the ADCI for collection, the ADCI for administration, and the ADCI for analysis and production.

[9] Tenet, George J, "The Worldwide Threat in 2003: Evolving Dangers in a Complex World," testimony presented to Congress, February 11, 2003.

[10] Toffler, Alvin, *Future Shock*, New York: Random House, 1970, p. 2.

to this argument feel that steady, evolutionary change is the best approach to dealing with any new threat or crisis that might arise, and these changes are already planned within the Intelligence Community. As a participant commented at a January 2003 RAND-sponsored Revolution in Intelligence Affairs workshop, "Transformation does not occur overnight. Even something as dramatic as creating a new organization does not show improvement overnight. The 'decision' may be revolutionary, but implementation is always incremental. 'Incrementalism' is the insurance that we don't go precipitously in the wrong direction. If the change is important, it will remain important over time."[11]

CENTRAL ARGUMENTS FOR EVOLUTIONARY CHANGE

There are many other arguments advanced by evolutionary, as opposed to revolutionary, change advocates. The following arguments are among those posited most often:

- **"A revolution is not necessary—the challenges we face today are not fundamentally different from those we have faced in the past."** This argument suggests that neither terrorism, nor weapons of mass destruction, nor any other threat that the U.S. faces today is new, but is instead the product of a natural evolution of the threats that have existed for the millennia. Therefore, evolutionary improvement in U.S. intelligence capabilities is the only fix that is needed.
- **"Revolutions are disruptive—we cannot afford to be distracted from today's crises."** There is not the time, energy, people, or dollars available to experiment with innovations when the Intelligence Community must constantly support military conflicts or brewing crises.
- **"You cannot predict the outcome of a revolution in intelligence affairs—there may be serious unintended consequences."** The United States cannot afford to tamper with the primary resource it has in waging the war against

[11] The term "incrementalism" describes change that is made one small step at a time.

terrorism, diffusing regional conflicts, and conducting other such activities. Besides, U.S. intelligence has been largely successful, so why fix what isn't broken?

- **"A revolution in intelligence affairs requires sustained commitment and focus--we'll never get that**." One of the drawbacks of a democratic government is that government institutions cannot count on continuity of approach or emphasis from one administration to the next. Thus, an RIA begun under one DCI may not survive the next.
- **"An incremental approach allows for the opportunity to adjust or correct the course."** Doing so assures that one thing is not inadvertently "broken" in the process of fixing something else.
- **"Most 'reformers' are looking for the quick fix."** Politicians in both the Executive and Legislative Branches are anxious to "make a difference" during the short time they are in office. But once they leave, the revolution is over.
- **"Revolutionary change is likely to be expensive—we'll never get a long-term commitment of dollars."** Budgets are subject to change on an annual basis. A project funded today may be gone next year, especially if it has not immediately proven its value.
- **"The American public won't support the real changes that are needed."** Most people do not care about the unglamorous but necessary work that must be done to revolutionize intelligence laws, directives, policy, and procedures. If *the public* does not care, members of Congress will not care—they will focus on the easy solutions.

Table 3.1 lists more general obstacles to systemic change that are characteristic of most complex organizations as well as the Intelligence Community.

Table 3.1

Major Impediments to Systemic Change Across U.S. Intelligence

• Ambiguous authorities	• Failure to communicate
• Overlapping turf	• No coalition for change
• "Not-invented-here" syndrome	• No singular focus
• Non-participatory change process	• Legal restrictions
• Risk aversion	• Congressional politics
• The defensive reflex	• Limited constituencies
• Reform fatigue	• Mature bureaucracy
• Lack of incentives	• Defenders of status quo
• No guarantees of sustained financing	• Far-flung community with diverse cultures

In sum, there are many real impediments to change—cultural, psychological, financial, and practical—that would need to be overcome before any change of real significance could be implemented in the U.S. Intelligence Community. For example, ambiguity over who is in charge of the Intelligence Community hampers the ability of even the strongest leaders in the community to effect change. While the DCI is the titular head of the Intelligence Community, the secretary of defense has operational direction and control over nearly half of the Intelligence Community agencies and influences most of the Intelligence Community's resources. As Lt. Gen. Patrick Hughes, former director of the DIA said, "I sat down one day and counted up all of my bosses—there were 15."[12] When too many people are in charge, no one is in charge—making coherent, systemic change under the current bureaucratic structure a near impossibility.

A lack of consensus on the way forward, the absence of an "architect" who can see the big picture and draw up the outlines of change, the lack of a coalition with sufficient clout to push

[12] Hughes, Lt. Gen. Patrick, U.S. Army (ret.), interview with author, March 7, 2003.

revolutionary ideas forward—all of these problems would need to be overcome before an RIA can proceed.

It is fair to ask why, however, if the Intelligence Community has shifted its focus and priorities, if reorganizations and other changes have occurred, and if the budget picture is improving, calls for reforming intelligence persist? Is it really necessary to open a wider debate when the way forward, at least to some, appears to be very clear? Is it not possible that the Intelligence Community will be able to meet whatever future challenge might come down the road without the pain and turmoil that more radical change creates? Is there a way to ensure that in bringing about fundamental change a capability already stretched thin will not "break" in the process? Can the nation afford the risk of bringing about change at a time when there are great demands being placed on intelligence every day? These are arguments that must be addressed, not ignored, if a more fundamental restructuring—a Revolution in Intelligence Affairs—is to be considered a viable and appropriate approach to addressing future U.S. intelligence challenges.

BREAKING THE MOLD: THE CASE FOR REVOLUTION

Although the principle of aligning intelligence capabilities with a changing environment may seem obvious to some, achieving that alignment is difficult in practice. Incrementalism, while certainly attractive to some participants in the intelligence debate, is not universally accepted as the only approach to accommodating the changed security conditions that confront the Intelligence Community today. A growing number of intelligence professionals and observers are convinced that the ineffectiveness of past external reform efforts, the accelerating pace of change in the security environment, the mismatch between today's threats and intelligence capabilities, the opportunities offered by new technology, and the rising chorus of new consumers calling for different types of intelligence combine to demand nothing short of an intelligence transformation. All of the changes of the past decade, they would argue, do not amount to an Intelligence Community optimized to address the threats and opportunities of today or tomorrow.

The would-be "revolutionaries" engaged in this debate argue that without a "Revolution in Intelligence Affairs" grounded in sound strategic thinking and operational reassessment, three unsatisfactory and possibly disastrous outcomes could potentially result:

- U.S. intelligence will continue to change incrementally through traditional planning, programming, and budgeting processes, which will only serve to institutionalize and, thus, virtually ensure continuing mismatches between rapidly changing external realities and slowly adapting intelligence capabilities; or
- U.S. intelligence will be reshaped "on the margins" by outside commissions, legislative reform groups, and others whose temporary assignment to the case will limit their focus to glaring problems and quick solutions; or
- fundamental changes will occur in a chaotic and incoherent manner as competing intelligence users push forward proposals that address parochial concerns, with little regard for synergies or common interests.

The small but growing band of revolutionaries that has begun to coalesce seeks a different outcome by seizing the opportunity to create intelligence capabilities that can both shape as well as adapt to the rapidly changing security environment. In their view, a major opportunity for fundamental change——for an RIA, if you will——lies in the obvious fact that the Intelligence Community is a mature bureaucracy that, like all bureaucracies, has become set in its ways. Thus, it is time for the U.S. Intelligence Community to step back and question whether it is doing things the way it is now because it has always done them that way. It should ask, if given the opportunity to recreate itself *tabula rasa*, whether it would come up with the same practices and approaches, policies, and structures that it has today. Or, would it start with something different——fewer agencies or agencies with different charters——or a shift in emphasis among various skills and technologies?

Peter Drucker argues that any organization, biological or social, needs to change its basic structure if it significantly changes its size. Any organization that doubles or triples in size needs to be restructured because it outgrows its policies and rules of behavior. If it continues in its old ways, says Drucker, it becomes ungovernable, unmanageable, and uncontrollable.[13] The Intelligence Community is far larger than it was in the Eisenhower Administration, but its basic structure, policies, and rules for doing government business and for managing people stayed the same. It is difficult to imagine that those who passed the National Security Act of 1947 envisioned that the DCI would one day be called upon to manage the complex enterprise that is the Intelligence Community today.

The size of the Intelligence Community also argues for addressing change in a comprehensive and coherent manner that treats the entire intelligence enterprise as a functional system, not as merely a blanket shorthand term to refer to a number of independent agencies and offices. This systemic view of the Intelligence Community is appropriate because activities and programs that are conducted by independent actors under varying degrees of secrecy are in constant danger of creating unwanted redundancies, coming into operational conflict or, worse, working at cross-purposes.

The changes that have been brought about incrementally in the Intelligence Community are neither systemic nor coherent——they are largely piecemeal, haphazard, and focused more on what is "doable" rather than on what needs to be done. Each of the organizations that constitute the Intelligence Community more or less determines, on its own, how to cope with changes in the external environment. When new organizations were established or existing ones were reorganized, there was no fundamental rethinking of the larger intelligence system. Often, new organizations and processes were layered on top of old ones, and internecine feuding increased. Legacy systems usually continued, rather than be replaced by new ones, thus shrinking funds available for innovations. Budget cuts tended to force organizations to stick with the

---

[13] Drucker, Peter, *Managing in a Time of Great Change*, New York: Truman Talley Books/Dutton, 1995, p. 290.

"tried and true" rather than invest in risky experiments that could lead to breakthroughs. By the beginning of the 21st century, revolutionary change proponents will argue, the United States saw the downside of incrementalism in the Intelligence Community--i.e., an intelligence system that was wholly unprepared for the new and different challenges that were to come.

COUNTERING THE INCREMENTALIST APPROACH

As discussed in the previous section, those who advocate a slower, more incremental approach to change have powerful arguments for why rapid change should not, or cannot, be attempted in the Intelligence Community. Those who would advocate an RIA would respond to the "Evolutionaries" in the following manner:

- **Evolutionary argument: "A revolution is not necessary—the challenges we face today are not fundamentally different from those we have faced in the past."**
  Revolutionary response: While neither terrorism nor WMD is a new phenomenon, the intersection of the two *is* a recent occurrence. This dangerous situation is likely to worsen with time as the knowledge and ability to manufacture WMD inexorably spread and the availability of WMD increases, whether for monetary, political, or ideological gain on the part of the sources of those weapons.
- **Evolutionary argument: "Revolutions are disruptive—we cannot afford to be distracted from today's crises."**
  Revolutionary response: There is never a good time to undertake comprehensive change. Most who have successfully brought about truly significant change in the past, however, did so by creating parallel processes—one set of process that changes things slowly and another that constantly questions the status quo, experiments with new ideas, and pushes for implementation of new ideas whenever possible. The best organizations ensure that both of these parallel processes are strong, credible, and exist cooperatively, if not harmoniously.

- **Evolutionary argument: "You cannot predict the outcome of a revolution in intelligence affairs—there may be serious unintended consequences."**
  Revolutionary response: It is true that unintended consequences may come of revolutionary change, but it is not predetermined that they will. One way to avoid negative outcomes is to objectively evaluate all change proposals to determine what functions, structures, and processes will change and if intelligence performance will improve as a result. Another is to conduct field experiments, a sort of *in vitro* laboratory, to evaluate in a practical fashion the impact of change proposals on real-world processes and activities, much as the military services did for many years.
- **Evolutionary argument: "A revolution in intelligence affairs requires sustained commitment and focus—we'll never get that."**
  Revolutionary response: Those who successfully brought about revolutionary change in their institutions recognized that continuity in leadership is essential. While leadership at the top of the Intelligence Community might change from one administration to the next, the vast majority of managers at the next level down will stay the same. It is those leaders who must buy into the vision for the future and ensure that it continues after political appointees move on. If the need for change is compelling enough, this constancy of purpose can be achieved.
- **Evolutionary argument: "An incremental approach allows for the opportunity to adjust or correct the course."**
  Revolutionary response: There is no reason a revolutionary approach cannot allow for the opportunity for course correction. In fact, if the revolution from the outset builds in a dynamic approach to accommodating change, adjustments will be made more often and more rapidly than would be the case in an incrementalist approach.

- **Evolutionary argument: "Most 'reformers' are looking for the quick fix."**

  Revolutionary response: It is true that politicians in both the Executive and Legislative Branches are anxious to "make a difference" during the short time they are in office. This can be a real advantage to an institution that needs to "jump start" its revolution--it can rely on the permanent bureaucracy to see that the revolution continues. Again, buy-in throughout an organization is essential. If the leadership doesn't make the case for revolutionary change throughout the organization at all levels, the effort is likely to fail.
- **Evolutionary argument: "Revolutionary change is likely to be expensive—we'll never get a long-term commitment of dollars."**

  Revolutionary response: This argument is true, unless Congress is a willing partner. If Congress is invited to become part of the "coalition" that envisions and promotes revolutionary change, chances are much greater that funding for new technologies, operations, and organizations will follow.
- **Evolutionary argument: The American public won't support the real changes that are needed."**

  Revolutionary response: It is true that most people are not paying attention to intelligence laws, directives, policies, and procedures, but they are beginning to care——and care a great deal——that this country's intelligence capabilities may not be up to the task of meeting future challenges. Heightened congressional scrutiny, establishment of the Joint Inquiry and Kean Commission investigations into the 9/11 attacks, and even the comments made during the 2004 presidential campaign are a direct result of increased public interest in intelligence. Many realize that intelligence is the best and perhaps the only hope for preventing another September 11. Americans expect their government to push for whatever change is needed to ensure that an event on the scale of 9/11 never happens again.

Many of the challenges facing intelligence today seem daunting, and some problems envisioned for the future appear to be, given current thinking, insolvable. However, a unique benefit of a Revolution-in-Intelligence-Affairs approach to change is that it would unleash people's talents and imagination so that they may consider solutions that were previously inconceivable or not obvious. As in the corporate research and development institutions that have pursued futurist visions, this is usually accomplished through an infusion of fresh thinking and unbiased interest. The "revolutionary" process, once established within the Intelligence Community, could bring together people with diverse backgrounds—technologists, cultural anthropologists, theologians, chaos theorists, lawyers, and analysts, to name a few—to contemplate a wide range of solution sets, free from normal bureaucratic constraints. Furthermore, a revolutionary process could accommodate a structured intellectual debate that allows leaders to anticipate external changes, devise new strategies and paths for innovation, and gain insights into alternative ways of conducting the business of intelligence.

4. THE PROSPECTS FOR REVOLUTION

"Revolutions are not made, they come."

Wendell Phillips
Abolitionist, orator
From a January 1852 speech

This chapter examines the historical record to provide benchmarks for evaluating the feasibility of fundamental change in complex organizations. The discussion focuses on case studies involving the transformation of the U.S. military, various approaches undertaken by commercial business entities in response to technological changes and competitive challenges in the 1980s and 1990s, and the formative years of the Intelligence Community itself in the aftermath of the Second World War. From these experiences, one may conclude that revolutions indeed have and therefore can occur within complex bureaucracies. The discussion in this chapter further distills the key elements, forces, and relationships in common across these instances of bureaucratic revolution to inform the Intelligence Community's current struggle with change.

MODELS OF REVOLUTIONARY CHANGE

If, as this report argues, revolutionary change in the Intelligence Community is needed, the question remains whether it is *possible* to deliberately drive and manage such change. Change "management" has become a hotly debated topic in recent years, and there are many different schools of thought on what constitutes the most important elements of a successful approach. Some of the more prominent change-management theorists suggest that only those on the outside can drive meaningful change within a bureaucracy. Outsiders, they argue, are the only ones willing to consider possibilities that fall outside of bureaucratic norms and to challenge the status quo without fear of repercussion. While this approach is clearly a proficient method of

generating change proposals, it is far less proven as an effective means for implementing those proposals. Bureaucracies have many ways of ignoring or resisting "outside help."

Another school of thought suggests that revolutionary change occurs only if there is a strong leader (the "great man" theory of change management) who develops the "vision," convincingly drives home the need to change, and cuts through bureaucratic resistance. This is the approach often favored by political appointees who have to make their mark on a system within a limited window of opportunity. This approach often yields impressive, short-term results, but unless the changes are accepted and internalized by the bureaucracy, they often end up being superficial and last only as long as the proponent is in charge. According to Chris Turner, a self-described "corporate outlaw" at Xerox Corporation for many years, when revolutionary change is mandated and driven by one person in an organization "all the energy goes into pushing and resisting."[1] Both the "outsider" and "strong leader" approaches have been tried during attempts to reform intelligence, with mixed results.[2]

A third approach—one that maintains that large, bureaucratic institutions can *learn* how to undergo continuous self-assessment and generate their own revolution when necessary as a prerequisite to survival—holds greater promise in bringing about an RIA. Critical to this third approach is the *endorsement* of a strong leader and help from knowledgeable outsiders; thus, it blends the strengths of the first two approaches. This "coalition for change" approach is likely to have the best chance of success in a bureaucratic enterprise like the Intelligence Community because it avoids the dependencies of the other options, and it has the benefit of involving the Intelligence Community workforce in shaping its own destiny. Since the type of revolutionary

---

[1] Turner, Chris, *All Hat and No Cattle: Shaking Up the System and Making a Difference at Work*, New York: Perseus Books, 1999.

[2] A good example of intelligence reform generated on the outside was "IC21," the comprehensive reform proposal generated by the House Permanent Select Committee on Intelligence in 1996. DCI John Deutch was arguably a "strong" leader with a political mandate who attempted to bring about significant change within the Intelligence Community, with mixed results.

change that is envisioned earlier in this report requires an influx of new ideas (from both outsiders and short-termers) *and* needs to be sustained over time, the discussion in this chapter emphasizes case studies that reflect implementation of this approach.

It is instructive to begin with a summary look at how U.S. military and corporate institutions moved away from a mindset constrained by stability and routine to one that promotes critical self-examination and continuous flux. This chapter also examines the internal and external conditions that led to dramatic changes in American intelligence during a period (1947-1956) when, one may argue, there was an earlier Revolution in Intelligence Affairs. The goal of this examination is to identify the variables that shape successful and enduring transformational change efforts.

CASE STUDY: DEFENSE TRANSFORMATION

The United States military, with its centuries of tradition, is often criticized for holding fast to that legacy. Many believe that even when the U.S. military recognizes the need for institutional change, it looks backward instead of forward, and is always preparing to "fight the last war."

One of the most interesting aspects of the recent conflict in Iraq, however, is how different the combat phase of that military operation was from the *successful* operation of the first Gulf War little more than a decade earlier. By all accounts, the U.S.-led military coalition overwhelmingly defeated in 1991 what was ranked as one of the largest standing armies in the world. Why then, when the previous victory was so lopsided, did the U.S. military feel compelled to try a completely different approach in Iraq in 2003 to address what was arguably a more difficult and riskier challenge?

Some believe that the man responsible for the radically new strategy that drove Operation Iraqi Freedom is Secretary of Defense Donald Rumsfeld. It is clear is that from the moment he arrived at the Pentagon, Rumsfeld relentlessly pressed for the "transformation" of the U.S. military and the Department of Defense. In particular, he focused on organizing, planning, programming, and budgeting for activities that

would transform the way the military fights in years to come. However, the truly revolutionary aspects of today's U.S. military—the new military theory, strategy, doctrine, tactics, and innovations that yielded impressive results during the combat phase of the war in Iraq—have been under way long before the arrival of the Pentagon's most recent architects of reform.

It was the Soviets in the 1970s who first considered the impact of revolutionary change in technology development as a force multiplier that favored its main enemy—the United States. U.S. military thinkers, however, took this Soviet analysis and methodology to the next level during the 1980s and 1990s. The result was the relatively controversial concept of a Revolution in Military Affairs, which described a process by which technological innovation and new organizational and operational concepts drive fundamental changes in military strategy and doctrine. Proponents of the RMA concluded, after studying the interplay of technical development and other military capabilities, that it was possible to gain a strategic advantage in military force posture, at least temporarily, if military operations and organizations could be transformed to leverage what technology offered.

The simplicity and elegance of that definition belie the difficulty and complexity inherent in, and the creative energy required to actually achieve, an RMA. While the U.S. military is arguably in the midst of such a revolutionary change with its "transformation" effort, the antecedents of this effort can be traced to several military reform movements that are decades old. Military thinkers, challenged by the record of Vietnam and the potential offered by technology development, sparked the debates and change initiatives that led to a new AirLand Battle doctrine, a new unified military establishment and staff organization, and more agile military forces equipped with state-of-the-art tools to achieve a battlefield advantage.

Andrew Marshall and the Military Technical Revolution

Many defense scholars would argue that today's military transformation process is actually the latest manifestation of a decades-old movement that began as a theoretical debate about a

"Revolution in Military Affairs." The genesis of RMA theory is usually traced back to Marshal Nickolay Ogarkov, a brilliant strategic thinker and head of the Soviet General Staff, who first wrote about a "Military Technical Revolution" (MTR) in the 1970s. Ogarkov believed that "history's linear evolution is occasionally interrupted by rapid discontinuities" and that a major change in warfare had already begun. He viewed some of the technological breakthroughs in U.S. conventional force capabilities—such as long-range strike—as indicators of a discontinuous shift, and feared breakthroughs such as this would allow the United States to fight and potentially win a theater-level conventional war in Europe.

Intrigued by Ogarkov's theory, Andrew Marshall, director of the Office of Net Assessment in the Office of the Secretary of Defense, began to look at whether certain technological innovations over the course of history gave a lopsided advantage to one combatant over another. He quickly concluded that it was not technology alone that provided a decisive advantage; rather, it was the ability of a military force to transform its operations and organizations to leverage what technology offered that provided the advantage. Thus, the more appropriate term to describe the changes that are under way is RMA, not MTR. Not to be confused with "revolutions" driven by societal and political change, RMAs are conceived and directed from *within* military institutions (and not without a good measure of institutional resistance). According to Marshall, RMAs usually "emerge over time from problem-solving directed at specific operational and tactical issues."[3]

---

[3] Examples of past RMAs are the changes in French military concepts and institutions in the 17th century under King Louis XIV and the combined arms tactics of World War I. For information on military revolutions and RMAs, see Knox, MacGregor, and Williamson Murray, *The Dynamics of Military Revolution*, Cambridge: Cambridge University Press, 2001, pp. 59-73.

Table 5.1
A Brief History of Recent Developments in the Revolution in Military Affairs

1970s	1980s	1990s	2000s
Talk of an MTR appears in Soviet writings (Marshal Ogarkov)	Office of the Secretary of Defense (OSD) Net Assessment Director Andrew Marshall begins investigating MTR and RMA concepts	AirLand battle, OODA [observe-orient-decide-act] loop, and joint warfighting concepts influence operations in the first Gulf War	RMA theory and concepts help shape the Quadrennial Defense Review and "Defense Transformation"
	Significant advances in computer technology	OSD Net Assessment director publishes seminal study on RMAs	New organizational and operational concepts build on technological innovations of the 1970s, 1980s, and 1990s
	Defense Advanced Research Projects Agency (DARPA) develops the Internet	Joint Staff, senior military schools study/debate topic; think tanks and academics join the fray	RMA concepts influence military operations in Afghanistan and Iraq
	Army and Air Force develop the AirLand Battle concept focused on theater-level warfighting	Body of scholarly literature developed; some ideas influence defense planning and programming	
	Military reform and Goldwater-Nichols debates under way		

Army historian Williamson Murray agrees that RMAs can be deliberately generated from within an institution. "The record of the past . . . suggests the existence—alongside and within the great military revolutions—of clusters of less all-embracing changes," he said. "These lesser transformations are best conceptualized as the revolutions in military affairs. . . . They do appear susceptible to human direction, and in fostering them, military institutions that are intellectually alert can gain significant advantage." Murray makes a distinction between, for example, the "military revolution" prompted by nuclear weapons and ballistic missile systems and the "RMAs" associated with precision reconnaissance and strike, stealth, and computerized command and control.[4]

Andrew Krepinevich, a military assistant on Andrew Marshall's staff in the early 1990s and current director for the OSD Center for Strategic and Budgetary Assessment, wrote a seminal piece in 1992 that described what he believed would be the characteristics of the upcoming RMA and the strategic management issues it would raise. He argued that what determined an RMA was the *recognition* that the character of conflict changed dramatically, usually in the aftermath of a conflict (like the Gulf War).[5] In the foreword to his document, Krepinevich describes how he met with Marshall during the early days of the Gulf War campaign to discuss whether they were witnessing a fundamental discontinuity in military operations. He concluded that the United States was "likely at the beginning" of such a period, and that this change would probably occur "over an extended period of time, perhaps 10 to 20 years."[6] In the introduction to his study, Krepinevich notes that the early thinking on the MTR, and later the RMA, was informed by the debate among many Department of Defense experts and by experts in the larger national security studies community that continues well over a decade later. In a one-on-one interview for this study, Krepinevich opined, however, that

---

[4] Murray, 2001, p. 12.

[5] Krepinevich, Andrew, *The Military-Technical Revolution: A Preliminary Assessment,* Department of Defense Office of Net Assessment, July 1992.

[6] Krepinevich, 1992, p. 32.

it is the new leadership in the Pentagon that provided the "critical mass" in moving the transformation process forward.[7]

Table 5.2
Notable Characteristics of a Revolution in Military Affairs

- Are rarely brought about by dominant players
- Bestow an enormous and immediate military advantage on the first nation to exploit them in combat
- Are often adopted and fully exploited first by someone other than the nation inventing the technology
- Are not always technology-driven
- Technology-driven RMAs are usually brought about by combinations of technologies, rather than individual technologies
- Do not necessarily involve new weapons
- Appear to have three components: technology, doctrine, and organization
- As many fail as are successful
- Often take a long time to come to fruition
- The military utility is frequently controversial and is in doubt up until the moment it is proven in battle
- Also occur in the business world
- Are the result of multiple innovations

SOURCE: Hundley, Richard O., *Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us About Transforming the U.S. Military?* Santa Monica: Calif.: RAND Corporation, MR-1029-DARPA, 1999, pp. 7-11.

The RMA that has emerged, or is emerging (depending on your point of view), is the progeny of numerous congruent activities, some of which were prompted by Andrew Marshall's initial inquiries, while others were independently developed. In addition to the contributions of Marshall's Office of Net Assessment, this report considers three other separate but pivotal transformational streams that fed the RMA over the past two decades. Through these multiple efforts, one can trace the development of new theory, strategy, doctrine, and innovation that provided the solid intellectual foundation for the latest round of transformation efforts. One of the most important contributions, it should be noted,

[7] Krepinevich, Andrew, director, Center for Strategic and Budgetary Assessment, interview with author, February 12, 2003.

came not from the top leadership in the Department of Defense, but from a retired Air Force colonel.

Military Theory, Operational Innovation, John Boyd, and the Reform Movement

While some observers regard Ogarkov and Marshall as the intellectual fathers of the current RMA, others see the performance of the U.S. military in Vietnam as the event that foreshadowed its birth. The less-than-satisfactory results of the Vietnam conflict left young military officers unhappy, demoralized, and eager for change, while many senior officers searched for explanations. Whereas Ogarkov and his theories provided an intellectual impetus for change, Vietnam provided a tangible one.

After Vietnam, the professional military "needed new ideas about war," argues Robert Coram in *Boyd: The Fighter Pilot Who Changed the Art of War.*[8] "They needed something they could hold in their hands and study far into the night, something they could debate and argue, something that had the power to galvanize them and the troops under them with new and powerful knowledge. In short, they needed a new military theory that would enable them to win wars," Coram wrote.

The unlikely developer of this new military theory, according to Coram, was an irascible Air Force colonel and fighter pilot named John Boyd. In 1975, Boyd retired from the U.S. Air Force and began to devote all of his time to studying military theory. Four areas drew most of his attention: general theories of war, the blitzkrieg, guerrilla warfare, and the use of deception by great commanders. After a year of intensive study, he wrote a paper in 1976 entitled "Destruction and Creation" and developed a briefing that summarized his new theory of warfare.

Boyd's paper was an exercise in learning theory[9] and attempted to describe the mental patterns that human beings use to shape, and be

---

[8] Coram, Robert, *Boyd: The Fighter Pilot Who Changed the Art of War,* Boston: Little Brown and Company, 2002, p. 318.

9 Interestingly, Boyd's "learning theory" of rapidly adapting to changes in the combat environment can be applied to not only the individual seeking to work inside an enemy's decision cycle but to organizations as well. Much of the change-management literature now

shaped by, their environment. Using the improbable combination of Godel's Proof, Heisenberg's Indeterminacy Principle, and the Second Law of Thermodynamics to prove his point, Boyd argued that the uncertainty and disorder generated by an inward-oriented system in its attempts to match up its concepts with reality only increase the *mismatch.* The only solution to this paradox, Boyd argued, is for a system to go through the process of first destroying the established thought patterns of the participants of that system, then reforming them, and then repeating the process of destruction and restructuring until a new concept is developed that begins to match up with reality.

Understanding this dialectic "engine," Boyd said, is the key to independent action on the battlefield. It would allow individuals to continuously update their conception of, and thus cope with, their environment. If an individual can be trained to speed up this process in combat, Boyd argued, he could disorient an adversary by reshaping the environment faster than an enemy can react to the reshaped environment. Boyd summarized these ideas in a briefing entitled "Patterns of Conflict" and crystallized them in a concept he called the "OODA-loop," or the process of observe-orient-decide-act.[10]

In "Patterns of Conflict," Boyd laid out a framework for assessing different technological approaches and promoted the application of scientific and engineering knowledge to human behavior in war. He generated a group of loyal followers, later known as the "Reformers," who believed that the American military misapplied its technological advantages. This group of well-placed Pentagon insiders built alliances with the media and with Congress, specifically with the Congressional Military Reform Caucus, to press for change.[11]

---

focuses on the ability to rapidly adapt to the external environment by observing patterns of behavior.

[10] A fuller explanation of Boyd's OODA-loop can be found at the Defense and the National Interest Web site (www.d-n-i.net/second_level/boyd_military.htm).

[11] For further discussion on the misapplication of technology, see Fallows, James, "The Muscle-Bound Superpower," *Atlantic Monthly,* October 2, 1979 and Fallows, James, "National Defense", *Commentary,* Vol. 72, No. 2, August 1981.

Because of this small coalition, who firmly believed in Boyd's theories, many of the concepts Boyd developed over a quarter of a century ago were brought to bear during the Gulf War in 1991 and Operation Iraqi Freedom in 2003. His acolytes claim that he is the greatest military theoretician since Sun Tzu. While it is not the purpose of this report to argue that point, it is worth noting that many believe Boyd's new theory of maneuver warfare consequently led to the development of new military strategy and doctrine. It also led to innovations in operations and tactics that would enable the U.S. military to undertake a new approach to fighting wars.

AirLand Battle Strategy and Doctrine

Throughout the late 1970s and 1980s, the various military services analyzed and debated Boyd's theories about maneuver warfare. Among the people Boyd influenced was then-Army Lieutenant Colonel Huba Wass de Czege.[12] Wass de Czege was one of a team of officers who worked for General Donn Starry, then head of the Army's Training and Doctrine Command, who oversaw development of a new doctrine called AirLand Battle, which incorporated some of Boyd's theories on maneuver warfare.

The U.S. Army, like most of the military services, did some serious soul-searching in the late 1970s. By nearly all accounts, it did not perform well in Vietnam, at least in terms of achieving operational and strategic objectives. Its 1976 attempt at writing a new doctrine, entitled "Active Defense," was not well received by either commanders or troops in the field. After a series of international events, ranging from the Soviet invasion of Afghanistan to the establishment of a Communist regime in Nicaragua, President Jimmy Carter devised a new U.S. National Strategy that once again emphasized the Soviet Union as the primary threat. General Edward C. Meyer, then Army Chief of Staff, in turn developed a new strategy for the U.S. Army that reflected this view and emphasized offensive operations at the tactical level in Europe.[13]

---

[12] Coram, 2002, pp. 370-371.

[13] D'Amato, First Lieutenant Martin J., "Vigilant Warrior: General Donn A. Starry's AirLand Battle and How it Changed the Army," *Armor,* May-June 2000, p. 18.

In 1977, the Army also began to rewrite its doctrine to support the new strategy and its emphasis on the Soviet Union. "The Soviets had changed their doctrine, so we needed to change ours," Starry said in an interview for this study in January 2003.[14] "They believed they needed to fight and win a conventional war. We believed we could only last ten days, then needed the nuclear option." Starry was convinced NATO would never agree to nuclear release, and believed the Army must figure out a way to win the first battle conventionally.

Starry's view was that the Army had to rethink the way it fought, combining a new strategy and opportunities presented by new technology—particularly technology that would allow them to attack the second echelon of Soviet forces. In the interview, Starry talked about walking the battlefield after the Yom Kippur war, while thinking about how the successful Israeli Army handled the second-echelon problem. He said that as the former V Corps Commander in Europe, he was in a unique position to be the "architect" of change for the Army's transformation in the late 1980s and early 1990s. The architect, he said, must be someone at the operational level who has actually "walked the battlefield and led the troops," because the architect determines what needs to be changed and helps to write the new doctrine. As just such an architect, Starry wrote a concept paper that later appeared in *Military Review* under the title "Extending the Battlefield."[15] Starry makes a point of noting that the concept paper took eight years to write, and the new doctrine another year. The development of revolutionary new concepts does not happen overnight, he stated emphatically.

Starry also successfully undertook the difficult task of changing the culture and behavior of the Army. He believed that this would be the most difficult aspect of implementing the new doctrine. Before writing AirLand Battle doctrine, Starry talked to the troops on the ground in Europe. He asked how they were going to fight the battle and saw how unhappy they were with the current doctrine. He gave them a draft of his

---

[14] Starry, General Donn, U.S. Army (ret.), interview with author, January 22, 2003.

[15] Starry, General Donn A., "Extending the Battlefield," *Military Review,* March 1981.

ideas and constantly asked for feedback. He was the catalyst, he said, but the troops convinced themselves that (a) it was a good idea and it would work, and (b) it was their idea. He revised his briefing based on their input and estimates that he presented his briefing on "Extending the Battlefield" a thousand times before publishing it in *Military Review.*

Starry sees one other major reason for the success of AirLand Battle doctrine—he recognized that TRADOC (the Army's Training and Doctrine Command) was not the place to write doctrine. He believed that for doctrine to take hold, the people who *teach* the doctrine should *write* the doctrine. Starry noted that the Eisenhowers and Bradleys of World War II fame went to Ft. Leavenworth for two years to study operational concepts. Starry was instrumental in reforming the Army's military school system so that the school system could both write new doctrine and teach the Army how to fight with it.

The AirLand Battle doctrine that Starry helped to develop proposed using long-range strikes and electronic warfare to slow and confuse the enemy in its rear echelons. Like Boyd's theories, Airland Battle incorporated the German concept of *Auftragstaktik* to allow subordinate leaders to change the mission (within the commander's intent) without permission, a concept that is key to the Army's maneuver warfare doctrine today.[16]

A Center for Army Lessons Learned report discusses the "Starry-Wass de Czege Paradigm" for affecting change in an Army. It examines eight requirements for encouraging "clear focused intellectual activity in the matter of any change."[17] Seven of these requirements—architect of the future, common leadership culture, proponency, consensus building, leadership continuity, top-level support, and testing—are ascribed to Starry, while the eighth requirement—theory—is ascribed to Wass de Czege. According to the report, these "constants" for affecting change could "serve as a prism for understanding and evaluating post-1973

---

[16] D'Amato, 2000, p. 20.

[17] Morris, Rodler F., Scott W. Lackey, George J. Mordica II, and J. Patrick Hughes, *Initial Impressions Report: Changing the Army*, Center for Army Lessons Learned, forthcoming.

change in the Army" and be used as a descriptive tool and guide to action.

Both Boyd and Starry recognized that a military transformation required going back to first principles and challenging some deeply held convictions as well as changing the military's doctrine and culture. Both led a coalition for change composed of both outsiders (primarily from Congress and the media) and Pentagon insiders. Both welcomed debate and alternative views. Both ignored the traditional procedural route to change, knowing that they would hit an institutional brick wall. Both sought and found support from the men and women in the field who would prove to be the most important advocates for change.

Goldwater-Nichols Legislation

No revolution is complete until new operational and organizational concepts catch up with theory, strategy, doctrine, and technology. And no element of change is more emotionally charged and difficult to achieve than rearranging the human relationships in a mature institution. The military, with its rich cultural traditions, is unusually resistant to organizational change.

Rarely was this more evident than during the five years preceding the 1986 enactment of the Goldwater-Nichols Act. At the time, Goldwater-Nichols was by all accounts the most comprehensive organizational reform of the Department of Defense undertaken since the National Security Act of 1947. Its far-reaching legislation touched the Joint Chiefs of Staff (JCS), the military services, and the Unified Commands, and the civilian side of the Department of Defense. Goldwater-Nichols is the story of transformational change imposed largely from the outside and the lessons, both positive and negative, to be learned from such an approach.

The story begins in the late 1970s and early 1980s when powerful Army, Navy, Air Force, and Marine Corps officials and organizations dominated the Pentagon. According to James R. Locher III, at the time a staffer on the Senate Armed Services Committee, this dominance by the services was a legacy of the National Security Act of 1947 that superimposed a "National Military Establishment" over the War and Navy

Departments.[18] The 1947 Act created a weak secretary of defense with a small civilian staff and a big task—integrating the work of the military departments. The 1947 act gave legal standing to the Joint Chiefs of Staff (JCS) created during World War II but provided no chairman. It also left the service secretaries in place as powerful cabinet members and members of the National Security Council.[19]

According to Locher, the net result was a military effort still largely uncoordinated. The commands were weak and incapable of adequately waging multiservice warfare. Advice from the JCS was poor. Some viewed the military's record in Vietnam, Lebanon, and Grenada, and incidents such as the Pueblo and the Iranian hostage rescue attempt, as the direct result of the inability to implement the concept of a unified command. In addition, the charges of waste, fraud, abuse, and acquisition mismanagement leveled at the Department of Defense by military reformers were largely attributed to a weak secretary of defense.

In February 1982, this state of affairs took an unexpected turn when General David C. Jones of the U.S. Air Force, then chairman of the JCS, testified before a closed-door session of the House Armed Services Committee that reform of the JCS system was badly needed. "Although the history books glorify our military accomplishments, a closer examination reveals a disconcerting pattern: unpreparedness at the start of a war; initial failures; reorganizing while fighting; cranking up our industrial base; and ultimately prevailing by wearing down the enemy—by being bigger, not smarter," Jones told the committee.[20]

Jones knew that both the civilian and military bureaucracies would unite against him, and so took the unusual step (for a uniformed military officer) of seeking the support of the Congress, the media, and the retired military community. Locher said that a push from a respected insider like Jones, along with support from a handful of other senior

---

[18] Locher, James R. III, *Victory on the Potomac,* College Station, Tex.: Texas A&M University Press, 2002, Chapter 1.

[19] Locher III, James R., "Has It Worked? The Goldwater-Nichols Reorganization Act," *Naval War College Review,* Autumn 2001.

[20] Locher, 2002, Chapter 2.

officers such as Generals Meyer and Starry, were critical to eventual passage of the legislation,[21] as were the four powerful committee chairmen—Senators Barry Goldwater and Sam Nunn and Representatives Bill Nichols and Les Aspin—who were the "champions" for reform in Congress. The Packard Commission, led by the late Hewlett-Packard co-founder and CEO David Packard, focused on acquisition issues and brought additional clout to the "coalition for change." And while Jones was the initial "architect" of JCS reform, that role was picked up and expanded by committee staff (to include Locher) and others.

The legislation that was eventually passed, by most accounts, helped to improve the military's ability to operate effectively as a joint warfighting force. It strengthened the operational warfighting commands and improved officer education. The result is improved military performance in strategy making and contingency planning, as well as in both operations and peacetime activities. Combat successes in Panama, Afghanistan, and Iraq are often attributed to more-unified American military forces.

The Goldwater-Nichols Act also strengthened the authority of the secretary of defense and the chairman of the JCS. It made clear the responsibilities of the military service secretaries in support of the secretary of defense. There were, however, false starts and unintended consequences.[22] For example, some observers believe that the quality of the Joint Staff's work now overshadows that of the Office of the Secretary of Defense (although, according to former Secretary of Defense

---

[21] Locher, 2002, Foreword.

[22] One of these unintended consequences was the impact Goldwater-Nichols had on U.S. intelligence. In a paper prepared for Harvard University, former ADCI for Administration James M. Simon, Jr. noted that, among other things, Goldwater-Nichols encouraged the commanders-in-chief (then called CINCs, now Combatant Commanders) to become increasingly reliant on national intelligence at the expense of other intelligence consumers; deprived the Defense Intelligence Agency of any opportunity to centralize and help manage defense intelligence efforts; compromised the contributions of the CIA, which no longer devotes serious resources to military analysis, and eroded the role of the DCI in setting priorities and determining how to satisfy requirements. Simon, James M. Jr., "Crucified on a Cross of Goldwater-Nichols," incidental paper, Cambridge, Mass.: Center for Information Policy Research, Harvard University, July 2001.

William Cohen, "It is the civilians, not the soldiers who have abdicated their responsibilities.").[23] Neither the development of joint doctrine nor joint training has yet to fully mature. Still others, like former Navy secretary and Goldwater-Nichols foe John Lehman, continue to insist the legislation was a mistake. Lehman believes it contributed to a "military-civilian cultural gap" and "limited not only the scope of military advice available to the political leadership, but also the policy- and priority-setting roles of the service chiefs and civilian service secretaries."[24]

In hindsight, Locher, one of the original architects of the legislation, believes that the legislation does not live up to all its expectations. Locher said he would give an A to the improvements in the "quality of military advice to the national command authority" and to "operational effectiveness" but would give a D to other attempted reforms, such as a "more efficient use of resources" and "defense management and administration."

The process that preceded enactment of the Goldwater-Nichols Act supports the argument that transformational change can be accomplished, even when there is strong institutional resistance (most of the Pentagon fought it). This reform "from the outside" approach does have the benefit of being able to overcome even the staunchest protectors of the status quo. It tackles prerogatives that insiders hold most dear—thus leading to more substantial reform than insiders would ever agree to take on. However, it demonstrates that without the cooperation of the institution itself, the fight is likely to be long and difficult, and the successes will be mixed.

It is difficult to say how much more successful the Goldwater-Nichols Act might have been if there was a greater attempt at achieving consensus within the Pentagon or if then Secretary of Defense Caspar Weinberger championed it. It is also difficult to assess how much the enactment of Goldwater-Nichols was helped by other significant changes

---

[23] Locher, 2002, p. 439.

[24] Lehman, John, and Harvey Sicherman, in "America the Vulnerable," *America the Vulnerable,* Philadelphia: Foreign Policy Research Institute, 2002, p. 6.

under way—led by Marshall, Boyd, Starry, and others—in the areas of military theory, technology, strategy, doctrine, and operations. What can be said is that when Secretary of Defense Rumsfeld arrived at the Pentagon in early 2001, many of the seeds of transformation were already sown.

Rumsfeld and Defense Transformation

Preceding Rumsfeld's arrival at the Pentagon, several decades of argument about the RMA had yielded new military technologies such as microelectronic sensors, stealth aircraft, and precision-guided munitions. The military reformers and the professional military institutions had contributed many new ideas on theory, strategy, doctrine, and tactics as well as acquisition reform. Goldwater-Nichols changed the way the military was organized to fight and win wars and also established a more effective JCS. But according to historian Colin Grey, "Great RMAs are made by people with powerful and generally quite specifically political motives, even if the process of innovation includes a lengthy period of gestation, experiment, and evaluation in peacetime."[25] In other words, it would take someone like a Donald Rumsfeld to bring about a "great" RMA.

Rumsfeld found upon arriving at the Pentagon, however, that despite these previous efforts at systemic change, the military services were still very powerful, still resistant to Goldwater-Nichols and other recommendations, and still wedded to many traditional operational and organizational concepts and systems. Although Rumsfeld is an experienced and politically powerful leader, his attempts to transform the U.S. military met very stiff resistance (during his first year in office, critics predicted that he would be the first member to leave the cabinet). This underscores the argument that while strong leadership is an essential ingredient in bringing about transformational change, it is not the only thing that will win the day.

---

[25] Grey, Colin S., *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History,* London, UK: Frank Cass Publishers, 2002, p. 271.

Without the dedication of a handful of insiders—Generals Starry, Wass de Czege, and Jones to name a few, bringing about revolutionary change within the Department of Defense and the military services would have been far more difficult. Insiders alone, however, could never have brought about the magnitude of change that has been accomplished to date. Outsiders served as provocateurs, while strong leaders infused a sense of urgency and a mandate for making the recommended changes happen. All contributed, in their way, to the Revolution in Military Affairs.

Summary

There are several lessons to be learned from the early RMA debate, the writing of AirLand Battle doctrine, the arguments of the military reformers, and Goldwater-Nichols--four separate streams of thought and innovation that are continuing to feed today's efforts at defense transformation.

The first lesson is that serious strategic thinking *before* a mature institution attempts to fundamentally change is absolutely essential. Often, this is neither a coherent nor collegial process. The RMA debate was highly contentious, with seven or eight competing schools of thought, but the end result was a richness of new ideas, with the best ones emerging from the crucible. Any institution serious about transformation must create the opportunity for creative tension between radical new ideas and the status quo.

A second lesson is that accomplishing the revolution is neither a quick nor a painless process. Revolutions in large institutions do not happen overnight, as the structure, systems, practices, and culture of bureaucracies tend to impede change rather than facilitate it. It takes time, trial, and error for large institutions to digest emerging technology and formulate new organizational and operational concepts. Core competencies are challenged and new ones are advanced—and those who are directly affected believe themselves to be either winners or losers and dig in their heels accordingly. It takes time to build consensus both inside and outside an institution. It takes time to train the leadership in the new ways of behavior, and for them in turn to

teach the next generations of leaders. Development of a doctrine that is shared across organizational boundaries is essential to changing behavior. The challenge is to generate a sense of urgency to get started, and accept that it may take a while to get it right.

Third, the military learned that it is essential to create a culture of continuous reassessment and self-improvement. The challenge for U.S. intelligence will be to speed up the cycle that today would take many years to accomplish. The process of transformation, much like John Boyd's OODA-loop, needs to become part of the marrow of the organization—an on-going, continuous process that will keep it moving faster than any adversary can keep up.

Fourth, and perhaps most important, as the transformation process unfolds with all of its twists and turns, someone always needs to keep his or her head above the fray and focused on the ultimate objective or objectives over time. This person can be an Andy Marshall, a Donn Starry, or a Jim Locher (the official title is unimportant), but this person needs to be around long enough to maintain focus and continuity throughout the most difficult moments of the change effort.

Military reform and change efforts did not proceed from a highly regimented and structured process within the Pentagon. Instead, they evolved from a tradition of individual action, intellectual rigor, and military scholarship embedded in the military system. To some extent, these forces of change naturally converged, but Pentagon leaders and other advocates amplified that convergence to bring about the improved performance displayed in integrated military operations in Iraq in early 2003. This ability to harness decades of transformational change planning and then to achieve an effective military advantage through implementation of that planning is the end game in the RMA model.

In sum, the U.S. military's transformation can inform the Intelligence Community's consideration of the nature of revolutionary change. The creative and often chaotic process of reevaluating first principles and foundational ideas often ignites the spark of transformation. The change process is also iterative and demands collaboration, particularly because reform movements and change initiatives tend to leverage one another over time.

Patience is also required. Work must be done to build coalitions, educate leaders, and draw insights from those who will be required to execute the changes. No revolution is complete until new operational and organizational concepts catch up with theory, strategy, doctrine, and technology. And, even if all of the constituent elements of a transformational change model are brought together effectively, changing the culture remains the hardest target. No element of change is more emotionally charged and difficult to achieve than rearranging the human relationships in a mature institution.

Today's revolutionary blueprint will become tomorrow's prison if the change process is not institutionalized so that the organization can continuously adapt to ever-increasing rates of environmental change. Part of this challenge is to have someone responsible for staying focused on the ultimate long-term objective amidst the creative chaos of the short term. The Pentagon's experience in managing transformational change for several decades helps to point the way for those who would take on similar challenges in the Intelligence Community.

CASE STUDY: DYNAMIC BUSINESS TRANSFORMATION

During much of the 20th century, large industrial-age companies dominated the corporate American landscape. For many years, those companies approached change not unlike the way bureaucracies approached change. The same employees, with the same skill sets, often worked for the same company for 30 years. They defined themselves by their core products and loyal customers. Their business models focused on either improving those core products or selling loyal customers new things. It was not until the last decade or two that corporate America realized that this incremental approach to change would no longer work. The old approach began to threaten the existence of even the most well-run companies, especially industry leaders who were lulled to complacency by their successful past track records.

If 20th-century corporate America was disrupted by fluctuations in prosperity, its 21st-century counterpart will have to deal with the even more destabilizing effects of the information age. Just as in the realm of military affairs, this collision with accelerated reality had an

aftermath: The focus on core products and loyal customers gave way to a focus on adaptation and speed. The competition between capitalism and various collective economic models is augmented by an astounding level of complexity—in mergers and acquisitions, anti-trust suits, new corporate regulations, economic fluctuations, unions, global market competition, and rapid technological changes.

This changed corporate landscape elevated "change" itself, and the need for adaptation to it, to the status of a central organizing principle for the modern business organization. And this reordering of the corporate universe has stimulated everyone, not just business leaders or analysts, to understand how change has changed and how, in the business sense at least, profitability is now all about staying ahead. Although government operations lack that specific bottom-line orientation, there are still lessons to be learned from the after-effects of the collision between the world of commerce and the apparently unstoppable force of rapid change.

One such lesson is that the dynamic and fluid business environment has overwhelmed established corporate programs, procedures, and strategies. Companies that remain focused on "core" products and services are at an extreme risk of going the way of the "buggy whip" manufacturers in the wake of Henry Ford. Those that place their emphasis on customers and try to flow with the market are better off, but the trend line is clearly to build change management into the very structure of the organization. This trend is consistent with the approach of military thinkers in cultivating an RMA and should inform efforts on behalf of intelligence transformation.

A growing number of change theorists believe that it is not only possible to bring about revolutionary change, it is imperative that every large organization that intends to survive find a way to do so. According to Daryl R. Conner, a researcher who specializes in observing organizational change, in the early 1970s some 60 percent of companies believed they would face no significant change in the future, while

35 percent anticipated sporadic, incremental change. Only 5 percent anticipated what Conner describes as continuous, overlapping change.[26]

By 2000, this view vastly changed. Only 1 percent of companies now believe that there will be no significant change in the future, 24 percent anticipate sporadic, incremental change, and nearly 75 percent believe that they need to prepare for "an era of unending transition." Most organizations now believe that these changes will be disruptive, extremely challenging to absorb, and require sophisticated planning and sustained effort. "Learning how to view and manage change in a new way is possibly the most important change that you will ever make," Conner advised today's corporate executives. Microsoft's Bill Gates agrees that the whole organization must be poised to react rapidly to change: "The goal is to make business reflex nearly instantaneous and to make strategic thought an ongoing, iterative process—not something done every 12 to 18 months, separate from the daily flow of business."[27]

Over the past two decades, many approaches to change management have been tried, from downsizing to outsourcing to balanced scorecards and Total Quality Management, economic value analysis, benchmarking, and reengineering. Most of these processes, however, do not transform an organization but simply focus on how to do the things that they are doing better. Sometimes, companies are doing all the right things but cannot separate themselves from old realities. When that occurs—as was the case for industry giants such as Ford, IBM, and Kodak—even a well-run industry leader may quickly find itself fighting for its survival.

In much the same way that the military must be constantly aware of changes in the security environment, industry must maintain a constant awareness of the external business environment. It is not unusual for corporate executives to attempt to diagnose trends and their implications as far out as 50 years. According to several change theorists, the most highly sought skill in a CEO today is the ability to

---

[26] Conner, Daryl R., *Managing at the Speed of Change: How Resilient Managers Succeed and Prosper Where Others Fail,* New York: Villard Books, 1992, p. 44.

[27] Gates, Bill, *Business at the Speed of Thought: Succeeding in the Digital Economy,* New York: Warner Books, Inc., 1999, p. 408.

lead a workforce through times of change, rather than long-term experience in the company.[28]

The same competing schools of thought on how to manage military transformations seem to apply to corporate transformations as well. There is one school of thought, for example, that believes outside consultants and strategists must be brought in to bring about successful corporate transitions. The "great man" theory is alive in industry as well (a new CEO is often brought in to lead a transformation effort). And, as in the military, these are important, but insufficient ingredients—successful business transformations require more than that.

To test the hypothesis that certain variables are essential to any successful transformation effort, it is useful to examine those elements that served as the intellectual underpinning of the military's transformation—theory, strategy, and doctrine—and innovation in the areas of technology, operations, and organizations. Although the terminology in the corporate world is different, research shows that the same elements of successful transformation appear in the private sector as well as in the public one.

Business Theory

Much like military theory, new economic theories, market theories, and business theories have been advanced in response to the changing external environment. Peter Drucker, one of the gurus of organizational change, argues that every organization has a "theory of the business" whether they are a business or not.[29] Organizations begin to recognize the need for transformational change when their theory of the business no longer works. The case of IBM is illustrative. When the personal computer first appeared, every computer producer believed it would fail because the theory regarding computers was that individuals had no use for them. IBM embraced the PC as the new reality, changed its business model, and a short time later became the world leader in PCs. However, when it came time to challenge the underlying assumption that the

[28] See Drucker, Peter, *Managing in a Time of Great Change*, New York: Truman Talley Books/Dutton, 1999; Conner, 1992.

[29] Drucker, 1999, p. 22.

computer industry is hardware driven, IBM did not change its theory of the business and lost its leadership position.

Once acknowledged, the theory of the business becomes "culture." As an organization becomes successful, it takes its theory for granted, becoming less and less conscious of it. The theory of the business has to constantly be tested—it is a hypothesis about things in constant flux. Built into the theory of the business must be the ability of the organization to change itself, says Drucker, because every theory of the business eventually becomes obsolete and then invalid. Every organization, he believes, needs to build in a systematic process for monitoring and testing the theory of the business.

Business Strategy

Gary Hamel is a professor at the London Business School, a frequent contributor to the *Harvard Business Review,* and a man *The Economist* calls "the world's reigning strategy guru." Hamel believes that developing a revolutionary new business strategy is key to "capturing more than your fair share of tomorrow's opportunities."[30] The trick, he says, is to actually come up with one because developing a new strategy is difficult.

Hamel firmly rejects the notion that a new strategy is the product of strategic planning. Strategies that result from an annual planning process, he argues, are "procedural, reductionist, extrapolative, elitist, and easy." The planning process, he says, narrows the scope of discovery, the breadth of involvement, and the amount of intellectual effort expended, and the goal is something far short of revolution. "The assumption that strategy is easy says more about the inadequacies of our planning processes than the challenge of creating industry revolution," he says. "Giving planners responsibility for creating strategy is like asking a bricklayer to create Michelangelo's Pieta."[31]

So how does one generate a radical new business strategy? Does one seek the assistance of outside consultants or establish an on-staff

---

[30] Hamel, Gary, *Leading the Revolution,* Boston: Harvard Business School Press, 2000, pp. 20-21.

[31] Hamel, 2000, p. 20.

corporate guru? Hamel believes these people "know a new strategy when they see one," but have no ideas on how to generate one. How about the "strong leader" theory—that you need a CEO that is a genius or a visionary? "That's rubbish," says Hamel. "How often does the revolution start with the monarchy?" He adds, "Today's visionary is often tomorrow's intellectual straitjacket. They don't stay visionaries forever. More times than not, a fading visionary who is also CEO or chairman unwittingly strangles a company's capacity for radical innovation. That is why visionary companies seldom live beyond their first strategy."[32]

Instead, it is an organization's "activists," he believes, that come up with innovative strategies. People like Nelson Mandela, Vaclev Havel, Mahatma Gandhi, and Martin Luther King Jr. all disrupted history, with passion, not power, Hamel points out. "The age of revolution requires not diligent soldiers, throwing themselves at the enemy en masse, but guerilla fighters, highly motivated, and mostly autonomous. . . . In the new industrial order, the battle is not democracy versus totalitarianism, or globalism versus tribalism, it is innovation versus precedent."[33]

Hamel believes that new business strategies are "always, always the product of lucky foresight . . . some cocktail of happenstance, desire, curiosity, ambition, and need." How do you increase the probability that radically new strategies emerge in your organization? By creating an environment that encourages leaps of human imagination. Ideas with merit, he says, attract talent and capital the way a flower captures the attention of a honeybee. "Grey-haired incumbents and acne-faced newcomers" must both embrace a "New Innovation Agenda," that builds on, among other things, both continuous improvement *and* nonlinear innovation, product/process innovation *and* business concept innovation, serendipity *and* capability, visionaries *and* activists. "Never forget," Hamel says, "that good companies gone bad are simply companies that for too long denied the reality of strategy decay."[34]

---

[32] Hamel, 2000, pp. 21-24.
[33] Hamel, 2000, pp. 25-26.
[34] Hamel, 2000, p. 28.

Business Doctrine

It is unlikely that the word "doctrine" will ever appear in the annals of corporate change literature. But if one defines doctrine as the fundamental principles by which individual elements guide their actions in support of an institution's objectives, then doctrine is the glue that binds even corporate transformation efforts together. Many corporations now invest significantly in developing corporate business principles and teaching them to their employees.

The Boeing Company is a case in point. Boeing, like many other corporate giants, realized that one way to bind its far-flung corporate empire was to invest in a leadership school. This school focuses on teaching employees at all levels of the corporate structure the principles that govern corporate behavior and allow it to carry out its corporate strategy.[35]

Much like the professional military leadership schools, a great deal of time and effort is spent on inculcating Boeing executives with new business principles. For example, if an overarching strategy is to provide "full-service, balanced, and integrated aerospace solutions across all businesses," the leadership school works to teach executives what the implications of that strategy are to those who work on commercial airplanes or military aircraft or space systems. It describes what that means in terms of teamwork across organizations, work structures, global presence, and customer support.

Boeing's top executives apparently believe that developing a corporate strategy and the business principles that support it, then ensuring that every member of the leadership team hears and internalizes them, are among the most important things they do. Jeanie Daniel Duck, senior vice president of The Boston Consulting Group, notes the importance of shared doctrine/principles to align the leadership of a company. Lack of alignment among leaders is the most common cause of failure for major change efforts, she says. When leaders are not aligned, factions and subgroups break out, and the top executive has to expend enormous energy playing peacemaker. The longer this lack of

---

[35] The author had an opportunity to attend and observe the Boeing Executive Leadership course in August 2002.

alignment is allowed to continue, the less likely the change initiative is to succeed, Duck says.[36]

New management principles are a key theme throughout the Boeing Executive Program. Linear management structures are now considered serious impediments to innovation, risk-taking, and optimal performance. Instructors emphasize the need to attract, hire, and keep highly qualified people. Several program modules focus on attracting talent, keeping people motivated, listening to subordinates, and moving people both laterally and vertically within the company.[37]

Gary Hamel believes that to embrace the new innovation agenda, a company needs to challenge every management principle it inherited from the "age of progress," such as "top management is responsible for setting strategy," "being revolutionary is high risk," and "our real problem is execution." New doctrine revises this thinking, and large organizations send this message throughout all their levels by teaching their leadership team what is expected of it, having the next level of leadership model the new behaviors in its own suborganizations, and then holding those groups accountable for the results.[38]

Technological Innovation

At one time, it was believed that revolutionary change was predicated by the discovery of a radically new technology. Even in the business world this is not necessarily so. Although development of a new technology is often the precursor to a new market, many companies have found that figuring out a new application for an existing technology can be just as important.

Upstart or new companies are often created around a new technology. For existing companies, however, reforming all of their business processes and structures around a new technology that directly competes

---

[36] Duck, Jeanie Daniel, *The Change Monster,* New York: Crown Business, Random House Publishing, 2001. See the chapter on "Alignment," pp. 94-97.

[37] An excellent text used in the Boeing Executive Leadership Program is *Love 'em or Lose 'em; Getting Good People to Stay* by Beverly Kaye and Sharon Jordan-Evans (1999). It outlines 26 strategies for keeping talented employees.

[38] Hamel, 2000, pp. 220-222.

with an established product line is far more problematic. Examining how a mature, established company adapts to a new "disruptive" technology, says Clayton Christensen in *The Innovator's Dilemma,* can be instructive to bureaucracies interested in transformational change.[39]

Often, a mature company will chose to focus on "sustaining" technologies, that is, technologies that will improve the products they already make. This approach works well, says Christensen, if the company is trying to satisfy existing customers who are not ready to adapt to a new technology. However, if the company wants to attract new customers, or if it has existing customers who are ready to move on to the new technology, then the company has no choice but to adapt to the new technology or lose market share.[40]

There are many reasons why only a few successful companies manage to adapt to new technologies repeatedly. Industry leaders (like dominant militaries) rarely come up with "breakthrough" ideas because they have little incentive to innovate and challenge their own core competencies. Also, Christensen says, loyal customers hold leading firms captive, enabling attacking entrant firms to topple the incumbent industry each time a disruptive technology emerges. Another reason for the failure of some companies to adapt to technological change is that the pace that markets demand is different from the progress offered by technology. Moreover, resource allocation decisions usually rest in the hands of staff locked into the mainstream value network—i.e., the people who make the investment decisions are usually wedded to the status quo. The only way out, Chistensen says, is for a company to establish an atmosphere that is conducive to creativity and risk-taking.[41]

"Creativeness in industry has never been unimportant, but it has never been as important as it is now," says Antony Jay in *Management and Machiavelli*.[42] If you look back on a number of creative movements, says

---

[39] Christensen, Clayton, *Innovator's Dilemma: When New Technologies Cause Great Firms to Fall,* Boston: Harvard Business School Press, 1997, pp. 132-134 and 199-202.

[40] Christensen, 1997, pp. 4 and 24.

[41] Christensen, pp. 54-55.

[42] Jay, Antony, *Management and Machiavelli: Discovering a New Science of Management in the Timeless Principles of Statecraft,* Amsterdam: Pfeiffer & Company, 1994, p. 89.

Jay, there is one pattern that seems to repeat itself—the pattern of a leader who is himself a highly creative person working with a small group of creative individuals surrounding him.

Operational Innovation

Microsoft has been an industry leader in taking existing information technology and developing innovative new ways to use it. In *Business at the Speed of Thought,* Bill Gates says that digital information technology will enable process breakthroughs that are impossible with paper systems today. According to Gates, "If the 1980s were about quality, and the 1990s were about reengineering, the 2000s will be about velocity." He refers not only to investing in things that will speed up processes, but about how quickly the nature of the business will change.

Even in the business world, too often companies use new technology to update their existing operations. Many executives and managers believe that finding a new technology and having a clear plan is all that is required for transformation, and that operational changes will somehow occur. Transformational change, companies have found, requires changing workforce mindsets and work practices. It exhausts people to rethink their daily work and change their ways of operating. "People long for an excuse to quit the hard path of transformation," says Duck.[43]

The early work of management theorists such as W. Edwards Deming and Joseph M. Juran focused on improving work practices. For many companies during the 1980s, it took them a decade or more to grasp and internalize "quality" as an operational capability. It will take companies at least that long, says Hamel, to grasp and internalize "continuous concept innovation" as an operational capability. This means that the focus of their business will no longer be on improving business operations, but on completely changing them even as they are being perfected.[44]

---

[43] Duck, 2001, p. 30.

[44] Hamel, 2000, Chapter 9.

Organizational Adaptation and "People Are the Most Important Thing"

Few things evoke a greater emotional response than when personal relationships are threatened with change. When faced with the prospect of change, individuals are not focused on "What is our new business strategy?" and "How can I apply this new technology?" but on questions such as, "Who will be my new boss? How will my performance be measured? Will my skill set still apply? What are my chances of success?"[45] A reluctance to address these questions head-on is where most transformations break down in government, as well as in the corporate world.

Two organizational challenges face would-be corporate revolutionaries. First, there are the structural changes necessary to make better use of innovative technology and to change a company's business processes. Many large corporations are the end product of a series of mergers, sometimes of many small companies that have nothing in common (a loose confederation that seems surprisingly similar to the Intelligence Community). The workforce is often far flung. Some people telecommute, others work as consultants, and still others are temporary workers. As a result, many companies are modeling themselves after "complex adaptive systems" that cluster around certain tasks, and then reform with different players around new tasks. The second challenge is to help the workforce adjust to the process of continuous change. Jeanne Daniel Duck says that for a change initiative to succeed, the emotional and behavioral aspects of employees must be addressed as thoroughly as the operational issues. If managed correctly, Duck says, "Change can be exhilarating and bring about the best work of a lifetime." If it is not, it can be filled with "tension and anxiety, alienation and resistance." People in the workplace feel most distressed, she adds, as the result of three things: high demand, high visibility, and concern for competence. With a major change, all three things are in play.[46]

Duck says that exceptional leaders of change realize that their most important legacy to an organization is in teaching the organization how to perpetually change and adapt, and helping it muster the will to

---

[45] Drucker, 1999, Chapter 7.

[46] Duck, 2001, p. 273.

do so. Every business quarter, good leaders stop to reflect on the morale, pace, and spirit of their organizations. Often, people who are asked to participate in organizational change will agree with the mission, the strategies, and the tactics of the change, but will balk when the moment of truth arrives. Many individuals do not know how strong their emotional resistance is to change until that resistance is tested.[47]

Organizations do not change until the beliefs and behaviors of the people within it change. Conner, Duck, and others observe that people experience a common pattern when they go through major change. Organizations, like individuals, have a speed of change at which they operate best. That rate of speed reflects the degree to which the organization can absorb major change while minimizing dysfunctional behavior. Conner says that managers must carefully orchestrate the flow of change, guiding their actions by asking such questions as, where will this change have its greatest impact and at what speed? Should we proceed? Who is going to absorb it first? How do I prepare that part of the organization for what will happen?[48]

Summary

What all of the business gurus, consultants, visionaries, and executives have in common is a sense that indeed "change is changing," and that any successful corporation in the 21st century must figure out a way to deal with that fact in order to survive. All businesses are trying to figure out ways to institutionalize the transformational change process and give themselves and other businesses a better chance for success with a process that often leads to failure.

What can the Intelligence Community learn from corporate transformation? Strategic thinking and management needs to be an ongoing, iterative process. The bright ideas that transform an institution often come from outside the organization, and the institution must be able to locate those good ideas. Technology should reshape organizational behavior, not simply enhance existing processes.

---

[47] Duck, 2001, p. 272.
[48] Conner, 1992, p. 56.

These findings are also lessons learned from military transformation. Other parallels between the military and business-change models are apparent. Theory, strategy, and doctrine come first and need to be integrated later with technological innovation and operational and organizational adaptation. Business theory helps to define corporate culture, but when theory is taken for granted in complacent, nonadaptive cultures, the results can be stagnation and lost market share. Likewise, strategy plays a role in business that is parallel to the role played by military strategists in the RMA; both are efforts to plan and shape the future. This strategy is not the product of some formulaic business procedure; rather, it comes from the creative energy and imaginations of activists in companies to provide a vision of the future and an innovative pathway to reach it. Again, the parallels with the dynamic intellectual climate within the military change model are evident. The primary need is the harnessing of adaptive planning behavior.

Although "doctrine" is not a popular word in the corporate lexicon, strategy is nonetheless translated by companies into basic principles that guide and govern corporate actions. These basic principles are all the more important in a dynamic, fluid environment; many corporations now invest significantly in developing their basic principles and teaching them to their employees. This is an investment in getting everyone on the "same page" on what the corporation is about; it serves to minimize factional infighting and discord and promotes the modeling of new, adaptive corporate behavior.

The Intelligence Community should also take heed of the fact that many change efforts fail. In his seminal piece on transformation, "Leading Change: Why Transformation Efforts Fail," John Kotter argues that most transformation efforts come to naught even when top executives who feel the urgent need for change are correct. Often, the companies cannot sustain significant change and end up facing crises.[49]

---

[49] Kotter, John, "Leading Change: Why Transformation Efforts Fail," *Harvard Business Review,* March-April 1995.

Table 5.3
John Kotter's Eight Principles for Successfully Leading Change

- Establish a sense of urgency
- Form a powerful guiding coalition
- Create a vision
- Communicate the vision
- Empower the others to act on the vision
- Create short-term wins
- Consolidate improvements and sustain the momentum for change
- Institutionalize the new approaches

SOURCE: Kotter, 1995.

There is hope, however, for companies in crisis. Kotter says, "The most general lesson to be learned from the more successful cases is that the change process goes through a series of phases that, in total, usually requires a considerable length of time. Skipping steps creates only the illusion of speed and never produces satisfactory results. . . . Making critical mistakes in any of the phases can have a devastating impact, slowing momentum and negating hard-won gains."[50]

Attempts to understand and accommodate change in the corporate commercial world take many paths, but the pace of the arrival and departure of many businesses speaks to the volatile nature of the corporate environment. The lesson to be learned is that there is no simple or easy approach to transformation, and evidence shows that quick solutions are fleeting and perishable. Instead, the goal should be to develop the capacity to ask the right questions and engage in iterative and timely learning. This same core notion is embedded in the RMA and RIA concepts, although bureaucratic entities tend to value the durability of methods over quick solutions.

To make all this strategizing and risk taking productive, modern corporations have to innovate operationally. The business imperatives in today's environment are to transform business practices and to help

[50] Kotter, 1995, p. 59.

members of the workforce to overcome their weariness with constant changes by building innovative change management into the fabric of the organization. Managers are key to both tasks because they must deal effectively with the emotional impact of change on employees, modulate the pace of change to minimize dysfunctional behavior, and allow the organization to function effectively even as it changes.

As in government, corporations face a daunting task in learning to continuously change complex systems. And, in both environments, the quest for new ideas, the ability to leverage technology, and the emotional health of the workforce all contribute to effective transformational change management. In the end, the capabilities and the adaptability of people matter most. All of the learning acquired by corporate America about the importance of theory, strategy, principles of behavior, and innovations in technology, operations, and organizations can inform a Revolution in Intelligence Affairs.

CASE STUDY: A PREVIOUS RIA (1945-1956)

The years immediately following World War II emerged as a period of discontinuous and revolutionary change in U.S. intelligence, largely out of concern over the fragmented nature of intelligence activities during the war years and the failure to warn of the impending Japanese attack on Pearl Harbor in 1941. The response of the government was to centralize the coordination (but not the management) of intelligence activities, create a new agency (the Central Intelligence Agency) as the cornerstone of that centralization, and base the entire structure on a new statutory foundation—the National Security Act of 1947.

World War II forced innovations in strategy and technology that drove the first "Revolution in Intelligence Affairs." German and Japanese aggressions convinced Washington that the United States had to play a global role to support its allies and deter hegemonists before they grew strong enough to attack the United States directly. At the same time, long-range bombing and the advent of atomic weapons showed that terrible destruction could be wreaked upon the homeland.

President Harry S Truman and Congressional leaders recognized the urgency of having to reform America's defense and foreign policy

structure and to revamp intelligence as part of this larger shake-up. The rapid emergence of the Soviet threat dominated the subsequent evolution of the missions, capabilities, and organizations of the new "intelligence community." A decade of innovation ensued in which new doctrines, procedures, and tools were devised to collect information on the difficult Soviet target, to understand the Soviet Union's nuances, and to counter its moves around the world.

The successful prosecution of the war established the value of intelligence, at least in government's inner circles. Simultaneously, the importance of technological developments became obvious during and immediately following hostilities, which reshaped capabilities such as reconnaissance and signals intelligence. The scene was set to apply improved organizational management to harness the potential advantage intrinsic in knowing and understanding the secret intentions and actions of the new adversary, the Soviet Union.

Several factors gave urgency to the need to develop knowledge of this new threat to U.S. national security. As the early 1950s progressed, human intelligence proved an unreliable platform from which to gain insights into the Kremlin's intentions and actions. Technological developments further expanded U.S. capabilities in reconnaissance and signals intelligence—and both were transformed when combined with the development of high-altitude aircraft (and later missiles) capable of achieving earth orbit. Finally, technical developments by the Soviets--nuclear and missile-based weapons, nuclear submarines, and long-range strategic bombers--presented new threats to U.S. security. Developments in the political arena were hardly reassuring: communist proxy states emerged in Europe and Asia, and the Soviet Union itself became at once a closed society and an aggressive antagonist on the world stage.

The challenge was daunting and must have seemed almost impossible to engage successfully, but it is that degree of challenge that sometimes spurs the creative thinking, innovation, and energy needed for revolutionary change. The state of U.S. intelligence at that time had some advantages compared with the intelligence situation today: the Intelligence Community was small and bureaucratically less complex than

it is now; likewise, Congressional oversight, to the extent it existed beyond the provision of funding, was informal, leaving the real decisionmaking to the Executive Branch. It should also be noted that the CIA was staffed with a small group of highly motivated and influential veterans of wartime intelligence activities.

Changes in the External Environment and a Sense of Urgency

In the late 1940s, the surprise attack on Pearl Harbor was still fresh in the minds of both elected officials and the American public. Much of the world was weary of war and anxious to find new methods of resolving disputes peacefully. The United States was concerned with growing Soviet military power and the spread of communism. Thinkers inside and outside of government pondered the possibility that chronic instability and depression could plunge the world into a third global war—this time with nuclear weapons being used by both sides.

The development and use of an atomic weapon during World War II is recognized as an historical discontinuity that fundamentally changed how the United States viewed its security. According to historian John Ranelagh, Americans "understood that Hitler's empire could have prevailed had he had the atomic bomb. They also understood that Stalin could create a worldwide empire with one." Ranelagh argues that the U.S. government became convinced that it should never risk isolation again; it was far more acceptable to undertake the risks of engagement. "This was the spirit of the founding generation of the CIA, of NATO, and of the Marshall Plan," Ranelagh says.[51] At the dawn of the nuclear age, weapons had become so destructive that the United States could not afford another strategic surprise—it would need some way to successfully warn of an impending disaster.

As an instrument of national security, intelligence dramatically increased its worth during World War II. Both sides exploited physical contact (documents, mail, interrogating prisoners), espionage, aerial reconnaissance, and signals intelligence (or tried to) with varying degrees of success. New technology, such as radio communication, proved

[51] Ranelagh, John, *The Agency: The Rise and Decline of the CIA,* New York: Simon & Schuster, 1986.

to be both an advantage and a disadvantage, as signals intelligence became the most prolific and reliable intelligence source.[52]

Given the experiences of World War II, and despite its distaste for secret organizations, the U.S. government believed it needed a peacetime intelligence apparatus that could provide strategic warning of threats to the United States. The JCS argued in 1945 that an "efficient intelligence service" was more vital than it had ever been before and that "failure to provide such a system might bring national disaster."[53] President Truman, despite his distaste for secrecy, agreed to establish an independent agency to centralize intelligence efforts—the Central Intelligence Group (CIG), which later became the CIA.

During a recent interview, A. Denis Clift, president of the Joint Military Intelligence College, maintained that while Truman gets most of the credit for the establishment of the Intelligence Community, it was actually President Eisenhower who established the capability we now know as U.S. intelligence. "In the Eisenhower administration, U.S. policymakers attached urgency to acquiring hard facts about Soviet strategic and conventional military capabilities—a tall order when dealing with a closed-society target covering one-sixth of the earth's land surface," said Clift. He described how under Eisenhower the United States embarked on the CORONA reconnaissance satellite program: "There would be a dozen failures, four years of tremendous effort—with Eisenhower steadfastly giving his backing—before the first successful mission in 1960, just 110 days after the downing of Francis Gary Powers' U-2 aircraft."[54]

The nature of peace also changed during the period from 1945 to 1956. The threat from countries in most of Europe diminished as a new

---

[52] Hinsley, Sir Harry, "World War II: An Intelligence Revolution," *The Intelligence Revolution: A Historical Perspective, Proceedings of the Thirteenth Military History Symposium,* 31st Harmon Memorial Lecture, U.S. Air Force Academy, Colorado Springs, Colo., October 12-14, 1988.

[53] "Establishment of a Central Intelligence Agency upon Liquidation of OSS," Joint Chiefs of Staff, September 19, 1945, in Department of State, *Foreign Relations of the United States, 1945-1950, Emergence of the Intelligence Establishment*, Washington, D.C.: Government Printing Office, 1996, p. 41.

[54] Clift, A. Denis, president, Joint Military Intelligence College, interview with author, January 6, 2003.

alliance (NATO) was formed. The Marshall Plan and the economic recovery in Germany and Japan helped to remove the two countries from the list of aggressor nations. Western Europe was ready to work toward a lasting peace through new processes and institutions like the United Nations, and hot wars between major combatants were replaced with proxy confrontations in faraway places like the Korean peninsula.

In short, the challenges facing intelligence in 1945-1956 bore some striking similarities to the changing externalities that the United States faces today. The Soviet Union had the capability to cause massive destruction within the U.S. homeland, seemingly with little or no warning. Given the state of technology at the time, preventing such a catastrophic event must have seemed like an impossible intelligence challenge. However, as other institutions learned, it is exactly this type of impossible challenge that spurs creative thinking and innovation. It is important to note that new theory, strategy, doctrine, and innovations also played a role in the successful transformation of intelligence at that time.

Theory

Up until World War II, most military leaders accepted the need for intelligence during conflict, but few in power believed that an organized foreign intelligence capability was desirable during times of peace. Secretary of State Henry Stimson's admonishment in 1929 that "gentlemen do not read each other's mail" was typical of the view that "spying" was a repugnant business, justifiable only in times of war.

During the war, however, several prominent men who were considering how to shape the postwar environment had a different notion about the use and importance of intelligence. Most vocal among them was William Donovan of the Office of Strategic Services (OSS), who was convinced that America needed "a coordinated intelligence system" to function in peace as well as in war.[55] Nevertheless, suggestions that a new

[55] Memo from William Donovan to Harold Smith, White House Bureau of Budget, August 25, 1945, in Department of State, *Foreign Relations of the United States, 1945-1950, Emergence of the Intelligence Establishment*, Washington, D.C.: Government Printing Office, 1996, p. 20.

centralized intelligence organization be created and report directly to the president, not the military, prompted widespread resistance.

By 1947, supporters of a centralized, active U.S. intelligence apparatus won the day. This was largely the result of President Truman's insistence on modernizing the creaking national security structure that had proved so cumbersome in wartime. Once Truman made the critical decision to embrace the theory that intelligence was as critical to maintaining the "peace" during those dangerous times as it was to winning wars, other decisions rapidly followed.

When the Central Intelligence Agency was established in 1947 it was given two missions: first, to provide intelligence to avoid strategic surprises and, second, to coordinate clandestine activities abroad. "With a world up for grabs and with the Soviet Union taking what it could get, the CIA was charged with laying the U.S. claim," says Ranelagh.[56]

Strategy

The U.S. national security strategy changed dramatically in the 1940s to focus on global engagement and confronting totalitarian threats. The strategy developed for the use of intelligence was, in turn, to use a combination of new technology and secret intelligence alliances to monitor Soviet weapons developments, scientific activities, and most important, leadership plans and intentions toward the Soviet Union's neighbors. The focus of the Intelligence Community during this period was primarily on preparing for as well as preventing war with the Soviet Union.

Doctrine

Although not described as "doctrine" per se in intelligence literature, the U.S. Intelligence Community nonetheless developed a set of operating principles that would guide the actions of intelligence officers throughout this early and critical phase of the Cold War.

Reliance on analysis was a key part of the developing intelligence doctrine. Sherman Kent, a Yale history professor and OSS veteran, is

---

[56] Ranelagh, 1986, p. 119.

credited with developing some of the early intelligence doctrine during the first RIA. In one of his essays in 1955, he describes intelligence as "an exacting, highly skilled profession, and an honorable one." He was instrumental in explicating new analytical methodologies, overt and covert techniques, and "orderly and standardized ways of doing things." At the time, however, he saw a serious deficit in the lack of intelligence literature to serve as the "institutional mind and memory of our discipline." Both theory and doctrine are enriched, he believed, by such a body of literature.[57]

The literature Kent spoke of had several important aspects to it. It dealt with first principles, such as the definitions and missions of intelligence. He believed that the Intelligence Community has more than one mission and that many observers were confused not only about the number and character of the many missions, but also about how each relates to the others. Kent argued that there were many methods of meeting the different missions and believed in the importance of an elevated debate: "Now if all this sounds ponderous and a drain on time, I can only suggest that, so far, we of the Western tradition have found no faster or more economical way of advancing our understanding. This is the way by which the Western world has achieved the knowledge of nature and humanity we now possess.".[58]

Technological Innovations

Improvements in signals and imagery elevated the importance of intelligence during World War II and convinced observers that the side that best applied technology would win. The postwar period saw rapid development of special devices for clandestine operators, the U-2 reconnaissance aircraft, the beginnings of the space program, and the earliest mainframe computers.

Richard Bissell, the CIA's driving force in reconnaissance systems in the 1950s, cited in his memoirs the importance of candid advice from

---

[57] "The Need for an Intelligence Literature," *Studies in Intelligence,* September 1955, reprinted in *Sherman Kent and the Board of National Estimates Collected Essays,* Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency, 1994.

[58] "The Need for an Intelligence Literature," 1994, p. 3.

leaders of the nation's scientific and industrial communities. One advisory panel, chaired by Edwin Land of the Polaroid Corporation, "played a major role in initiating the development and deployment of a series of reconnaissance systems that drastically expanded the scope of the whole United States intelligence collection process," Bissell said.[59]

Bissell wrote of the atmosphere of creativity and innovation driven by the need to address the Soviet threat, and of the speed with which such breakthroughs occurred. "The go-ahead for the U-2 project was given to Clarence "Kelly" Johnson of Lockheed Aircraft by telephone on December 1, 1954, according to Bissell. "The first overflight of the USSR took place on July 4, 1956. . . . Two months after the first overflight of the Soviet Union, Col. Jack Gibbs and I started defining a successor to the U-2. . . . In March 1955, influenced by RAND Corporation studies [and others] . . . a general operational requirement for a photoreconnaissance satellite [was issued], thereby initiating a different technical approach to overhead reconnaissance."[60]

Bissell notes that although there were scattered failures thereafter, there has never been a major lapse in the flow of intelligence from satellite reconnaissance since then. "It is no exaggeration to say that what was accomplished in this period of less than ten years was a revolution in intelligence collection. The desperate rivalry of the Cold War, of course, provided the major stimulus for our activities."[61] Bissell's observation underscores the importance of a major impetus, or unmet challenge, to spur the kind of creative effort and action that leads to "breakthroughs."

Operational Innovation

Leveraging the various plans and technological developments during the early years of centralized intelligence required corresponding

---

[59] Bissell, Richard M., Jr., *Reflection of a Cold Warrior: From Yalta to the Bay of Pigs*, New Haven, Conn.: Yale University Press, 1996, p.92. This statement recalls the comment by Antony Jay earlier in this section that a small, creative group is usually behind the creation of any new technological innovation.

[60] Bissell, 1996, p. 92-93.

[61] Bissell, 1996, p. 93.

changes in operational sophistication. Using the new technology effectively meant not only developing new technical knowledge but also forging overseas relationships to support the technology's infrastructure. Making the best use of the new technology also required new procedures and techniques for dealing with dramatically increased volumes of information and technical complexity, which brought corresponding demands on the intelligence producers to be able to translate the results for intelligence consumers.[62] For example, a procedure called "Quickmove" was developed to allow deployment of a U-2 either from a remote airfield or from the detachment base, with the landing at a remote airfield. The goal was to hide any clues to the location of a U-2 takeoff or landing.

Bissell notes the tremendous changes that were needed in the analytical process to make use of all of the new data that the new technology supplied. The CIA built a *national* asset—the ability to analyze sensitive photos and produce intelligence of relevance to the president, to economic analysts, and to military planners. Bissell and others realized that entirely new processes and skills would need to be developed to make maximum use of what the technology offered.

Organizational Innovation and Adaptation

Two significant changes in the national security structure—the creation of the National Security Council and the Department of Defense—played pivotal roles in the way the CIA was created in 1947. President Truman's competing desires to placate the military services and at the same time centralize intelligence operations and intelligence communication to the president, led to the creation of a CIA that had the charter to centralize all intelligence but was headed by a director of Central Intelligence who lacked the authority to do so.[63]

Both the CIA and the National Security Agency were created and grew in stature during the late 1940s and early 1950s. Their internal

---

[62] Pedlow, Gregory W., and Welzenbach, Donald E., *The CIA and the U-2 Program, 1954-1974,* Washington, D.C., Center for the Study of Intelligence, Central Intelligence Agency, 1998, pp. 82-83.

[63] Zegart, Amy, *Flawed by Design: The Evolution of the CIA, JCS, and NSC*, Stanford, Calif.: Stanford University Press, 1999, Chapter 6.

structures were fluid for several years, with frequent (and sometimes disruptive) reorganizations. It was not until significant thought about the individual functions of intelligence were hammered out, however, that a more lasting organizational structure for intelligence began to take form.

Other Factors that Contributed to Successful Change

In addition to a coherent conceptual framework for the creation of a peacetime intelligence apparatus based on new theory, strategy, doctrine, and innovation, other factors contributed to revolutionary change during the 1945-1956 period. These factors helped the fledgling Intelligence Community to overcome the institutional resistance, turf battles, funding shortfalls, and other impediments to change discussed above.

- **Experimentation and risk.** The impetus to prevent a surprise Soviet attack led to bold experimentation and heightened risk during these years. Projects such as the U-2 (which was developed in just over eight months) were put into operational use while still being tested. Breakthrough technologies were conceived of and developed by the U.S. government in close collaboration with industry, and commercial applications of those technologies followed their use by the military and intelligence communities.
- **Architect(s) of change.** Over this period, there were a number of visionaries, or architects, who brought about significant change. The most important, by all accounts, was Bill Donovan, the head of OSS who argued for "the establishment . . . of a foreign secret intelligence service which reported information as seen through American eyes." [64] Although his proposal met with spirited resistance, in the end, a peacetime intelligence apparatus was established which was coordinated and centralized under the overall control of the president, much as Donovan envisioned. Donovan's emphases on analysis and clandestine activities played

[64] Ranelagh, 1986, p. 96.

an important role in the growth of technical intelligence during this period.

- **Champion(s).** There were several champions who helped drive the creation of a peacetime U.S. intelligence apparatus. Without the support of President Truman, the CIA would not have been established or preserved. President Eisenhower, who gained an appreciation for what intelligence could provide during World War II, pushed intelligence to do all it could and more to anticipate a Soviet surprise attack. DCIs Walter Bedell Smith and Allen Dulles were also strong advocates for change during this period.
- **Leadership continuity.** After rapid turnover before the Korean War, the leadership of the Intelligence Community remained in strong and seasoned hands during the 1950s. Its major components—the CIA, FBI, and NSA—worked under long-serving directors dedicated to the ideals and missions of their agencies.
- **Internal consensus.** During these years, the Intelligence Community was smaller and relatively united in a common mission—to prevail against the Soviet threat. While there were disagreements on how best to accomplish that mission, few questioned the need to invest heavily in new technology or the benefits that new technology would offer.

While it may be debatable whether these fundamental changes in U.S. intelligence during its formative years amounted to a Revolution in Intelligence Affairs, few argue that the practice of U.S. intelligence was not dramatically altered between 1945 and 1956. And, given the changes the United States is currently experiencing in the post-Cold War national security environment, it would seem that the same extraordinary strategic thinking, skills, creativity, and spirit of innovation are urgently needed to address the types of threats that are looming.

The threat of weapons of mass destruction in the hands of terrorists and the global digital revolution are changes of a magnitude similar to that of the security shifts the United States experienced in World War II. The United States was able to introduce fundamental changes in its intelligence practices and structures during the early

days of the Cold War——a time of unsettling dangers and uncertainties equal to those of today.

Perhaps the attributes of the current Intelligence Community will make instituting fundamental change more difficult than it was during this earlier RIA. Today, during the postwar years, sudden crises always have the potential to push the change agenda off center stage and extinguish the flame of inspiration and innovation. Finding leaders and champions, building coalitions, probing for technological innovation, and setting out to change organizational cultures and operational methods seem like a tall order in an environment in which threats evolve rapidly and the intelligence workforce is consumed by the demands of operational response. But, if the nation is at risk, and if the Intelligence Community is still designed to defend against threats that have significantly changed, addressing this disparity is a fairly urgent matter. Inarguably, the transformation of the Intelligence Community will be a long and arduous process, but the challenges this transformation presents would not faze the pioneers and innovators who had reinvented U.S. intelligence within ten years of its birth.

5. THE POTENTIAL FOR IMPLEMENTING A REVOLUTION IN INTELLIGENCE AFFAIRS

"For managers, the dynamics of knowledge impose one clear imperative: every organization has to build the management of change into its very structure."

Peter Drucker
Managing in a Time of Great Change, 1995

If the case for change in the U.S. intelligence apparatus is sufficient to warrant a revolutionary response, and the prospects for a successful revolution are enhanced by the successes of other complex bureaucratic institutions, the question to then be answered is, how does one implement a Revolution in Intelligence Affairs? This chapter discusses the difficult process of implementing revolutionary change, culled from the sometimes painful experiences of other large organizations, and lays out in detail the steps necessary to continuously transform the Intelligence Community so that it will always be one step ahead of the next intelligence failure.

The overarching lesson to be learned from the examination of past revolutions in bureaucratic institutions is that there are common threads that can be discerned among both the successes and failures of those revolutions. Reorganization almost never tops the list of necessary precursors to success, nor does a large infusion of money (although neither necessarily leads to failure either). Organizational complacency, leadership dissension, poor communication throughout the institution, failure to anticipate and remove barriers to change, lack of leadership vigilance, and lack of continuity once the current leadership has departed are among the elements that have typically led to failure in other institutions. Some, if not all, of these elements have been present in past efforts to reform intelligence.

The historical case studies of defense transformation, corporate transformation, and the "RIA" of 1945-1956, as discussed in Chapter 4, suggest that the following model provides the guideposts for a dynamic transformation process within the Intelligence Community:

1. A critical mass of people within the Intelligence Community must believe that there are times when change of a more fundamental nature is the *only* way to meet certain challenges—and that now is one of those times.
2. Key players within the Intelligence Community must be identified who will be responsible for guiding and implementing change, overcoming roadblocks, and informally establishing a dynamic change process—and they must partner with a powerful coalition for change *outside* the Intelligence Community.
3. Solid strategic thinking that focuses on theory, strategy, and doctrine must precede any attempt to implement systemic change.
4. Continuously updated strategies must prompt and guide innovations in technology, operations, and organizations and lead to revolutionary change proposals that touch all of these domains.
5. Revolutionary change proposals should be objectively evaluated to determine if they lead to desired transformational outcomes.
6. Experimental designs and new performance measures must be developed to objectively assess alternative intelligence management processes, operations, activities, organizational structures, and new technologies.
7. A new set of incentives and rewards must be developed to institutionalize the dynamic-change management approach.

ACHIEVING CRITICAL MASS AND IMPLEMENTING DYNAMIC CHANGE

The two claims argued in the first chapter of this report are that the larger national security environment within which intelligence must operate is changing dramatically, and that if future intelligence "failures" are to be avoided, or at least minimized, the Intelligence Community must change more rapidly. Due to the nature of the Intelligence Community's perishable products and services, this report argues that the Community must learn to continuously transform itself—sometimes quite radically—if it is to continuously accomplish its mission. This means that at all times there are two competing streams of change activity—one evolutionary and the other revolutionary—and the

institution can move from one to the other based on the amount of flux in the larger national security environment.

If there is to be a series of revolutions, one after another, how then does one instill a continuing "sense of urgency" within at least a portion of the workforce and avoid the kind of organizational complacency that Kotter and others argue is the death knell of most transformation efforts? The first step is to ensure that a sufficient number of people in the workforce have an inherent sense of when trouble is looming over the horizon and can identify a major discontinuity when they see one coming. This is not a commonplace skill, but the Intelligence Community typically has more of these trend-spotters than does the typical bureaucracy. In addition, the Intelligence Community needs people who have a healthy preoccupation with anomaly and surprise because they recognize that there are opportunities to learn from them.

However, while these trends are often identified by the Intelligence Community and communicated to policymakers and others for action, they do not necessarily translate into actions that are undertaken within the Intelligence Community itself. For example, while the Intelligence Community correctly anticipated many developments in modern warfare that helped the Department of Defense chart the Revolution in Military Affairs, revolutionary changes in military intelligence often lagged behind.

It is essential that the Intelligence Community identify the activists in its midst, encourage and protect them, and empower them to go beyond just challenging the status quo so that they may translate their concerns into action. Those who have this job would identify unmet challenges and begin to consider ways of meeting those challenges. They would draw upon political, social, cultural, and technological experts both inside and outside of government who have their ear to the ground, are big conceptual thinkers, and who have unique ways of solving problems. Ideally, these change agents would report directly to, and be protected by, the most senior Intelligence Community leaders.

One way to do this would be to establish a group or office, whose main objective is to "disturb the system," as Chris Turner put it.[1] Such a group or office would be small and unobtrusive, and its purpose would be to constantly look beyond the far horizon. It would *not* be part of the normal planning, programming, acquisitioning, and budgeting processes but would regularly challenge the decisions made through those processes. If this group/office is doing things right, there will always be creative tension between what it is promoting as alternative ways of doing business and what the status quo is trying to protect. The mark it would make would be based on the merits of its arguments, not its place in the hierarchy.

One of the primary tasks for this activist group would be to encourage the incubation of new ideas. Today, there are many groups who serve as these "incubators" in the Intelligence Community or who routinely challenge the status quo. In-Q-Tel, the Intelligence Science Board, and the Intelligence Technology Integration Center (ITIC) are among those that focus on new technologies and their possible application in addressing tough challenges. Other groups within the individual agencies, such as the CIA's Global Futures Partnership, the NSA's Advanced Research and Development Agency (ARDA), and the NGA's Innovision, challenge the organization's thinking and seek alternative solutions. Educational institutions, such as the Joint Military Intelligence College and CIA University, also encourage nonlinear thinking. But none of these small organizations have a charter that spans the entire Intelligence Community and its complex set of challenges, nor do they network in such a way that the collective effort equals more than the sum of its parts. Few of these organizations are plugged into the main decisionmaking processes within the Intelligence Community and therefore operate largely on the periphery of the Community.

In today's environment, it would be critical for this activist office or group to regularly interact with *all* who have a vested interest in the future of intelligence within the government. This would

---

[1] Turner, Chris, *All Hat and No Cattle: Shaking Up the System and Making a Difference at Work*, New York: Perseus Books, 1999.

include the Intelligence Community, the Department of Defense, Department of State, the Department of Homeland Security, the FBI, the White House and National Security Council (NSC) staff, the Congress, Office of Management and Budget (OMB), and others. It would also need to tap into scholars, academics, think tanks, government labs, industry, and others who could supply innovative ideas that might not be generated from within the institution. It would constantly scan the horizon for the next big important ideas that will influence foreign policy and international security.

The activist office would also focus on tracking change within Intelligence Community organizations. This does not necessarily mean that quantitative data or metrics should be tracked. It might simply mean setting milestones and seeing that they are met. It should focus on the big things and whether or not they are being addressed. It should pay close attention to what customers are saying about the quality of their intelligence and whether their needs are being met. It should pay attention to customers' plans to ensure that they are congruent with intelligence plans. If there is an intelligence failure, the group should immediately get busy and strive to find out why it happened.

Eventually, the entire institution must become comfortable with ambiguity, uncertainty, and rapid change. The revolutionary impulse must go beyond small groups and become part of the culture. There must be a management ethos that embraces critical self-examination, maintains a healthy paranoia regarding the nation's adversaries, and constantly reassesses trends in the external environment, not simply trends regarding threats but also trends leading to opportunities. Intelligence management must help the Intelligence Community workforce prepare for and adapt to not just one but a continuing series of revolutionary changes.

The key to instituting these measures will be to build continuous change into all intelligence processes—from the gathering and analysis of data, to the sharing of intelligence, to the management and governance of intelligence, to the protection of intelligence sources and methods. Some of these processes are seriously out-of-date. In addition to the already robust evolutionary change process, the

Intelligence Community must deliberately set up a separate revolutionary change process that can compete with the evolutionary one. The Intelligence Community must give revolutionary ideas room to grow, and must do so without total control over its policies, procedures, or budgets.

Whatever method the Intelligence Community adopts to make revolutionary change occur, a willingness to undergo a continuous transformation process needs to be embedded in the culture. How this is done, and who is in charge of doing it, are important issues to sort out before any fundamental change proposal is adopted. The Intelligence Community leadership does not need to have *everyone* onboard, but it does need a critical mass of change agents. These change agents must come from outside as well as from all levels of the institution. While legislation or presidential directives can get the ball rolling, the institution itself must embrace change. Those on the outside will never be able to determine if the changes are taking hold until it is perhaps too late and another intelligence failure has occurred.

KEY PLAYERS IN THE DYNAMIC-CHANGE APPROACH

A dynamic-change process is highly dependent on the involvement of the right kind of people. The process more than people committed to change—it requires the *delegation of responsibility* for change to specific individuals, and holding them accountable for the outcome. Everyone in the Intelligence Community will need to know who these people are and what their roles are in the change process. Most important, it must be known that these change agents possess "top cover" from senior leadership to protect them from powerful forces that are often marshaled to resist change. Based on some of the lessons learned from the case studies presented in the previous chapter of this report, the difficulties of transformation are lessened significantly if it is clear who is fulfilling the following roles.

The Champion

The most important person in the change management process is someone at a very senior level who endorses change, gets strongly behind the new strategy, and protects the change agents. Revolutionary change

rarely happens without a strong leader behind it and is far easier to implement if the person at the top recognizes the need for change and fully and visibly supports it. Such was the case with General Edward C. Meyer, Senators Barry Goldwater and Sam Nunn, Secretary Donald Rumsfeld, and others who led revolutionary changes in defense affairs, and with corporate titans such as Jack Welch of GE, Andy Grove of Intel, Carly Fiorina of Hewlett-Packard, and Lou Gerstner of IBM. Within the Intelligence Community, the ideal champion of revolutionary change would be the director of central intelligence, although others were instrumental in the first RIA discussed in the previous chapter (the president, the secretaries of state and defense, and others).

The champion helps establish a sense of urgency that prompts a shift from the evolutionary change process to the revolutionary one. He or she also clearly establishes the victory conditions, including both short-terms wins and long-range objectives. The champion pays attention to milestones and helps the organization celebrate when those milestones are met. While the champion must have a broad sense of where the organization or institution needs to go, he or she does not need to be the "architect" who establishes all of the parameters and begins articulating the details. The champion should explicitly designate an architect, however, and let everyone know that the architect has the champion's trust. Once provided with a change proposal that he or she can endorse, the champion cannot waiver or lose faith when times get tough (and they inevitably will). Constancy of purpose and leadership is essential.

The champion needs to give all of the change agents wide latitude to be creative and generate new ideas. It is important not to set the parameters for change too early, but once the plan is set the champion must endorse a "short list" of the most important things to do, rather than try to do too much all at once.

The final responsibility of the champion is to obtain support at the highest levels from outside of the Intelligence Community—from Congress, the OMB, the National Security Adviser and the NSC, the White House, the secretary of defense, and the secretary of state. Without this support, attempts to bring about true systemic change in

intelligence affairs will run into insurmountable difficulties, as it has in the past.

The Architect

The Intelligence Community architect should be someone with experience at the operational level who understands the larger context for change, knows how things are done today, and understands from experience where change is needed. The architect is responsible for capturing and developing new ideas and drawing up the parameters of change. The architect will be most effective if he or she is as inclusive as possible in the search for new ideas.

Part of the Intelligence Community architect's responsibility in bringing about truly revolutionary change would be to identify those breakthrough innovations in technology, operations, or organizational structure that would challenge a core competency (imagery collection, signals intelligence, or strategic analysis, for example) in intelligence today.

The Intelligence Community architect must be able to clearly describe what is to be done and how it will differ from the way things are done today. The architect will be instrumental in crafting new intelligence doctrine. Ideally, the architect is someone at a point in his or her career at which the penalties of taking on "sacred cows" is no longer a worry. (It should be noted that attempts to establish an Intelligence Community architect in the past have not met with resounding success.) Most important, the architect must have the ability to remain objective and stay above the fray, and be knowledgeable enough about the way things really work to recognize the difference between legitimate organizational concerns and bureaucratic obstinacy.

The Coalition with Clout

Transformational change within government bureaucracies is best accomplished as a partnership among those who are inside the institution and those on the outside who have a vested interest in the institution's future. This coalition must be composed of influential people who are willing to act as change agents and should be as inclusive as possible.

Ideally, this group works with the architect to determine the parameters of change and to develop and protect important innovations.

For the Intelligence Community, this coalition should include influential think tanks and academics, outside contractors, independent consultants, retired intelligence officers, and other interested and knowledgeable third parties. It should also include members of Congress and the OMB. Intelligence Community customers can also be very influential members of the coalition, particularly when advocating change that will ultimately be of benefit to them. Other individuals, such as the business executives and former government executives on the president's Foreign Intelligence Advisory Board and the DCI's National Security Advisory Panel, can also be powerful advocates for change. As other organizations have learned throughout their transformation processes, the more diverse the coalition, the better.

Because true transformation often takes time, this coalition must maintain its focus on seeing the transformation process through to the end while faced with day-to-day distractions. This group must act as the "conscience" that reminds participants in the process to be true to the ultimate objective as they struggle with predictable obstacles.

The Change Manager

The change manager has an important behind-the-scenes role in the transformation process—keeping the champion informed on the progress of the transformation. The change manager's job is to keep an eye on changing external dynamics by maintaining a constant, open dialogue with key constituents. In keeping an eye on the process, the change manager must ensure that the Intelligence Community develops a "rolling reassessment," not a blueprint for the next ten years. The change manager must ensure that there is a constant influx of new ideas and that the creative tension between the new ideas and the status quo—and even between the new ideas and the latest change proposal—is allowed to exist.

In the Intelligence Community, the change manager must sit at the corporate-management level, reporting directly to the person who champions change, preferably the DCI. The change manager must ensure

that all key players are talking to each other, constantly providing feedback, and refining the approach as the process unfolds. This individual should be constantly checking in with the workforce to see how things are going. Because the change manager is responsible for measuring performance against goals, he or she should have enough knowledge of the inner workings of the components of the Intelligence Community to track implemented changes and assess the results. This person must ensure that new insights, evaluation results, and recommended course corrections are fed into Intelligence Community business processes (i.e., planning, programming, and budgeting) and identify the people and organizations who are creating impediments to needed change.

The Willing Workforce

Not everyone who works inside the system needs to be wildly enthusiastic about proposals for change. But the case studies presented in the previous chapter suggest that the chances of successful transformation are far greater if a critical mass within the workforce recognizes the need for, and willingly accepts, the proposed change (e.g., the U.S. Army after Vietnam). The most difficult phase of any transformation process is the implementation phase—when people have to actually change their attitudes, behaviors, and daily routines. If a significant number of middle managers and their subordinates resist, rather than accept, the proposed changes, this is the point at which the effort will die (and has died in the past).

Middle managers must inspire their subordinates to at times put the good of the "Community" or even the "government" ahead of parochial interests (something that does not happen often enough today). It will at times require putting the organization's interests ahead of personal interests. It will certainly mean creating an environment in which experimentation and risk are not only tolerated but are encouraged. It means establishing rewards for new behaviors and disincentives for old ones.

The notion of ongoing and continuous transformational change is likely to be unsettling to some in the Intelligence Community workforce.

The solution, according to "change guru" Daryl Conner, is to increase resilience in both managers and those they manage. Resilience, says Conner, is the ability to demonstrate both strength and flexibility in the face of frightening disorder. Resilience must become part of the Intelligence Community's culture through managers that demonstrate resilience themselves, teach resilience skills, and hire those predisposed to taking change in stride.[2]

Astute managers anticipate and are ready to address with their subordinates the emotional and behavioral aspects of change. These managers internalize new theory, strategy, doctrine, and various innovations in their area of responsibility and find ways to translate them into action. To do so, they design projects and tasks to implement the needed changes, and either help their teams to develop the necessary new skills or hire those who already have them. Perhaps most important, these managers communicate the need for change to all levels of the organization and ensure that all questions are thoughtfully considered and answered.

The Congress

The congressional committees with oversight responsibilities are critical partners in any government agency transformation process. They craft needed legislation, provide a venue in which new ideas can be aired, and approve funding as needed. They carefully assess—and then support—appropriate innovations (although some observers complain that congressional committees have become micromanagers consumed with details rather than grand strategy). As in the case of the Goldwater-Nichols legislation discussed in the previous chapter, the U.S. Congress can play a pivotal role in overcoming institutional resistance to change.

In an ideal world, the Congress would work with the Executive Branch and the Intelligence Community as partners in the coalition, but not with the objective of reaching a consensus in which everyone is

---

[2] Conner, Daryl R., *Managing at the Speed of Change: How Resilient Managers Succeed and Prosper Where Others Fail*, New York: Villard Books, 1992.

satisfied bureaucratically (as was the case in the ambiguous compromise legislation drafted in 1947.) That said, the more agreement that can be reached among these players on the most important aspects of how to go forward with change, the more likely real change will take root.

It will also be very important for the Congress to look to the DCI to champion the change process, not the many agency and department heads who will want to take this on. This procedural nod would put the DCI in a stronger leadership position when addressing the inevitable turf issues, and give the DCI, even if informally, whatever "authorities" are necessary to bring about real change. Perhaps most important, the Congress needs to accept that the transformation may be "murky" for a while and that it will take some time for a clear picture of it to emerge. As Congress keeps pressure on the Intelligence Community to maintain constancy in its change efforts, it can help garner public support and understanding that real change does not happen overnight.

THE INTELLECTUAL FOUNDATION: THEORY, STRATEGY, AND DOCTRINE

Throughout this report, the case is argued that new theory, strategy, doctrine, and innovation must be the strategic and intellectual underpinnings of any intelligence transformation, which in turn will ultimately lead to changes in people's behavior and day-to-day activities. If sufficient progress is not made in these areas in the Intelligence Community, then transformation of intelligence will not only be made more difficult, it will almost be an impossibility. Changes can certainly be made, but not changes that are likely to lead to dramatic improvements in capability and performance.

Strategic thinking on intelligence should not be limited to, or the sole responsibility of, the senior leadership in the Intelligence Community. Ideas should be generated at all levels throughout the Community and outside of it. Senior leaders must make the tough decisions, but should not do all the legwork leading up to those decisions. The coalition for change should take responsibility for nurturing new concepts and strategies. This should not be a formal annual process, which can lead to rote, formulaic thinking. Rather, it needs to be a constant, ongoing process.

The change management group would prod and provoke the best thinkers on intelligence and assure that the debate sustains its momentum. This can be accomplished through conferences, informal gatherings, scholarly articles, and papers. The theoretical debate, for example, should include the widest assemblage of bright minds in the country. The important aspects of each of these essential elements of transformation are addressed next.

Theory

Theory is a systematic thought process that seeks to understand why things happened as they did in the past and how those cause-and-effect relationships might affect present and future conditions. Intelligence theory might question such things as the relationship between intelligence and the end of the Cold War, or whether intelligence helps policymakers to make better decisions. Theory attempts to discern, as CIA historian Michael Warner argues, the "intrinsic something" that defines intelligence.[3]

Military theory has been around since Sun Tzu wrote *The Art of War* 2,400 years ago and is tested and challenged on a frequent basis. Likewise, economic theory has been debated for centuries. There has been very little theoretical work done in the area of intelligence, however, largely because much of the data needed to prove or disprove a theory is unavailable to the scholars and academics that have an interest in it.

Theorizing about the larger issues and patterns of intelligence can help to inform decisions on future intelligence systems, structures, or functions by establishing causal links between intelligence and national security outcomes. One problem with the intelligence reform movement in the 1990s was that a robust body of intelligence theory did not exist; hence "rethinking" intelligence was problematic. Without a new theory on the use of intelligence in a post-Cold War world, changes in U.S. intelligence were driven largely by the anticipated "peace dividend."

---

[3] Warner, Michael, "Wanted: A Definition of Intelligence," *Studies in Intelligence,* Central Intelligence Agency, Vol. 46, No. 3, 2002.

Downsizing and outsourcing drove many of the changes, coupled with "patching up" the inevitable problems as they arose.

How might new theory lead to revolutionary change in intelligence? In his seminal book, *The Structure of Scientific Revolutions,* Thomas Kuhn describes two types of science: "normal" science and "revolutionary" science.[4] Normal science applies and refines theory and tests hypotheses that already exist. Revolutionary science challenges the theory itself when there are too many anomalies to continue to support existing hypotheses. A revolutionary theory of intelligence would challenge at minimum the theory behind the creation of centralized intelligence in 1947 and ideally challenge any updated theories that followed thereafter.

The most recent thoughtful attempt at articulating new intelligence theory was made by Loch Johnson, a professor at the University of Georgia. In his article "Bricks and Mortar for a Theory of Intelligence,"[5] he offers a number of observations and hypotheses, but for the sake of brevity, I explore only three here. First, Johnson describes intelligence as the combination of three separate activities: gathering, interpreting, and distributing information (otherwise known as "foreign intelligence"); secretly manipulating events abroad (covert action); and guarding against foreign intelligence agencies and other hostile organizations (counterintelligence). He argues that no perfect intelligence system can be devised and that failures are an existential reality of trying to anticipate world events. Success in all three areas, he claims, is dependent on national wealth. He believes that the problems of inadequate intelligence sharing and the imbalance in military/diplomatic intelligence can be remedied only by elevating the stature of the director of central intelligence.

A revolutionary theory of intelligence, however, would take issue with some or all of these claims. For example, in the aftermath of September 11, there are perhaps *four* different sets of activities that

---

[4] Thomas, Kuhn, *The Structure of Scientific Revolutions* Chicago: The University of Chicago Press, 1962, Chapter IX.

[5] Johnson, Loch, "Bricks and Mortar for a Theory of Intelligence," *Comparative Strategy*, Vol. 22, 2003, pp. 1-28.

constitute intelligence: foreign intelligence, covert action, counterintelligence, and *domestic* intelligence. This change in theory--including domestic intelligence as a fourth activity in the intelligence sphere--might prompt one to view the establishment of a director of national intelligence, one who would presumably oversee all of these spheres, in a different light.

So, too, one might challenge the hypothesis that successful intelligence is at least in part a function of national wealth. The Soviet Union, even as it was fiscally imploding, was good, if not superior, to most states at conducting foreign intelligence. Al Qaeda, to cite a more recent example, has developed a global intelligence capability, adapted the latest commercial information technology for their purposes, and exploited seams in U.S. security defenses.[6]

A final hypothesis--that only an elevated DCI can correct the imbalance between military and diplomatic intelligence--might also be challenged. Recent histories of the Department of Defense decisionmaking process, particularly since Goldwater-Nichols, suggest that the imbalance is partly a result of the elevation of the stature of the combatant commanders and their need for strategic intelligence, and partly the diminished voice of the Department of State in articulating its needs for national intelligence.

A revolutionary theory of intelligence might suggest that greater centralization of intelligence is not the answer. Rather, as some observers have suggested, U.S. intelligence needs to be organized and behave much more like the adversary: decentralized and ever-changing, and difficult to both detect and deceive. How such a "system" would be regulated, managed, and operated remains to be seen, but if the constantly shifting external environment suggests we need to know something about nearly everything all the time, organizing intelligence along the lines of how an adversary is organized might be a more sensible model than a centralized one.

---

[6] O'Connell, Kevin, and Robert T. Tomes, "Keeping the Information Edge," *Policy Review,* December 2003–January 2004 (http://www.policyreview.org/dec03/oconnell.html).

Some ideas currently floating around regarding the reorganization of intelligence are interesting but not profound and, with few exceptions, are not even new. The establishment of a director of national intelligence, for instance, would perhaps make clear who the necessary "champion" of an RIA must be (the DCI can bring about an RIA today only through moral suasion), but will this change alone improve how U.S. intelligence tackles the problem of the super-empowered angry man? Or improve how it warns first responders? Or how it handles "zillions" of pieces of data? Or how it improves the speed and fidelity of intelligence to Army troops on the ground in a war zone? By putting all the departmental intelligence elements under a DNI rather than under the department that they service, it is possible that new problems might arise as others are solved.

Going back to first principles—what is intelligence and what are all of its roles and missions—is the necessary first step in the RIA. Assumptions about the external environment, the mission, and the core competencies of intelligence are out of date—from new missions such as support to homeland security to core competencies such as technical collection and strategic analysis. Distinctions between foreign and domestic, strategic and tactical, collection and analysis, and intelligence and information are shopworn; a new intelligence taxonomy is needed.

Military operations, indications and warning of strategic surprise, diplomatic peace initiatives, international and national security policy, and other security functions are increasingly dependent on intelligence—both qualitatively and quantitatively. Every night on the news, Americans see demonstrations of the impact that good intelligence—and bad intelligence—have on U.S. security and how good intelligence leads to better choices. New theory should help illuminate what intelligence can and should do, and what it should not do. It should help establish proper new functions for intelligence in light of the dramatically changing security environment and help establish the kind of results that should be expected.

As Clausewitz suggests, theory must remain closely tied to the historical record, at least as we can know it. The historical record of

U.S. intelligence is becoming clear as more information becomes declassified and more scholars and historians take up the challenge of drawing theoretical inferences from the data. Drawing these inferences is neither a quick nor a simple process. However, without serious consideration of the past and its lessons regarding intelligence successes and shortcomings, there will be no solid analytical basis for serious debate about potential paths for the future.

Strategy

Strategy is simply the means to achieving an objective. Two types of strategy are necessary to prompt an RIA. First, new mission-related strategies are needed for addressing developing threats such as global terrorist movements or rogue nations with weapons of mass destruction. Also needed, however, are "business-related" strategies for transforming how organizations operate and perform. Mission strategies have typically been developed within subordinate organizations, although in recent years, a few have been developed Community-wide.

Dramatic changes in the external national security environment should automatically lead to concomitant changes in intelligence strategy. After a new National Security Strategy is published, a new *intelligence* strategy for meeting new mission priorities should follow. The strategy should then shape the doctrine, and the innovations necessary to meet the strategy all should be linked. It should be noted again that strategy—and strategic management and behavior—are not the same thing as strategic planning. Strategy is less detailed than strategic planning but more ambitious in its scope and direction.

Unfortunately, all too often government budgets drive strategy, rather than strategy driving budgets. The U.S. Intelligence Community saw the negative outcomes of that approach. The development of new intelligence strategy must begin by describing the end state that the United States wants for intelligence, followed by a description of the means to achieve that end.

New intelligence strategies should be developed collectively by the coalition for change and led by the architect who understands both the parameters of the current system and the end state in the future. The

strategy must begin with a vision of the end state 10 to 20 years in the future. It should clearly describe desired outcomes. It should include a view of the transformation of existing institutions, the creation of new capabilities, and, in some cases, the replacement of existing organizations that will inevitably become less relevant as the transformation occurs.

The Intelligence Community should end its current practice of devising individual, competing strategies among the intelligence agencies. An overarching intelligence strategy is the only way that intelligence can work as a "system of systems" without one set of activities confounding the others. While a group in the Intelligence Community already exists to do collective strategic planning, real strategy remains a prerogative of the individual agencies that continue to compete with each other for resources, status, and primacy.

After a new, overarching U.S. intelligence strategy is developed, making choices about technology, personnel, organizational structures, and all of the other elements of the revolution will be far easier. The next step is to determine the innovations that are integral to the new strategy. As part of the strategy-making effort, the collective Intelligence Community leadership must make the difficult perennial choices between flexibility and efficiency, timeliness and accuracy, security and privacy, analytical breadth and analytical depth, and readiness and experimentation. With collective thought, perhaps U.S. intelligence can improve on the trade-offs made between these choices in the past.

One key element of strategy for the Intelligence Community must be to establish priorities and explicitly identify and discuss those areas that will go beyond the realm of intelligence activities. This discussion must take place with members of the National Security Council. The establishment of intelligence priorities through a process called the National Intelligence Priorities Framework is in its earliest stages, but it has already begun to help consumer agencies to know if the analytic help they need falls into an area of low priority for intelligence. Knowing that, those agencies can decide whether or not to

allocate resources in house, find replacement nongovernment advisors, or make plans to do without that help.

For revolutionary change to occur, it is critical that the entire leadership team understands the motivation for and the parameters of change so that each member of the team can determine how to implement change in his or her own directorate, office, or group. But in the Intelligence Community, there is no leadership "team." Each agency still retains a great deal of autonomy, and the head of each organization articulates his vision and establishes the parameters of change. Unfortunately, this vision might work in opposition to the plans and intentions of another agency's leadership, resulting in harmful competition for primacy and resources and the expectation that someone else is covering "the gaps" when no one particular agency is explicitly given the lead. Strategic planning and policymaking at the corporate management level in the Intelligence Community can help to mitigate some of these problems, but planning and policymaking are long and painful processes that are dependent on Community-wide consensus—hardly a viable path toward the realization of revolutionary change. The establishment of a DNI with stronger authorities in these areas could greatly improve this situation.

In sum, the RIA strategy must be a living document that will set forth (1) how an RIA is to be created, revised, and adopted; (2) the process of participation; (3) the means by which ownership and consensus is to be obtained; and (4) how the details will be fleshed out. The person or people in charge of strategy should be explicitly named and have ready access to both the champion and the architect for change.

Doctrine

The U.S. military defines *doctrine* as the fundamental principles by which national security elements guide their actions in support of national objectives. "Doctrine" is not a word typically associated with the national Intelligence Community; however, and certainly no one develops doctrine for the *entire* intelligence profession. But, as the case studies of successful transformations of large organizations have shown, a new set of guiding principles must be developed and then widely

communicated and explained. The lesson General Donn Starry insists must be taken from the experience of the Army after Vietnam is that changing the doctrine is the only way to change a culture within an organization, *especially* the leadership culture.[7]

General Starry also emphasized the role and importance of senior schools in the development of doctrine. A number of schools within the Intelligence Community—including the CIA University, the Joint Military Intelligence College, and training institutions within each agency—teach the art and science of intelligence. But these schools do not teach or develop common Intelligence Community-wide doctrine or tradecraft, even in the wake of a new national security strategy or major changes in intelligence legislation.

Well-developed doctrine, as both Starry and military theorist John Boyd understood, is critical to flexibility and adaptability. After doctrine is shared and understood, subordinate units then have the flexibility to improvise, as long as the activity is within the leadership's intent, which allows them to operate more quickly and efficiently. This flexibility is critical to "getting inside" the adversary's decision cycle by anticipating what he will do before he does it. As intelligence and operations become more closely integrated, as the National Security Strategy says they must, logic suggests that *intelligence* also must operate within the adversary's decision cycle. Thus, intelligence analysts and operators, too, must have the ability to improvise if they are to adjust rapidly to unfolding events.

Military intelligence organizations routinely develop intelligence doctrine in coordination with the Joint Staff. Joint Publication 2-0, *Joint Doctrine for Intelligence Support to Operations,* is updated every few years to "govern the joint activities and performance" of military intelligence components, and "provide the doctrinal basis for U.S. military involvement in multinational and interagency operations." Like all military doctrine, it is "authoritative" and "will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise." This language might adequately address the doctrinal

---

[7] Starry, General Donn, U.S. Army (ret.), interview with author, January 22, 2003.

needs of military intelligence components, but what of the rest of the Intelligence Community? Neither the CIA nor the departmental intelligence organizations of the Departments of State, Homeland Security, or Energy or the Federal Bureau of Investigation would find such doctrine appropriate or helpful in guiding new behaviors within those cultures.

If revolutionary change is ever to permeate the entire intelligence enterprise, these impediments to the development of a common doctrine must be overcome. A common doctrine has been a missing component of reform efforts to date. When changes have been made by legislation or by new leadership, individual intelligence agencies and components have typically been left to interpret those changes on their own. It should come as no surprise, then, that the changes are often interpreted differently.

The first and most essential step to development of a new intelligence doctrine, then, is recognition by the Intelligence Community leadership that doctrine or something akin to it is needed. As soon as a new revolutionary strategy is developed, revolutionary doctrine should follow right behind it. The schools and the training institutions in the Intelligence Community, based on constant interaction with the architect and other important players in the change process, should lead this effort. If, for example, a decision is made to more tightly centralize the Intelligence Community, new doctrine must describe how activities are to be conducted under such a model. Even more important would be doctrine on how activities are to be conducted under a decentralized model—what security principles must be adhered to, who reviews assessments for accuracy, who shares what information with whom, and the like. Central to any revolutionary doctrine must be new principles related to timeliness, accuracy, integrity, collaboration, respect for individual privacy, risk-taking, and the like. These core principles must be closely integrated into the new concepts, strategies, and innovations needed to transform the intelligence enterprise.

Changing the leadership approach and organizational culture within a large institution is easier said than done, but it is essential to

completion of the transformation process. Organizational culture does not change without being replaced by some other form of behavior. Every intelligence officer in the 15 intelligence organizations needs to know how he or she will be expected to do his or her job differently to carry out the strategy. If formal doctrine and training do not provide this information, it must be made clear to those in the organization and to senior management what other mechanisms will.

IMPLEMENTING THE STRATEGY: TECHNOLOGICAL, OPERATIONAL, AND ORGANIZATIONAL INNOVATION

The development of new technology, or the innovative application of existing technology, is often the catalyst of revolutionary change. The recognition that a mission-related challenge cannot be met often drives this type of innovation. The Intelligence Community has traditionally been very good at developing innovative technology, particularly during the earlier RIA (discussed in the previous chapter).

During the decade of reduced or flat intelligence budgets in the 1990s, the ability to experiment and take risks with new technology was more limited. According to DCI George Tenet, the Intelligence Community is not operating under tight resource constraints at the moment,[8] so this appears to be another moment in time when a culture of technological innovation might once again flourish.

Since the 1980s, however, the government no longer has a monopoly on technology breakthroughs. Government organizations across the board now rely largely on commercial entities for innovation. This is particularly true in the areas of information technology, communications, and knowledge management, where there have been profound changes in the speed and quantity of data. The pace of these developments, which the government no longer controls, is now so rapid that it presents government institutions with the difficult challenge of rapidly changing its operational and organizational structures to keep

[8] Tenet, George J., "The Worldwide Threat in 2003: Evolving Dangers in a Complex World," testimony presented to U.S. Congress, February 11, 2003.

up with what technology has to offer. Furthermore, off-the-shelf technology does not always meet the government's specialized needs, and more time is spent customizing commercial products, which compounds the time lag.

For U.S. intelligence, it is necessary to develop integrated solutions to problems, rather than try to solve them with a single piece or type of technology. Furthermore, technological solutions must be in sync with operational and organizational adjustments. But this presents a particular challenge for a system not tied together by a common strategy. A common strategy would help the Intelligence Community make choices among all the technological innovations that arise, many of which are very expensive choices. Today, new technology applications are developed in insular organizational "stovepipes" and are not necessarily shared with others who could make use of them, or worse, are duplicated when duplication is unnecessary.

Organizations like the Intelligence Technology Integration Center will play a very important role in the Revolution in Intelligence Affairs because they not only scan the horizon for new technological opportunities but also can provide a forum for technologists to interact with analysts, linguists, case officers, line managers, and others. There must be a translation mechanism of some sort that will allow intelligence analysts and operators to describe what they need in a way that can be translated into new technology.

Which technologies (currently fielded or under development) have the potential to effect a dramatic change in the character and conduct of intelligence? The answer to this question could be instrumental to the RIA. However, areas of technological innovation that could lead to revolutionary breakthroughs cannot be explored in an unclassified publication such as this. But one important point learned from both defense and corporate transformation is that it is preferable for those involved in the transformation process to focus on as short a list of technology innovations as possible when it comes time to take the technology from research to actual applications. One failed experiment is a learning process; many failed experiments will break the bank. The Intelligence Community might do well to study the applications of

technologies that have formed the basis of recent innovations in military affairs and business affairs.

The Intelligence Community must also emulate, as much as possible, the culture that rewarded experimentation and risk during the first RIA following World War II. Congress must be a willing partner in this process and not punish those who experiment if the experiment does not pan out. There must be a way for the Intelligence Community to move on quickly if the technologies picked for experimentation prove to be the *wrong* ones. In the past, declining budgets, an over-reliance on industry to come up with new ideas, a lack of willingness to experiment, and reluctance to let go of technologies that have not "proven themselves" led the Intelligence Community to hang on to legacy systems and incremental improvements longer than it should have. The cautionary tale is that a government institution should never commit to overly complex technologies too soon because it is exceedingly difficult to terminate programs after they are funded over several years and are well underway. More experimentation, more often, and on a smaller scale, is essential to keeping pace with technological innovation and developing breakthrough applications.

Operational Innovation

The Intelligence Community does not typically attach the same priority to operational and organizational innovation as it does to technological innovation. However, new technologies may well require the development of innovative new intelligence functions and structures to bring about revolutionary change. Operational innovation within the Intelligence Community can be defined as significant change in intelligence processes and activities, which requires changing work practices as well as traditions, cultures, and learned experience. The challenge becomes exponentially more difficult when attempting to change functions and behaviors in more than one agency simultaneously, and has proven to be nearly impossible when attempting this effort across the entire intelligence enterprise.

Information sharing is a case in point. Up until ten years ago, sharing intelligence information rapidly across many agencies was a

fairly difficult technological exercise. Today, that is no longer the case; technology, for the most part, provides the means to make this happen. When information sharing and analytical collaboration do not happen today, it is largely because policies and procedures have not changed enough to establish new behaviors and change the way people do their work.

An example of a new operational innovation, therefore, might start with the determination at senior leadership levels that information technology *will* change the way the Intelligence Community operates, and from this point forward, information sharing and analytical collaboration *will* be a central part of the intelligence mission. Making this happen will require more than simply saying it will. It means shifting the doctrine of "need to know" to "need to share." It also means changing the mindset of many managers, data collectors, and analysts. As former ADCI for administration James Simon noted, "Despite periodic paeans to teamwork, analysts believe in their hearts that only *they* truly understand."[9] In other words, they are perfectly happy to arrive at their judgments alone. Some analysts feel that collaboration with others impedes or detracts from their work rather than enhances it. To change such attitudes, managers must ensure that they reward only the new and desired behaviors and not the old ones.

For the Intelligence Community, operational innovation must focus on changing and perhaps completely rethinking core functions, such as foreign intelligence collection, analysis, clandestine activities, data processing, dissemination, and scientific research and development, as well as "business" functions such as strategic planning, program and cost analysis, systems requirements and acquisition, performance evaluation, personnel management, and security. It should question whether existing functional distinctions—such as the distinction between collection and analysis—should continue to exist. Each of these activities, practices, and procedures should be examined in light of new

---

[9] Simon, James M. Jr., *Crucified on a Cross of Goldwater-Nichols,* Boston: The Center for Information Policy Research, Harvard University, July 2001, p. 4.

or even extant technologies that offer new ways of doing business. Too often, people are unwilling to give up comfortable and familiar old practices unless an intervention in the form of new doctrine, policy, or even legislation shakes things up.

During the 1990s, declining resources drove many of the operational changes in the Intelligence Community. Congressionally directed actions and budget decisions pushed real deadlines and real decisions and, as a result, much of the management focus, strategic thinking, and intellectual energy during the 1990s was devoted to acquisition, programming, and budgeting. This is what Congress and the OMB were paying attention to during the years of the hoped-for "peace dividend" and, therefore, it was what the Intelligence Community leadership paid attention to as well. Unfortunately, these changes lead to incremental improvements in existing processes and not the kind of change that would lead to an RIA.

True operational innovation should be driven not by diktat but by unmet challenges, new strategies, and new technological opportunities. Effective leaders will be required to reframe the thinking of the individuals they guide. Focused management attention and rewards for new behaviors are essential to implementing and completing the transformation process.

Organizational Innovation

"The lesson of September 11th," stated Senator Richard Shelby in his report on the events of 9/11, "should not be simply that we need to reform ourselves so as to be able to address the terrorist threat but also that we need an Intelligence Community agile enough to evolve as threats evolve, on a continuing basis. Otherwise, the IC will face little but a future punctuated by more intelligence failures, more Congressional inquiries, and more Commissions."[10]

---

[10] "September 11 and the Imperative of Reform in the U.S. Intelligence Community: Additional Views of Senator Richard C. Shelby, Vice Chairman, Senate Select Committee on Intelligence," excerpt, December 10, 2002, p. 27. Senator Shelby served as the vice chairman of the Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001.

How should the Intelligence Community be organized in an age when producers and consumers of both raw and finished intelligence are proliferating rapidly and are likely to continue to do so? Or when roles and missions change rapidly and wax and wane in importance? Over the past decade, much of the debate about how to "reform" intelligence has centered on reorganizing the Intelligence Community. In addition to centralizing intelligence under a DNI, new reorganization schemes that group activities by intelligence missions or by transnational topics that cross multiple agencies have all been contemplated.

Organizational innovation, however, requires much more than "rewiring" the organizational charts. If a true Revolution in Intelligence Affairs is to take place, and new missions, roles, and functions are to be established, some organizations should grow, some should stay the same, and some should go away, depending on their relevance to fulfilling new tasks. Form should follow function.

In the wake of September 11, a number of new entities that are either producers or consumers of intelligence have sprung up to address new tasks related to homeland security and the terrorist threat. Few attempts appear to have been made to carefully design these new entities as part of a larger, integrated system. Rather, different advocates had different solutions to the same problems, and if they were powerful enough, they each prevailed. As a result, many of the responsibilities and authorities, and much of the overlap in jurisdiction, have yet to be sorted out.

As Senator Shelby suggests, if all of the current focus on intelligence reform yields nothing more than a new blueprint drafted for dealing with the terrorist threat, the reform effort is likely to be overtaken by events before it is even partially implemented. Over the course of the next few years, for example, it will be interesting to see the impact that a new Cabinet-level department——the Department of Homeland Security (DHS)——will have on intelligence organizations. Today, a number of the intelligence agencies are designated "combat support agencies" and see the Department of Defense as their primary customer. How many of these agencies will also support DHS? Will they give DHS the same attention and priority they give to the Department of Defense? If

not, the proliferation of intelligence organizations is likely to continue as new ones are formed to address DHS requirements.

It will likewise be interesting to watch the development of another new organization, the Office of the Undersecretary of Defense for Intelligence (USDI). Until recently, intelligence was one of several responsibilities under the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. "The USDI was created because the Secretary of Defense takes intelligence very seriously," said Richard Haver, former special assistant to the Secretary of Defense for Intelligence. "He sees intelligence as a core competency, and 'Undersecretaries' do not get ignored."[11] The new USDI has a particular interest in the transformation of intelligence activities that will support a transformed U.S. military. How much of intelligence transformation will be driven by the USDI, rather than the Intelligence Community, remains to be seen.

It would be far better to first focus the energy of an RIA on devising new strategy and doctrine and other innovations to address the vast array of intelligence missions than to begin with reorganization. Until these first steps are completed, it is difficult to know if some organizational elements need to remain intact and if there might be good reasons why they cannot or should not be changed. None of the transformations examined in the case studies discussed in the previous chapter began with a large-scale reorganization. Because reorganizations cause so much anxiety and disruption in the workforce, they should be undertaken only if absolutely necessary.

An important part of the RIA should be a search for "information-age" organizational models that are functioning well today that could serve as a template for intelligence transformation. Complex adaptive systems or networks, for example, might prove to be more appropriate than industrial-age, hierarchical models. Flexibility and adaptability of design are essential.

---

[11] Haver, Richard, former Special Assistant to the Secretary of Defense for Intelligence, interview with author, January 23, 2003.

EVALUATING AND IMPLEMENTING CHANGE PROPOSALS

The next step in the dynamic-change management process is to ensure that revolutionary change proposals are objectively evaluated to determine if they will lead to desired transformational outcomes. One of the real downsides of revolutionary change is that it is entirely possible to make a strategic blunder and take the wrong course of action. There may be serious consequences that result from revolutionary change, *and* it might take a long time to recover from them. The public has little tolerance for government agencies that devote people and resources to activities that appear to have wasted the taxpayers' dollars.

Is it possible then, before embarking on a revolutionary course of action, to accurately assess the outcome? Can the Intelligence Community set up an evaluation process or analytical framework that will allow its organizations to experiment and take risks, assess their progress toward stated goals, and then change course fairly easily if necessary? Is there a way to avoid mistakes before even proceeding? The answers to these questions should be the responsibility of the RIA change manager.

This subsection lays out a five-step framework that can help a change manager or anyone else who wishes to evaluate change proposals to ensure that the outcome produces the transformation everyone desires. The framework can be used to objectively assess change proposals as sweeping as proposals related to the establishment of a director of national intelligence or to organizing intelligence analysis and planning around missions, or to proposals as specific as creating a new Intelligence Community security system. The five steps in the framework are as follows:

1. **Understand and verify the impetus for change.** What is the context for this change? What is the scope of what it is trying to address?
2. **Clarify mission and business objectives.** What impact will this proposal have on meeting overarching intelligence objectives?
3. **Evaluate proposed innovations.** Which are the best choices?

4. **Determine utility**. Will this change actually improve intelligence performance?
5. **Assess feasibility,** What is the likelihood this transformation can be achieved?

It is important to note that an evaluation process that critiques change proposals is not a substitute for solid, strategic thinking that *generates* change proposals. Generating a revolutionary change proposal or series of revolutionary change proposals requires a combination of talented people at all levels of the organization who can think and challenge the status quo. In an ideal situation, the RIA architect would be responsible for *generating* systemic change proposals, while the change manager would be responsible for objectively evaluating them and overseeing their implementation. The rest of the coalition for change should weigh in on both undertakings.

Understand and Communicate the Impetus for Change

Helping the Intelligence Community workforce understand what motivated a revolutionary change proposal is so important that no evaluation should begin without a thorough investigation and articulation of the "who, what, and why" behind the proposed change. Are the proposed changes designed to address a specific problem or a systemic problem? For example, the proposal to create a Terrorism Threat Integration Center in the aftermath of September 11 was generated to specifically address a perceived problem in integrating terrorism threat data. The proposals related to establishing a director of national intelligence, on the other hand, are motivated by the perception that an individual who is at once both head of the Intelligence Community and head of the CIA cannot manage the Intelligence Community.

Understanding the motivation behind a change proposal helps the intelligence workforce to better understand the problem, issue, or opportunity the change proposal is attempting to address. If the change proposal is not self-initiated, it should be made clear what other factors are motivating the proposed change. Those factors may be legal, political, economic, technological, sociological, or jurisdictional. If

a change proposal seems to be motivated largely by politics, for example, considerable groundwork would need to be done to get the buy-in from the workforce that is needed to actually implement the change effectively. Similarly, for example, if the workforce does not accept that a certain event was the result of an intelligence "failure," the proposed fix to prevent another such failure may not be well accepted.

In an ideal world, revolutionary change proposals would be generated by the Intelligence Community's own dynamic change process that includes many outside participants. One or more revolutionary change proposals would be rapidly generated whenever there appears to be an unexpected, discontinuous change in the external environment. The change proposals would be motivated by the identification of a significantly new or different challenge—with the intent to *preclude* an intelligence failure. Ideally, an entity such as the National Intelligence Council, along with a group of outside experts, would undertake broad "scans" of the security environment (e.g., such as the NIC's Global Trends process)[12] not every five years but whenever a significant discontinuous event occurs.

The evolving security context summarized earlier in this report is one example of an exercise in discontinuous trend analysis, although other trends might be examined regularly (e.g., cross-border insurgencies, human trafficking, piracy, global warming, spread of civil violence). The eight trends outlined in Chapter 1 can be further developed and extrapolated to contemplate the most serious new challenges that intelligence may face far over the horizon (10 to 20 years out). The Intelligence Community would then contemplate *new* core competencies for intelligence that might be required to keep it two steps ahead of any adversary. To take the first of the eight trends as an example, the dangers presented by super-empowered individuals and weapons of mass destruction, if taken to their logical conclusion, will be a global problem, not simply a U.S. problem. Therefore, those involved in the dynamic change process would question a number of

---

[12] National Intelligence Council, *Global Trends 2015: A Dialogue About the Future with Nongovernment Experts*, December 2000 (http://www.cia.gov/nic/NIC_globaltrend2015.html).

current assumptions. Will the United States one day need to be part of a larger international intelligence enterprise? If so, should it be part of an intelligence alliance that addresses an even larger set of threats, from poverty to virulent diseases to environmental hazards? How such threats will be addressed in the future are policy decisions, but some form of "intelligence" will always be needed in whatever security regime develops. The RIA debate should include consideration of new decisions that would have to be made regarding the sharing of intelligence within such an alliance *before* deciding to participate in such an alliance.

With regard to the changing nature of warfare, warfighting concepts such as effects-based operations, operational net assessment, and full spectrum dominance are all highly dependent on intelligence that will be far different from the type of military intelligence performed in the past. Consideration of these trends suggests that knowledge of language, culture, and history are going to be as important, if not more important, than the kinds of expertise the Intelligence Community has emphasized in the past.[13] Intelligence will also prove to be increasingly important as foreign reactions to U.S. defense transformation begin to manifest themselves. Few countries, if any, have the economic means to build and maintain a fighting force equal to that of the U.S. and thus are more likely to innovate and develop asymmetric means to counter overwhelming U.S. force. Such asymmetric responses—whether undertaken by states or nonstate actors—are becoming the dominant characteristic of most threats to the United States. Thus, the potential for a technological breakthrough or surprise by an adversary cannot be ignored. Being able to recognize an embryonic foreign RMA may be among the intelligence challenges of the future.

A scan of the future environment would also shed light on rapidly changing concepts in international and national security policy as well as futurist views of military strategy, doctrine, and tactics. A scan of this environment would include taking account of potential technology

---

[13] Murray, Williamson, *Transformation Concepts for National Security in the 21st Century,* Carlisle, Pa.: Strategic Studies Institute of the U.S. Army war College, September 2002, p.16.

breakthroughs that could transform the battlefield and the intangibles that factor into combat, such as motives, politics, loyalties, religious views, levels of education and training, information, and media sources. The strategic dialogue between the Department of Defense and the Intelligence Community must be thorough and continuous.

In the future, populating databases related to potential terrorists or critical infrastructure vulnerabilities is likely to be just as labor intensive and demanding as populating databases on foreign weapons systems and military forces. The need for real-time and highly accurate intelligence of a completely different nature than that of military intelligence is likely to continue to grow, as will the numbers of customers in the homeland security, diplomatic, and law-enforcement communities. The strategic dialogue with these consumers of intelligence also must be thorough and continuous.

Once these scans of the future environment are completed, the dynamic change process would go beyond simply looking at the context for the change and begin a process of critical self-examination by asking questions such as the following:

- Is there a sense that there is a mission, or missions, that the Intelligence Community could not successfully accomplish today or tomorrow because of significantly changing events?
- Is there an impetus for change felt by enough members of the Community to overcome the resistance of those who believe otherwise?

With this survey and assessment as a backdrop, Intelligence Community leaders should regularly and systematically go through a self-appraisal process that will help to anticipate future performance. This can be done through exercises, red teaming, modeling, simulation, and other methods. The insights drawn from this analysis would illuminate the mismatches between what intelligence is, does, and will be expected to do, and what is in fact the current reality as well as currently envisioned end state. This type of exercise should constantly be done, even when the Intelligence Community is performing flawlessly.

The final task in step one of evaluating a change proposal is to determine the intended linkage between the change proposal being considered and the projected outcomes. Which existing or future problems is the proposal trying to solve? Can a plausible case be established that the change will have the intended effect? Is there historical evidence that such a change has succeeded in bringing about the desired outcome when implemented in the past? A good theoretical base can help predict the likelihood of a particular intervention leading to a expected outcome.

Clarify Objectives

The next step in the evaluation process is to understand what a specific revolutionary change proposal hopes to achieve in transforming existing systems, operations, and organizations. Is the objective to radically change mission performance—e.g. providing timely, specific information to warfighters, or warning of an impending attack? Or is it to improve business performance, i.e., the acquisition of new intelligence technology, information sharing, analytical collaboration, data processing, and the like? Will transformation efforts encompass both? Clearly determining and articulating objectives allows one to determine the victory conditions, which are critically important to all those affected by the transformation process. The development of an overarching strategy for achieving both mission and business objectives is an essential element of the transformation process.

Although a new National Security Strategy comes out every year, the strategy published in 2002 was the first one published in the wake of the September 11 attacks. If one assumes that threats from super-empowered individuals will be with us for a while, one may further assume that many of the objectives articulated in the Strategy are likely to be with us for a while.

Intelligence missions are derived from national security missions. The 2002 National Security Strategy describes a set of missions that are different from those articulated in past strategies, particularly in terms of priority:

- defeat global terrorism
- prevent attacks on the homeland
- prevent attacks on our friends and allies
- defuse regional conflicts
- prevent adversaries from acquiring WMD
- develop agendas for cooperative action
- reassure allies and friends
- dissuade future military competition
- decisively defeat adversaries if deterrence fails.

Intelligence has a role to play in supporting each of one these national security missions. Examining the role intelligence should play in supporting these missions in the future, as well as potential new missions that have not yet fully matured, will be critical to clearly articulating what an RIA could achieve. It is important during this process to stretch the mind to think about what could possibly be done to meet challenges never met before—those things that typically fall into the "too hard" category.

It is also important to clarify the business objectives in the transformation process. Which internal intelligence processes will need to improve significantly? Are there new processes or ways of doing business that will be created? An illustrative list of intelligence business objectives might include the following:

- streamline response time to key customers
- adapt more quickly to unanticipated threats
- improve sharing of information internally
- develop new analytical methods
- improve language skills
- enhance diversity of workforce
- improve analytical depth in certain areas
- innovate more quickly (technologically, operationally, organizationally)

- improve collaboration with intelligence customers in meeting mission demands
- better integrate intelligence and operations.

In the process of clearly articulating both mission and business objectives, some thought must be given to measuring progress in meeting these objectives. The contributions of intelligence are particularly difficult to measure. Some things, like improvements in mission performance, or improvements in the quality of analysis presented to decisionmakers, are not easily quantifiable, nor are the data that would need to be compiled easily attainable. But for a transformation effort to be successful, the Intelligence Community will need to both demonstrate dramatic improvement in performance and recognize small victories along the way, or the workforce will become frustrated with the transformation process. There will be a need to keep track of some data, but not an unreasonable amount, to determine forward progress. The challenge is to identify a handful of tangible differences that are critical to the success of the overall effort. Some of these may be quantifiable, like the number of terrorists captured, or attacks disrupted. Others, such as quality of the intelligence that leads to an important policy decision, will not be. But informally gathering data from customers on policy decisions made on the basis of good intelligence, and its impact on overall mission success, is one way of attempting to measure success by other than quantifiable means.

Today, the only metric that the American public is typically aware of is the number of intelligence failures. This does not further help the cause of a reasoned and reasonable debate. It would be an important by-product of the dynamic change process to somehow reference the occasion, if not the specifics, of intelligence successes.

Evaluate Proposed Innovations

If the dynamic change process does lead to a "Revolution in Intelligence Affairs," innovations in technology, operations, and organizations will be essential components of the RIA. The evaluation of proposed innovations is the responsibility of the architect. In his

books on fast tanks and heavy bombers, historian David Johnson describes how the U.S. Army infantry fought with the cavalry over how to best use tanks.[14] Each saw the tank as only a way of complementing how they already waged combat; neither could conceive of using it in a completely new way.

Part of the architect's responsibility is to evaluate proposed innovations in the context of new theory, strategy, and doctrine. How will a proposed new technology give us a fresh approach to meeting enduring challenges? How might this technology allow the Intelligence Community to collect and process data better? What proposed changes in intelligence operations, processes, and activities would allow the Intelligence Community to maximize these technological opportunities? Is this innovation feasible? Is it affordable? How perishable is it? The key to answering these questions will be for someone—preferably the architect—to describe how intelligence work will be performed and organized differently around the new technology. Every attempt should be made to gain this understanding before the transformation process proceeds.

The architect should also ascertain whether there is a "sunset clause" or exit strategy that can be used if an innovation does not work. An important component of an environment that is conducive to experimentation and risk-taking is the ability to "pull the plug"—at the appropriate time—if an innovation does not appear to be working or is unlikely to bear fruit.

Determine Utility

The fourth step in the evaluation process is to determine how useful a revolutionary change proposal will be. During the 1990s, many of the change proposals were made on the basis of achieving efficiencies. The downsizing and outsourcing of intelligence was driven by the overarching objective of achieving a peace dividend that could be applied to domestic spending. Thus, those change proposals that resulted in fewer people and organizations, scaled-down projects, or reduced budgets were useful in achieving that higher goal. Today, the primary

[14] Johnson, David E., Fast Tanks and Heavy Bombers: Innovation in the US Army, 1917-1945, Cornell Studies in Security Affairs, n.d.

goal is mission effectiveness, and cost is a secondary consideration (a condition that is not likely to last for long). The next round of change proposals will be most useful if the proposals strike a balance between maximum efficiency and maximum effectiveness.

To determine the utility of change proposals, certain questions must be answered in regard to improving effectiveness and efficiency:

In Improving Effectiveness:

- Will we meet the mission objectives better than we can today?
- Will we meet the business objectives better than we can today?
- Will this give us a specific advantage over our adversaries?
- Will this better position us to meet new or unanticipated challenges?

In Improving Efficiency:

- Will this allow us to do the job with the same or fewer people?
- Will this allow us to do the job with the same or fewer dollars?

For reasons stated earlier, it is always much easier to measure efficiency than effectiveness in the intelligence world. To evaluate how much more effective U.S. intelligence will be at the end of a transformation process, it will be necessary to describe what is meant by the "quality" of knowledge, or productivity, in the intelligence business. Is quality the equivalent of accuracy? Or is it a combination of timeliness and accuracy? Is it the ability to influence a decision? Does it include good writing? Must it have analytical depth? Is it a combination of all these things? Determining "productivity" is also problematic, because an increase in the data collected, or an increase in analytical reports or products, is not necessarily indicative of improved intelligence.

Determine Feasibility

The final step in the evaluation process should be to determine the likelihood that the transformation can be brought to fruition. The earlier examination of case studies and historical patterns that preceded successful transformations is illuminating in that it helps to identify the necessary internal and external conditions that most often are the precursors to successful revolutionary change.

The final step in the evaluation process could begin by asking the following ten questions to assess whether the necessary conditions for change are in place:[15]

1. Is there a clear and compelling *impetus* to change--i.e., a mission or threat that cannot be met as the organization is currently structured and operating?
2. Is there a new *strategy* for meeting those missions or threats?
3. Is there an institutional *"doctrine"* that spells out the behaviors necessary to support the new strategy?
4. Does the environment encourage technological, operational, *and* organizational *innovation* and a willingness to take risks?
5. Is there a visionary or *"architect"* that can draw up parameters for change and communicate clearly to the workforce and others what needs to be done?
6. Is there a process for building *consensus* on what change is needed and how it should be adopted?
7. Is there a *champion,* or champions, at the top who will help overcome institutional resistance?

[15] A number of these criteria has been adapted from the Starry-Wass de Czege paradigm discussed in the previous chapter of this report; Morris, Rodler F., Scott W. Lackey, George J. Mordica II, and J. Patrick Hughes, *Initial Impressions Report: Changing the Army*, Center for Army Lessons Learned, forthcoming. Also see Hundley, Richard O., *Past Revolutions, Future Transformations*: *What Can the History of Revolutions in Military Affairs Tell Us About Transforming the U.S. Military?* Santa Monica, Calif.: RAND Corporation, MR-1029-DARPA, 1999, Chapter 6.

8. Will the organization follow a *spiral,* rather than linear, approach to testing, evaluating, adjusting, accepting or rejecting, and then implementing proposed innovations?
9. Is there *leadership continuity,* to bring consistency to the process of change over time?
10. Are there *outside advocates and supporters* of proposed changes that will help generate new ideas and overcome institutional barriers?

In sum, the dynamic change management process must have a way to objectively evaluate change proposals—both those generated by a revolutionary "coalition for change" as well as those motivated by reformers with more limited objectives. The RIA advocates must have a way to convince those who are skeptical that in the end things will not only be very different, but much better, as a result of revolutionary change. The Intelligence Community will respond far better to a change proposal that is grounded in a serious, analytical approach. The approach recommended here could serve as a straw man for developing that analytical approach.

Experimental Designs and New Performance Measures

The Intelligence Community must find ways to experiment a great deal more, not only in technology but also in new operating concepts, new security measures, new personnel systems, and new organizational structures. This is the best way to try out a revolutionary concept before the entire enterprise commits to it. This approach worked well during the first "RIA" after World War II when new reconnaissance techniques, new tradecraft, and new organizations that eventually became the CIA and the NSA were created. The approach at that time was to push forward bold new ideas, however imperfect, and then improve upon them as time went on. This approach requires a willingness to take risks—financial risks, career risks, and perhaps other risks. Congress, OMB, and other overseers would need to accept such an approach and support it financially.

Greater experimentation, the use of pilot projects, modeling and simulation, scenarios, war games, exercises, and the like will be successful, however, only if a rigorous evaluation process guides experimentation, and good performance measures are established up front. Today, every organization in the Intelligence Community does this differently. For an RIA to take place, the architect must help choose and guide the RIA experiments and, working with the change manager, he or she must ensure that a rigorous evaluation process is in place. The architect and change manager must then help select the best of these experimental efforts, giving them an RIA "gold star" of approval to signify that they have been through a thorough vetting process, and making those efforts compete directly against current practices and activities for funding and personnel. These experiments should then lead to the creation of competitive activities and organizations that, if successful, will grow and supplant outdated ones.

New Incentives and Rewards for Embracing Change

The final step in the RIA is to ensure that there are incentives for workers at all levels, particularly for middle managers, to embrace this new approach to change. If the Intelligence Community is to enter a period of dynamic, continuous change that will lead to a Revolution in Intelligence Affairs, the intelligence workforce must stay engaged and committed, and not lapse into "change fatigue." Change must continue after current political leaders move on. Constancy of leadership and purpose is essential. Small victories accomplished along the way must be celebrated from the top on down.

This is easier said than done. The key is to hire middle managers and supervisors who are models of resilience and adaptability and move those who are not. Today, most intelligence managers and supervisors are promoted because of their expertise in one of the intelligence functional areas, not necessarily because they have a broad grasp of intelligence functions and organizations, understand when to leave parochial interests at the door, or are particularly skillful in questioning their own business practices and conducting real lessons learned. What are needed are managers and supervisors who understand the

strategic objectives of the RIA and can translate them into the new behaviors they expect of the people they supervise.

If an RIA is to take place, the Intelligence Community must begin to hire, reward, and promote people with new skills and ideas and novel ways of thinking. In particular, the Community must hire, reward, and promote managers who are adept at managing change and who seek similar skills and abilities in those they supervise. Everyone in the Intelligence Community knows who these people are, even today. The RIA will not take place until these people are in visible positions of authority.

The challenges and opportunities outlined in this report are too important and too complex to be solved by one person or even a small group—they require serious and deliberate thinking on the part of many people at all levels both within and outside of the government. Only when a critical mass of people interested in a better intelligence capability in the future comes together and resolves to design and implement change will the RIA truly be underway.

SUMMARY

The Intelligence Community has a particular responsibility to change not *with* the times, but *ahead* of the times. This report argues that the U.S. Intelligence Community must undergo a Revolution in Intelligence Affairs to address the difficult issues facing the U.S. Intelligence Community of the future. To achieve an RIA, there must be a dynamic change management process within the Intelligence Community that constantly reassesses the need for change and generates bold and unique solutions. This process, which constantly generates options for *revolutionary* change, must be allowed to exist in parallel with the *evolutionary* change process—not only when a discontinuous change occurs, but all the time. Thus, if a revolutionary approach is needed, it does not need to be generated from scratch after it may be too late to prevent an intelligence failure. The revolutionary process should involve enough outsiders and contrarians to ensure that a completely different way of doing business is *always* considered.

Without a more strategic examination of the intelligence apparatus, it is possible that proposed changes in policy or legislation might degrade the Community's ability to perform some missions while improving others. Perhaps thinking of the Intelligence Community as the U.S. Intelligence *System* instead might encourage whole-system thinking, such as a Venn diagram of overlapping circles rather than a diagram composed of straight lines and boxes. A whole-system approach might also encourage a diagnosis of what is wrong with the system, rather than what is wrong with its piece parts.

Revolutionary change in the Intelligence Community will no doubt be very difficult to bring about. It will require significant time and attention on the part of management. It must involve *real* change--it cannot be merely a political tactic or a quick fix. It will require consistent senior-level attention within the Intelligence Community and long-term Congressional, Executive Branch, and external support. It may take time to bring the Revolution in Intelligence Affairs to fruition, but it is a matter of urgency to begin the revolution today.

REFERENCES

Berkowitz, Bruce D., and Allen E. Goodman, *Best Truths: Intelligence in the Information* Age, New Haven, Conn.: Yale University Press, 2000.

Bissell, Richard M., Jr., *Reflection of a Cold Warrior: From Yalta to the Bay of Pigs,* New Haven, Conn.: Yale University Press, 1996.

Central Intelligence Agency, Office of Public Affairs, *A Consumer's Guide to Intelligence,* Washington, D.C.: CIA, 1994.

Center for the Study of Intelligence Publications Web site, (http://www.cia.gov/csi/pubs.html).

Christensen, Clayton, *Innovator's Dilemma: When New Technologies Cause Great Firms to Fall,* Boston: Harvard Business School Press, 1997.

Clift, A. Denis, president, Joint Military Intelligence College, interview with author, Joint Military Intelligence College, Washington, D.C., January 6, 2003.

Conner, Daryl R., *Managing at the Speed of Change: How Resilient Managers Succeed and Prosper Where Others Fail*, New York: Villard Books, 1992.

Coram, Robert, *Boyd: The Fighter Pilot Who Changed the Art of War*, Boston: Little Brown and Company, 2002.

D'Amato, First Lieutenant Martin J., "Vigilant Warrior: General Donn A. Starry's AirLand Battle and How it Changed the Army," *Armor*, May-June 2000.

Defense and the National Interest Web site (http://www.d-n-i.net/second_level/boyd_military.htm).

"DIA Workforce of the Future: Creating the Future of the Defense Intelligence Agency," DIA internal publication, May 15, 2003.

Donovan, William, memorandum to Harold Smith, White House Bureau of Budget, August 25, 1945, reprinted in Department of State, *Foreign Relations of the United States, 1945-1950, Emergence of the Intelligence Establishment*, Washington, D.C.: Government Printing Office, 1996.

Drucker, Peter, *Managing in a Time of Great Change*, New York: Truman Talley Books/Dutton, 1999.

Duck, Jeanie Daniel, *The Change Monster*, New York: Crown Business, Random House Publishing, 2001.

"Establishment of a Central Intelligence Agency Upon Liquidation of OSS," Joint Chiefs of Staff Report, September 19, 1945, reprinted in Department of State, *Foreign Relations of the United States, 1945-1950, Emergence of the Intelligence Establishment*, Washington, D.C.: Government Printing Office, 1996.

Fallows, James, "The Muscle-Bound Superpower," *Atlantic Monthly,* October 2, 1979.

Fallows, James, "National Defense," *Commentary,* Vol. 72, No. 2, August 1981.

Friedman, Thomas, *The Lexus and the Olive Tree*, New York: Anchor Books, 2000.

Gates, Bill, *Business at the Speed of Thought: Succeeding in the Digital Economy*, New York: Warner Books, Inc., 1999.

Gentry, John A., "A Framework for Reform of the U.S. Intelligence Community," prepared for the Brown-Aspin Commission on the Roles and Capabilities of the United States Intelligence Community, June 6, 1995 (from Federation of American Scientists [FAS] Web site, www.fas.org/irp/gentry/index/html).

Gilmore Commission, *Implementing the National Strategy: Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction,* December 15, 2002 (http://www.rand.org/nsrd/terrpanel/).

Grabo, Cynthia M., and Jan Goldman, *Anticipating Surprise: Analysis for Strategic Warning*, Washington, D.C.: Joint Military Intelligence College, March 2002.

Grey, Colin S., *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History,* London: Frank Cass Publishers, 2002.

Grove, Andrew S., *Only the Paranoid Survive: How to Exploit the Crisis Points that Challenge Every Company and Career*, New York: Currency Doubleday, 1999.

Hamel, Gary, *Leading the Revolution*, Boston: Harvard Business School Press, 2000.

Harknett, Richard J., and the Joint Center for International Security Studies, "The Risks of a Networked Military," *Orbis*, Winter 2000.

Haver, Richard, former special assistant to the secretary of defense for intelligence, interview with author, Washington, D.C., January 23, 2003.

Hinsley, Sir Harry, "World War II: An Intelligence Revolution," *The Intelligence Revolution: A Historical Perspective, Proceedings of the Thirteenth Military History Symposium*, 31st Harmon Memorial Lecture Series, Colorado Springs, Colo.: U.S. Air Force Academy, October 12-14, 1988.

Hoffman, Bruce, interview with author, RAND Corporation, Washington D.C., January 2003.

Hughes, Lt. Gen. Patrick, former director of DIA, U.S. Army (ret.), interview with author, Washington, D.C., March 7, 2003.

Hundley, Richard O., *Past Revolutions, Future Transformations*: *What Can the History of Revolutions in Military Affairs Tell Us About Transforming the U.S. Military?* Santa Monica, Calif.: RAND Corporation, MR-1029-DARPA, 1999.

Jacoby, Lowell E., vice admiral and director of Defense Intelligence Agency, interview with author, Washington, D.C., March 12, 2003.

Jay, Antony, *Management and Machiavelli: Discovering a New Science of Management in the Timeless Principles of Statecraft,* Amsterdam: Pfeiffer & Company, 1994.

Johnson, David E., *Fast Tanks and Heavy Bombers: Innovation in the US Army, 1917-1945,* Cornell Studies in Security Affairs, n.d.

Johnson, Loch, "Bricks and Mortar for a Theory of Intelligence," C*omparative Strategy*, Vol. 22, 2003.

Kaye, Beverly, and Sharon Jordan-Evans, *Love 'em or Lose 'em; Getting Good People to Stay*, San Francisco: Berrett-Koehler Publishers, Inc., 1999.

Kent, Sherman, "The Need for an Intelligence Literature," *Studies in Intelligence*, September 1955, reprinted in *Sherman Kent and the Board of National Estimates Collected Essays,* Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency, 1994.

Kent, Sherman, *Strategic Intelligence for American World Policy,* New Haven, Conn.: Yale University Press, 1949.

Kindsvater, Larry C., "The Need to Reorganize the Intelligence Community: A Senior Officer's Perspective," *Studies in Intelligence,* Central Intelligence Agency, Vol. 47, No. 1, 2003.

Knox, MacGregor, and Williamson Murray, *The Dynamics of Military Revolution*, Cambridge, UK: Cambridge University Press, 2001.

Kotter, John, "Leading Change: Why Transformation Efforts Fail," *Harvard Business Review*, March-April 1995.

Krepinevich, Andrew, "*The Military-Technical Revolution: A Preliminary Assessment,* Washington D.C.: Department of Defense, Office of Net Assessment, July 1992.

Krepinevich, Andrew, interview with author, Center for Strategic and Budgetary Assessment, Washington, D.C., February 12, 2003.

Kuhn, Thomas, *The Structure of Scientific Revolutions*, Chicago: The University of Chicago Press, 1962.

Laquer, Walter, *A World of Secrets: The Uses and Limits of Intelligence*, New York: Basic Books, 1985.

Lehman, John, and Harvey Sicherman, "America the Vulnerable," in *America the Vulnerable*, Philadelphia: Foreign Policy Research Institute, 2002.

Locher, James R. III, "Has It Worked? The Goldwater-Nichols Reorganization Act," *Naval War College Review*, Autumn 2001.

Locher, James R. III, *Victory on the Potomac*, College Station, Tex.: Texas A&M University Press, 2002.

Morris, Rodler F., Scott W. Lackey, George J. Mordica II, and J. Patrick Hughes, *Initial Impressions Report: Changing the Army,* Fort Leavenworth, Kan.: Center for Army Lessons Learned, December 1996.

Murray, Williamson, *Transformation Concepts for National Security in the 21st Century,* Carlisle, Pa.: Strategic Studies Institute of the U.S. Army War College, September 2002.

National Intelligence Council, *Global Trends 2015: A Dialogue About the Future with Nongovernment Experts*, Washington, D.C.: NIC, December 2000, p. 14.

O'Connell, Kevin M., and Robert T. Tomes, "Keeping the Information Edge," *Policy Review,* December 2003–January 2004 (http://www.policyreview.org/dec03/oconnell.html).

Pavitt, James L., speech to the Standing Committee on Law and National Security Breakfast Program, American Bar Association, January 23, 2003.

Pedlow, Gregory W., and Donald E. Welzenbach, *The CIA and the U-2 Program: 1954-1974*, Washington D.C.: Center for the Study of Intelligence, Central Intelligence Agency, 1998.

Ranelagh, John, *The Agency: The Rise and Decline of the CIA,* New York: Simon & Schuster, 1986.

Rumsfeld, Donald H., "Transforming the Military," *Foreign Affairs,* May–June 2002.

"September 11 and the Imperative of Reform in the U.S. Intelligence Community: Additional Views of Senator Richard C. Shelby, Vice Chairman, Senate Select Committee on Intelligence," in U.S. Senate Select Committee on Intelligence and U.S. Permanent Select Committee on Intelligence, *Congressional Reports: Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks* of *September 11, 2001*, December 2002 (at GPO Access Web site, http://www.gpoaccess.gov/serialset/creports/911.html).

Simon, James M. Jr., "Crucified on a Cross of Goldwater-Nichols," incidental paper, Cambridge, Mass.: Center for Information Policy Research, Harvard University, July 2001.

Starry, General Donn A., U.S. Army, "Extending the Battlefield," *Military Review,* March 1981.

Starry, General Donn, U.S. Army (ret.), interview with author, Fairfax, Va., January 22, 2003.

Steinbruner, John D., *Principles of Global Security,* Washington, D.C.: Brookings Institution Press, 2000.

Strategic Intelligence Web site, The Loyola College Department of Political Science (http://www.loyola.edu/dept/politics/intel.html).

Tenet, George J., "The Worldwide Threat in 2003: Evolving Dangers in a Complex World," testimony presented to U.S. Congress, February 11, 2003.

Toffler, Alvin, *Future Shock*, New York: Random House, 1970.

Toffler, Alvin, and Heidi Toffler, *War and Anti-War*, New York: Warner Books, 1993.

Treverton, Gregory F., *Reshaping National Intelligence for an Age of Information*, Cambridge, UK: Cambridge University Press, 2003.

Turner, Chris, *All Hat and No Cattle: Shaking Up the System and Making a Difference at Work*, New York: Perseus Books, 1999.

U.S. Senate Select Committee on Intelligence and U.S. Permanent Select Committee on Intelligence, *Congressional Reports: Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks* of *September 11, 2001*, December 2002 (at GPO Access Web site, http://www.gpoaccess.gov/serialset/creports/911.html).

Warner, Michael, "Wanted: A Definition of Intelligence," *Studies in Intelligence,* Central Intelligence Agency, Vol. 46, No. 3, 2002.

The White House, President George W. Bush, *The National Security Strategy of the United States of America,* September 2002 (http://www.whitehouse.gov/nsc/nss.html).

"Written Statement for the Record of the Director of Central Intelligence Before the Joint Inquiry Committee," October 17, 2002 (http://www.fas.org/irp/congress/2002_hr/101702tenet.html).

Zegart, Amy, *Flawed by Design: The Evolution of the CIA, JCS, and NSC*, Stanford, Calif.: Stanford University Press, 1999.