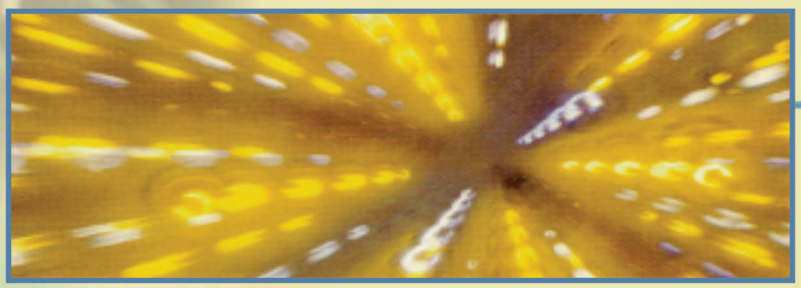


DIA WORKFORCE OF THE FUTURE

CREATING THE FUTURE OF THE DEFENSE INTELLIGENCE AGENCY

Acknowledgements

DIA WORKFORCE OF THE FUTURE:

CREATING THE FUTURE OF THE DEFENSE INTELLIGENCE AGENCY

May 15, 2003

This White Paper was prepared by

Toffler Associates®
Jeff Barnett
Ian Bramson
Dr. Jae Engelbrecht
Dennis Kirk
Alexander Shartsis
Dick Szafranski

and

Dove Consulting
John Theriault

With the assistance of the
Defense Intelligence Agency Workforce Planning Project Team

Drew Bewick
Diana Bradham
Marty Emory
Frank Esquivel
Dan Hooton

TOFFLER ASSOCIATES®

DOVE CONSULTING

CONTENTS

EXECUTIVE SUMMARY 1
Introduction 1
Competition 1
The Future Environment 1
Technology 2
Explosive Growth: Get Real 4
Precision Intelligence 5
Process 5
Timely and Timeless Business Ideas 5
Structure 5
Attachés 6
Partnerships 7
People 7
The Beginning of the Workforce of the Future 7
Intelligence for Cause and Effects 8
Strategy 8
Successful Transformation: According to the General Accounting Office 9
The Not-So-New Strategy of Prevention 9
Summary and Recommendations: Getting to the Future with a Sense of Urgency 9
Begin Building a Cadre of Experts 10

INTRODUCTION 11
Everything Is Changing Simultaneously 12
Creating the Future Demands Insight and Integrated Strategic Movement 12
"The Reformer Has Enemies in All Those Who Profit by the Old Order" 13
And Even If You Do It All Right, It Could Turn Out All Wrong 15

THE FUTURE ENVIRONMENT 17
A New World 18
The Globalizing Information Economy 19
The Hyper-Empowered 19
The Emerging Information Age Redefines Value 21
The Future Budget Environment Will Challenge Us 22

TECHNOLOGY 25
Vectors in Information Technology Continue Upward 27
Ramifications to Technology Projections 28
Vectors in Biology Will Continue to Converge With Information Technology 31
Biology Will Continue To Be Weaponized 31
Vectors in Conventional Weapons Remain Important 33
Precision Weapons Will Increasingly Dominate 33
Sensors Increase in Quantity and Quality 34
Stealth Aircraft and Electronic Countermeasures Rise in Importance 34
Unmanned Aerial Vehicles (UAVs) Increase in Numbers and Capabilities 34
Hyper-Empowered Warriors 35
Projecting the Impacts of Global Persistent Surveillance 35
Summary: It's the Convergences That We Need To Watch 37

PROCESS 39
Information Overload Means Competing for Attention 40
1. Newness: Tell Me Something I Don't Know 41
2. Compelling: Tell Me Why I Should Pay Attention 41
3. Aggregated: Tell Me Everything at Once 42
4. Quality: Tell Me I Can Trust You 43

CONTENTS

5. Customization: Tell Me In My Own Way 44
The Process of Developing Processes 44
Developing Results Oriented Processes 45
Processes Occur on Two Levels: In Action and in the Mind 46
Scenario Planning to Identify and Mitigate Risk 46
Social Network Optimization to Support Innovation 47
Structure And Processes: Form Follows Function 48
Networked Processes Need Strong Project and Information Management 48
Continuous Customer Focus Helps Assure Value 48

STRUCTURE 51
Today's Challenges Drive Tomorrow's Structure 51
Some Businesses Model New Approaches 53
Structure Is Not an "Either-Or" Decision 55
Structure Leads to the Defense Intelligence Agency's Excellence 56
Toward a More Vigilant Structure 57
Audacious Operating Goals Encourage Achievement of Measurable Effects 59
A Revitalized Advisory Board Provides Fresh Ideas And Continuity 59
The Director Serves a Five Year Term 60
The Organization and the IT Structure Mutually Reinforce Each Other 60
The Defense Intelligence Agency Can Lead the Intelligence Community 60

PEOPLE 63
Redefine the Workforce 65
Specialists 66
Generalists 67
Contingent 67
Workforce Design Objective: Small Core, Large Flexibility 69
Workforce Attributes 69
Attribute Development: Four Levels of Progress 72
The New Diversity: Cognitive Diversity 72
An Open Market Culture Fosters Imagination 73
Future Training and Development Includes Structured Experiences 74
The Human Resource Function Changes With the New Workforce Design 75
Continuous Development of Technological Expertise 78
Using JMIC to Advance a Broader People Strategy 78
The Way Forward 79

STRATEGY 81
Step One: Articulate a Compelling Vision 82
Step Two: Craft An Engaging Strategy 83
Step Three: Align or Fail 85
Step Four: Execute With Discipline 85
Step Five: Ensure Durability 85
Step Six: Measuring Results Speeds Renewal 86

SUMMARY AND RECOMMENDATIONS 89
Plan Changes to Occur Epoch-By-Epoch 89
Epoch 1: Build the Infrastructure For Good Growth 89
There Are Low-Hanging Fruit in the Technology and Process Arenas 91
Epoch 2: Prototype the Analyst of the Future 92
Epoch 3: Structure for Strategic Effect 92
Epoch 4: The New DIA 92
Epoch 5: New End State 92

CONTENTS

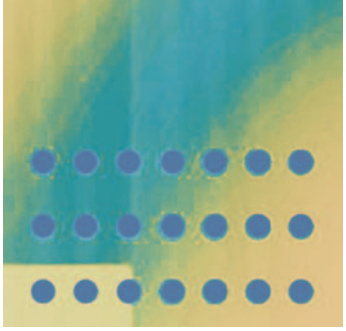
Success Begins With Implementing These Recommendations 92
Hire the Best, Inspire and Test, Retire the Rest 93
Recognize and Reward New Behaviors, Dissuade Old Ones 93
Make Hiring "Decentralized Competitive" and "Centralized Supported" 94
Focus on the Building of Technology Skills and Technology Capability 94
Begin Building a Cadre Of Experts 95
Summary: We Are Behind 95

APPENDIX 1 97

APPENDIX 2 99

APPENDIX 3 105

ENDNOTES 115



EXECUTIVE SUMMARY

Introduction

This paper describes a vision of a Workforce of the Future for the Defense Intelligence Agency. The Introduction asserts that both the future and the workforce that the Defense Intelligence Agency requires to remain vital in that future emerge from the complex interactions of technology, process changes, changes in competitive behavior, organizational structures, people, and strategy … all interwoven to create the future operating environment. The paper depicts the future operating environment for the Agency and the salient technologies that will help create the capabilities, opportunities, and threats of the future.

The Introduction makes five warnings. First, it warns that the Defense Intelligence Agency must change now. Second, it counsels that change must be strategic; driven by transformational goals and supported by companion changes in Agency structure and intelligence community policy. Third, it argues for introducing change as a well-orchestrated and continuous series of small projects that progressively move the Agency toward achieving its strategic ambition. Fourth, it cautions that making fundamental changes will be far more difficult than contemplating such changes. It asserts that the proof of strategy is outcome. Finally, the Introduction illuminates likely sources and manifestations of resistance to change … along with remedies … and the need for alignment and funding to create the workforce of the future. Unless the Department of Defense and the Congress express an authentic and material commitment to change, and unless Agency changes are harmonious with broader changes required in the intelligence community, change efforts in the Defense Intelligence Agency could be for naught.

Competition

A sidebar on "Competition" underscores the importance of a revitalized Defense Intelligence Agency and the urgency of its need to change, given the persistence and complexity of competition … including mortal competition … in the future. The paper asserts that history has not ended, that the state structure is not obsolete, that geography, ethnicity, and culture remain important, and that large-scale state-to-state conflict in the future is possible, even while increasingly unlikely. As technology creates new tools and new weapons, and as rivals, adversaries, and enemies better understand the sources of our strength, they will compete with us in ways we cannot expect today. An organization with the capacity to know that which an enemy wishes to hide in order to anticipate and checkmate competitive surprise is critical to our survival.

The Future Environment

The Workforce of the Future will exist in a future that it helps create. That future will be unlike the past. Witness a recent change: in ways remarkable for their depth and breadth, the United States has gained a position of extraordinary power and influence among the world's nations. It is the global leader in economics, culture, technology and weaponry, among others. This leadership will continue for the near future. No country or group of countries has demonstrated the willingness and capability to surmount American advantages in any of these areas — never mind all of them simultaneously.

Today's challenge is to do more than simply maintain this inheritance. Rather, the need is to exploit America's unique position to shape international change in ways consistent with America's enduring values and goals.

A New World Victory in the Cold War changed the world leadership role of the United States. No longer just the coalition leader of the free world, the United States is now the de factoguarantor of international order throughout the world. Unfortunately, in a world engulfed by change, there is no international consensus as to either the vector or the velocity of change or in America's role in setting that vector or velocity. As a result, America's post-Cold War leadership position has made it both an ill-defined umpire for the uncertain and a target for the dissatisfied.

The Globalizing Information Economy The information revolution continues to unseat centralized hierarchies, supplanting them with decentralized networks. The resulting globalization of economics, finance, business, culture, technology and force is driving societal shifts analogous to the industrial revolution. One destabilizing result is that domestic hierarchies are losing some of their monopolies on power.

The Hyper-Empowered The events of 9/11 demonstrated the potential of hyper-empowered individuals. Small groups are gaining powers previously reserved for states. They include the disenfranchised of the less-developed world, who, paradoxically, are empowered by the same forces of globalization they seek to destroy.

At the same time, the growing power of individuals and groups does not make conventional conflict obsolete. Traditional threats will remain a concern; North Korea is one example. What has changed is the level of risk plus the dynamics of response. We are entering an era where the Cold War strategy of deterrence is giving way to the post-9/11 strategy of preemption.

The Emerging Information Age Redefines Value Today's information-based, post-industrial age has made knowledge the number one factor in the creation of wealth. Physical products increasingly appear more like commodities than competitive advantages. The overwhelming premium is on knowledge, speedily applied.

For the intelligence community, redefining value means delivering information that is fast, integrated and anticipatory. Fast means quickly getting intelligence to the right decision makers in an easily understood form. Integrated means fusing all sources, including open sources, to speed and improve the quality of decision-making. Anticipatory means anticipating requests; waiting for formal tasking only makes many responses late. These aspects of the speed imperative, which apply throughout modern business and government, pertain directly to the Defense Intelligence Agency.

The Future Budget Environment Will Be Challenging The fast, integrated and anticipatory Defense Intelligence Agency of the future will face severe budget pressures. We should anticipate that all federal budgets will come under increasing strain as the "Baby Boom" generation enters the eligibility window for Social Security beginning in 2011.

Technology

Although threats can grow independent of technology, the magnitude of most threats remains dependent on technology. It is a dominant driver of transformation, creating entire capabilities, undercutting established bureaucracies and defining new concepts of operation. Therefore, by appreciating the scope of future technology we can outline the potential of most future threats.

Reasonable projections of future technologies include the following:

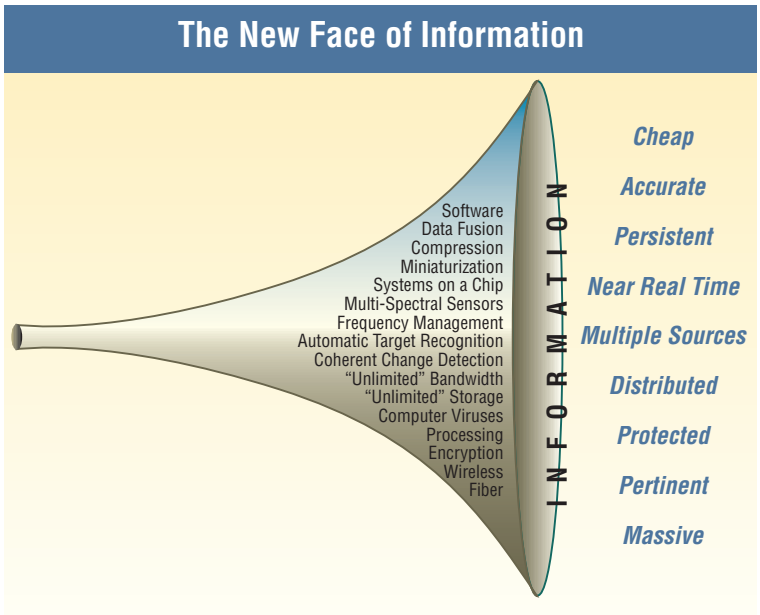
- Advances in data compression, processing, frequency management, miniaturization and sensors will allow data networks to move voice, data and images at speeds 50 times greater than today.

- The combination of multi-spectral miniature sensors and automatic target recognition algorithms will allow a greater degree of autonomous weapons.
- Sophisticated encryption protocols.
- Sophisticated computer viruses.
- Advances in processing and software will allow accurate data fusion at rates 104 times faster.
- Miniaturization will allow data storage capabilities of 103 times greater than today.
- Practically "unlimited bandwidth," the result of advances in wireless infrastructure, fiber and satellites.
- Systems on a chip.

These technologies will enable:

- Cheap information. The value of information will reside less in its existence and more in its analysis and integration.
- Accurate, protected information within open access systems.
- Near real time (NRT) information from multiple sources to tactical decision makers.
- Massive amounts of data accessible by all echelons of command.
- Pertinent information while filtering out unnecessary data.
- Persistent surveillance (augmented by coherent change detection).
- Real-time communication between customers and analysts.

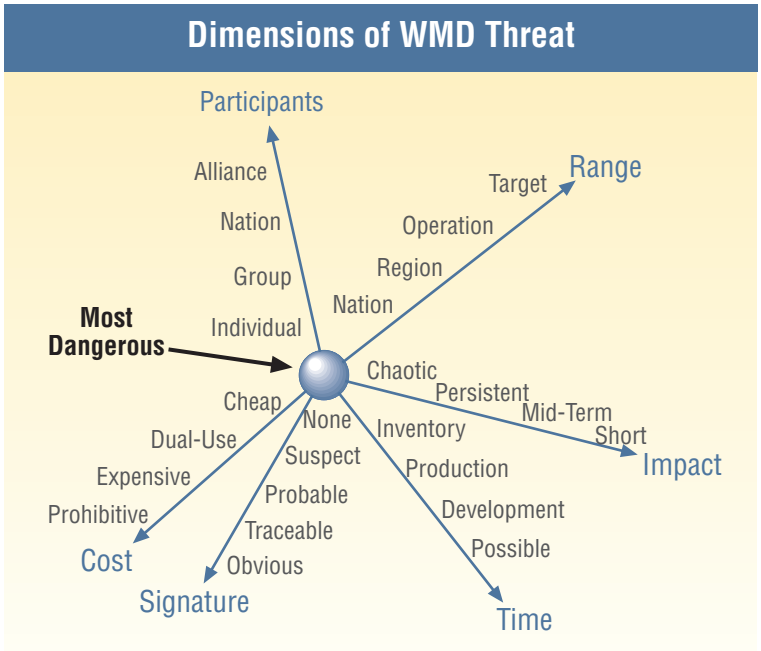
None of these projections, taken individually, appear strange or disruptive. All spring from current developments, continuing a pace of progress we have almost come to assume. The ramifications of these combined projections, however, are a different matter. When each of these advances comes to fruition, whether that is in 10 or 15 or 20 years, they will recombine to forge new possibilities and products. Their whole will be greater than the sum of their parts, with possible ramifications in four general areas.



First, most workers are already overwhelmed with present levels of technology. We should expect heightened resistance to new capabilities that require additional human interaction. Only those technologies that simplify workloads by employing machines as the interfacing tool (e.g., machine-to-machine interfaces) will find broad acceptance in the mid term.

Second, a combination of reliable encryption, unlimited bandwidth, unlimited storage and high performance personal computers would demassify many intelligence analyses. Technology will allow more distributed analyses, enabling the Defense Intelligence Agency to bring a variety of people to bear on current issues.

Third, the United States is surging ahead of other countries in terms of embracing the information age. The digital divide between the U.S. and target countries is widening. Analysts of the future will need concentrated training to surmount this additional cultural divide.



Fourth, because one of the Defense Intelligence Agency's tasks is to identify threats to U.S. interests before they occur, analysts need knowledge of possible targets. These targets will look increasingly less like those of the past — and more aligned with the emerging technologies of the information age. To identify threats to these nodes, Defense Intelligence Agency analysts will need specific training to understand their importance.

Weaponization of Biology From an intelligence perspective, the most important development may be the weaponization of biology and its convergent fields.

Bioterrorism meets most of the criteria for what constitutes a dangerous threat. Individuals or groups can surreptitiously produce bioweapons and deliver them without signature. They have the potential to affect an entire nation for an extended time, which would lead to chaotic developments. Such weapons may already be available and could be cheap to produce. For these reasons, bioterrorism augers a new an unfamiliar arena of war, one for which a new defense paradigm will be needed.

Vectors in Conventional Weapons Remain Important When forecasting weapons of the future, it is important to remember the weapons of the past-the Defense Intelligence Agency will need to factor advances in legacy systems into its technological future. This is especially true in four general areas: precision weapons; networked sensors; Unmanned Aerial Vehicles; and, signature reduction.

Projecting the Impacts of Global Persistent Surveillance Multi-spectral sensors deployed on satellites, unmanned aerial vehicles (UAVs), aircraft, ground stations and underwater will soon provide 24/7, all-weather global coverage. This global sensor network, combined with the global communications network and the intense "flashlights" of public media will reveal — and quickly transmit — unprecedented amounts of information on the actions of even the most reclusive nations.

The emerging opportunity for the Defense Intelligence Agency is to operationalize global persistent surveillance. Technology will afford the Agency the ability to orchestrate collection, reporting and publicity to do more than inform combatant commanders and the acquisition community. It will afford the power of observation to operationally affect the behavior of targets who may give up without ever resorting to untoward actions. The challenge for the Agency will be to organize, conceptualize and equip to take advantage of the manipulation mission. No one has yet developed the doctrine and methods of this weapon, nor is there a consensus with the defense community as to how to employ it. Developing the doctrine, methods and organization for this emerging weapon will become a major initiative.

Explosive Growth: Get Real

Harmonizing the human structure with the information technology structure will be a massive undertaking. Today, over 3 billion email messages … over 1 billion of these relating to business … connect a growing 400 million Internet users. The sidebar relates that "Second generation

systems being deployed now — based on untangling presence and messaging services — support integration into existing applications, like portals, sales force apps, help desk, supply chain and so on. But the next generation, based on the emergence of reformulated enterprise architecture stacks, will drive an enormous transformation at every level of the enterprise architecture." The Defense Intelligence Agency information architecture appears unprepared for the technology future.

Precision Intelligence

Precision weapons change warfare in many ways: they allow us to render the key node inoperative; they reduce unintended effects … today called "collateral damage" … and unnecessary physical damage; and they reduce the logistics tail required to support the engagement tooth. Such weapons are precise only to the degree that intelligence makes them precise. Precision intelligence is the prerequisite for deterrence and for the precise application of force … kinetic, non-kinetic, electronic, and diplomatic … should deterrence fail. To maximize the contribution precision weapons can make to deterrence and conflict resolution, the Defense Intelligence Agency must create precision intelligence analysts.

Process

Technology and acquired knowledge allow changes in how the Defense Intelligence Agency produces knowledge. Process is the manifestation of an organization's strategy the means by which it achieves its ends. While today the Defense Intelligence Agency may have some strength in its processes; today's strengths are contextual. Given the context of the future, current capabilities, the core competence of present success, will become disabilities and the basis for future incompetence the next context.

In the future, capturing customers' attention and preserving their trust help differentiate the Agency from other multi-source information providers. Each Defense Intelligence Agency process must focus on producing a strategic end. We envision that the Agency will design and improve processes to meet its customers' needs and its strategic ambition. Organizing in cross-functional teams, using scenarios to stress-test processes, social network optimization, and closer relationships with customers will help the Agency acquire and refine the competencies the future demands.

Timely and Timeless Business Ideas

A sidebar relates the five best business insights of 2003. They are: (1) Know where you are in the business cycle — and be ready to get out; (2) New processes will be less linear than the ones they replace; (3) A critical leadership competency — emotional intelligence; (4) Leadership is a group activity; and (5) Know the tangible and intangible assets and liabilities of the organization.

Structure

Structure follows strategy and form follows function in an effective organization. As the environment changes, strategies change and functions evolve, and the functions grow, diminish, or disappear. Thus, effective organizations place a premium on agility and adaptability. Having the right people organized in the right basic structure is critical to maintaining the advantage. Teams are the right structures to create knowledge networks for the future. The paper proposes cross-functional teams to manage functional areas or issue areas … such as Weapons of Mass Destruction, Terrorism, Life Sciences … in the context of geographical regions, such as China, the Americas, and so forth. The paper asserts that a capstone team, Global Warning, synthesizes the most pressing threats across the regions and across the functional areas and envisions where future dangers are likely to emerge and what they might be. Audacious goals drive both the Agency and the teams. Adjuncts to the structure are a revitalized Advisory Board of "outsiders" serving a Director with a

five-year controlled tour. The paper asserts that even in the fast-paced future, persistence requires the stability to do such things as harmonizing the silicon elements of structure … information technology and applications … with the human carbon elements.

Attachés

Given explosive growth in technology and communications, and given that adversaries will learn to "hide in plain sight" from persistent surveillance, human intelligence (HUMINT) becomes

Second Wave Attribute	Third Wave Attribute	Value to the Defense Intelligence Agency
Producing	***Thinking***	***Provide insight to customer and peers; considers a range of possibilities; innovative and creative***
Cognitive Attributes		
Technically Proficient	Culturally Intuitive	Permeates "hearts and minds' of target; nuanced thinking
Identifies Issues	Identifies Patterns	Draw connections between non-linear events and occurrences, considers possibility of low probability — high impact events
Parochial	Global Thinker	Understands global operationg environment; sees implications in a connected series of diplomatic and economic contexts
Assessing	Imagining	Can formulate highly original concepts and prospectives
Core Competence	Multi-Disciplined	Brings a range of ideas to group discussions and issues
Judgement Attributes		
Accepts Judgment	Questions Assumptions	Guards against the development of "group think"
Risk Averse	Calculated Risk Taking	Offers predictive intelligence which inherently carries risk
Communication Attributes		
Computer Oriented	Interaction Oriented	Communicates "live" with customer; conversational manner
Insular	Networked	Seeks out experts with a diverse array of knowledge sources and keeps them at the ready.
Information via Reports	Real-Time Collaboration	Adapts to new technologies and customer's desire for speed
Explanation	Story Telling	Uses narratives to allow understanding of complexity
Report Writing	Scenario Writing	Ability to develop scenarios based on facts and intuition
Presents Occurrences	Presents Context	Provides on-going, additive perspective to the customer
Technical Attributes		
Technology or Social Science	Technology and Science	Understands something about both disciplines; is aware of both technological and social science issues/impacts/solutions
Accepts Technology	Shapes Technology	Highly adept at identifying, selecting, and tailoring technology solutions for the demands of the work
Role Attributes		
Responsive, Reactive	Anticipatory, Proactive	Seeks to understand and constantly anticipate client needs
Role Focused	Customer Focused	Works to ensure data is useable and overall client success
Product Oriented	Outcome Oriented	Seeks tangible mission outcomes from the work conducted

more important. Just as there is persistent technological surveillance, the paper argues for persistent human surveillance: five year-controlled tours for attachés, with retired senior officers becoming the preferred source for future defense attachés.

Partnerships

Security risks the creation of insularity. Those isolated from the outside world lose touch with the world and its developments, diversity, and emerging dangers. Facility in creating transitory and expedient partnerships … teaming to solve problems … is a beginning. Teamwork in an internal network is more difficult. Partnerships of shared equities, risks, and rewards are more difficult still. Even so, partnerships, in concert with the creation of an internally-networked organization, will be a critical factor in the future success of the Defense Intelligence Agency and the intelligence community.

People

Given the challenges and missions that Defense Intelligence Agency will face in the future, building a wide-ranging network of expert resources is critically important. The future Agency will employ a relatively small core of its people internally — it will enlist the services of many at think tanks, companies, NGOs, universities and other organizations. In the future, generalists, specialists, and a "contingent workforce" will comprise the Agency workforce. The "contingent workforce" will be larger than the Defense Intelligence Agency full-time employee base.

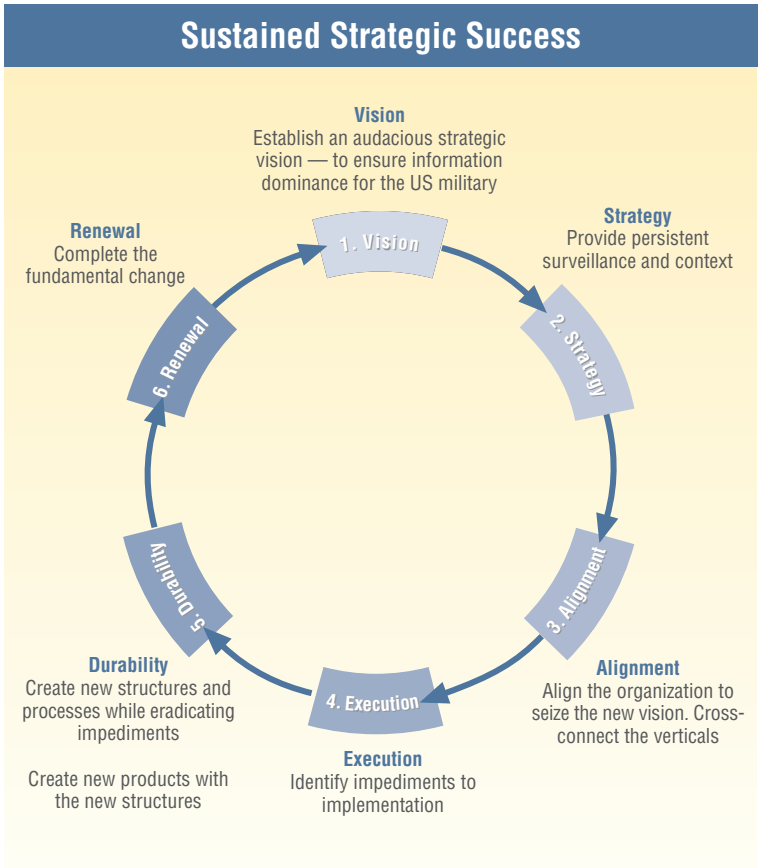
The future demands employees selected for attributes, rather than merely skills. New screening tools help screen for these attributes as do new recruiting methods that cast the net wider to acquire applicants. The table above summarizes the required attributes.

As the workforce changes, the human resources (HR) function changes in parallel. We expect that the human resource function, while maintaining a centralized administrative core of key activities, will move significantly toward becoming a "distributed" function. Centralized record-keeping, database maintenance, physical records, cross-Agency policies, and some training and executive development will persist, although distributed functions will increase. Many of the personnel normally assigned to a corporate HR office today will instead be "forward deployed" — or distributed among their internal customers — to work more closely with the business units they serve. An executive committee will oversee these distributed functions and, with the advice of human resource policy professionals and the general counsel, make the larger, strategic personnel decisions.

As the Agency shifts and realigns in response to the operating environment, its support functions will do the same. This realignment will create a need for continuous planning and adjustment in every area of human capital investment, development, and utilization to ensure that the workforce and its support systems remain on parallel tracks of evolution and development. This section of the paper describes companion changes to human capital planning, recruitment, hiring, retention, compensation, training and development, leadership development and succession planning, technology skill development, and the role of the Joint Military Intelligence College (JMIC) as a facilitator of these changes.

The Beginning of The Workforce Of The Future

A sidebar argues that in the future, recruiters will become "human capitalists", spending most of their time proactively seeking out and interviewing targeted candidates from around the world for potential inclusion in the Agency's talent pool. Applying sophisticated targeted marketing and branding strategies — and the Defense Intelligence Agency's compelling vision to attract individuals from around the globe.



To be successful, the human capitalist must be "an extraordinary individual who wants more than just a job," someone with "superior intellectual ability, toughness of mind and a high degree of personality" who can work in "fast-moving, ambiguous and unstructured situations." In other words, recruitment work will possess high similarity to a case officer type of role, working both formal and informal networks to land leads to the best sources of candidates. Human capitalists also move quickly. Human resources business processes must support the speed with which recruiters move.

The paper describes the characteristics of the specialist, generalist, and contingent categories of workers and how to best develop and compose them in adaptive, flexible, reconfigurable teams. The changes in the workforce profile and composition, as required by the future environment and the transformation of the Defense Intelligence Agency, will have the secondary affect of placing new demands on training and development. The new requirement will be to enhance resident attributes and cognition versus discrete tactical skills. As such, the emphasis will shift from imparting information to imparting experience, and preparing the workforce to comprehend and respond to multi-dimensional complexity of the operating environment.

Intelligence for Cause and Effects

Future effects-based analysts will not be experts in the data of multiple disciplines; they will apply the causal theories of different disciplines. Think of effects-based analysts as learners of theory, not as subject matter experts.

Effects-based intelligence officers will also be risk-taking gamers. At the tactical level, in a world of machine to machine interfaces, analysts will manage three dimensions simultaneously. First is hypothesis negation or confirmation to confirm the right cause-effect relationship. Second is Blue's next desired effect and action. Third is the target's reaction. Examining multiple scenarios is key to anticipating. And effects-based analysts will artfully weave these situations into captivating stories to elicit the operator or statesman's attention and real values.

Future effects-based intelligence experts will be masters of new science and art.

Strategy

The paper argues that in the future, the Defense Intelligence Agency's achievements will result from a relentless focus on customers and a continual assessment of customers' needs and the quality of the services delivered to them. The keys to sustained strategic success begin with having a set of audacious aspirations expressed as a "vision" or "strategic ambition."

Strategy follows directly from that vision, defined in terms of the measurable outcomes that prove it. Given a strategy, the successful organization engineers vertical and horizontal alignment. Alignment throughout the enterprise is critical. Once the organization aligns to the strategy, the process of execution begins. Execution is a learning process as the organization refines its processes to ensure that it repeatedly and predictably achieves success. Finally, the organization renews itself as it learns and as it senses or anticipates changes in the environment.

A set of ambitious corporate strategic measure accompanies this cycle of activity. The measures illuminate performance compared to aspiration and test every area of the organization's capacity.

Successful Transformation: According to the General Accounting Office

A sidebar details what General Accounting Office (GAO) research and analyses asserts are the critical elements of a successful transformation effort. There is, as one should expect, high fidelity between the findings, conclusions, and recommendations in this paper and the GAO's experience.

The Not-So-New Strategy of Prevention

The strategy of preventive war will demand new attributes from the Agency's workforce. Cognitively, Agency analysts and attachés will have to be global thinkers, able to imagine surprising permutations and reconstruct enemy plans. They must have sound judgment, and be able to take the calculated risks necessary to disrupt enemy strategies. They must be communicators, capable of real-time collaboration and facing their customers in person. They will have to shape technology, and with it their future. And — above all else — they must be anticipatory and proactive, focusing not only on outcomes delivered to their customers but the outcomes which their customers aim to achieve in their operations.

Summary and Recommendations: Getting to the Future with a Sense of Urgency

The last section of the paper offers a roadmap for change implementation, suggesting a new and more audacious end-state vision to propel the process. It asserts that once leadership affirms

Epoch 1: Build the Infrastructure for Good Growth	**2003** ■ Know critical requirements for and attributes of the Analysts of the Future (AOTF) ■ Build the nformation infrastructure ■ Identify impediments for eradication
Epoch 2: Prototype AOTF	**2004** ■ Eliminate impediments ■ Create functional and regional teams to satisfy informational needs ■ Consolidate issues teams electronically ■ Publish initial annual Defense Intelligence Assessments from teams
Epoch 3: Structure for Strategic Effect	**2004-2005** ■ Hire the best, inspire and text, retire the rest to become all-source with effect ■ Change the Defense Attaché system and school
Epoch 4: The New DIA	**2005-2006** **Be a partnership of highly skilled people and leading edge technologies providing warfighters, policy makers, and planners with assures access to required intelligence.**
Epoch 5: New End State	**2006-2007** **Be a partnership of highly skilled teammates helping prevent destructive conflict nfrom erupting, and helping predetermine the outcome of destructive conflict in favor of the US.**

the vision and strategy, change should be "chunked" into smaller projects occurring continuously over four "epochs." Since 2003 and 2004 are critical times, the leadership should focus on tightly coupling its workforce initiatives with significant and much needed enhancements to its core business processes of collection, analysis, and information management.

The paper asserts that people … the right people … underpin the process of fundamental change, and suggests that not all the present workforce will be up to the challenge.

We suggest and detail five urgent actions to begin the process of fundamentally changing the Defense Intelligence Agency by fundamentally changing the workforce: (1) Hire the Best, Inspire and Test, Retire the Rest; (2) Recognize And Reward New Behaviors, Dissuade Old Ones; (3) Make Hiring "Decentralized Competitive" And "Centralized Supported"; (4) Focus On The Building Of Technology Skills And Technology Capability; and (5) Use the hiring of a Chief Training Officer and the redevelopment of training to institute a group and individual training program that not only builds skills, but also builds the culture that the Defense Intelligence Agency strives for in the future.

Begin Building A Cadre Of Experts

We conclude by asserting that if the Defense Intelligence Agency seizes the vision to "Be a partnership of highly skilled teammates helping prevent destructive conflict from erupting, and helping predetermine the outcome of destructive conflict in favor of the United States," as its end-state vision, it will need a different cadre than a more modest vision would require. A more modest vision … "Be a partnership of highly skilled people and leading edge technologies providing warfighters, policymakers, and planners with assured access to required intelligence" … if taken at face value, risks merely fixing what is judged broken today.

In summary, as you read this we are nearly halfway through 2003. If fundamental change is the goal, our judgment is that the Defense Intelligence Agency is behind. Our opinion is that we can … and should … both catch up and get ahead.

INTRODUCTION

Time has run out for the old Defense Intelligence Agency.

"United States intelligence must be a community effort in fact as well as name, which means that effective coordination of intelligence as a truly national effort must be achieved. By far the preponderant part of U.S. intelligence in terms of manpower and money is that undertaken by the DoD. Great strides toward a more closely integrated community would result from improved intelligence coordination within the DoD."

The President's Board of Consultants on Foreign Intelligence Activities

"It must be considered that there is nothing more difficult to carry out nor more doubtful of success nor more dangerous to handle than to initiate a new order of things; for the reformer has enemies in all those who profit by the old order, and only lukewarm defenders in all those who would profit by the new order; this lukewarmness arising partly from the incredulity of mankind who does not truly believe in anything new until they actually have experience of it."

Nicolo Machiavelli
The Prince

The forces that converged to create the Defense Intelligence Agency — geopolitical reconfigurations, changes in the sources of wealth and the distribution of power, new threats to American security, the unacceptability of corrosive interservice rivalries, and the need for better integration and more rapid and accurate intelligence assessments — ought not to be unfamiliar to us. Nor should we be surprised that, in spite of the changes that have occurred over the last 40 years, so little has changed. The President's Board of Consultants on Foreign Intelligence Activities penned the first exhortation above 43 years ago this month.[1] So little has fundamentally changed because initiating change, as Machiavelli observed, is both "difficult to carry out" and "dangerous to handle."

Scores of interviews and hundreds of hours of research forced the conclusion that time has run out for the old Defense Intelligence Agency. Like many other entities in the intelligence community[2], the Agency must change, or it will lose its remaining vitality to more aggressive, adaptive organizations. Numerous policy makers and intelligence community constituencies draw the same conclusion, and like Admiral Jacoby, argue for fundamental transformation. Appendix 2 provides a sampling of the criticism prior to and following September 11, 2001. Given the Agency's role as the primary provider of intelligence for military operations, it must lead this change in the community to ensure the security of forces around the world and national security at home.

There are, fortunately, major differences between the drivers of change in 1960 and the drivers today. These include the fact that the Defense Intelligence Agency exists and that the Defense Intelligence Agency, mindful of the difficulties and dangers, intends to recreate itself for the future. Another difference between today and 1960 is leadership: the top-down commitment of the leaders of the Department of Defense and of the Defense Intelligence Agency to engineer change by using the right human capital and such tools obtainable now and those that may become available to it in the future. Thus, the Defense Intelligence Agency plans on using these mechanisms — technology, process improvements, and structural

changes — to craft a new and more adaptive strategy, a strategy that allows the Defense Intelligence Agency to create, develop, and engage its future workforce to understand and overcome whatever threats the future poses.

Everything Is Changing Simultaneously

There are perturbations in every element of the Defense Intelligence Agency value chain (Illustration 1). Customers are proliferating and levying new demands. Logistics, operations, distribution channels, and supporting functions are changing all at once.

Strategy formulation in this environment requires a comprehensive understanding of how separate elements interact and their critical dependencies. It also requires control of the timing of change, because production cannot stop during the progressive, epochal introduction of necessary changes. Thus, the first requirement is self-awareness of what the Defense Intelligence Agency is and how it works. Changing the workforce — the "production units" — is a necessary first step, but the Agency has to take that step strategically.

Creating the Future Demands Insight and Integrated Strategic Movement

Strategy is key. "Organizations," former Secretary of the Navy, the Honorable Richard Danzig, told us, "contain the fossil record of their history." Today's Defense Intelligence Agency workforce was formed by past strategies, indoctrinated in what were proven processes, trained in the technologies of its day, and organized according the policies and rules that governed its workforce epoch by epoch. To stare at today's workforce and try to understand it apart from the context that helped create it invariably leads to error. To avoid error, the leadership of the Defense Intelligence Agency knows that creating the workforce of the future is an outcome of the

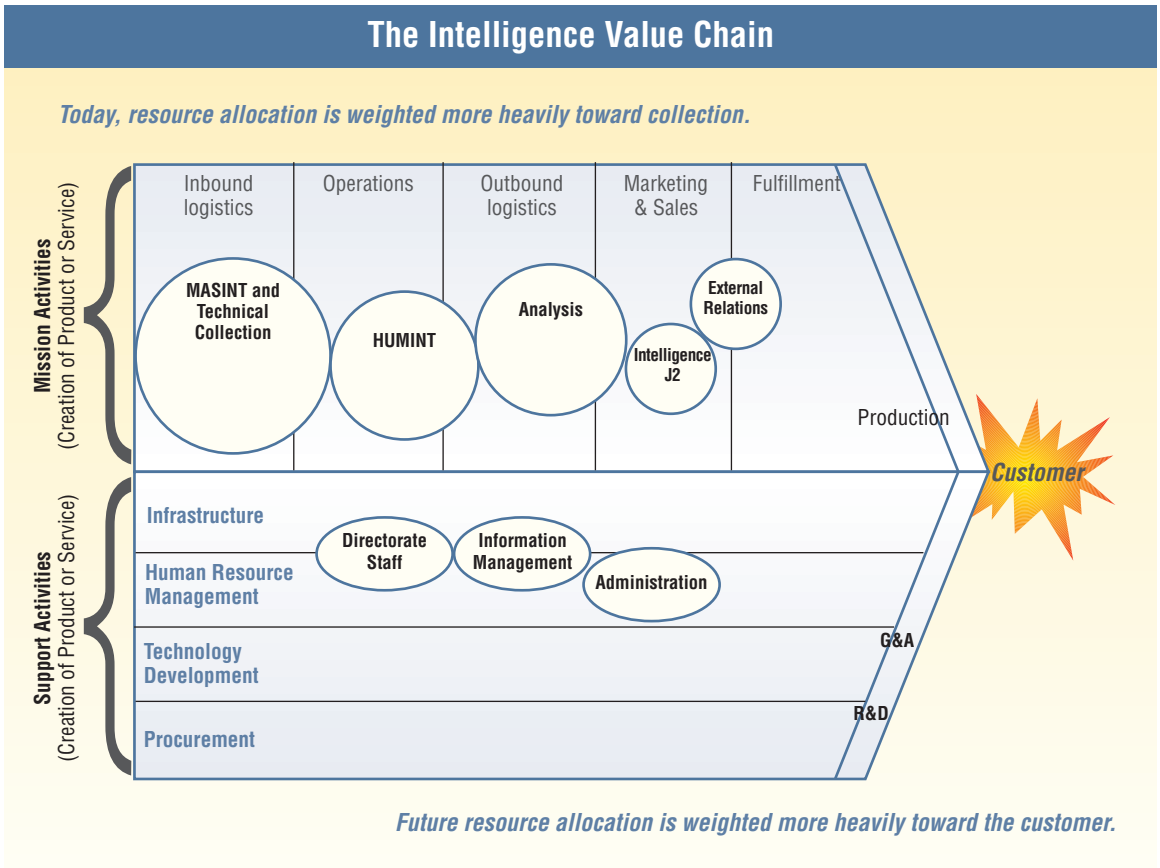


Illustration 1: The Intelligence Value Chain

"The past is done. Finished. The future does not exist. It must be created, microsecond by microsecond, by every living being and thing in the universe."

Edward Teller

Defense Intelligence Agency's strategy for the future. And its future strategy to enhance the value of its service to its stakeholders should not be constrained — today or in the future by its workforce.

Although the central focus of this paper is the human capital Defense Intelligence Agency must acquire, develop, and nurture to serve our country in the future, we know from experience that we cannot narrow our focus exclusively to human capital, to tinkering solely with the mechanics of today's personnel administration systems. Among the interactive and convergent elements that work together in the environment to create the future are technology, processes, competitors, partners, and organizational structures. These spheres intertwine inextricably and none can be separated or safely ignored when envisioning a future workforce. None of these can be neglected in designing a strategy for the future.

While strategy is key and necessary, strategy without implementation plans becomes daydreaming. Actually achieving desired outcomes is the proof of strategy. Alignment around a strategy, with implementation plans that focus on achieving specific audacious outcomes that support the strategy drives organization success. Outcomes that are not measured or measurable become vagaries victimized by chance. Since implementation is critical, it must not be ignored. Attending to strategy, planning, alignment, and implementation to assure achievement, success may still elude the Defense Intelligence Agency. Change is very difficult.

"The Reformer Has Enemies In All Those Who Profit By The Old Order"

Introducing fundamental change is hard work. In our experience, success is always — as Wellington described his victory at Waterloo — a near-run thing. There are five reasons for this and five remedies.

First, organizations are like living organisms. They take in resources to create energy and movement, expel waste, and reproduce their competencies as they adapt to their environment. Change is about pre-adapting to the future environment; crossing the chasm between today and the future. Since the future does not exist as an experienced environment, but only as a mental construct, the organism often senses cognitive dissonance during the change process. Having a set of vivid, concrete near-term outcomes that focus attention and progressively shape or change the environment can prevent cognitive dissonance. Fundamental change succeeds if it becomes a series of small, manageable changes.

Second, change requires alignment around a vision of the future end-state. The passionately held beliefs that the future state is superior to the present state, and that the organization can shape its future, drive alignment. This passion must reside first and foremost in the leaders of the change coalition, but it must also permeate the organization. The individuals leading the guiding coalition may depart before major elements of change have been implemented. If sufficient energy and passion depart with these human hosts, the change process will falter. Turning key elements of change into policy and process, and strategically creating a multi-tier coalition to sustain the passion and energy for transformation will help ensure change is successful. If there are changes at the top, the middle and the bottom can continue, and have the tools of policy and process to sustain them. Partners help. If partners have shared equities in the success of the change process, they can help sustain it. But they must all align around a unifying vision of the future.

Third, change requires not only intense focus on an end-state, but also the willingness to deviate from plan to accelerate change. When opportunistic deviations occur, critics will accuse the guiding coalition of uncertainty, vacillation, or self-servingly creating change

for change's sake. The guiding coalition can prevent this, however, by declaring at the outset that the broad outlines of the epochal path to the end-state are accurate, but cannot be precise in any way. The future, as Teller said, is co-created "microsecond by microsecond." If the new plan maintains the end-state vision, the deviation should not scuttle the process.

Fourth, change requires surrendering the local optimum to pursue a global optimum. It requires exchanging the views, capabilities and plans written by bureaucrats in small cubbyholes with their noses buried in their few responsibilities for visionary, enterprise-wide renaissance. Change, especially fundamental change, is a risky process because some decrements in capability always occur, and those responsible for those capabilities will cry out and insist change is moving them backwards. Leadership must understand and management control must monitor the critical few performance measures that signal the potential precursors of unsatisfactory performance so that it can remain confident that the changes they make are positive, forward progress and not simply action with no substance, or with negative substance. Simultaneously, they measure progress against aspirational measures, indicators of movement toward the audacious attainments of new global optima.

Fifth, and finally, leadership must understand that the nature of bureaucracies is to resist change. "The staff," one intelligence community general officer told us, "exists to protect the organization from its boss." Bureaucracies, and especially hierarchical government bureaucracies, have, over time, perfected countervailing strategies to resist reformers. Two of these dominate: the slow-roll, and the end-run.

The slow-roll is a strategy of delay. This strategy appreciates that rotation in and out of government positions is a fact. For military and political positions, this tour of duty length is often predictable and usually too short to allow leaders to affect significant change. A signal of the slow-roll is paralysis by analysis. Escalating demands for more information, pressures for more analysis, broad searches for more alternatives, or insistence on more analysis of alternatives during the change process, indicate the presence of conscious or subconscious slow-roll tactics. While the slow-roll is an effective and passive strategy of foot-dragging, a more active and aggressive strategy usually accompanies it: the end-run.

The end-run is a form of resistance that avoids change by "going around" any new structures or rules to capitalize on the apparent (or alleged) confusion that fundamental change causes. The end-run also can introduce the resistance of others by stimulating customers or partners to complain about the effects that change is having on them. The end-run sometimes seeks to depart from the organization and appeal to superiors to reverse or challenge key elements of a change strategy. Sometimes what alleges to be whistle-blowing accompanies the end-run. Even false allegations introduce delays and frustration. The end-run is most crippling when used in conjunction with the slow-roll.

The remedies for these forms of resistance range from effective communication to ensuring everyone understands the value of change, to the warning or removal of those who resist. Whether resistance is caused by parochial self-interest, misunderstanding, lack of trust, different assessments of the problem change intends to solve, or different assessments of the potential solutions, many people and many organizations have low tolerance for

John Kotter's Eight Strategic Change Errors

1. Allowing too much complacency.
2. Failing to create a suffiently powerful guiding coalition.
3. Underestimating the power of vision.
4. Under-communicating the vision by a factor of 10 (or 100, or even 1000)
5. Permitting obstacles to block the new vision.
6. Failing to create short-term wins.
7. Declaring victory too soon.
8. Neglecting to anchor changes firmly in the culture.

Illustration 2: John Kotter's Eight Strategic Change Errors[3]

change (see Illustration 2). Many change processes fail to answer the three key questions posed by the workforce: (1) What's in it for me? (2) What's in it for me? And (3) What's in it for me? This may be especially true for change initiatives undertaken in government bureaucracies.

And Even If You Do It All Right, It Could Turn Out All Wrong

Change initiatives in the Defense Intelligence Agency could fail if there are not equally significant changes in the larger defense intelligence context. Greater sense of community within the intelligence community (IC) will be required, as will reform of the requirements process and multi-billion dollar improvements to the all-source information infrastructure underpinning both the IC and its customers.

The entire intelligence community must work together to create the future they collectively envision. If they do not embrace the notion of community, it is unlikely that change initiatives of the Defense Intelligence Agency will succeed.[4]

Other changes are required. Two of these bear emphasis: reforming the intelligence "requirements" system and the satisfying the need for multi-billion dollar enhancements to the "all-source" information infrastructure.

Today's intelligence requirements process is not outcome oriented. The process separates requests for specific pieces of information and the priority assigned to those requests from the desired outcome or value of possessing such information. Because it accepts customer requests and customer-assigned priorities almost at face value, urgent and high priority requests can constipate the system, often creating the appearance that providers are unresponsive to customers. Fundamental structural and procedural changes would improve this system and indeed are necessary as technology provides the wherewithal to move from reconnaissance to persistent surveillance. Knowing "something about everything all the time" requires either that customers and providers agree on "why" knowing is valuable and "what" it is that they need to know, or that the provider be empowered to decide the "what" based on knowing and appreciating the "why." It would do little good to create an "Analyst of the Future" or an "Attaché of the Future" only to enslave him or her to the requirements process of the past.

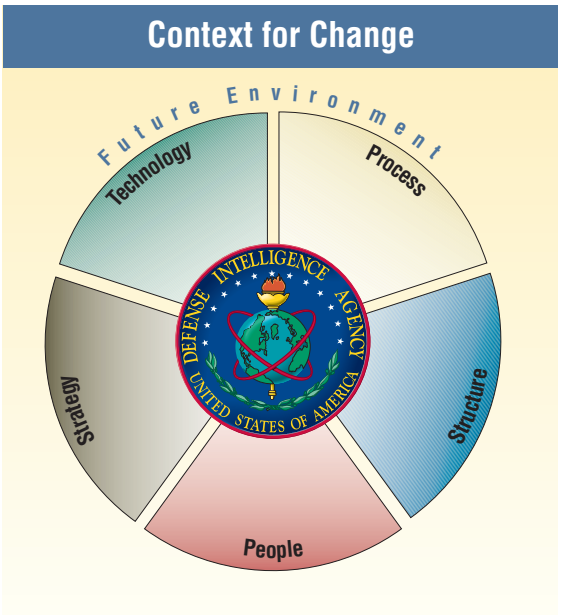
The Defense Intelligence Agency also may fail in its change initiatives unless it has the information infrastructure to support and sustain changes in its core business areas of collection, analysis, and information management. Today, for example, no intelligence agency is responsible for determining and enforcing data and metadata standards, search and access protocols, best applications, or best commercial practices for information management. Consequently, content is unmanageable, and all source content cannot be integrated for rapid manipulation or display. Absent standards and processes for managing data across the community, contemporary capabilities — such as fusion — and future capabilities — such as inductive analysis and visualization — are unattainable. Unless there is commitment from the Department of Defense and funding from the Congress to support and introduce fundamental change across every element of the Defense Intelligence Agency value chain (Illustration 1), creating the world's most effective and agile intelligence workforce may be to no avail.

Edmund Burke's century-old advice remains relevant because time has run out for the Defense Intelligence Agency. It must change. The fact that it must change liberates the Defense Intelligence Agency from the burden of choosing much beyond the sequence of change activities. The timing of change — now or never — has been determined already. What remains is the hard work of change, of pre-adapting to the future.

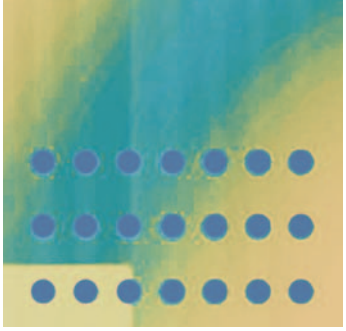
"Do Not Despair, But, If You Must, Work On In Despair."

In the pages that follow, we focus the Defense Intelligence Agency on the future. For it is in creating and adapting to that future that the workforce we describe will flourish. Among the interactive and convergent elements that work together in the environment to create that future are technology, processes, competitors, partners, and organizational structures.

What do we know about each of those elements in that future? Read on.



The graphic above illustrates the components of change that the Defense Intelligence Agency will consider as it embraces transformation. In the sections that follow, we discuss each component in turn, beginning with the Future Environment, progressing around the circle and ending with Recommendations.



THE FUTURE ENVIRONMENT

Future security will depend upon preempting the violent enemies of the United States. Hyper-empowered individuals will be the primary generators of this threat, not nations or groups of nations. To thrive in this environment, the Defense Intelligence Agency provides key decision makers with fast, accurate, integrated and anticipatory information. This information, however, may have to be generated with resources far below today's levels.

"Jody Williams won the Nobel Peace Prize in 1997 for helping build an international coalition to bring about a treaty outlawing land mines. Although nearly 120 governments endorsed the treaty, it was opposed by Russia, China and the United States. When Jody Williams was asked, 'How did you do that? How did you organize one thousand different citizens' groups and non governmental organizations on five continents to forge a treaty that was opposed by the major powers?' she had a brief answer: 'E-mail.' Jody Williams used the networked world to super-empower herself."

Thomas Friedman, New York Times

"The days of net assessment — having one large enemy like the Soviet Union — are over."[5]

Chief Scientist, Fortune 500 Company

In ways remarkable for their depth and breadth, the United States has gained a position of extraordinary power and influence among the world's nations. This leadership will continue into the near future. No country or group of countries has demonstrated the willingness or capability to surmount American advantages in any significant area. If anything, the United States is poised to lengthen its overall lead. Continuing American investments in innovative research and development (both military and civilian) outpace those of any competitor.

Today, the United States has achieved unprecedented levels of global leadership across key aspects of national power. Economically, the United States generates a quarter of the world's goods and services. This percentage has been rising for a decade. Culturally, American mass media (news, film, music) reach practically every nation. Our values are spread even deeper by the half million foreign students who attend American colleges and universities each year (half of all students who study abroad). In technology, the most important advances in biotechnology, information processing and materials manufacturing have either their genesis or their leadership in the United States. And in military operations, American weaponry and personnel are insurmountable, with a generation of combat-tested professionals wielding world-class systems in every category.

This enviable condition took years to build. Previous generations of national leaders bequeathed it to us. Today's challenge is to

Competition

"War is a nation's way of eating."

Tribes and clans, nations and states, governmental organizations and non-governmental ones, philanthropic and sinister groups, and good and malicious individuals have always populated the planet. There should be no doubt they will continue to populate it in 2020. The future may see a shift in the relative power of the world's competitive actors-economic city-states possessing the financial power of some states,[6] non-governmental organizations rivaling some states in influence, or even a dramatic increase in the power of hyper-empowered individuals, but individuals, groups, and states most certainly will co-exist as competitors in the future. Appreciating that the forms that competition will take in the future may change; the nature of competition nonetheless will not change. The philosopher-historians Will and Ariel Durant observed that

> *Our states, being ourselves multiplied, are what we are; they write our natures in bolder type, and do our good and evil on an elephantine scale. We are acquisitive, greedy, and pugnacious because our blood remembers millenniums through which our forebears had to chase and fight and kill in order to survive, and had to eat to their gastric capacity for fear they should not soon capture another feast. War is a nation's way of eating."*

States and nations are as unlikely to wither away in the future, as "history" is unlikely to end. In the future, the United States and the Defense Intelligence Agency must reckon with the facts of geography, ethnicity, culture, and nationalism. "Globalization" is an

do more than simply maintain this inheritance; that would be too modest and static a goal. The world is changing rapidly and the United States must adjust. There is little chance the economics, technology, culture and military operations of today will extend in a straight line indefinitely into the future. We must continually refresh these tools in order to protect America's unique position in the world and to shape international change in ways consistent with America's enduring values and goals.

Such shaping must start with an appreciation of the emerging global environment. While many trends seem consistent with those of the past, they differ in fundamental ways, and those differences are widening. As former Secretary of State Henry Kissinger wrote, we are at "a defining juncture" in international affairs.

A New World

The end of the Cold War saw the reordering of global politics and undermined the rationale for geopolitical relationships. National minorities redrew borders while individual states questioned the relevance of alliances. Divisive forces continue to stress borders and alliances as economic and technological changes irritate cultural and ethnic schisms.

Victory in the Cold War changed the world leadership role of the United States. As schisms abounded, groups and nations turned to the United States to adjudicate. No longer just the coalition leader of the free world, the United States is now the de facto guarantor of international order.

Unfortunately, there is no international consensus as to either the vector or the velocity of change or in America's role in setting that vector or velocity. The world has no idea where or by whom it should be led. Existing candidates, such as the United Nations, have questionable abilities and emerging candidates, such as the European Union, have yet to demonstrate the ability to lead. As a result, leadership has defaulted to the United States. However, because America's post-Cold War leadership status is far from unanimous, it has become an ill-defined umpire for the uncertain and a target for the dissatisfied.

"There is not a country we need fear. Increasingly, the fear is of individuals."[8]

Chief Scientist, Government Agency

important set of phenomena, but these signify the globalization of means, not the homogenization of ends.

Thus, we believe that the acquisitive, greedy, and pugnacious will remain among us, but the ways that individuals, groups, and states choose to compete will change to take advantage of emerging tools to hurt their adversaries. Unlike natural evolutionary competition, competition may be revolutionary. Bruce D. Henderson writes in "The Origin of Strategy":

> *Natural competition is wildly expedient in its moment-to-moment interaction. But it is inherently conservative in the way it changes a species' characteristic behavior. By contrast, strategic commitment is deliberate, carefully considered, and tightly reasoned. But the consequences may well be radical change in a relatively short period of time. Natural competition is evolutionary. Strategic competition is revolutionary."*[9]

What surprising new forms of competition will emerge? None can know for certain, but to prevent strategic surprise, to help prevent destructive conflict from erupting, and to predetermine the outcome of destructive conflict in favor of the United States, the Defense Intelligence Agency must be prepared for all. Advancements in science could offer the potential for new weapons. Improvements in manufacturing or logistics could signal a magnification in capability. Whether one accepts the all-inclusive construction of Qiao Liang and Wang Xiangsui depicted below,[10] in Figure 3 "The Forms of Unrestricted Warfare," or some more modest framework, the potential for revolutionary changes in the forms that competition takes is high.

The Globalizing Information Economy

The information revolution continues to unseat centralized hierarchies, supplanting them with decentralized networks. Moore's Law (the number of integrated circuits on a chip doubles every eighteen months) and Metcalfe's Law (a network's value is the square of its members) iterate on a daily basis to produce exponential impacts on nearly every aspect of society through the flow of global information.

The resulting globalization of economics, finance, business, culture, technology and force drives societal shifts analogous to the industrial revolution. Wealth shifts among regions, nations and constituencies, creating unimagined opportunities for humankind. At the same time, these shifts generate fear among losers and overconfidence among winners. Those in the middle sway back and forth, as divisions in both extremes preclude consensus and compromise. The lack of tools to measure success or failure in this emerging era confuses everyone.

In this globalized environment, distinctions between "domestic" and "foreign" are increasingly ambiguous. When networks are the center of society, whether fifty feet or fifty degrees of longitude separate two terminals has little relevance. Routine decisions on technology, crime, justice, agriculture and taxation, once considered "domestic" in nature, can have major impacts abroad in a globalized system, and vice versa. The changes transform the notion of power in the future.

The Hyper-Empowered

The events of 9/11 demonstrated the potential of hyper-empowered individuals. Small groups proved their ability to affect American sovereignty in ways their state havens could never hope to do. Their potential calls into question the Westphalian principles of sovereignty, which held that individual citizens of each

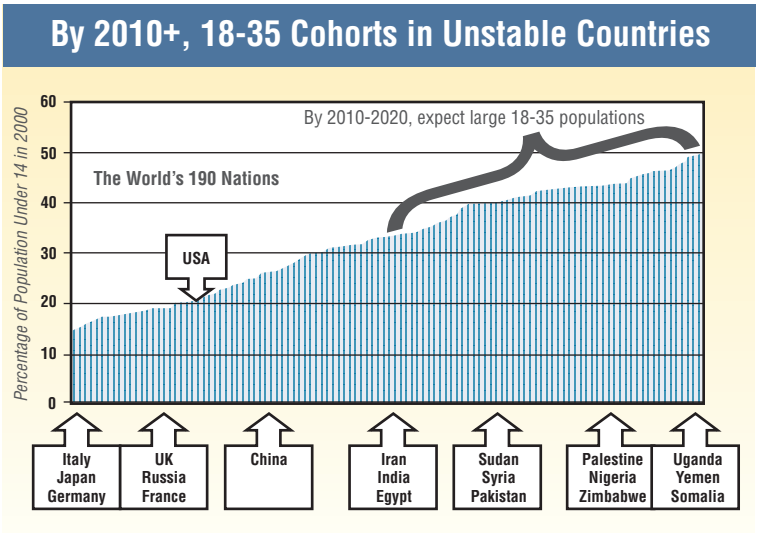


Illustration 3: By 2010+, 18-35 Cohorts in Unstable Countries

The role of the Defense Intelligence Agency cannot be restricted to an exclusive focus on what Qiao Liang and Wang Xiangsui describe as "military war" or even "beyond military war." Serving policy-makers requires the ability to support the multi-dimensional approaches that policy-makers take.

Military War	Beyond Military War	Nonmilitary War
Nuclear	Diplomatic	Financial
Conventional	Internet	Trade
Bio-Chemical	Information Ops	Natural Resource
Ecological	Psychological	Economic Aid
Space	High Tech	Law and Regulation
Electronic	Smuggling	Sanctions
Guerrilla	Drug	Media
Terrorism	Deterrence	Ideological

Illustration 4: The Forms of "Unrestricted Warfare"

Twenty-five centuries ago, a Chinese warlord said, "In movement nothing is more important than the unexpected. In planning nothing is more important than not being knowable."[11] Persistence surveillance may become a fact in the future, but for the Defense Intelligence Agency, it may not be a pleasant fact. The "observed," knowing that they are under surveillance, will invariably discover new ways to "hide in plain sight." As the Under Secretary for Intelligence asserted, "We are looking to create intelligence capabilities that emphasize persistence and greater resistance to denial and deception."[12] To do that the Defense Intelligence Agency must have the workforce prepared for the denial and deception intended to mask destructive conflict in any of its potential manifestations.

state were immune to interference by foreign states. This most important tenet of the nation state system, which has endured for 350 years, may be obsolete in an era of hyper-empowered individuals. It may not survive our era of stateless terrorism, criminality and uncontrolled disease.

The problem is that small groups, even individuals, are gaining powers previously reserved for states. For example, a single currency speculator, George Soros, brought down the Bank of England and had a large role in the Asian financial panic of 1997. A profile in the London Observer described him as "the only U.S. citizen with his own foreign policy."[13] Osama bin Laden and his Al Qaeda network did more harm to the United States from their base in Afghanistan than the Afghani government could ever have hoped to do. Israel has more to fear from an organization like Lebanese Hizballah than it does from a state like Egypt. To an unprecedented extent, small groups now emerge as serious threats to world order.

In a world where the integrating visions of the Information Age replace the defining divisions of the Cold War, the enemies of integration pose the most serious threat to world order.

These enemies are seldom states; they are individuals and groups. They include the disenfranchised of the less-developed world, who, paradoxically, are empowered by the same forces of globalization they seek to destroy. Countries with rapid urbanization and high birth rates combined with poverty and political corruption are propagating dissatisfied young men, and demographic studies show that the most troubled areas of the world contain disproportionate numbers of young people (Illustration 3). They can use the Internet as an incredible force-multiplier to move money, communicate with cells and obtain intelligence. Operating with little warning, they can use technologies like GPS to build weapons with devastating effects. In the age of the "suicide bomber," these "hyper-empowered individuals" pose an undeterrable threat to national security and a major challenge for intelligence agencies.

This challenge includes the threat of individual terrorists and groups with weapons of mass destruction. As noted by the President's "National Strategy For Combating Terrorism,"

"The probability of a terrorist organization using a chemical, biological, radiological or nuclear weapon, or high-yield explosives,

has increased significantly during the past decade. The availability of critical technologies, the willingness of some scientists and others to cooperate with terrorists, and the ease of intercontinental transportation enable terrorist organizations to more easily acquire, manufacture, deploy, and initiate a WMD attack either on U.S. soil or abroad." [14]

This undeterrable threat is driving the new national strategy of preemption. The United States has announced its intention of attacking such threats as soon as the intelligence community identifies them. There is no willingness to wait until a threat manifests itself. Rather, the nation will now attack on warning. As stated by Secretary Rumsfeld, if the Nation waits to find a "smoking gun," it will have waited too long.

The strategy of preemption is a major policy shift for the United States. It is a reaction to the new strategic environment evidenced by 9/11.

Preemption dramatically increases the responsibility placed on the intelligence services. The minimal signatures of some weapons, particularly biologicals, make them extremely difficult to detect. At the same time, their potential impacts — which could range into the millions of casualties — make their detection a national imperative. This detection imperative falls to the intelligence community.

The growing power of individuals and groups does not make conventional conflict obsolete. On the contrary, familiar threats will doubtless continue. The military forces of specific states, such as North Korea, will remain of interest. Combatant commanders will need up to date information on the command and control, readiness and equipment of specific militaries. This is especially true in cases where potential enemies begin to understand the emerging era of the hyper-empowered soldier. We discuss this further in the Technology chapter "Vectors In Conventional Weapons Remain Important". In areas where war can start without warning — and an immediate U.S. response would be required — traditional intelligence requirements will remain valid. Similarly, current intelligence requirements will remain for foreign missile and weapons of mass destruction developments.

The level of risk posed by traditional threats, however, has changed. Whether an event might happen and the downside if it does, combine into our single calculus of risk. From this perspective, the risks posed by theater conflicts to U.S. national sovereignty are far less than what they were during the Cold War. The days of "M-Day equals C-Day equals D-Day" are thankfully over.[15]

These factors, and their chaotic and iterative side effects, are combining to shift the strategic calculus of the global community. They are driving an era where the Cold War strategy of deterrence is giving way to the post-9/11 strategy of preemption — and where the engines and measures of wealth are in flux, driving near continuous adjustments in national power, both real and perceived. Overlaying these dynamics are the unique frictions and opportunities offered by America's leadership position in practically every sphere of national power.

The unique attributes of this emerging era cannot help but redefine our institutions. Greater changes are already on the table.

The Emerging Information Age Redefines Value

Today's information-based, post-industrial age places a premium on knowledge. It has become the number one factor in the creation of wealth. While fiscal capital will always remain important, the value of intellectual capital is on the rise. With the right information at the right time, other resources become less valuable. There is less need for capital, time, labor, energy, materials and infrastructure when the right information is properly applied. Intellectual capital, an inexhaustible resource, becomes the principal determinant of wealth and power.

Information infrastructures worth hundreds of billions of dollars stand ready to move knowledge, thanks to investments by business and governments in fiber, satellites, servers, desktops and software. Information infrastructures enable today's key differentiator between

"There's pressure on government officials to make decisions much faster, so there's pressure on us to produce answers in days, sometimes hours. Our tradition has been studies that take months."[16]

Chief Information Officer, Government Agency

competitors: "economies of speed." They supplanted industrial age "economies of scale" as the most important metrics of value.

The overall goal of leading businesses today is to create a dynamic organization focused on specific customers and optimized for speed. Today's companies treat physical products more like commodities than as competitive advantages. The overwhelming premium is on knowledge, speedily applied.

Leading institutions quickly integrate data from structured (proprietary) and unstructured (external) sources and then customize it for key decision makers. Rapidly fused intellectual capital, accessed and applied in a case-by-case basis, replaces the "one size fits all" approach from the mass production age. The intent is to speed each decision by facilitating integration and delivery. This track requires highly specialized workers willing to innovate to meet specialized demands. They must also be willing to withstand constant changes in organizational structure as customers, issues and infrastructure change.

This premium on speed is obvious to military professionals. As demonstrated during the 2001-2003 operations in Iraq and Afghanistan, the modern imperative in military matters is speed.[17] From the kill chain to acquisition to logistics, today's decision makers demand speed in every step of the process — with as few processes as possible. Practically by definition, whatever accelerates or skips a process is good; whatever slows or adds a process is bad.

For the intelligence community, this means delivering information that is fast, integrated and anticipatory. Fast means quickly getting intelligence to the right decision makers in an easily understood form. Integrated means fusing all sources (including open sources), lest decision makers be forced to delay while waiting to incorporate other facts.[18] Anticipatory means predicting requests, beginning to answer questions before they are asked. Waiting for formal tasking only makes many responses late. These aspects of the speed imperative, which apply throughout modern business and government, pertain directly to the Defense Intelligence Agency.

While previous generations of military decision makers also wanted "fast, integrated, and anticipatory" intelligence, modern leaders demand it to an unprecedented extent. Their demands are rooted in the expectations of modern society.

The Future Budget Environment Will Challenge Us

The fast, integrated and anticipatory Defense Intelligence Agency of the future will face severe budget pressures. We should anticipate that budgets to prosecute both traditional and emerging missions will come under increasing strain.

The "Baby Boom" generation, which began in 1946, will enter the eligibility window for Social Security beginning in 2011. When this occurs, many boomers will shift from being net contributors to the trust fund to a net drain. As retirees, they will push less money into the trust fund while, at the same time, greatly increase withdrawals. As shown in Illustration 5, they will also shift the ratio of workers to retirees from the present five to one (five workers for every retiree) to three to one by 2025.

Because current federal budget deficits would be much larger without offsetting surpluses provided by "loans" from the Social Security trust fund, all federal discretionary programs,

including defense, will come under pressure. Due to the massive deficits this transition will probably drive, leaders of the intelligence community should prepare alternatives in case severe budget cutbacks in the post 2011 time-frame become a reality.

Tomorrow's premium will be on coaxing an uncertain world towards preempting the violent enemies of the United States. Hyper-empowered individuals will be the primary generators of this threat, not nations or groups of nations. To thrive in this environment, the Defense Intelligence Agency will provide key decision makers with fast, accurate, integrated and anticipatory information. It will likely, however, need to generate that information with resources far below today's levels. Said another way, given fiscal forecasts, failing to act today may preclude acting tomorrow.

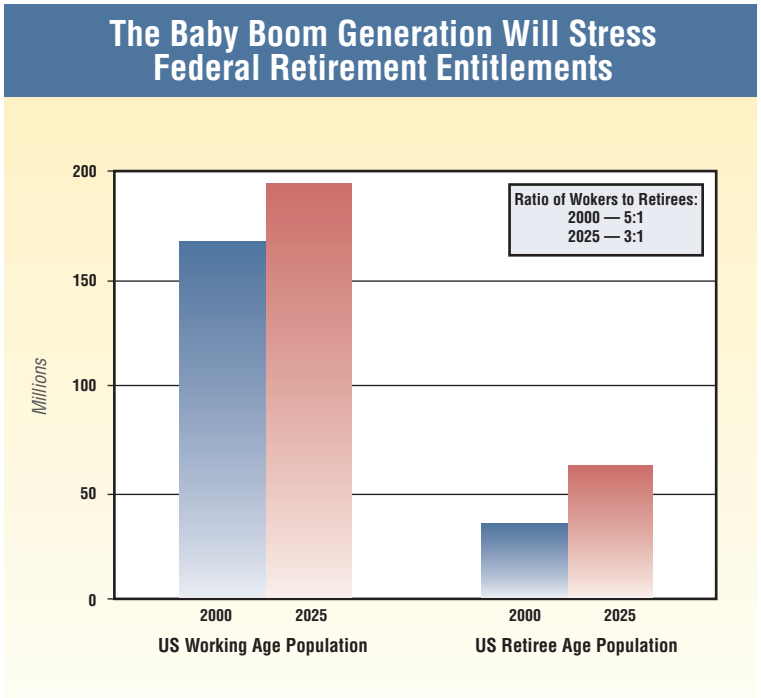
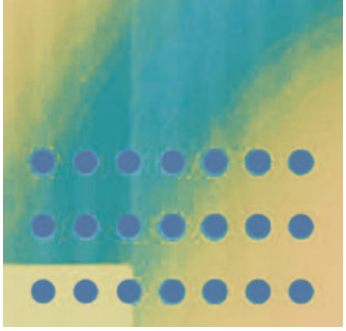


Illustration 5



TECHNOLOGY

Over the next two decades, a series of technological advances will converge to drive a new Defense Intelligence Agency.

> ***"Companies cannot see or read about a new technology today and deploy it tomorrow. It takes time to study it, to understand its significance, to conceptualize its potential uses, to sell those uses inside the company and to plan the deployment."***
>
> **Hammer and Champy, *Reengineering the Corporation***

As we seek to forecast the future operating environment for the Defense Intelligence Agency, the "great growling engine of change" is technology. Technology drives transformation, creates entire industries, undercuts established bureaucracies and defines new cultures. George Orwell went so far as to equate a generation's value with the technology it produced.

By Orwell's standard, our era has done well. In our lifetimes, we have seen the integrated circuit underwrite the information age, revamping business and society. Nuclear power redefined warfare and international politics, creating new alliances and organizations. Biotechnology introduced enormous social and cultural shifts. By any measure, these and other technologies drove fundamental shifts in the ways of nations, groups and individuals. They proved the historical tie between technological advance and fundamental change in our political, social and economic environments.

This is not to say that all change has a technological parent. Social, religious and emotional factors also drive change. The political and racial aspirations of Germany and Japan, for example, contributed to the upheavals of World War II. Adolph Hitler, Osama bin Laden, Slobodan Milosevic and Saddam Hussein rose from a mix of personal ego, social ideology and nationalist fear.[19] Technology was not their genesis. Rather, their threats arose independent of technology.

Having said that, these individuals used technology. The magnitude and character of each threat had a strong technological base. Hitler needed Panzers and Stukas to pose an international threat. Absent these weapons, Nazi Germany's menace to the international community would have been far less. One can say the same for the Soviet Union with its missiles and weapons of mass destruction.[20] Bin Laden exploited airliners, cell phones and the Internet. These and other villains turned technology to their own terrible ends. Whereas their "bows" sprang from politics or ideology, technology formed their "arrows". We can anticipate a parallel dynamic from their future counterparts.

From this perspective, the value of technological foresight is apparent. Although threat can grow independent of technology, the magnitude of most threats remains dependent on technology. Therefore, by appreciating the scope of future technology we can outline the potential of most future threats. While the personae of future threats are inherently unknowable, we can outline the weapons at their disposal in advance.

"The encryption algorithms used today will be marginalized. Quantum encryption will emerge ten years or so into the future, but we will not turn off legacy systems. There's a 10 — 15 year gestation system — that's just the way things work".[21]

Chairman, U.S. Government Board

The same is true for forecasts of organizational change. While laws, markets and leadership regularly change, in many organizations, it is also true that technology changes the workplace. The web, PC, PDA, email, fax and cable television are visible examples of technological change in the workplace. Less visible technologies, such as servers, sensors, software, fiber optics, network switches, lasers and technical training support these changes. The sum of these technologies changed the modern workplace, making it unrecognizable to those of a generation ago.

In fact, our willingness to accept technology may be the key limiting factor in forecasting change in our workplaces. Managers have substantial latitude over how they adopt technology. They can dictate, within budget constraints, how much of a new technology they will employ, but usually take a conservative straight-line approach. They apply new technologies only to perform traditional tasks better, faster, or cheaper and neglect to envision how technologies can help change their business or industry.

Fortunately, there is a time lag between a technology's introduction and its adoption. Isaac Asimov observed that, "Science can amuse and fascinate us all, but it is engineering that changes the world." It takes time to engineer the science of the laboratory into the tools of work and war. By understanding the state of the current laboratory, we can forecast the future operational environment. We can forecast with some fidelity the future technological tools available to organizations such as the Defense Intelligence Agency and to our nation's adversaries. Accurate forecasts of trends in technology can help us scope — at least in part — the tools of our future environment.

Historically, there is a lag between the laboratory and the workplace, between development and acceptance. In the past, we usually measured that time lag in decades (Illustration 6).

Key drivers of technological change inched their way into our every day lives. They did not simply arise out of the ether and burst into the Defense Intelligence Agency. They took time to evolve. This time lag is significant. It provides a reasonable starting point for projections of future technologies. We know much of what will be available to managers ten years from now because we know what is in development now.

As a result, although the velocity and range of technological change are unknowable, its vectors are visible. There will be unexpected breakthroughs and disappointments to be sure, but we know enough about the future to identify probable developments in technology. With this information, we can project minimal steps needed to prepare

The First …	Year
Cable TV	1948
Laser Guided Bomb	1964
Internet (ARAPANET)	1969
E-Mail	1971
Personal Computer	1975
GPS (Block 1)	1978
Cell Phone	1979
WWW	1991
Linux System	1991
PDA	1993

Illustration 6: Time Lag

"Technology really becomes important when it fades into background-when we take it for granted".[22]

Vice President, Fortune 500 Corporation

organizations for at least those developments. There are reasonable technological vectors that conservative planners should incorporate into their vision of the future operating environment.

Vectors in Information Technology Continue Upward

Despite the dot-com meltdown of 2000-2002, information technologies continue to progress. Every day the journals report some type of new breakthrough. Moore's Law, which predicted the doubling of transistors per square-inch on integrated circuits every eighteen months, continues to hold true — as it has for almost four decades (Illustration 7). The consensus among experts is that Moore's law will continue to hold for the next two decades — and probably beyond.

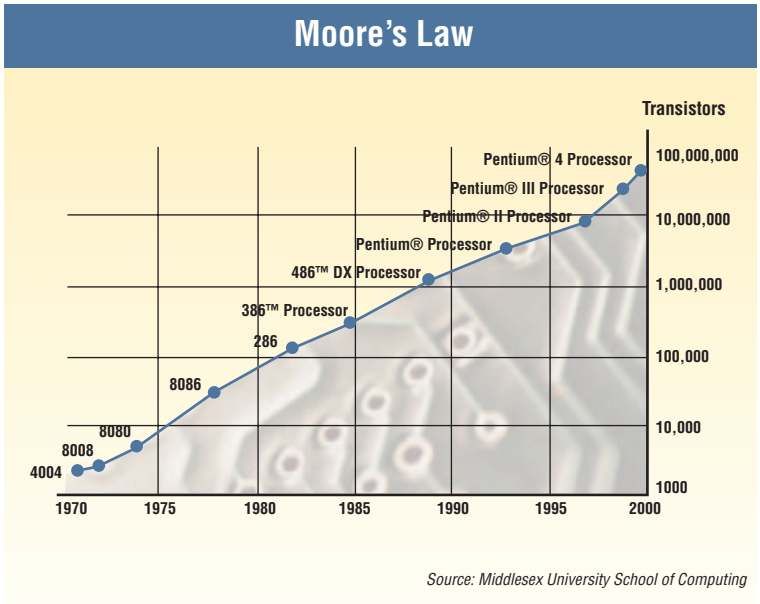


Illustration 7

Over the past three years, worldwide Internet usage has doubled. Half a billion people use the Internet today.[23] Information available via the Internet doubles every six months. Transmissions (now via optical fiber networks) are at rates 200 times faster than just five years ago. Laboratories have demonstrated data rates of 3 terabits per second.[24]

Supercomputers today reach speeds recently considered science fiction. The latest Cray supercomputer is capable of 52.4 teraflops, or trillion mathematical calculations per second. By 2010, Cray anticipates an "X1 system" capable of a petaflop, or 1,000 trillion mathematical calculations per second.[25]

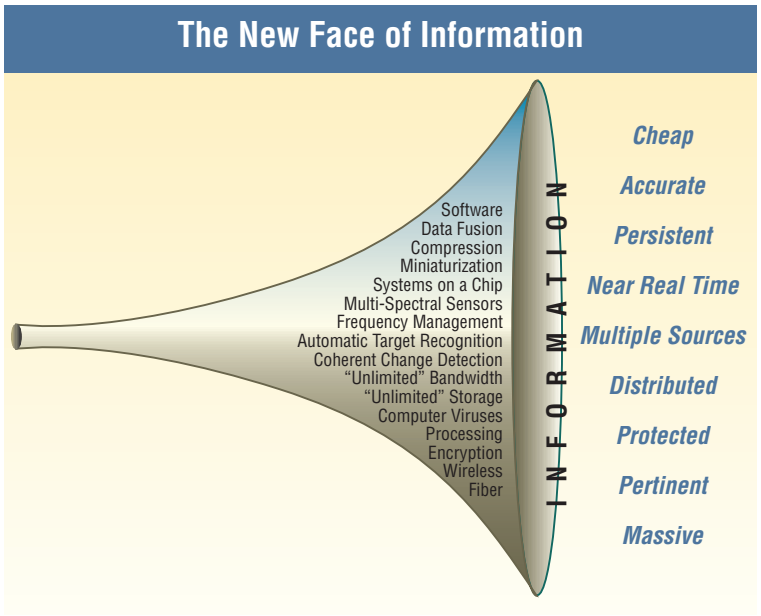


Illustration 8

Reacting to this rate of technological advance, defense intelligence professionals forecast information-based systems far more capable than today's. Over the next 15 years, these advances could include:

- Advances in data compression, processing, frequency management, miniaturization and sensors that will allow data recognition algorithms to allow a greater degree of autonomous weapons.
- The combination of multi-spectral miniature sensors and automatic target networks to move voice, data and images at speeds 50 times greater than today.

"Our analysts are being given products from new sensors (e.g., hyperspectral and UGS), but few actually use them. They don't understand them. If one analyst finds a new source that works for him/her, s/he spreads the word to others — and the new sensor actually gets used. But the process is slow. Only 10% of the guys [sic] actually use the new sensors".[27]

SES, Intelligence Community Agency

- Sophisticated encryption protocols.
- Sophisticated computer viruses.
- Advances in processing and software that will allow accurate data fusion at rates 104 times faster than today.[26]
- Miniaturization that will allow data storage capabilities of 103 times greater than today.
- Practically "unlimited bandwidth," resulting from advances in wireless infrastructure, fiber and satellites.
- Computer Application Systems on a chip.

These technologies will enable:

- Cheap information. The value of information will reside less in its existence and more in its analysis and integration.
- Accurate, protected information within open access systems.
- Near real time (NRT) information from multiple sources to tactical decision makers.
- Massive amounts of data accessible by all echelons of command.
- Pertinent information while filtering out unnecessary data.
- Persistent surveillance (augmented by coherent change detection).
- Real-time communication among customers, collectors, analysts.

Ramifications to Technology Projections

There is a subtle point to note in technology projections. Taken separately, few if any are strange or disruptive. All spring from current developments, continuing a pace of progress we have almost come to assume. Many people with an eye to the future will be comfortable with aggressive projections of individual technologies.

They might be less comfortable, however, with the ramifications of these combined projections. When each of these advances comes to fruition, whether that is in 10, 15, or 20 years, they will recombine to forge new possibilities and products. Illustration 9 depicts how these forces act to give information new power. Their whole will be greater than the sum of their parts, with possible ramifications in four general areas.

First, most workers are already overwhelmed with present levels of technology. Current desktops offer capabilities beyond the comprehension of practically all of us. We have difficulties programming our VCRs, cable TVs, Personal Data Assistant (PDAs)s and telephones. Voice recognition software and GPS-enabled navigation systems now installed in new cars remain a mystery to most; few features are actually used. So when someone promises even faster, broader and more extensive IT products, the announcement often generates more fear and doubt than excitement. People are increasingly wary of eating large servings of new technology when they are still digesting previous courses.

As a result, we should expect heightened resistance to new capabilities that require additional human interaction. Only those technologies that simplify workloads by employing machines as the interfacing tool (e.g., machine-to-machine interfaces) will find broad acceptance in the mid term.

"PKI is a certainty in the future. It will improve dissemination and cross talk among the agencies. However, progress is glacial."[28]

SES, Intelligence Community Agency

"Today's target states of interest are changing so rapidly that DIA's analysts are out of date."[29]

Combat Arms Major General

Managers should therefore emphasize the downloading of work from analysts. Some Defense Intelligence Agency analysts do not utilize data from some sensors due to unfamiliarity. With new technologies making even more data available, it will be imperative for managers to shift some data integration to machines. In an era when analysts are drowning in data, data management will go hand in hand with personnel, task and budget management.

Second, the combination of reliable encryption, unlimited bandwidth, unlimited storage and high performance personal computers will demassify many intelligence analyses. There will be less need to secure all analysts in a common facility to enable classified interaction. Rather, technology will allow more distributed analyses, enabling the Defense Intelligence Agency to bring a variety of people to bear on current issues. Academicians, overseas residents, business people, retirees, contractors, scientists, clerics — whatever expertise the Agency needs — will have as much technical connectivity to information from their home or business as a current analyst has from his or her workstation at the Defense Intelligence Agency. The only impediment to accessing these sources will be that which the Defense Intelligence Agency imposes for security reasons. The Agency will continually question this security impediment, as it will increasingly need to access expertise on emerging issues that resides outside the organization.

Lower tier countries are the spawning grounds for modern conflict. Terrorism is more likely to originate in Sudan, Afghanistan or Somalia than it is one of our Cold War enemies. Because the next threat may come from areas outside specific Defense Intelligence Agency focus areas, it makes sense for the Defense Intelligence Agency to maintain the capability to incorporate diverse knowledge into its day-to-day operations. Such day-to-day incorporation, which goes beyond mere access, would allow the Defense Intelligence Agency to fuse classified information with data from the private sector (generated by corporations and non-governmental organizations). The new networking technologies will enable this fusion.

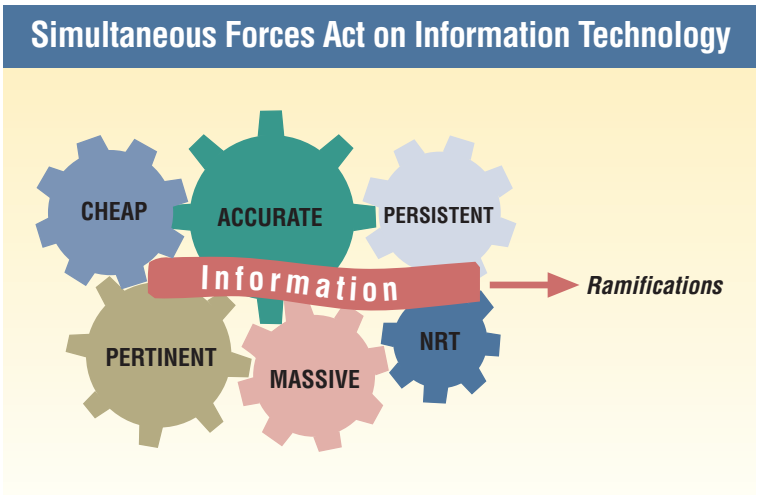


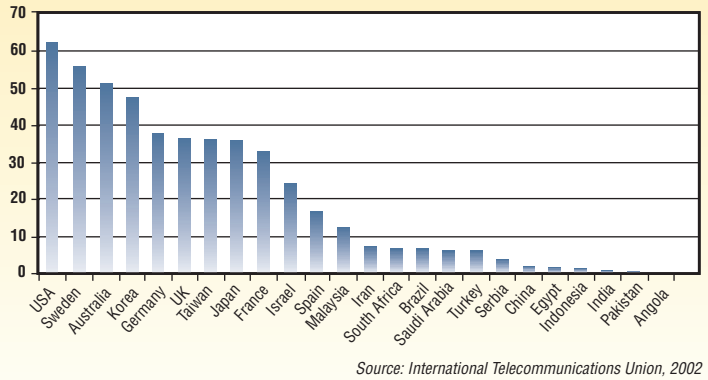
Illustration 9: Simultaneous Forces Act On Information Technology

Third, the United States is surging ahead of other countries in terms of embracing the information age. The U.S. leads the world in personal computer (PC) use. Many supposed competitors lag far behind in this important metric (Illustration 10). Practically all leading IT research and business development in the world is concentrated in the U.S. Europe, for example, has only two indigenous world class IT firms (Nokia and Ericsson). Five former IBM employees actually founded Europe's top software firm, SAP. With the possible exception of the UK, little improvement is perceptible on the horizon. Systems based on industrial-age architectures dominated by the politics of aging populations slow change in Japan and Europe. China and India, two nations often cited as Third Wave rivals of the U.S., still have 90% of their populations engaged in First Wave subsistence agriculture. For these reasons, it is entirely possible the United States will find itself increasingly differentiated from the rest of the world.

"DIA's biggest vulnerability is Information Security (INFOSEC). Information warfare is the most cost effective way to attack us. It is the principal weapon of the future."[30]

SES, Intelligence Community Agency

Personal Computers per 100 People (2001)



Source: International Telecommunications Union, 2002

Illustration 10: Worldwide personal computer availability

If the U.S. does set itself apart, young people brought into the Defense Intelligence Agency may view military-technical developments in target countries through a false prism. Raised in the information age environment of the U.S., where information technologies are engines of wealth and power, they may misinterpret change in rival nations that retain an industrial age basis. This was not a problem during the Cold War when many measures of national power in the United States and the Soviet Union were roughly comparable (for example, natural resources, industrial output and military force structure). Analysts raised in the American industrial age knew, for example, that steel production was important and what it entailed. As a result, they had a frame of reference when tasked to analyze steel production in the USSR or China. However, as our nation increasingly diverges in terms of economy and society from other major nations, new personnel tasked to monitor those nations will need to bridge an additional cultural divide, the digital divide. The singular information age culture of the United States will skew their biases for judging value in other systems. Analysts of the future will need concentrated training to surmount a growing technological and cultural divide.

Fourth, all Defense Intelligence Agency analysts, current and accessions, must understand new technologies in order to understand American infrastructure. Other militaries will certainly attempt to attack the United States. That is a given; only the time and place are unknown. When enemies attack, they will strike sources of U.S. power. To the extent our power depends on technology or advanced engineering, future enemies may target those nodes. Just as enemies in the past might target shipping or railroad yards or banking centers, future targets will include Internet nodes or gene manipulation facilities.

Because one of the Defense Intelligence Agency's tasks is to identify threats to U.S. interests before they occur, analysts need knowledge of all possible targets. These targets will increasingly look less like those of the past — and will align more with the emerging technologies of the information age. To identify threats to these interests and protect them, intelligence professionals will

Technological Expectations

- Online ordering and configuration by customers
- Moore's Law continues
- "Unlimited" bandwidth (including wireless)
- "Unlimited" storage
- Software lags hardware
- More reliance on Internet
- Progress in Artificial Intelligence
- Progress in sense-making
- Better data management tools
- Persistent surveillence (with coherent change detection)
- Awash with real time information
- Expansion of MASINT capabilities
- Expansion of sensors
- Custom pharmaceuticals

Illustration 11: Examples of Expected Technological Advances

need to understand their structures and technologies.

Illustration 11 lists some of the technologies that will be especially important to the business of intelligence in the future.

Vectors in Biology Will Continue to Converge With Information Technology

We are surrounded by tremendous advances in biology. Advanced microscopy and imaging deepen our understanding of nutrition and health. New tools will fit inside the body to speed repair and enhance performance. We see advances in fields like microfluidics and biohybrid technologies leading to major new biosensors. Scientists, having sequenced the human genome, are now working on its expression in the proteome. The outcome will enable the customization of pharmaceuticals and nutriceuticals to individual patients.

The digital revolution is just phase one in the development of an entirely new information age techno-economic system. In the first phase of this wave, information technology revolutionized biology. The Human Genome Project is one example. Computers and networks allowed scientists to determine the DNA sequence of the entire human genome. In the next phase, biology will revolutionize information technology. Biological structures and processes will allow information transfers at speeds and complexities unimagined today. This revolution may be fifteen to twenty years in the future. However, when we reach this phase we will, once again, revolutionize economics, society and conflict.

Convergence of sciences is not new. Other disciplines emerged at the intersections of well-established fields such as physics, chemistry and mathematics (e.g., biophysics). More recently, newer fields like computer science blurred the lines separating them from older pursuits like biology, as evidenced by the rapid growth of the new bioinformatics field. In the future, we can expect to see physical science fields fusing more with social science fields. Psychopharmacology, treating mental disorders with drugs, is one such well-known fusion. It is possible that future mechanical and computer chip implants in human beings could stimulate new directions in anthropology and sociology. Such convergences of technologies offer potential advances far beyond those of an individual technology exploited alone.

Biology Will Continue To Be Weaponized

From an intelligence perspective, the most important development may be the weaponization of biology and its convergent fields. The potential for abuse of any technology always exists, and biology is no exception. In 2002 the White House declared, "One of the most important missions we have as a Nation is to be prepared for the threat of biological terrorism — the deliberate use of disease as a weapon." The U.S. Food and Drug Administration reports,

> ***"Preparedness for and response to an attack involving biological agents are complicated by the large number of potential agents (most of which are rarely encountered naturally), their sometimes long incubation periods and consequent delayed onset of disease and their potential for secondary transmission. In addition to naturally occurring pathogens, agents used by bioterrorists may be genetically engineered to resist current therapies and evade vaccine-induced immunity. Pathogens that have been identified as potential biological warfare agents include those that cause smallpox, anthrax, plague, botulism, tularemia and hemorrhagic fevers."***[31]
>
> ***U.S. Food and Drug Administration***

Unfortunately, this is not alarmist hyperbole. Illustration 12 indicates the multiple dimensions to assess the threat of a weapon of mass destruction. Bioterrorism meets most of the criteria for what constitutes a most dangerous threat. Individuals or small groups could produce and subsequently deliver a bioweapon with no signature. It could affect an entire nation for an extended time, which would lead to chaotic developments. Such weapons may already be available and could be cheap to produce. For these reasons, bioterrorism augers a new an unfamiliar arena of war, one for which a

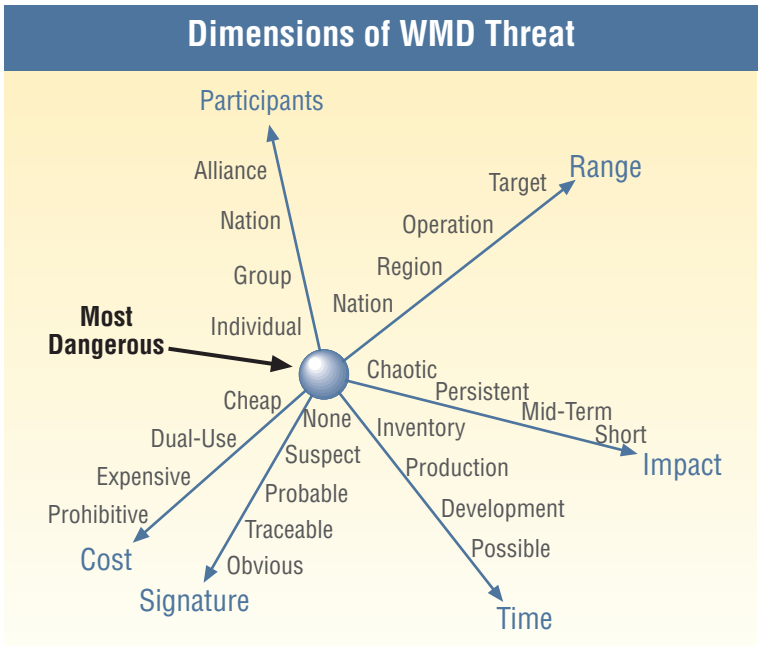


Illustration 12: Dimensions of WMD Threat

new defense paradigm is needed. Further complicating this bioterror threat are several key facts.

First, bioterrorism is most effective when directed against civilians. Although we could conceivably protect military forces against a biological attack (e.g., anthrax shots), the size and nature of the American civilian population makes it inherently vulnerable to attack by biological weapons. There are simply too many non-cooperative targets to defend simultaneously, 24/7.

Second, as the United States continues to progress with its information age, knowledge-based economy, the rich-poor gap between the United States and other nations will widen. Such gaps have historically caused conflicts. As evidenced by the two wars with Iraq, few nations can hope to win a conflict by competing symmetrically with the United States military. Terrorism, the asymmetric response, has traditionally been the weapon of the weak. Among the weapons available to them, biological terrorism may emerge as an optimum means of asymmetric competition.

Third, the line between peaceful biological research and the weaponization of disease is murky. It is difficult to definitively ascribe one or the other to every specific facility. It is even more difficult to identify every possible facility. A single laboratory at a single university could produce a viral strain of catastrophic effect.

Fourth, unlike other weapons of mass destruction, bioterror weapons know no boundaries. Nuclear weapons have a blast radius. Heat and dispersion affect chemical weapons. However, in theory, a biological weapon such as a virus or plague could put everyone on the planet at risk. It would also put the perpetrator at risk — but in an age of suicide bombers, that is not a deterrent.

Lastly, considerable expertise on biological weapons exists outside the United States. As shown in illustration 13, a third of the doctorate degrees in the biological sciences conferred by American universities go to foreign citizens. Ten percent of them are citizens of nations on the State Department watch list for terrorism. When added to the educational resources existent overseas, the open nature of

US Bioscience Doctorates

PhD Conferred in US	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001
Biological Sciences, Non-US	1,403	1,552	1,725	1,805	2,061	1,908	1,886	1,751	1,749	1,579
Biological Sciences, Total	4,799	5,092	5,203	5,375	5,724	5,789	5,846	5,583	5,849	5,678
% Non-US Citizens	29%	30%	33%	34%	36%	33%	32%	31%	30%	28%

http://www.nsf.gov/sbe/srs/nsf03300/pdf/secta.pdf

Illustration 13: U.S. Bioscience Doctorates

most research material and the broadband connectivity of millions of computers, it is fair to say the genie will be out of the bottle on potential biological weapons production. For these reasons, the United States may find its most serious threat in the realm of biological science.

The convergence of these facts is the key problem. Any one fact may be surmountable. Their sum, however, is a different matter. The gap between the weak and the United States will continue to grow, and terrorism is the weapon of the weak. The United States will remain exposed to bioterror attack because perfect defenses, whether active or passive, are impractical. The expertise to build bioterror weapons resides outside U.S. influence and will continue. In theory, this expertise could build the most powerful weapon in the history of humankind. Finally, some group or nation may believe they can develop such a weapon in secret. For these reasons, in terms of future threats to United States sovereignty, the bioterror threat may top the list.

Vectors in Conventional Weapons Remain Important

When forecasting weapons of the future, it is important to remember the weapons of the past. The weapons of war, after all, are additive. New weapons enter the present inventory, but very seldom do we render old classes of weapons totally obsolete (cavalry, swords and sailing ships are among the few examples of obsolete weapons). In practically all cases, we keep old weapons and concepts in the inventory, albeit with lesser importance. We still teach soldiers to fight with knives and dig foxholes; we still equip ships and planes with guns. A significant percent of the bombs in Operations Enduring Freedom and Iraqi Freedom were unguided ("dumb bombs"). The point to remember is that even when new types of weapons emerge to assume dominant roles on the battlefield, the legacy weapons of war remain.

We must factor the capabilities of these legacy systems, which we will improve, into the mix for the Defense Intelligence Agency's technological future. As noted in an earlier section, the traditional conflicts of the past will continue (although the threats they pose will be less critical to American sovereignty). There will remain a need for the Agency to collect on legacy systems, especially in terms of technological advances.

From today's perspective, improvements in legacy systems will probably be concentrated in four general areas: precision weapons; networked sensors; Unmanned Aerial Vehicles (UAVs); and signature reduction.

Precision Weapons Will Increasingly Dominate

In the 1990s, precision-guided munitions (PGMs) emerged as the centerpiece of a revolutionary style of modern warfare. The clear trend since the first Gulf War is that precision-guided weapons represent a steadily increasing percentage of munitions delivered: about 8% in Iraq, 30% in Kosovo and 60% in Afghanistan and Iraq. Other significant trends include the increasing number of PGMs delivered per sortie and the rising percentage of PGMs delivered in adverse weather (from 13% in the 1991 Gulf War to almost 90% in the 2003 Iraq war). Finally, trends suggest new capabilities stemming from increased payload fractionation (larger loads of smaller guided weapons) and mass precision (rapid delivery of large numbers of PGMs in short time periods).

"Various technologies are enabling advances in MASINT — nano, miniaturization — new ways of getting close access to sniff, to listen, all the other senses metaphors — mini-remote sensors will inform MASINT in a fundamentally different way than ever before."[32]

Group Manager, Fortune 500 Corporation

"Coherent change detection is an area of major potential. By overlaying separate 'pictures' of the same area, practically any disturbance, to include tire tracks, can be detected. This capability will probably be fielded in 10 years. However, this delay is solely due to funding priorities. The basic technology is known. It could be fielded right now if it was funded."[33]

SES, Intelligence Community Agency

Sensors Increase in Quantity and Quality

We will see an explosion of new multi-modal sensors, led by advances in airport security and medical biosensors. These sensors will underwrite the shift towards "network-centric warfare" by providing extensive situational awareness. Underpinning this promise are technologies to create network-centric architectures consisting of high-quality sensors and rapidly transmitted data streams. The services and combatant commanders are transforming command and control centers to fuse and exploit this data. We can see parts of this transformation in terms of better of integration of communications, command, control, computing intelligence, surveillance and reconnaissance assets between the two Gulf Wars.

In the future, trends in sensor technology toward less expensive, more capable and lighter sensors will support intelligence-quality sensors networked around the battlefield. Assuming that data streams from multiple sources can be integrated in a timely fashion — a tall order — future commanders will enjoy even greater situational awareness to employ their forces more effectively.

Networks are one of the great advances in industrial organization. Over the course of the last half-century, the vertically integrated company has given way to the networked enterprise, an organizational structure characterized by greater agility and adaptability. Successful firms today intertwine layers of information, raw materials, analytical data, customer communication and service and network infrastructure — at unprecedented speed — while maintaining countless secure relationships with third-party organizations, such as suppliers, technology outsourcers and government regulators. They work within stovepipes, such as marketing, but also fuse networks of networks, such as marketing and research, production and finance. Military organizations that can parallel this private sector performance will dominate the emerging environment.

Stealth Aircraft and Electronic Countermeasures Rise in Importance

From the first Gulf War to Kosovo and back to the Gulf, joint commanders employed low observable aircraft (such as the F-117 and B-2) with remarkable success and revolutionary impact. Low observable technologies allowed combat aircraft to operate with relative impunity against sophisticated air defense systems. The ability of stealth aircraft to operate independently reduced the requirement for large strike packages laden with supporting escort aircraft. At the same time, electronic warfare assets were critical in enabling non-stealthy aircraft — the mainstay of the current force structure — to survive in non-permissive threat environments. Continued emphasis on airpower-centric campaign plans will ultimately demand renewed investment in the twin pillars of stealth and electronic countermeasures. Intelligence systems should pay particular attention to these twin enablers of high tempo airpower-centric operations.

Unmanned Aerial Vehicles (UAVs) Increase in Numbers and Capabilities

Since the 1950s, the U.S. has invested billions to develop and field UAVs, primarily for ISR (intelligence, surveillance and reconnaissance) missions. This investment produced unmanned systems that demonstrated their operational utility over the battlefield, enabled by advances in satellite guidance and communications, computerized flight control systems and sensor technologies. Due in large part to improvements in range, carriage, endurance, on-board sensors

"Not everything that counts can be counted and not everything that can be counted counts."

Albert Einstein

and data transmission, unmanned systems continue their advance.

Used initially as decoys during the Gulf War, by Operation Enduring Freedom (2001), UAVs had evolved into sophisticated, air breathing, hunter-killer platforms. For example, the Hellfire/Predator combination was a fusion of fused ISR and shooter technologies. This fusion is leading the way towards an ever tighter kill chain. Decisions are moving to the left in this kill chain, placing a higher premium on accurate target data and compressing the time available for intelligence analysis.

It is worth noting that the price of some types of UAVs is declining. The U.S. Navy has an "Affordable Cruise Missile" in development with an expected cost per unit of $40,000.[34] If the engineering advances for this cruise missile migrate to UAV developments, we might see an era where ubiquitous UAVs blanket a crisis area. If that happens, relatively cheap cruise missiles may emerge as a dominant factor in future wars.

Hyper-Empowered Warriors

Progress in these key areas of technology (precision weapons, networked sensors, signature reduction and UAVs) will give rise to the hyper-empowered warrior of tomorrow. Small groups of soldiers will project effects in ways previously reserved for battalions and brigades. This is one of the lessons from the 2001/2003 battles in Afghanistan and Iraq. Small special operations units, highly networked into a precision strike architecture and using their inherent stealth while supported by persistent surveillance, "defeated" conventional formations a hundred times their size. Similarly equipped divisions defeated entire armies defending their home ground. The lesson was clear. Just as hyper-empowered individuals will draw on advanced technologies to affect entire societies, hyper-empowered soldiers will affect entire battlefields. The "Army of One" is not just recruiting hyperbole.

How potential enemies employ this emerging concept should be a major collection requirement for the Agency. Once we detect integrated progress in the precision weapons, networked sensors, signature reductions and UAVs of a target military, the intelligence challenge should move beyond the performance specifications of these systems. Rather, the intelligence challenge will be to assess the strengths and vulnerabilities of a robust, interoperable, synchronized system of systems.

Projecting the Impacts of Global Persistent Surveillance

The realm of possible knowledge will include enemy fleets, logistics, industry, bases, command and control, armies, air forces and lines of communication. There is every indication that technology will magnify this exposure for the foreseeable future.

The emerging opportunity for the Defense Intelligence Agency is to operationalize global persistent surveillance. Technology will afford the Agency the ability to orchestrate collection, reporting and publicity to do more than inform combatant commanders and the acquisition community. Technology will afford the power of observation to operationally affect the behavior of targets.

This concept is similar to the use of observation during the 1995 Dayton Accords and the 1962 Cuban Missile Crisis to influence negotiations and allied opinion, but on a daily, routine basis. Persistent surveillance operators

"The more precisely the position is determined, the less precisely the momentum is known in this instant, and vice versa."

Werner Heisenberg

"The joint force must be able to take advantage of superior information converted to superior knowledge to achieve "decision superiority" — better decisions arrived at and implemented faster than an opponent can react, or in a noncombat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission. Decision superiority does not automatically result from information superiority. Organizational and doctrinal adaptation, relevant training and experience, and the proper command and control mechanisms and tools are equally necessary."

Joint Vision 2020

can select the most opportune times to prompt diplomatic discussions, publicize events, steer the media, confirm media reports or share intelligence with others. Target states will, of course, know the U.S. has this ability; they will take off-setting measures (such as concealment). However, they cannot hide all deployments and they cannot know exactly how much the U.S. knows at a particular time, or how the U.S. intends to exploit its information. This uncertainty, in itself, will be a lever available to persistent surveillance operators. Enemies will modify their behavior based on assumptions of American surveillance of their moves. However, the main weapon will be the ability to exploit the information gained through persistent surveillance.

While it is true that persistent surveillance will allow the Agency to do present missions better, it is also true that persistent surveillance will open up an entirely new opportunity for the Agency. The challenge for the Agency will be to organize, conceptualize and equip to take advantage of the manipulation mission. No one has yet built the doctrine and methods of this weapon, nor is there a consensus with in the defense community as to how to employ it. Developing the doctrine, methods and organization for this emerging weapon should be a major initiative.

And persistent surveillance truly is a weapon. In 1927, Werner Heisenberg introduced the "uncertainty principle." He theorized that it is impossible to observe an atom without changing it. The mechanics of observation inevitably affect the target of observation.[35]

Anyone who has shined a flashlight on bugs in the basement understands this principle. As soon as you shine the light, they start scurrying about. By observing them you change their behavior.

This principle has implications for the emerging technologies of persistent surveillance. Multi-spectral sensors deployed on satellites, UAVs, aircraft, ground stations and underwater will soon provide 24/7, all-weather global coverage. To some degree this has already occurred. This global sensor network, combined with the global communications network and the intense "flashlights" of public media will reveal — and quickly transmit — unprecedented amounts of information on the actions of even the most reclusive nations.

These technologies offer a unique opportunity. The technologies of the information age offer the potential to impose Heisenberg's principle on the behaviors of nations. If we observe each nations' every action, and if the very act of observation can affect actions, then it follows that skillfully applied observation can have a dynamic effect on adversary nations.

In essence, we can manipulate enemies through skilled observation.

"Microsoft is doing great work with service-based architectures. Once all our sectors use common code sets for like information, they can manipulate common functions across portfolios. Service-based architectures will also allow us to simultaneously update all architectures across the stovepipes."[36]

Fortune 500 CTO

"Computing, storage and communications will be practically free."[37]

Chief Scientist, U.S. Government Agency

Summary: It's the Convergences That We Need To Watch

In terms of technology, it is important to look beyond advances in any single technology. That they will only tell you part of the story. Rather, it is more important to identify big convergences and convergences of convergences that will eventually propel massive technological change. These are the drivers of fundamental advance. The Intel chip combined with Microsoft's DOS propelled the PC industry. The PC plus the Internet plus fiber optics propelled the networked IT advances of today, which enabled the Human Genome Project. No single technology moved these advances and, in turn, affected economy and society. Rather these fundamental advances resulted from convergences of convergences.

Over the next two decades, a series of technologies will converge to drive a new Defense Intelligence Agency. A partial list might include the following:

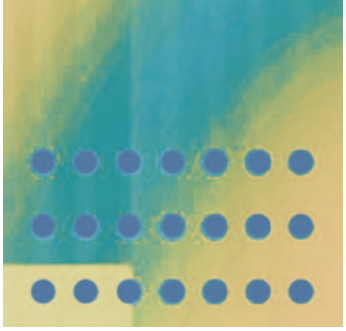
- Information will be cheap, accurate, near real time, massive, pertinent and persistent.
- It will flow via data networks that are 50 times faster than today's, producing practically unlimited bandwidth.
- Encryption and viruses will proliferate.
- Data storage will also become a commodity, with practically no limits.
- We can also expect data fusion at rates 104 times faster than today.

The effects of these advances will directly affect the Defense Intelligence Agency's workforce. Personnel will be overwhelmed with information unless the Agency moves to greater dependence on machine-to-machine data manipulation. Networks and robust databases will allow unprecedented levels of collaboration among analysts and subject matter experts situated around the world, resulting in dramatically improved predictive intelligence. Networks will allow the Defense Intelligence Agency to demassify intelligence, distributing analysis to a broader array of vigilant customers seeking to reduce threat levels. These threats may, unfortunately, multiply as the technological gap between the U.S. and the rest of the world widens, which will increase cultural antagonisms.

These antagonisms may provoke attacks on the U.S. information structure. They may also provoke biological attacks. Either type of attack would require specific expertise within the Defense Intelligence Agency (and its network of experts) to anticipate and prevent.

Progress in conventional weapons may be the easiest to foresee. There is considerable momentum along four aspects of weaponry: precision, sensors, stealth and UAVs. More progress within these confines, centrally networked, is probable. The central challenge for the Defense Intelligence Agency will be to produce analysis within the greatly accelerated kill chain used for conventional weapons employment.

These and other technologies have the potential to converge in ways that will produce a defense intelligence establishment of unparalleled impact. If George Orwell was correct, emerging technologies will confer an extraordinarily high value and responsibility on the Defense Intelligence Agency of the future. The Agency, however, will require extensive adjustments to realize the full potential of convergent technologies. Although we do not know the exact phenomenology of emerging technologies, we do see aspects of their inevitable outline are visible. By recognizing these potentials in advance, the Defense Intelligence Agency will create its future.



PROCESS

Changing an organization's processes can drive and sustain transformation, unleashing organizational potential. Processes express strategic intent, vision, and values manifest as actions — they are where the rubber meets the road.

"An organization's capabilities reside in two places. The first is in its processes — the methods by which people have learned to transform inputs of labor, energy, materials, information, cash, and technology into outputs of higher value. The second is the organization's values which `are the criteria that managers and employees use in the organization use when making prioritizing decisions... The very processes and values that constitute an organization's capabilities in one context, define its disabilities in the next."[38]

Clayton Christensen, The Innovator's Dilemma

Of the changes described in the preceding sections, one in particular will have direct and significant impact on the processes of the Defense Intelligence Agency. Rapid advances in technology will reduce information to a commodity. It will become even cheaper to produce, faster to deliver, and in more abundant supply than it is today.

The "commoditization" of information, driven by technology, will redefine the value equation between the Agency and its customers. While information will be in abundant supply, the attention of customers will not be. It will become scarce, scattered, and competitively sought after. Already, the Intelligence Community competes with the mass media on some level for attention. Walk into any senior official's office and see the television tuned to CNN and a copy of Jane's on the coffee table. Outside sources bombard the Intelligence Community customers with information on a daily basis. Going forward, new systems will add to this data flow, creating customers' demands for increased speed, ease of use, and mass customization. In short, customers will demand "more, better, faster" customized information in the future.

This new definition of value will fundamentally change the way the Agency carries out its processes. It will therefore require an underlying change to the mindset that drives new processes. In the quotation at the opening of this section, Dr. Christensen points out, "The very processes and values that constitute an organization's capabilities in one context, define its disabilities in the next." This is

"In this new economy, capital, labor, information, and knowledge are all in plentiful supply...What's in short supply is human attention. Telecommunications bandwidth is not a problem, but human bandwidth is. At one point, software magnates had the ambition to put "information at your fingertips". Now we've got it, and in vast quantities. But no one will be informed by it, will learn from it, or will act on it"[39]

Thomas H. Davenport, The Attention Economy

Timely — and Timeless — Business Ideas from Harvard Business Review

Each year, the editors of the *Harvard Business Review* (HBR) release a list of contemporary business ideas they believe to be important at the moment. In an article released in the April 2003 edition, the editorial board chose five topics based on what they believe, "business executives should be thinking about as they look into the future".[54] The five ideas, reviewed in a synopsis below, provide relevant insights for the Defense Intelligence Agency as it embarks on a path of fundamental transformation.

1. Know where you are in the business cycle — and be ready to get out

Human nature instills in all of us a tendency to hold onto what we know, even if it's outdated and outmoded. In business, however, this can be fatal. If a product or service is on the wane and customers are moving on, the company that holds on to it out of a misguided sense of security or identity will be on a slow march to extinction.

For the Defense Intelligence Agency, the business of intelligence is rapidly evolving, primarily due to changes in the security environment, technology, and expectations of customers. In response, it needs to incorporate new capabilities, services, and processes. Equally important, however, is that organizations will need to divest old processes. The article refers to divesting as the "missing link" of strategy, because so many ignore it. The public sector tends to be especially guilty of this, lacking the financial pressure of shareholders, and regulated or man-

why fundamental change is necessary: current capabilities, the core competence of present success, will become disabilities in the future. Incremental change is not a form of evolution for the Defense Intelligence Agency — it is devolution.

In this section, we will examine a development path for new thinking and processes, beginning with the environmental factors that are driving these changes.

Information Overload Means Competing for Attention

Already, we see the shortage of attention becoming an important issue. Within the intelligence community, people speak of being "awash in information" as the capability to collect outpaces the capability to analyze. In the business community, Davenport refers to this phenomenon as the "assault of information," with millions of e-mail and voice mail messages sent each day requiring the constant attention of executives. We are already wary of it, as a recent survey of senior executives revealed. It assessed potential demand for a new in-flight e-mail and Internet access prod-

Challenge	Customer Desire	Implication
Newness	Customers will continually ask providers to "tell me something I don't already know".	The information paradigm for intelligence customers has grown beyond the walls of the IC and now includes mass media outlets such as CNN.
Compelling	Customers will increasingly want to know *why* they should pay attention to something.	The need to provide the "why" as well as the "what" will drive products and services to be 'contextualized' around multiple dimensions.
Aggregated	Customers will value those entities that can effectively pull together disparate sources of data into narratives that are easy to understand.	The desire for aggrefated data will change the nature of "all source" to include the culling of open source as part of the context provided.
Quality	Customers will continually need to question the quality of data and will value an organization that can vet information effectively.	The desire for vetted, reliable information will drive the continued resurgence of HUMINT along new and varied roles.
Customized	Customers will increasingly desire information to be presentedc in a way that is tailored to their specific needs.	The type of work J2 is currently doing by developing different slices of information for various leaders is a nascent example of what's to come.

Illustration 14: Five dimensions of the "Attention Economy" as applied to the Defense Intelligence Agency

dated activities tend to keep outdated processes in place.

2. New processes will be less linear than the ones they replace

The speed and transparency of information, the capacity to build virtual networks quickly, and the ability for individuals to work as empowered "units of one"[57] are colluding to change the conception and design of business processes. Many of the processes used in businesses today, the HBR editors argue, are a holdover from the manufacturing economy (Second Wave[58]), which required linear sequential processes — symbolized by the automobile production line. The editors believe that linear processes are a misfit with today's networked economy (third wave), where information and resources can come from anywhere at anytime.

In their view, linear processes limit an organization's potential because they don't allow for creativity or collaboration. New processes are more likely to be less structured, and possess a quality of "messiness" in contrast to the neat orderly flow of mass production. For the Defense Intelligence Agency, this has particular importance going forward for two reasons: a) the building of a contingent network as a component of the workforce will change the flow of work, and b) the redesign of the analytic process to take advantage of collaboration technologies and all-source will require a purposeful lack of rigidity.

> *"...before we leap in with more controls and regulations, remember that messiness isn't all bad...Much like a Jackson Pollack painting, it can be confusing and disorderly — defying conventional aesthetics — but at the same time pulsing and vibrant".*[59]

uct. Surprisingly, a sizeable percentage of those surveyed did not want in-flight Internet access. Instead, they preferred to use their flight time as an escape from the expectation of being constantly accessible. They needed downtime from information overload. As Davenport points out, human bandwidth is not endlessly scaleable.

The endless flow of information pitted against a limited supply of attention will create future challenges for the Defense Intelligence Agency as it reaches out to customers. We describe some of these challenges in Illustration 14.

These challenges will require changes in the processes by which the Agency collects, processes and disseminates information. We examine these dynamics and the implications for the Agency in detail below:

1. Newness: Tell Me Something I Don't Know

During the first Gulf War, CNN's live coverage became a potent factor in the decision-making process. An outgrowth of this development was a subtle change in how policy makers view the set of information resources available to them. It is now the norm to see a television in a policy maker's office tuned to CNN or similar news organization. This is symbolic of the change in reference. The immediacy, novelty and visual appeal of television reporting has changed the scale against which the intelligence community is measured:

> ***"I have three tests I apply to intelligence. The first is The Economist test. If I can learn more about something from reading the Economist than I do from your brief, you fail. The second is the Jane's test — same principle. The third is the much-dreaded CNN test. The difference with this test is that CNN doesn't even have to get it right, but they have to get it fast. Did yours get to me fast? Few intelligence briefings pass these tests."***[40]
>
> Intelligence Community Leader

In the future, the multiplicity of sources will raise this bar for what constitutes "new" information. One reason is the speed at which open source vehicles such as CNN can deliver information. Another is that sensors are becoming increasingly cheaper to produce, giving competitors access to their own sources of primary data. The availability of this type of information in the public domain will beg the question of how and where Defense Intelligence Agency will allocate collection and processing resources. We discuss this further in the Aggregated and Quality sections ahead.

2. Compelling: Tell Me Why I Should Pay Attention

3. A critical leadership competency — emotional intelligence

The concept of emotional intelligence, as developed by Daniel Goleman and collaborators, continues to hold weight within the management community. This is because organizational development professionals recognize a lack of people skills as a source of derailment for many executives on the fast track. The editors point out that executives often just don't see the problem, which is why companies are increasingly turning to coaches and other means to help leaders develop in this area.

For technical or analytical organizations, such as the Defense Intelligence Agency, this issue is particularly pertinent. Often highly skilled and valued technical or analytical employees have a difficult time transitioning to a supervising role. Without proper screening and development, these employees can prove to be a disaster in their new roles. The work the Defense Intelligence Agency has done in profiling technical managers is a positive step in this regard. The "People" section of this document discusses the concept of creating 'in place' promotions for valued technical employees who either don't display the necessary managerial attributes or simply don't wish to progress in that direction.

4. Leadership is a group activity

Effective CEO's are those that can build, empower, and motivate a first-rate executive team. Along with defining a clear and compelling vision, the ability to compose a high quality team and then optimize them is what sets truly effective leaders apart from the rest. The effectiveness of the team can drive change through the organization, which makes this important for the Defense Intelligence Agency. While the process of building an effective leadership team begins

In human nature, we look for signals as to whether the data is valuable as one response to information overload. The need to provide customers with such signposts will set into a motion a couple of important of processes related implications:

- Products will become more anticipatory, scenario driven, and predictive; production will require acceptance of risk and new forms of ownership over the products. Analysts will have to publicly stand behind their predictions as they present them in person before decision makers.
- Analysts will provide more contextualized information with cultural and functional insight, including for example, economic, political, military, humanitarian, and infrastructure.[41] Products will need to postulate the likely secondary, tertiary and lower level effects of an occurrence — not just report current happenings.
- The use of logical narratives and stories will become important as customers seek to place new data into their own frames of reference. Customers will look for information translated into stories and experiences that are relevant for their background.

3. Aggregated: Tell Me Everything At Once

The Google web site recently initiated a news portal that uses algorithms to aggregate, prioritize and "continuously update" stories from media sources all over the world. The company states that the program scans 4,500 outlets.[42] The sheer number of media sources available today makes it impossible to track them other than through such computerized algorithms, which is Google's value proposition. As these types of technologies develop in the public arena, they will change the information expectations from customers in the intelligence world.

Intelligence customers will be looking for a product that can deliver vetted all source information to one location, in way that is easy to use and customizable. And specific to the military, as technology makes information access possible from anywhere, this type of product will have important uses in supporting network centric operations:

> ***"As the brigade commander [issuing the] warning order, as I move into somewhere I want to be able to take out my computer map [on a hand held device], look at where we are using a light pen, and instantly understand how part of city operates. The computer gets every dimension. Everything the government knows about that area of the city — is available and piped to me instantly."***[43]
>
> Interview with Bob Leonhard, Author of Fighting by Minutes: Time and the Art of War

with careful selection, it must continue with an equally careful development and alignment of activities. This cannot happen by default.

The HBR editors warn leaders not to let their team fall into the trap of "unconscious collaboration," where members just follow along without comment. Instead, they encourage a proactive, healthy debate to ensure real engagement and commitment. In their view, it is as important to have good "followership" as it is leadership. This idea interconnects with the previous concept of emotional intelligence, because both underscore the importance of interpersonal and communication skills required of effective leaders for today's organizations.

5. Know the tangible and intangible assets (and liabilities)

The tangible assets of any organization would appear to be obvious, but this topic is more nuanced than it first appears. The point made by the HBR editors here is to know which tangible and intangible assets are of value to *customers* — not the leaders. That isn't always the obvious product or service — many times, it's the intangible piece (such as the convenience of a store's location or the atmosphere of a restaurant). Assets that don't provide value to customers are liabilities (because they require resources) and organizations should divest them. Gaining clarity around what customers want — both expressed and unexpressed — is critical for any organization, but particularly so for those going through transformation and reallocation of assets.

In the future, as the Defense Intelligence Agency moves from a 'product' to a 'product and service' orientation, this will become increasingly more important. In a service environment, customers will value the intangible interaction as much as the tangible report. This will require new thinking about human

Leonhard's quotation makes the point of saying everything the government knows. He is including in this information from the Department of Commerce, Energy, State, Agriculture and more. The objective of the Agency is not to own all sources of information internally, but to know where they reside. This means building a wide-ranging network of experts and a set of structures and processes that optimize them. We discuss this idea of building an extended network at great length in the Structure and People sections.

Open Source This concept of "aggregation" raises historic questions about the value of open source information, a controversial subject in the intelligence community, where concerns about denial and deception exist. The case for open source becomes more compelling, however, where the intelligence community has trouble collecting against new forms of targets. As one academic familiar with intelligence said, "Open source becomes more important as the nature of the threat changes, and it is more difficult to collect against this new kind of threat than our traditional 'countries of concern.' We don't do very well against Al Qaeda, and we're collecting too much against the threats we know."[44] The Agency will need to acquire innovative new processes for the assimilation and vetting of open source intelligence. One example is outsourcing open source production to an organization like Jane's or setting up less secure processing centers that allow people with cultural and functional knowledge to contribute even if they cannot qualify for a security clearance under current regulations.

4. Quality: Tell Me I Can Trust You

To be an effective "all source" shop in the future, customers will hold the Defense Intelligence Agency to a high standard of information reliability and trust. This requirement for reliability will create a need to increase the capacity for independently collecting and vetting information. The most effective means for the Defense Intelligence Agency to establish this reliability is to increase the size of its HUMINT capability. This is also true in light of the potential rise in encryption usage and the increasing need to get at target "intent".

"I don't want you to think that our analysis doesn't look at these other sources — but at the end of the day, we try to get vetted HUMINT that verifies anything we learn from another INT. Vetted HUMINT is first among equals in my view."[45]

Print Media Thought Leader

and technical processes. For example, as analysts work in real time with customers, the need to build and manage positive external relationships will become critical. And as customers log-in to use an on-line service, they will want the ability to search using natural languages and to customize views to their needs. This changes the profile of the workforce, because certain attributes (such as the ability to anticipate customer needs) will become predominant. The workforce of the future attributes chart contained within the "People Section" of this document reflects this idea.

The editors of HBR chose these five ideas because current technical and economic forces require business leaders to, "come to terms with their assumptions about business, leadership, and the people who make organizations work".[63] This is an apt description of the Defense Intelligence Agency's current situation, since the Agency faces essentially wholesale changes in its operating environment. Forces will come in the form of increased market demand, volume, and velocity — creating an unprecedented set of circumstances that will require "major paradigm busting" as one senior leader stated. However, by knowing the organization's real tangible and intangible assets, anticipating the customer's needs and sense of value, divesting outmoded processes, and building a strong and capable future workforce the Defense Intelligence Agency will be on the right path to success.

Determining what defines product quality is of paramount importance for the Defense Intelligence Agency, and will require an understanding of customer needs (both expressed and latent). It will also require anticipating needs by living in the customer space (see "Recommendations" section regarding the installing of attachés at customer sites), proactive customer education, and including customers at the outset.

Some urgency exists on this issue. During interviews conducted for this project there was a theme that customers are not as involved in the process as they should be. One intelligence community member remarked, "People have lost confidence in [the Agency's] product...As a result, there's not a lot of time that people spend trying to establish connections [with the Defense Intelligence Agency]....The issue is quality of product. If you have a valuable product people will look you up regardless of how hard you are to find... the line to customer will be shortened."[46] Said another, "Written reports are usually void of any insights... As a result, they are only useful long after the consensus has already moved to cover that area. In essence, written DIA products are usually void of relevant detail when it comes to emerging or controversial areas."[47]

5. Customization: Tell Me In My Own Way

The idea of 'mass customization' will take hold as information technology allows those providing or using products to tailor them. "My Yahoo" and Amazon's "My Store" are two examples of customized Internet applications in widespread use today. Both of these track on-line activities and reformulate the customer's view proactively recommending things based on relational algorithms.

As artificial intelligence and sense-making improves, the opportunity for highly sophisticated customization and presentment schemes will become available. For the Defense Intelligence Agency, these technologies may be suitable for taking a "first pass" at fulfilling lesser order of magnitude requirements, running manipulations of data to identify new patterns such as material movements that could indicate weapons of mass destruction (WMD), and lessening reliance on happenstance or synaptic connections of analysts.

The Process of Developing Processes

The point of departure in designing new processes is to understand that the environmental factors present will impose significant impacts upon the organization, its work, and its products. It must then understand how customer demands will dramatically change expectations of what the organization is delivering.

Both of these are present in the Defense Intelligence Agency's operating environment. By determining the key environmental factors present, the organization's leadership can then determine the change imperatives, and finally create a set of principles upon which to build the actual processes (Illustration 15).

Developing Results Oriented Processes

Understanding how the operating environment and customers change the formation of future processes, requires a logical path of inquiry. This path begins by scanning the operating environment to identify the factors most likely to have significant impact on the organization, its products, and services. It then marries this data with relevant customer knowledge to create a set of change imperatives for which the Agency will design new processes.

Once the Agency knows the factors influencing the environment, and determines imperatives for changes in processes, it establishes a set of guiding principles. These will form a set of doctrines upon which new processes will be developed, and as such, will serve as guidance to all those involved in process making going forward. The formation of such principles comes out of the engineering disciplines, but is serviceable and important for all types of processes. As an outgrowth of the principles, it often makes sense to determine the features desired in future processes as further guidance to the workforce.

For the Defense Intelligence Agency, this path of inquiry is an important step towards developing processes it can sustain against the operating environment and will deliver the outcomes needed. Given what we know about both the environment and customers, a notional view of how the Agency would develop processes appears in Illustration 15.

Factors As the illustration indicates, the factors identified would include any major impact on

Factors ⇨	Imperatives ⇨	Principles ⇨	Features ⇨	Results
■ Technology drives sharp increases in volume and speed of information ■ Network centric warfare systems drive up information demands ■ Shifts between war and peace missions change nature of information demands quickly ■ Competition for leadership attention intensifies as media outlets increase and as open/closed source information gap shrinks ■ Customer decision processes become increasingly real-time based	■ Information dominance leading to decision superiority is critical present and future DoD advantage ■ Customers bring expectations for "more, better, faster" information from external world ■ All-source intel composition demands integration of systems for sense-making ■ Knowledge usefulness requires linkages beween operator, exploiter, and analyst at outset ■ Balance of regional and functional threats/issues drives cross-functional knowledge approach	■ Forward looking; imaginative and innovative, insightful and predictive ■ Reduce and mitigate ambiguity and uncertainty via dealing in plausibility and possibilities ■ Drives for continual context by bringing together myriad of disparate data into logical narratives ■ Customer and outcome driven; modifies resources used to meet needs and continually reassess and refine ■ Opts for speed but balances with accuracy and usability by customer	■ Manages customer requirements ■ Collection based on operational needs ■ Leverages knowledge technology for 1st pass ■ Networked across IC, customers, experts ■ Robust workflow management for teams ■ Process sets the "what' not the "how" ■ Decision making is driven down levels ■ Rules are minimal versus plentiful ■ Culture supports innovation/taking risks ■ Builds shared sense of values/expectations	■ Intelligence cycles are aligned around customers/outcomes ■ Concentration of resources/effort on areas of most value; outsource of non-value added activities to partners/vendors ■ Middle management and product rules are heavily divested; new knowledge tools and experts invested ■ Products become product and service as interaction is valued as much as information ■ Innovation is introduced via cross-functrional, diverse teams with multiple frames of reference and scenario planning

Illustration 15: Elements of DIA's Future Process Development

the organization, ranging from changes in military operations to the aforementioned lack of customer attention. In essence, this effort requires the leadership team or others developing a specific process to conduct a form of scenario planning, bounded by the limits of the process to identify and vet all the potential factors.

Imperatives The development of imperatives requires the Agency to weight all the factors, influences, and demands on the organization. This assessment requires making a series of strategic trade-offs about the specific environmental factors and customer expectations that will be deemed important enough to warrant attention (and eventually resources). In considering these, it will be equally important to understand why something is not chosen as an imperative as much as what is, since all factors possess some potential form of impact on the organization.

The items shown on the diagram above, while notional, point to some key themes which will become cornerstones of the Defense Intelligence Agency's transformation, the most important being the move from a hierarchal structure to an agile networked organization. Another theme describes the progression from 'product' to 'product and service' (e.g. live interaction of analysts and customers). A third theme moves from an individual practitioner with an on-going focus to diverse, multi-perspective team based projects. The final theme requires processes and products to be anticipatory, imaginative, scenario driven, and risk embracing.

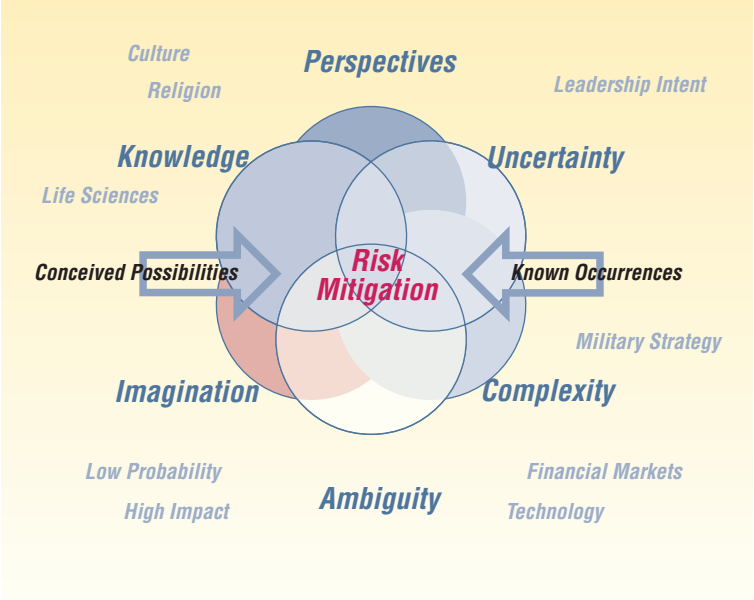


Illustration 16: Scenario planning brings together perspectives to unleash creativity

Processes Occur on Two Levels: In Action and In the Mind

Processes designed to be anticipatory and imaginative will perform successfully as guides on two levels. First, they will guide action— the allocation of resources and activities — in a way that aligns with customer needs and expectation. This guidance focuses action around outcomes and the delivery of real value. Second, they will guide cognition— the mental pathways by which the mind will interpret objectives and the processing of information. To achieve the type of innovation referenced in the "Results" section of Illustration 15, processes must have an understanding of the culture that exists and stimulate thinking, interaction, and the busting of individual and mental paradigms.

Scenario Planning to Identify and Mitigate Risk

The use of scenario planning has been in place at major corporations for a number of years, and with particular effectiveness at companies that must deal with a high level of risk and complexity. Royal Dutch Shell[48], for example, uses scenario planning to identify and assess complex and inter-related energy, economic, and geopolitical risks — very similar to the risks facing the Defense Intelligence Agency.

The use of scenario planning as a work process supports several of the principles outlined in Illustration 16 by being both forward looking and risk mitigating. Scenario planning accomplishes this by encouraging employees to operate mentally outside of the limits of their own experience and identity, and by taking advantage of the multiplicity of perspectives that it can gather in cross-functional, cognitively diverse teams. In addition, sce-

nario planning increases the chances for identification of new patterns and threats by bringing together those with different sets of information.

The ultimate capability would be to conceive events such as the low probability high impact threats that seem irrational to Americans, but are completely rational to someone waging asymmetric war against the United States. The postulation of difficult, unpleasant, and pessimistic possibilities is something that cognitive science tells us human beings physiologically seek to avoid. The use of structured group processes, underpinned by a culture that supports innovation, will be an important risk mitigation strategy in the future. Among the largest risks the Agency faces now and in the future is the failure to take risks — to postulate and contemplate the unthinkable, to move out the comfort zones and into the area of unknown but not unknowable.

Social Network Optimization to Support Innovation

The Agency will design processes on an awareness of the existing social network of the organization. Analyzing and understanding the existing network is not a tacit acceptance of its continued dominance, but is the first step in changing the existing "work network" as social scientist Karen Stephenson calls it in Illustration 17.[49]

The social network, which when layered with attitudinal attributes forms the culture, can either support change or become the silent killer of transformation. Several concepts outlined in this paper depend on management the social network for effective implementation and execution. For example, the creation of cross-functional teams depends on team composition. The idea of the contingent workforce depends on relationships within the network and stationary workforce.

The work of Stephenson takes the concept so far as to organize physical space around optimizing the social network. She creates a sort of planned serendipity of contact among employees by situating offices and pathways so they will cause beneficial interactions. Further, she performs a 'social network analysis' to determine who is an information node in the group, who is a connector, and who is a generator of positive interaction. This takes the Agency's concept of co-location to a new

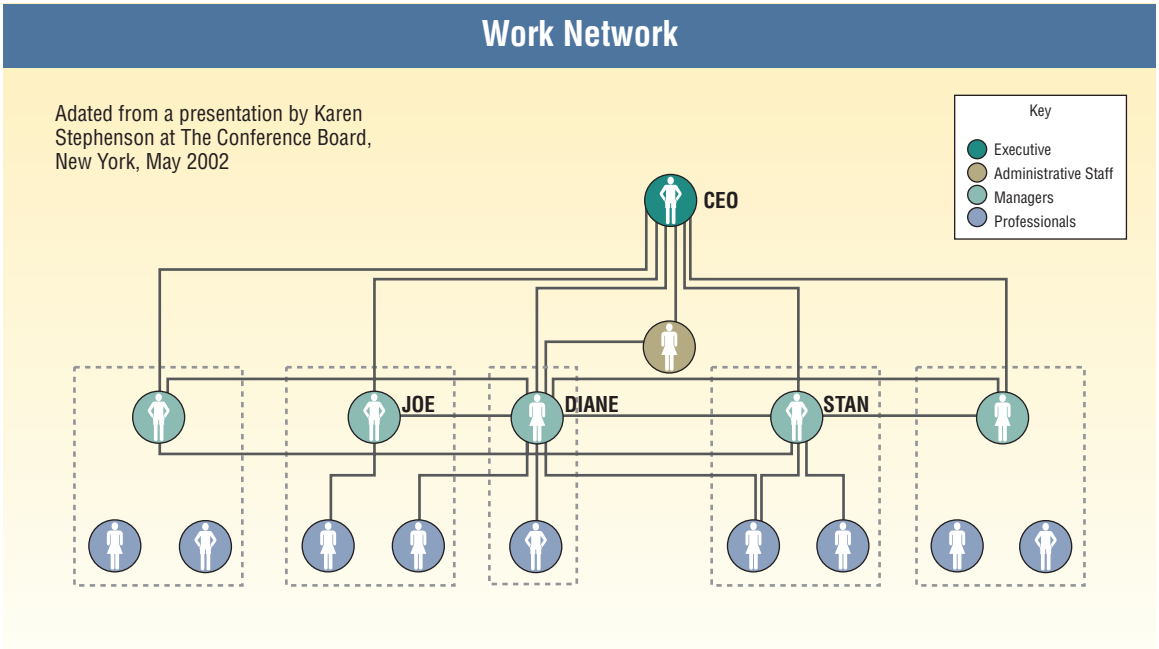


Illustration 17: Notional 'work network' by social scientist Karen Stephenson[50]

level, and seeks to optimize it at both the individual and group level.

Structure And Processes: Form Follows Function

The processes designed for a network organization are much different from those designed for its hierarchal predecessor. In a pyramid organization, Illustration 18, processes are linear and sequential, while in the network organization, Illustration 19, they are outcome based and many run in any direction. One feature of a network organization's process is that the locus of decision-making authority moves down the organization. It lies with those who have first hand knowledge of the data, interact with customers, and conduct collection activities. The intent is to "de-layer" processes in order to speed them up. Another difference is that the Agency can bring in customers early and make them an on-going part of process development to ensure value.

A recent article from the Harvard Business Review compares processes of the old and new economy this way:

> ***"By its nature, work in a mass production economy imposes order and conformity. But work in today's knowledge economy seeks variety and innovation. If the assembly line was the symbol of mass production, the messy desk is the icon of the information age. Furthermore, getting work done nowadays depends on getting employees to share information and make informed decisions — processes fraught with ambiguity and subjectivity."***[51]
>
> Editors, Harvard Business Review

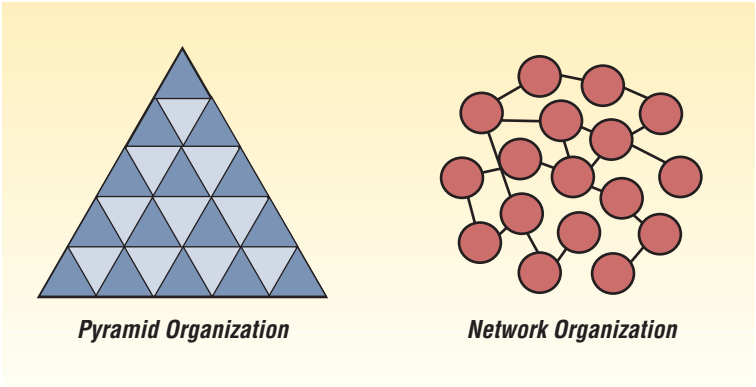


Illustration 18: Pyramid OrganizationIllustration 19: Network Organization

Networked Processes Need Strong Project and Information Management

Successful management of network-based processes requires a strong project and information management function. The emphasis of this function is not command and control, it is the opposite: facilitating work flow, ensuring the sharing of information, and the successful composition of diverse teams. Network systems are typically more productive when middle management is de-layered as much as possible and the norms encourage the sharing of insights and ideas. This, of course, does not reflect the current Defense Intelligence Agency organization, as it does not reflect most of the federal government.

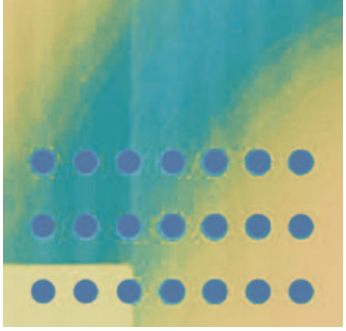
Continuous Customer Focus Helps Assure Value

At the operating level, the Agency will focus on proactive management of customer requirements as the single most important factor for aligning resources, outcomes, and expectations. All successful businesses strive for this alignment, but especially those with intangible output. Unless they postulate and refine the customer's need, they waste resources. In future processes, three forms of requirement vetting will be available: 1) customers enter the process early and remain, 2) putting an attaché type function in the customer space, and 3) making the process customer centric and continuously refining it to assure value.

> ***"The key is to change the culture of the leadership at top and change it at the bottom. Squeeze the middle level. This is where the biggest issue [of transformation] will be located. Mid-managers will hang on and will fight you tooth and nail. They're the most invested in the status quo — others want it".***[52]
>
> Federal Law Enforcement Community Leader

In Dove Consulting's organizational transformation work, the firm finds a clear link between structure and process. The highest resistance to change — including process change — is normally in middle management. This is why the idea of de-layering is so important. Change tends to penetrate the top of the house quickly because top leaders recognize the need for change and want to fulfill the vision of their boss. At the bottom, where broken processes are a fact of day-to-day work, the desire for change is strong as a vehicle for pain reduction. However, for the middle tier which has a high investment in the status quo, reform presents a more significant challenge.

In the next section, we will examine future structures in detail, and the opportunity to use these as an impetus for change and growth.



STRUCTURE

Structure follows strategy and form follows function in an effective organization. As the environment changes, strategies change and functions evolve-the functions grow, diminish, or disappear. Thus, effective organizations place a premium on agility and adaptability. Having the right people organized in the right basic structure is critical to maintaining the advantage.

"The knowledge of the world is only to be acquired in the world, and not in a closet."

Lord Chesterfield

In this section, we discuss the changing environment in which government and the Defense Intelligence Agency must function, and the structures that will emerge to facilitate their missions. Internal structures affect how people and process work together, how they gather and use information and how they interact with customers. Structure similarly facilitates or hinders external processes and interactions-with partners, suppliers, and customers. Technology enables opportunities for new kinds of structures, and properly applied, greatly enhances organizational power. We will consider the interrelationships of these factors as we envision future structures of the Defense Intelligence Agency.

Today's Challenges Drive Tomorrow's Structure

The behest of the Secretary of Defense to "know a little bit about everything" is by implication, an organizing principle. It requires both breadth and depth, and, within the limited resources available, invites a constant tension between what we need to know today, and what we'll likely need to know tomorrow. It must also be able to provide decision support in widely different time contexts-providing immediate data to the battlespace occupants and decision makers, and the ability to provide thoughtful, considered context built over many years of experience to planners and policy makers.

Today's and tomorrow's challenges come from rogue states and terrorists, and the greatest danger lies at the crossroads of radicalism and technology[53]. The structures of our national security organizations must enable them to preempt familiar and not yet familiar threats. The critical question, then, is how to best organize the agencies we charge to mitigate those threats. The ongoing war against terror triggered many reassessments of our approaches to national security. By assessing how adversary organizations are structured and the nature of information age violence, the Defense Intelligence Agency and the U.S. government can learn something about how to organize themselves to defeat them.

Although there are over one hundred terrorist groups on the national security radar screen, Al Qaeda is a top concern. Al Qaeda is regrouping after the death or capture of many of its leaders and trained operatives and, the

Attachés

In the global war on terrorism, U.S. intelligence agencies work closely with internal security forces around the world. This cooperation is critically important. Internal security agencies have local knowledge and access far beyond what U.S. agencies can replicate, including large numbers of immediately available personnel. Fortunately, most foreign intelligence services share a common interest in the global war against terrorism and routinely cooperate with the United States.

In many cases, U.S. military attachés are a primary link with foreign intelligence services. They convey specific intelligence requests and facilitate reciprocal questions. Attachés perform this and other intelligence functions in addition to their representational duties.

In the emerging environment, the role of attachés in HUMINT (human intelligence), particularly their ties with foreign intelligence services, may prove their most critical function.[74] It will often be through personal ties with an array of foreign intelligence forces, from police and militias to military intelligence and local nationals that will allow the U.S. to rapidly identify and preempt terrorist strikes.

Anyone who has lived abroad knows it takes time to build domestic ties. An attaché might build strong relationships with one or two military counterparts during a standard tour (two or three years), but that is not enough time to build ties with an array of local sources. Many countries have multiple intelligence services, not all of whom cooperate with each other. Non-governmental organizations (NGOs), local media, the business community and individual military members are also potential allies in the war on terrorism. Such a wide array of human intelligence relationships requires time and expertise to develop.

loss of support from the Afghan government. Surviving members are negotiating deals and alliances with other terrorist groups, and are furiously searching for state support from another government to replace that of the Taliban in Afghanistan.

Although Al Qaeda is not a nation-state, and has comparatively little in the way of capital equipment or even in manpower and financing-it has been fairly successful in carrying out high impact, attention-grabbing events. In fact, their strength and the strength of similar enterprises derives precisely from the fact they are small, fast, flexible and flat structure, while the American government is huge, slow, rigid and pyramidal.

Huge and pyramidal structures worked for World War II. They worked in the Cold War when the United States opposed an even more bureaucratic foe. But attempting to fight the deadly, fast-flitting, flea-sized terrorist enemy with pyramidal bureaucracies is a blueprint for failure.[55] Recent economic history is full of large bureaucratic institutions that were defeated by new, smaller, quicker and more agile competitors.

The Defense Intelligence Agency reflects the dominant organization structure at the time of its creation-a classic pyramidal bureaucracy. Although restructured many times since then, each iteration conforms to the classic government model that gathers information at the lowest levels, filters it, and then transmits that information through layers to the top where decision making occurs. This happens at the broad level of the organization as well as in smaller organizational units. Those filters compromise decision-making ability, and as the volume of the data stream explodes, those at the top are ill equipped to absorb and act on it. The current hierarchical structure comes from an industrial era facing a relatively monolithic threat. That structure is not harmonious with today's information environment and, without dramatic change, it will obstruct the Agency's primary mission of preventing surprise.

Alvin and Heidi Toffler describe another problem that occurs in bureaucratic structures like these: "When bureaucracies are forced to deal with a problem that fits into no one's existing cubbyhole, they behave in certain stereotyped ways. After some initial fencing, someone inevitably suggests setting up a new unit... This is instantly recognized for what it could easily become: a budget-eating rival of the older units..."[56] The result is a bureaucratic battle that detracts from a focus on the threat.

Another problem that occurs is a lack of horizontal integration and communication among departments and agencies engaged in doing similar work. Historically, agencies and operating units derived a degree of

Because military career tracks preclude long (more than five-year) assignments, retired colonels/captains with intelligence experience may be a preferred source for defense attachés. They have the rank and stability to develop and exploit a range of relationships in specific situations. This source would expand the pool of personnel available to the Agency (beyond what the services nominate). Using retirees would require legal and policy changes, but these changes may produce more effective attachés in the war on terror.

power from "hoarding" information. In the future, the agencies that share responsibility for producing the intelligence policymakers require to make better decisions, must collaborate, communicate, and freely share their data and information. U.S. national security is the beneficiary and maintains the advantage.

The future Defense Intelligence Agency is sufficiently self-aware and confident that it applies the right technology, processes, structures, and people to each potential threat. Reconfiguration is a way of life.

Some Businesses Model New Approaches

Large corporations have long faced similar problems and have devised partial solutions. Governments are not the same as companies, and intelligence agencies have special needs for secrecy. Nevertheless, the experience of business and the vast literature on the subject by organization theorists and management consultants can provide important lessons.

For dots to be connected, someone has to synthesize the information and develop the big picture. That is why bureaucracies also have

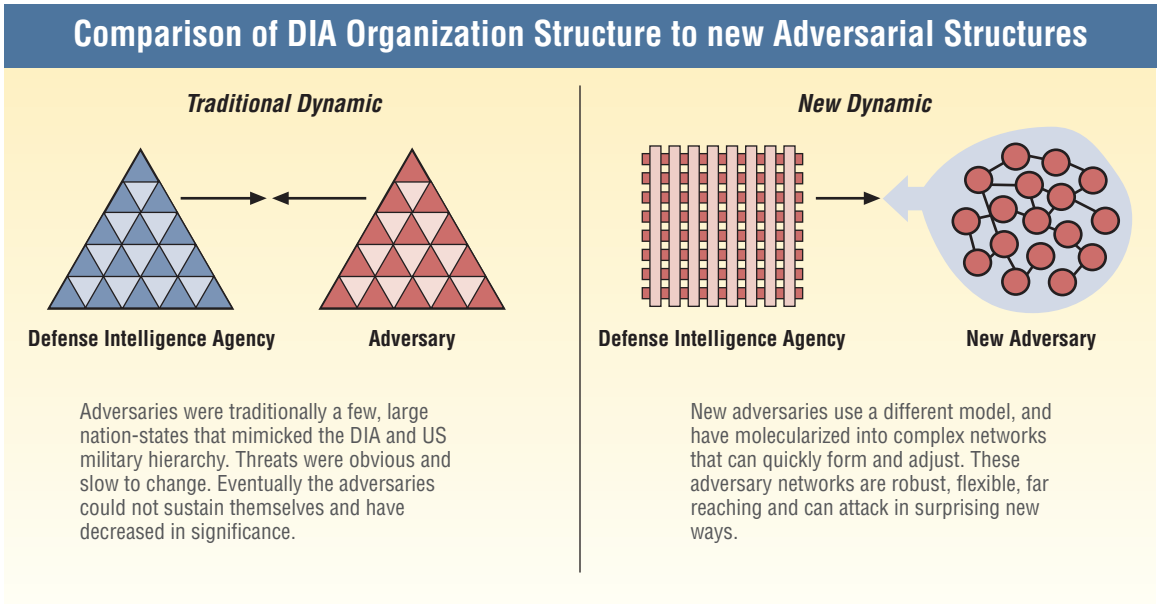


Illustration 20: Comparison of DIA organization structure to new adversarial structures

The Tenets of Effective Future Partnerships For The Defense Intelligence Agency

Over the next twenty years, the selection, building, and maintenance of effective partnerships will play a significant role in the Defense Intelligence Agency's success.

The future operating environment will present many forms of complexity. Primary among the drivers of complexity will be technology, because of the sophistication of the technology itself and the increased volume, velocity and variety of information is enables. This environment argues against the centralization of strategic assets because to do so would make it nearly impossible to effectively house the range of knowledge and skills the Agency requires. In addition, as an all-source organization, the Agency becomes conversant in a wide rage of issues to military, policy makers, and other constituencies.

These external drivers argue against centralization of technology and knowledge assets. They beg the question of how the Agency can best leverage its internal capabilities with external public and private resources. There are numerous strategic paths and organizational constructs, ranging from affiliation to outsourcing. However, every option—regardless of the terms of agreement—will require one thing: the effective building and sustaining of partnerships with organizations that possess different values and cultures.

How then can the Agency assess and determine the appropriateness and fit of partnerships? It must begin by looking inward, before it focuses outward on potential partner organizations. Consider three

Business Approach	Government Approach	Al Qaeda Approach
Smart firms have installed computers, networks and management information systems that make it possible for people to communicate electronically across horizontal lines and to skip echelons as they send information up and down channels, often bypassing the old gatekeepers.	Ironically, compared with business, US government agencies often have outdated computers and networks. Although today, the Defense Intelligence Agency has recognized the dangers associated with this lapse and is now upgrading its systems.	Al Qaeda uses cheap commercial communications technology to communicate with trusted members.
Companies have deliberately flattened their hierarchies, by eliminating the number of echelons between top leaders and employees at the bottom.	Civil service bureaucracies, where employees are unionized and pay scales are linked to hierarchical level rather than function or merit, offer resistance at the very thought of flattening.	It is unlikely that Al Qaeda has more than three or four levels, and its terrorists don't belong to civil service unions.
To combat monolithic rigidity some corporations break themselves into semi-autonomous business units, "profit centers," with their own boards of directors and instructions to act entrepreneurially, much as though they were small businesses. Unfortunately, many of the profit centers are themselves organized into pyramids — baby bureaucracies hived from the mother bureaucracy.	Bureaucracies typically organize around permanent functions, fields or disciplines, not projects. Even this kind of intermediate structure offers advantages over traditional government bureaucracy. The CIA's In-Q-Tel, which has evolved into a venture funding enterprise, is a government example of this kind of restructuring.	Al Qaeda, by contrast, is project-oriented. Each project is temporary and may involve people from different "disciplines"—bomb-making, money transfer, target surveillance specialties. Project participants either die — like the 9/11 terrorists — or move on to deadly new projects.
Large and small corporations increasingly conduct business across national borders, and in the Internet era, the lines between domestic operations and foreign operations continue to blur.	The United States prohibits the CIA from operating at home and only lately has begun sending FBI operatives abroad as it did during World War II.	Al Qaeda is said to have cells in 60 countries and moves its men, finances and ideas across borders at will.

Illustration 21: Compares Business, Government And Al Qaeda Approaches To Organization Structure[6]

points with respect to partnerships as part of the overall strategic planning process.

- Determine the areas where it makes sense for the DIA to set up some form of partnership and where to "go it alone" (including both mission and support areas)
- Consider a wide range of potential partnerships across the public and private sectors, including NGO's, academia, and others who seek new relationships
- Develop an order of magnitude for potential relationships, understanding that each partnership will require time, effort, and resources to maintain

Once the Agency identifies a partnership need, the process for identifying and selecting potential suitors closely mirrors the approach companies use in executing mergers and acquisitions. The merger and acquisition process begins with "due diligence" which, given the extraordinary mission of DIA, must be part of the initial step in reviewing candidates. The due diligence normally identifies a range of candidates, evaluates them according to predetermined criteria, and then conducts a thorough investigation. As the range of potential suitors becomes more widespread, the due diligence process is increasingly important.

As part of the evaluation process of mergers and acquisitions, companies must normally consider the full long term cost/benefit of a partnership in detail. This is a necessary practice for the Agency to adopt as well, since all the partnerships will require human and financial resources for long-term maintenance. Understanding the current and future value of a potential partnership to DIA's customers, and weighing that against a detailed cost estimate allows the

vertical "channels." At each level of the chain of command, a manager collects information from the cubbyhole controllers who report to her or him and decide whether to send it up through channels to the next higher authority. For example, such filtering did not work in 2001, when an Arizona FBI agent warned about potential terrorists enrolling in flight schools.[60]

Supporting the notion of a turf issue, a Defense Intelligence Agency executive noted, "The intelligence community is structured by its means, not its ends. Data is owned by the means [e.g., NSA collects the SIGINT, and also controls distribution]."[61] The future Defense Intelligence Agency has clear access to the level of data it needs.

This list could go on, but it is enough to suggest the intelligence community faces considerable challenges as it contemplates its own restructure. What, then, should the new structure look like?

Structure Is Not an "Either-Or" Decision

Some business consultants suggest that we replace all bureaucracies with networks, and discussions of organization tend polarize around these two organizational forms. In fact, it is possible to create flat networks within hierarchical bureaucracies, and bureaucratic units within networks. But there are far more than just these two basic models of organization.

In hierarchical Japanese corporations, employees who join the firm in a given year often form a cohort and maintain relations with one another throughout their subsequent career. Some might rise up the management ladder, others not. Irrespective of formal position, members of the cohort often dine together, drink together and swap information from all different positions in the firm, supplementing the information that flows through the formal chain of command. They share the real facts here, minus any official "spin." Which is why, once a decision is made, Japanese firms are quick off the mark. This dokika' system may be fading along with lifetime employment, but it suggests the importance of cross-communication even within bureaucracies and not just at the top.

Some political institutions in Germany and Austria are like a checkerboard, with a member of the majority party occupying the top spot, a minority member in the second position, a majority member in the third, opposition in fourth, and so on through the hierarchy, again assuring more sharing of information at various levels.

Then there are "skunkworks" — subordinate units inside a firm or government that are given a mission but kept free of the normal

Agency to assess relationships with full knowledge and credibility.

Once the Agency selects a partner, it establishes understandable ground rules between the organizations. This helps the leadership negotiate some form of contract, and ensure that the parties' expectations permeate both workforces. The downfall in most mergers and acquisitions happens after the agreement is complete: it is the integration of the organizations that fails. While a partnership does not require the full integration of a merger or acquisition, the two organizations must achieve some level of integration in order to succeed.

Seven ground rules will serve the Defense Intelligence Agency well as it establishes future partnerships.

1. Begin from a position of "mutual win" by identifying what makes for a successful outcome for both DIA and its partner

2. Establish a shared vision between Agency and partner that goes beyond tactical outcomes to include integrated values

3. Define the roles between partners carefully, with contingencies that either identify issues in advance and/or offer a mechanism for quick resolution

4. Establish expectations for trust, information flow, and security procedures — this will require a change in mindset that seeks to share rather than withhold information

5. Assign relationship owners who are specifically assigned to make the partnership work within a prescribed time with metrics

6. Seek to foster 'organic' connections between workforces by creating platforms for relationship creation via project design and social interaction

bureaucratic rules and formal organizational constraints. A famous example was the forerunner of the CIA, the Office of Strategic Services headed by William "Wild Bill" Donovan during World War II.[64]

These examples only begin to suggest the diversity of possible arrangements that are neither classically bureaucratic nor pure networks that need to be considered in any massive restructuring like that now under way in the United States-or in corporate reorganizations. Networks and bureaucracies are not the only options. It will take organizational creativity for countries to wage successful war against future threats.

Structure Leads to the Defense Intelligence Agency's Excellence

The Defense Intelligence Agency must understand and respond to present threats while it produces the capabilities required to checkmate emerging threats. Strategy harmonizes and balances the needs of a threat-based orientation with the demands of a capabilities-based orientation. Threats are now urgent, unrelenting, and voracious consumers of resources. Capabilities are over the horizon, reprogrammable, fungible, and unless respected in the organization's strategy, the development of capabilities is always at risk. The Defense Intelligence Agency's success in the future comes from its ability to align its mission, vision and strategy. Several structural moves facilitate that alignment.

The Defense Intelligence Agency will clarify and restructure its technological, social and operational architectures to better align with the characteristics of emerging threats. The goal is to provide better-networked, more responsive intelligence capable of surprising and countering U.S. adversaries through persistent and relentless coverage and a set of robust, resilient and hardened defense capabilities.[65] Organizational connections and the ways that the Defense Intelligence Agency uses them helps drive organizational effectiveness. The leadership will incorporate the missing pieces, establish a timeline, project the cost, obtain approval and execute. A staff team, expert in planning and budgeting, and familiar with the emerging operations issues develops the plans and budget that align with the strategy.

The Agency evaluates and rewards the planning team's effectiveness at anticipating and articulating the Defense Intelligence Agency's needs.

One Defense Intelligence Agency interviewee commented that there is already a positive trend towards a flatter reporting structure. An "Analyst's Note" goes straight to the J2 and the Director, Defense Intelligence Agency with no coordination required. A reviewer may check it

7. Regularly measure progress or success based on expected overall outcomes established at the outset

These ground rules, based on the principles used in mergers and acquisitions, provide a basis for effective partnerships by identifying mutually—desired outcomes and the necessary elements of agreement at the outset. In the intelligence community, where trust and sharing of information are against cultural norms, such rules will serve as an important signal that a change in outcome requires a change in mindset. However, the complexity of a future driven by technology will demand new ways of approaching the mission. Partnerships, in concert with the creation of a networked organization, will be a critical factor in the future success of the Defense Intelligence Agency and the Intelligence Community.

In this case, the past is not prologue; for the new operating environment is unprecedented.

for relevance, but these seldom short-circuit an Analyst's Note.[66] Speed of information becomes an even more critical success factor for the future Defense Intelligence Agency.

Toward A More Vigilant Structure

Structure follows strategy and form follows function in an effective organization. As the environment changes, strategies change and functions evolve—the functions grow, diminish, or disappear. Thus, effective organizations place a premium on agility and adaptability. Critical to adaptability are having the right people organized in the right basic structure. The Defense Intelligence Agency will find that structure based on an assessment of the future environment and an awareness of the capabilities it must possess to meet an expanded set of missions.

Given that states are not likely to wither away, and that the power of great states—witness the power applied by the United States in Iraqi Freedom — will not diminish,[67] the Defense Intelligence Agency will continue to take a geographical orientation in its mission. States will continue to be an organizing principle for competitive power, so culture and geography will continue to matter. Defense attachés will continue to serve in the venue of states, just as Department of State ambassadors will continue to possess accreditation as the Chief Executive's emissary to states.

However, geography and culture will not be the only things that matter. Regions will matter. Potential military capabilities and other forms of competitive advantage will matter. "Jointness" and an increased emphasis on understanding the employment of combined arms will not move the Services toward unification, but will change the attributes the Department of Defense seeks in military and defense attachés.

The Department of Defense and the Defense Intelligence Agency will grow to appreciate the advantages that accrue from using seasoned military professionals—retired general and flag officers and senior civil servants—as attachés. These attachés will serve longer in one country than they serve today. Attachés in the future will also have to work from their assigned states with an orientation broader than they possess today. They will have to understand the future's sources of competitive advantages that go beyond conventional military forces. Thus, the Defense Intelligence Agency must contrive an organizational structure that improves its ability to rapidly sense, analyze, and forecast changes in the competitive environment, and that both serves and capitalizes on a new view of attachés. This structure will balance a regional focus with a focus on the potential future sources of competitive advantage.

Competitive advantage in the future will continue to reside in the ability to match ends and means to create or exploit vulnerability in an adversary. Such advantages will not appear hostile, if done properly. They will be what we call today "dual-use." A danger in the future is that the Defense Intelligence Agency takes a narrow view of "defense" and overlooks or fails to see that which could damage the United States, our citizens, our interests, or our friends. The question that everyone involved in the production of intelligence knowledge must answer every day is this: "Why is the United States safer or less safe than it was yesterday and what ought the United States do in response to that change in the environment?"

A matrix organization with teams that reside in the intersection of geographic regions and potential sources of competitive advantage or competitive danger is the optimal structure to avoid surprise in the future. A matrix organization can rapidly sense, analyze, and forecast changes in the competitive environment.

Focused on understanding all the potential sources of danger, such an organization is best-equipped to help prevent destructive conflict or help ensure the outcome of destructive conflicts that cannot be avoided are predecided in favor of the United States. Illustration 22 depicts such a notional organization.

Note that we envision "functional teams" of analysts—many of whom are not full-time employees—organized as "global teams" charged to develop and articulate a global point of view in a particular issue area. (We describe these collective points of view as the annual Defense Intelligence Agency's "Annual Report to Stakeholders," or an annual defense intelligence assessment.) Thus, the "WMD" functional team is composed of experts in every aspect of weapons of mass destruction. Augmenting this functional team of experts are teammates from each of the regional teams who specialize in "weapons of mass destruction" for their assigned region of expertise. In this construction, for example, we would expect that there would be a greater number of WMD regional experts in the "Russia" regional team than there would be in the "Europe" regional team. Regional Teams may have more linguists than Functional Teams. Attachés report to both Regional and to Functional Teams, since both teams a have questions they need answered for internal and external customers.

The Defense Intelligence Agency will not design the Functional Teams to be mutually exclusive, collectively exhaustive, or orthogonal. Rather, the Defense Intelligence Agency will come to view some degree of "messiness" and overlap as beneficial. While overlap is advantageous, gaps are not. Hence, the "Global Warning" team is the capstone team.[68] Its role is to envision over-the-horizon, complex, and convergent dangers and probe issues and hidden dangers potentially concealed in the seams of the matrix structure. The Defense Intelligence Agency will also add and refocus Teams — functional or regional — as the environment demands. There may be a need, for example, for a "Cuba" team or task force, or an "Iran" team. The point is that the combined strengths of geographic or cultural expertise and subject matter expertise are infinitely reconfigurable and flexible.

A director of operations — or chief operating officer — sets organizational priorities for production of knowledge and oversees the attaches and the analysts. Analysts work on issue teams with crosscutting product lines. The analysts produce assessments and forecasts, supported as described above, by a contingent pool of subject matter experts. They function much as a Contracting Officer's Technical Representative (COTR) acquiring and contracting with cleared expertise from around the world, and they share in the responsibility for the product. They draw from their broad issue knowledge as well as from the data reported by the attaches. Attachés perform broad regional responsibilities as described above, although some regions may demand a particular kind of functional area expertise.

This new structure requires a radically new compensation structure to ensure its success. The Agency recognized that because the attachés and analysts must function together in multiple combinations of task

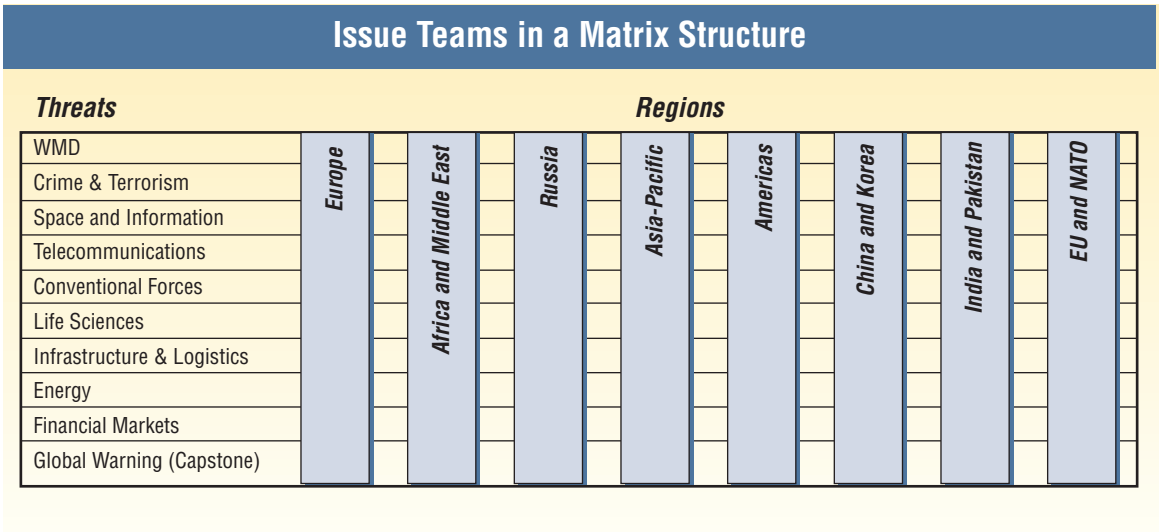


Illustration 22: Issue teams in a matrix structure.

groups, rewards need to encourage productivity from the entire group as a whole. Group incentives for achieving established goals accompany individual rewards for outstanding contribution.

Audacious Operating Goals Encourage Achievement of Measurable Effects

The role of the top management team is to lead the implementation and development of revolutionary innovations, enabling the organization to gain advantage over potential adversaries. The leadership team advises the director on the future vision of the organization and how to best achieve it. They direct the development of a coherent strategic planning process that accounts for greater ambiguity in threats, and is capable of comparing risks across time. The team ensures the timely flow of quality information from sensor to analyst to consumer, and makes continual adjustments to deliver quality and timeliness as defined by their outcome based metrics. The major difference from present day management is in this team's constant focus on importing new forward-looking, creative approaches to radically transform the value of intelligence to the consumer. Executives push day-to-day management to lower-levels for execution.

A Revitalized Advisory Board Provides Fresh Ideas And Continuity

The Advisory Board has two primary roles. The first provides the Defense Intelligence Agency with connections to the world's most creative and innovative thought leaders, connecting it with innovative business knowledge (Illustration 23); and the second is to serve as the Agency's "business brain" (Illustration 24). The Advisory Board members, accomplished executives in their own right, each bring with them multiple connections with the world outside defense intelligence and import superb management, technology, and socio-cultural expertise to the Agency.

These highly connected, successful executives serve on corporate boards or as government officials from defense and other departments, and serve as NGO leaders — they have led complex organizations through transformations or import a wealth of critical connections to the Defense Intelligence Agency. The Board furthers the leaders' strategic thinking through its strategic debates and risk assessments on the external environment and advises on positioning the Agency in a dynamic environment. This is the crucial debate of the board. These decisions are the future lifeblood of the organization."[70]

In the corporate world, a small network of powerful directors controls all major appointments and the direction of the Fortune 1000 companies. A similar network of alliances determines success in the biotech and the

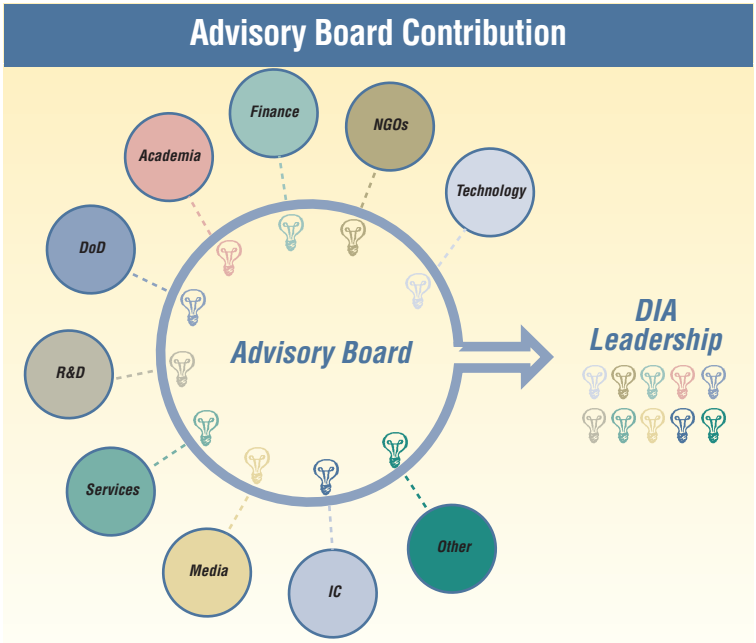


Illustration 23: An executive advisory board, composed of six to twelve senior executives, imports new ideas and expertise from multiple subject areas to DIA leadership.

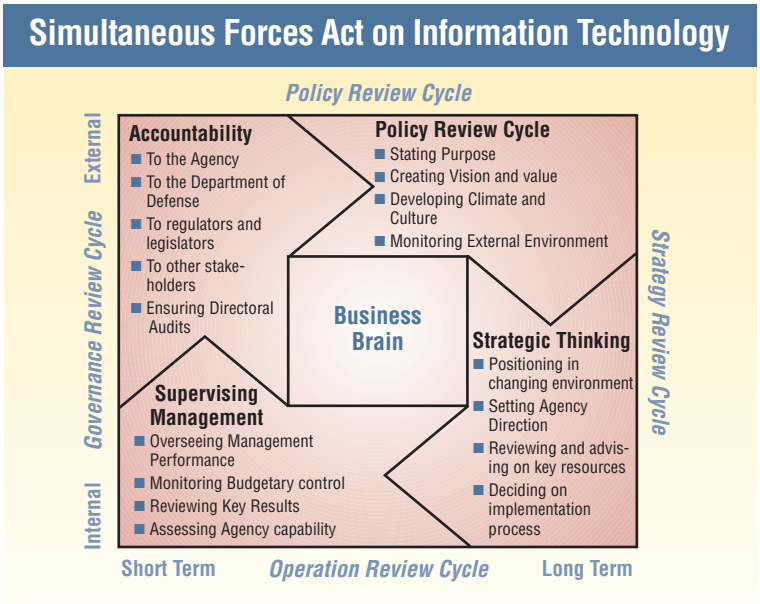


Illustration 24: The Advisory Board engages with leadership in strategic debate, monitors the external environment, and helps position the Agency[69]

motion picture industries. In the commercial world, the structure of the network within and among firms is responsible for the organization's ability to adapt to rapidly changing environmental or market conditions.[71]

The Director Serves a Five Year Term

A seasoned visionary with a demonstrated ability to lead an information organization requires more than three years to create significant organizational change. The incumbent's five-year term of service provides the time to implement the revolutionary change that the future will demand. Due to military progression, a longer tenure may require a civilian incumbent.

The Advisory Board and the executive team develop a broad web of trusted alliances, partners, and contingent staff to draw upon when specific needs arise, such as unusual activity or the need for surge capacity expertise in an arcane skill or ability. The entire intelligence community enhances its collective competitive advantage by freely sharing their data among trusted partners and allies through secure private networks.

The Organization and the IT Structure Mutually Reinforce Each Other

Gaining decision and information advantage requires an information and communications structure available to users and consumers on demand that they trust and depend on. The information network is accessible from a variety of platforms and locations. It possesses the correct levels of security and bandwidth relevant to its application.

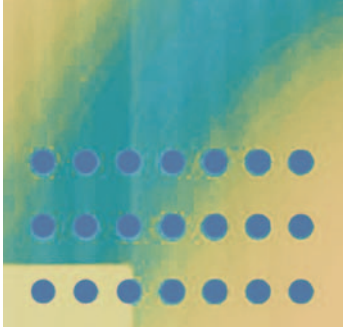
To meet future needs for decision superiority, the technology infrastructure provides seamless access to intelligence and continually updated open source information. It contains state of the art sensemaking ability, and innovative new ways to gain access to adversary information.[72] Finally, the future information network is capable of conducting information operations and aggressive counterintelligence while collecting persistent, responsive, exquisite intelligence.[73] All of these advances come from a carefully planned transition involving committed staff with an unblinking eye to customers' needs.

The Defense Intelligence Agency Can Lead the Intelligence Community

The new environment manifests a new level of cooperation between DoD and the intelli-

gence community — how they acquire, mange, and execute the overall intelligence program. New priorities in clandestine activities, space intelligence, surveillance, reconnaissance, and communications are just a few examples where the Department and the intelligence community collaborate closely. The Defense Intelligence Agency has risen to the challenge of leading the transformation in intelligence.

The technical, social and operational structures that the Defense Intelligence Agency develops will never be static. Environmental change requires constant reorientation that in turn necessitates an ongoing strategic vision and planning process that depict the outcomes the Agency must achieve. The Agency's new structures enable new ways of working within the Agency and with other agencies in the intelligence community as well as with the Department of Defense. Integration of national power is especially critical for overcoming unconventional adversaries. Military means alone are insufficient.



PEOPLE

To meet tomorrow's shadowy threats, the Defense Intelligence Agency will need a broad network of talent. The breadth and changing nature of this workforce will be beyond the means of any one organization. The new workforce will reside in DIA, other government agencies, NGO's, think tanks, universities, corporations and individuals. This future "networked workforce" will require changes in the Agency's workforce attributes and management skills.

"The key competitive difference in the 21st century will be people. It will not be process. It will not be technology. It will be people."

David Walker, Comptroller General of the United States

As outlined in the Structure section, the Agency of the future will move from today's pyramid design to one that contains matrix, network and hierarchical elements. Similar to the relationship between service chiefs and combatant commanders, where one provides trained/organized/equipped forces for the other to use, tomorrow's functional managers within the Defense Intelligence Agency will build networks of expertise then make them available to project managers to meet changing demands. The managers who recruit, train, discipline, motivate and assign the workforce will not be the same people who employ it. A separate set of project managers will draw from across the organization for specific situations. As situations change, so will the project managers and their teams.

This future structure, highly relevant to the Defense Intelligence Agency of the future, will challenge the Defense Intelligence Agency of the present. Despite its advantages, achieving this structure will pose significant challenges.

Matrix organizations are difficult to implement and even more difficult to manage. They are largely unproven in the public sector; no large government agency reflects a matrixed structure across the board. They are also countercultural to hierarchical military organizations. Split authorities conflict with the "unity of command" valued by military leaders. For these reasons, many managers prefer a pyramid structure that, like its namesake, is more stable, with authority and accountability clearly assigned. In a pyramid organization, managers own both the mission and the personnel to accomplish that mission. Incentives and training flow from this ownership. Fluidity and agility—hallmarks of seasoned matrixed organizations—are sacrificed for control. In the control-oriented pyramid, there is seldom a need to redefine offices and reassign personnel — hallmarks of immature matrixed organizations — which allows managers to avoid an additional layer of friction.

Unfortunately, managers in the Defense Intelligence Agency do not have the option of

The Beginning of the Workforce of the Future

Over the next couple of decades, the majority of the Defense Intelligence Agency's current knowledge workers will retire. In an environment where talented knowledge workers will be in universally high demand and equally short supply, recruiters will develop and apply unique candidate-centric approaches that enable the Defense Intelligence Agency to attract the elusive best and brightest.

Future demographics and mission requirements will place enormous importance and focus on the recruiter position, as they will be the ones charged with the actual day-to-day building of the workforce of the future. Recruiters must understand their organization's strengths, deficiencies, and aspirations to fully appreciate where they need to build capacity. They must also understand their organization's knowledge base and how it works, since hiring will be a key factor in maintaining and growing the Defense Intelligence Agency's knowledge capital, a precursor to ensuring information and decision superiority in the future.

Recruiters Become Innovative "Human Capitalists"

In the future, recruiters will become "human capitalists", spending most of their time proactively seeking out and interviewing targeted candidates from around the world for potential inclusion in the Agency's talent pool. Applying sophisticated targeted marketing and branding strategies and the Defense Intelligence Agency's compelling vision to attract individuals from around the globe.

To be successful, the human capitalist must be "an extraordinary individual who wants more than just a

avoiding these added frictions. The post Cold War, post 9/11, information age world has shifted the mission of the Department of Defense. Gone is the focused threat the Soviet Union posed for a half century. Gone is the specific threat that aligned fixed missions and job descriptions. In its place are networks of regional rogues and terrorist groups whose changing nature requires constant adjustments. The inherent inflexibility of a pyramidal hierarchy makes the necessary organizational adjustments difficult.

In fact, attempts to reorganize pyramids when the missions constantly change often fail. Today's opportunities and threats change too quickly and too often. By the time an agency completes a reorganization — it is already obsolete, generating another "re-org" on its heels. The resulting change fatigue in the workforce undercuts the credibility of senior management.

Constantly changing circumstances require a different management approach. The flexibilities provided by matrixed structures, despite the managerial difficulties they introduce, cut the reorganization "do loop." They acknowledge the fact that rapid change in daily operations is a given. Instead of constantly changing the organization, management organizes for change.

Because intellectual capital is the heart of the Defense Intelligence Agency, there is little chance the mission and structure of the Agency can change absent fundamental change in the Agency's workforce. Organizations transform not by redrawing the company wiring diagram

"In an age when terrorists move information at the speed of an email, money at the speed of a wire transfer, and people at the speed of a commercial jetliner, the Defense Department is bogged down in the bureaucratic processes of the industrial age-not the information age… The point is this: we are fighting the first wars of the 21st century with a Defense Department that was fashioned to meet the challenges of the mid-20th century. We have an industrial age organization, yet we are living in an information age world, where new threats emerge suddenly, often without warning, to surprise us. We cannot afford not to change and rapidly, if we hope to live successfully in this new world… If the Department of Defense is to prepare for the security challenges of 21st century, we must transform not just our defense strategies, our military capabilities, and the way we deter and defend, but also the way we conduct our daily business."

Secretary Rumsfeld testimony, 14 May 2003

job," someone with "superior intellectual ability, toughness of mind and a high degree of personality" who can work in "fast-moving, ambiguous, and unstructured situations." In other words, recruitment work will possess high similarity to a case officer role, working both formal and informal networks to land leads to the best sources of candidates.

The recruiter needs robust network contacts, combined with knowledge of the organization's issues and the psychology of team design, to develop innovative workforce solutions that ensure robust Agency intelligence capability. For example, if the Defense Intelligence Agency needs to understand Brazilian telecom alliances, the recruiter would not be limited to acquiring a Portuguese-speaking analyst or a South American regional expert. Instead, he or she could use a Korean-speaking analyst, since most of Brazil's telecom alliances are with Korea.

Recruiters Will Consider Complex Team Dynamics Issues

In the future, when the Defense Intelligence Agency organization consists of a series of cross-matrix issues teams, recruiters will target individuals for potential hiring based on the anticipated need for specific capabilities on one or more issue teams. They will use HR staff planning and evaluation technologies, as well as apply knowledge of team dynamics, to complement existing team performance. They may also create new teams and select members tailored intellectually and behaviorally to the specific task.

These new human capitalists will maintain a database of qualified candidates based on anticipated

but by changing the activities and behaviors of their people. As noted by Bossidy and Charan, "To put it simply and starkly: If you don't get the people process right, you will never fulfill the potential of your business."

Redefine the Workforce

The Defense Intelligence Agency will move away from the idea of exclusive control of intellectual talent to an inclusive model that draws on the best talent available, wherever it might be. This transition will redefine the concept of workforce within the Agency.

When unpredictable threats can field practically every capability at any place and time, hard requirements are difficult to establish. The shift in U.S. national strategy from a threat-based construct to a capabilities-based approach drives this transition. The strategic shift poses a significant challenge for the entire defense community. As then-Undersecretary for Acquisition Pete Aldridge noted in 2002:

> ***"The** threat-based **acquisition structure is obsolete against so unpredictable a threat, and incompatible with the groundbreaking technologies in play. Instead, we have gone to a** "capabilities-based" **acquisition. The difference… is that** capabilities based **acquisition results from assessments of the threat; of the available technology; and, based on those assessments, an appraisal of what can be built to do an acceptable job, rather than accommodate a hard requirement."*** [75]
>
> Undersecretary Aldridge

The absence of "hard requirements" is a tipping point for the Agency. Given the breadth of uncertain challenges the Defense Intelligence Agency will face in the future, it will be important to cast a wide net in building expertise and insight. The Agency can "own" some of those resources internally, but the scope of possible capabilities will be beyond its capacity to totally own and develop. As a result, the Agency will house more and more of its expertise at think tanks, companies, NGOs, universities, other government organizations and in individual professionals' homes. The Agency will need to "rent" expertise as needed, and bring contingent employ-

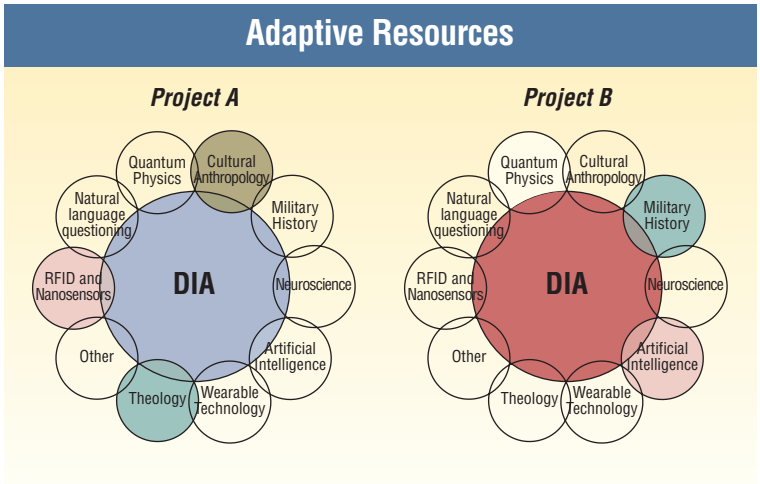
> ***"Ever since the dawn of the industrial revolution, it has been the organizing principle of society—people are what they do, defined by their corporate labels. But the modern corporation has begun its death march. There are now 25 million free agents-entrepreneurs, independent contractors, free lancers, and temps."***
>
> Daniel Pink, Free Agent Nation

needs of the organization for staffing. The database will contain candidates for both employee positions and the contingent workforce. The incentive comes from the Agency's performance system which reward its recruiters based on the speed, cost efficiency and value of the effects they enable.

Speed Rules: An example of 'human capitalism' in action

The leader of the Global Warning team identifies a need for an individual with knowledge of chemical weapons and Russian organized crime to complement the team. The recruiter sends several pre-screened candidates to the prospective unit for interview and selection. Candidates may come from teams within the Agency, or may be "rented" or hired from outside. The process of moving the new member onto the team is streamlined and efficient—the hiring officer on the issue team extends an offer following the interview, and the new recruit begins to familiarize him or herself with the work immediately, while background investigators complete their work over the next two weeks. The accelerated process is the result of significant improvement and automation of the clearance and testing processes conducted in advance of the interview.

Because of their intimate knowledge of the organization, its goals, and the dynamics of the Agency's extensive human and information networks, recruiters will play the critical role of advising on strategic structural features of the organization and will build workforce capacity at every level. In fact, of all of the human capital management capabilities, being able to attract and retain the people with the necessary attributes will be the highest and most critical. Hiring will be a key factor in increasing the organization's knowledge capital, the essential precursor to enabling decision superiority.



Illustraion 25: *Ad Hoc* Team Composition of Expertise

ees in and out of functionally-based, matrix teams. (Illustration 25.)

The Agency would pre-screen outside contingent staff who would routinely integrate with the core workforce as specific tasks warranted, such as:

- The Agency needs routine infusions of fresh perspectives.
- Higher caliber (e.g., more experienced) talent is available outside the Agency.
- Staff is fully committed to current projects and cannot retask without gapping important coverage.
- The Agency needs highly specialized expertise.
- The Agency needs specific expertise quickly; there is no time to retrain staff or wait for key personnel to become available.
- Because the Agency's customers will tap multiple sources for information and advice, the Agency needs to incorporate outside expertise in its deliverables.

The Defense Intelligence Agency will continue to have a strong permanent workforce in place (see Specialists and Generalists, below). However, it will routinely broaden this base with a wide ranging set of assets contained in a network that it could not (nor would it want to) financially maintain on a full-time basis. Members of this three part workforce of the future will serve on one or more cross-functional teams (Illustration 26).

Specialists

The Agency will always need specialists in a broad number of fields. Expertise on highly technical areas, such as foreign air-to-air missiles or biological weapon developments, may reside no where else. If the Agency does not grow this expertise, it may not exist when needed. Even when it can find better expertise elsewhere, the Agency will need to maintain experts in-house, particularly for expertise that it needs on a near daily basis.

The Agency also needs its own stable of experts to vet other experts. Because an Arab scholar or nuclear engineer, for example, can best evaluate the recommendations of his or her own colleagues, the Agency will need in-house experts across all disciplines. They must stay current with the state of the art and technology and access a wide circle of expertise when needed.

In essence, the Agency will always need in-house experts to cover unique areas, provide long-term expertise and evaluate inputs from outside experts.

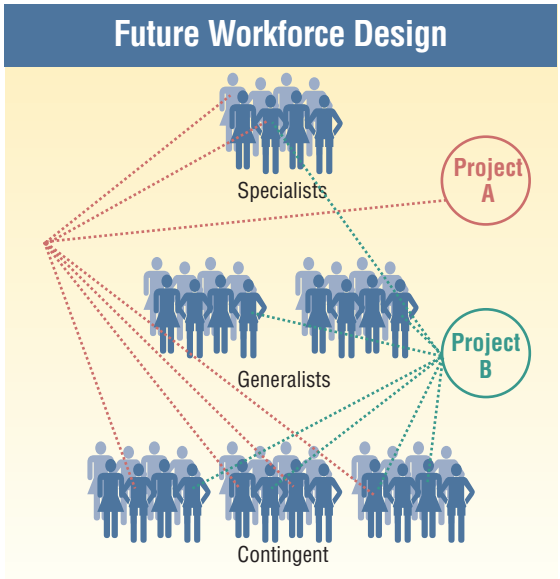
The specialist group should be smallest piece of the future workforce, since the focus should be on building expertise outside the core organization. The Agency would reserve this designation for roles requiring intensity of focus, constancy of demand, and/or unique expertise.

Specialists would seldom migrate to management positions. Their value to the Defense Intelligence Agency would remain in their technical proficiency, the circle of outside experts they build and their ability to work with matrixed teams. Their incentives, both pay and non-pay, would keep them on par with generalists but the Agency would not necessarily expect them to become generalists themselves.

Just as a brain surgeon does not need to become a hospital administrator to progress in the medical profession, certain specialists in the Defense Intelligence Agency will be highly valued solely for their functional expertise. Though limited in number, these experts will progress without the need to manage others.

Generalists

The second and larger group would be a set of generalists. These employees would be project based moving across the organization and adapting quickly to new issues and projects. They must be quick learners, using knowledge and fungible skills gained from previous situations in new and non-linear ways. They may come from attaché positions, they be former specialists who have acquired a variety of specialties. They must also understand customers, the interworkings of the Agency and team building/leadership.



Illustraion 26: Networked Workforce

The generalist group would be the largest part of the "owned" workforce of the Defense Intelligence Agency. They would be the core of the cross-functional matrix team concept described in the Structure section, and as such, would act as the facilitators and nodes among specialists, contingents and customers. These employees would be on a management trajectory, through a highly selective evaluation and development process.

Contingent

The third group, and by far the largest, would be the "on call" contingent workforce. This group would be a wide-ranging network of experts and uniquely skilled workers brought into the Defense Intelligence Agency when needed for a specific mission. They would bring leading edge knowledge and a wealth of external context to specific situations.

This group most closely reflects the new defense environment. Unlike the Cold War era, when we knew the "who" and "where" of the threat, and "how" was the major question, we don't always know today's enemies far in advance. The United States cannot forecast the "who" and "where" of the next war or terrorist strike, conflict or mission. Despite this lack of forewarning, military decision makers may need immediate information on formerly obscure, but suddenly

Intelligence for Cause and Effects

Al Qaeda and the U.S. Department of Defense both endorse "effects-based operations." The U.S. military recognize their operating environment is too dynamic to plan for the next threat and that designing and executing an adaptive, capability-based system demands greater fidelity in the effects that political leaders expect. Al Qaeda recognizes that it can achieve social and economic disruption with unconventional suicide attacks. The implications for 21st Century intelligence are tectonic.

Anticipating effects requires exquisite knowledge of causes. Future intelligence analysis is thus driven from the domain of art... to the domain of science... and back again. Since the beginning, good intelligence analysis has been revered as an art, passed down from the master to the apprentice. Judgment and intuition remain friends of the great analysts.

Technology and science help analysts manage ever-larger volumes of data, but scientific principles for analysis remain underdeveloped. No more. Understanding the causes of effects, and anticipating outcomes demands scientific rigors. Not the rigor of one scientific discipline, but the rigors of many.

We are all shaped by the disciplines we learned in our youth. Physicists learn theories about mass and energy. Engineers learn basic steps—define the problem, list the givens, list the unknowns.... Social scientists learn theories of group dynamics, election voting, legislative voting, alliances, and band-wagoning. Psychologists learn about cognitive dissonance and human change. Painters learn about texture, color, and perspective. Each scientific discipline applies slightly different explanations of cause and effect. Depending on the context, one or combinations of scientific hypotheses explain that A causes B. To accurately explain effects based operations, analysts

vital issues. Serbian leadership, Afghan air defenses and Yemeni terrorist cells provide three recent examples. We see the areas of interest to our national security becoming continually more diverse and complex. American military leaders may receive immediate taskings related to any of these areas, and will turn to the Defense Intelligence Agency for integrated information.

The breadth and dynamism of this purview exceeds the expertise of any agency. No one can keep such expertise on the permanent payroll. Fortunately, an alternative exists. High quality expertise on practically every conceivable security issue resides among American contractors, universities, NGOs, media, retirees and other government agencies. The Agency needs a structured approach to incorporate this expertise.

Similar to the traditional active-reserve relationship in the military, the Agency could build internal-external teams ready for immediate action across all relevant subjects. Experts would be sought in advance of actual need (the work flow system would have a significant planning component) and interviewed as though they were joining the Agency. The Agency would interview external staff, place them on a retainer (sliding scale according to value) and expect them to keep up with leading edge issues and trends. They would also interact regularly with permanent employees. The Agency would provide incentives to internal workers to continually broaden their network while keeping a core of experts readily available.

The model would go beyond today's standard consulting relationships. The Agency would need vigorous interaction between employees and contingent workers outside the bounds of carefully defined projects. Security clearances and communications networks would need attention. However, these obstacles are sur-

"We need an adaptable cadre of analysts, people who can adapt to changes in threat. We can't know what threats will emerge (and disappear) in the future, so our analytical corps must be adaptable. Twenty years from now, "analyst" should be an obsolete term. Analyst-only is way too narrow. They must integrate other skill sets. Primarily, they must understand how to get intell, not just analyze it. By being better at retrieving information, they will help the IC drive collection priorities. They can't just analyze the in-box. Rather, they must be aggressive operators of intelligence."

Active Duty General/Flag Officer

must apply the right discipline, theories, and hypotheses. Future intelligence analysts must be scientists who predict B will result from A and that C, D, E, and F will not also occur. Chaos and complexity theory often elevate the analysis. Successful knowledge workers that we observe hedge their bets by learning other disciplines' models or working in multi-disciplinary teams.

Future effects-based analysts will not be experts in the data of multiple disciplines; they will apply the causal theories of different disciplines. Electrical engineering will predict a precision strike will cut power. Social theory suggests an organized military will fire up back-generators and produce new hot targets, while the theory expects the terrorists to operate without power. Think of effects-based analysts as learners of theory, not as subject matter experts.

Effects-based intelligence officers will also be risk-taking gamers. At the tactical level, in a world of machine to machine interfaces, analysts will manage three dimensions simultaneously. First is hypothesis negation or confirmation to confirm the right cause-effect relationship. Second, is Blue's next desired effect and action. Third is the target's reaction. Since the effects assessment will be dynamic — which target, which weapon, which effect — won't analysts hone their skills in video games? At the strategic level, analysts will want to test many hypothesized cause-effect links in low risk games with customers. Effects-based analysts will have an array of scientifically-suggested situations to game with warfighters. Examining multiple scenarios is key to anticipating. And effects-based analysts will artfully weave these situations into captivating stories to elicit the operator or statesman's attention and real values.

Future effects-based intelligence experts will be masters of new science and art.

mountable given the pay-off. The Agency would gain the range of expertise needed to operate in today's era of "shadowy threats."

Workforce Design Objective: Small Core, Large Flexibility

The combination of the three categories of employee: specialists, generalists, and contingent workers will comprise the Defense Intelligence Agency workforce of the future.

This workforce design parallels the general direction of the military: a smaller active force augmented by a robust reserve. The mix will give the Defense Intelligence Agency the agile workforce it needs in the emerging dynamic, capabilities-based environment.

The key operational factors and implications involved with implementing this type of workforce design include:

1. Building a 'project mindset' inside the generalist workforce from the Agency's present role based culture. Today the focus is short-term, ad hoc and output based — versus long-term and outcome based.

2. Monitoring the number of specialist roles to ensure they do not become more than one-third of the population. Such positions will be easy to grow, but will eventually undermine the value of the contingent workforce.

3. Implementing a highly effective set of management processes to ensure it deploys generalists as current and future issues demand and provides the constant care necessary to maintain the contingent workforce.

Workforce Attributes

The federal government has long sought to improve its human resource systems by defining sets of core competencies for organizations and individual positions. While well-conceived understanding of the competencies required will always be a valuable exercise, the future workforce will need greater emphasis on innate attributes.

This change in emphasis springs from the recognition that a competency-centric personnel system can produce a technically proficient workforce — but not the generalist, multi-disciplined employee the Agency will increasingly need in the future. It recognizes the danger of tilting the reward structure towards predictable responsibilities, when the entire environment is becoming less predictable. A future that requires an intellectually agile workforce to adapt to changing circumstances demands this shift in emphasis.

Not all Agency personnel should become generalists, however. There will always remain the

need for detail-oriented experts who master critical aspects of the intelligence system.

The Agency will recognize and reward an evolving set of attributes that differ from those with which it has been more familiar. As the need for specific attributes changes, the incentive structure within the Agency will change in parallel.

We list some important attributes for the future workforce of the Defense Intelligence Agency (particularly analysts) in Illustration 27.

The illustration shows the attributes as "bucketed" into five categories. The first is Cognitive Attributes, which indicates an overall shift in work emphasis from producing (e.g. writing reports) to predicting (e.g., identifying unexpected patterns). The second category, Judgment Attributes, calls for analysts that make many more judgment calls as their intelligence product becomes more predictive. The third category, Communication Attributes, emerges from an increasing requirement for analysts to communicate real-time directly with customers, the creation of quality teams to review product and customers involved in initial collection decisions. The fourth category, Technical Attributes, reflects that technology will be a key driver of both role change and overall mission success in the future. The need to supplement varied types of knowledge with an understanding of technology will increase. The fifth category, Role Attributes, which seeks to match a person's orientation with role design, ensures the employee's suitability to deliver the outcomes sought by the customers.

We do not prioritize the attributes in Illustration 27. Their individual importance will rise and fall over time, and vary from analytical challenge to challenge. At present, the highest priority attributes include integrating social and technical knowledge, willingness to take risks, conduct the role in a more interactive manner, identify patterns among disparate knowledge and use imagination. These priorities reflect the need to change the conduct of the analyst role as well as the need to think differently about an asymmetric, adaptive threat. In addition, a key factor in developing these attributes requires building a culture that is supportive, empowering, and serves as an open market for the proactive sharing of information and ideas. We discuss this in more detail later in this section.

The best private sector organizations already balance the concepts of competencies and attributes. As one of the thought leaders interviewed for this project emphasized, Southwest Airlines has used this type of technique in hiring for years. He notes, "They have done very well by making personality type a primary determinant of hiring. Their view is we can train people to do all sorts of things but we can't make them a different type of person. For them, it's all about customer interaction — and they've recruited people whose personalities are good at that."[77] While Southwest Airlines certainly needs technical proficiency among its workforce (e.g., pilots, mechanics), their incentives reward customer-focused attributes, not just the completion of specific job competencies. Boeing, along with other leading companies, already uses this approach too.

Of course, the Defense Intelligence Agency cannot junk all competency-based job metrics. Current employment regulations and practices, especially in the recruitment phase, restrict the Agency's ability to emphasize attributes in the workforce incentive structure. However, as new psychographic tools develop (such as the use of video-game-like simulations) they will likely become more widely accepted. In addition, the Agency has made progress in the use of attributes today. For example, the effort by the Directorate for Information Management to explicitly define the profile of technical managers is an excellent start. The objective in this case was to create a

"Because you just don't get it," Haw said. "I didn't want to see it either, but now I realize they're never going to put yesterday's Cheese back. It's time to find New Cheese."

Spencer Johnson, Who Moved My Cheese?, 1998

"We didn't have a failure of intelligence on September 11th. We had a failure of imagination."[76]

Deputy Director of Signals Intelligence, NSA

Second Wave Attribute	Third Wave Attribute	Value to the Defense Intelligence Agency
Producing	***Thinking***	***Provide insight to customer and peers; considers a range of possibilities; innovative and creative***
Cognitive Attributes		
Technically Proficient	Culturally Intuitive	Permeates "hearts and minds' of target; nuanced thinking
Identifies Issues	Identifies Patterns	Draw connections between non-linear events and occurrences, considers possibility of low probability — high impact events
Parochial	Global Thinker	Understands global operationg environment; sees implications in a connected series of diplomatic and economic contexts
Assessing	Imagining	Can formulate highly original concepts and prospectives
Core Competence	Multi-Disciplined	Brings a range of ideas to group discussions and issues
Judgement Attributes		
Accepts Judgment	Questions Assumptions	Guards against the development of "group think"
Risk Averse	Calculated Risk Taking	Offers predictive intelligence which inherently carries risk
Communication Attributes		
Computer Oriented	Interaction Oriented	Communicates "live" with customer; conversational manner
Insular	Networked	Seeks out experts with a diverse array of knowledge sources and keeps them at the ready.
Information via Reports	Real-Time Collaboration	Adapts to new technologies and customer's desire for speed
Explanation	Story Telling	Uses narratives to allow understanding of complexity
Report Writing	Scenario Writing	Ability to develop scenarios based on facts and intuition
Presents Occurrences	Presents Context	Provides on-going, additive perspective to the customer
Technical Attributes		
Technology or Social Science	Technology and Science	Understands something about both disciplines; is aware of both technological and social science issues/impacts/solutions
Accepts Technology	Shapes Technology	Highly adept at identifying, selecting, and tailoring technology solutions for the demands of the work
Role Attributes		
Responsive, Reactive	Anticipatory, Proactive	Seeks to understand and constantly anticipate client needs
Role Focused	Customer Focused	Works to ensure data is useable and overall client success
Product Oriented	Outcome Oriented	Seeks tangible mission outcomes from the work conducted

Illustration 27: Future Defense Intelligence Agency workforce attributes

hiring process that would screen candidates for their interpersonal, teaming, and leadership abilities in addition to possessing technical knowledge. This type of approach to building tomorrow's workforce needs continued emphasis.

Attribute Development: Four Levels of Progress

Here we discuss a process of employee development that presents a distinct departure from the skills focus that characterizes most professional development today. The future Defense Intelligence Agency will develop employees' abilities to think— to become intuitive about the work, to seek and integrate ideas, imagine scenarios and identify patterns where only pieces of information exist.

The concept of workforce development in the future is less about building first-rate proficiencies than it is building first rate minds. At any given time, employees naturally display different levels in their thinking capacity based on attributes, work and educational experience, and their opportunities for development. Looking across the workforce, a "progression of thinking" begins to emerge. The Agency can apply this progression as a foundation of the design of its development program, placing everyone on a similar trajectory of attribute and competency development. A highly notional example of this curve follows in Illustration 28.

First Level Employees sift through the ocean of information available. They may be able to identify potential causal issues, but the team does not expect them to raise larger intuitive issues.

Second Level Employees can identify causal issues and represent them in a larger context, but remain within their assigned area of expertise. They do not take the initiative to investigate asymmetric possibilities.

Third Level Employees actively use attributes such as intuition, imagination and pattern integration on a periodic (but not consistent) basis. These employees extrapolate the underlying assumptions used by others and may even question them on occasion. They may also be able to create innovative scenarios from pieces of accrued information that can imagine potential events or threats.

Fourth Level Employees use cognitive attributes in a highly developed fashion and employ them consistently. Employees mix and match seemingly disparate pieces of information from distant, unconnected sources to create new sophisticated concepts, causal relationships and solutions. Employees at this level often question the operating assumptions of others to ensure they have considered all aspects of an issue. They are imaginative, and prod others to be equally innovative.

By outlining this path, the Agency can identify specific standards of proficiency, and then align incentives with these standards. It allows the Agency to move away from a primary focus on technical proficiency and reward attributes that are more important to success in a dynamic operating environment.

The New Diversity: Cognitive Diversity

During the 1960's and 1970's, the term "diversity" became shorthand for public mandates to promote social equality. In the future, the term will acquire additional meaning. The new meaning will include diversity of the mind.

Organizations that promote cognitive diversity, especially by combining people with different attributes, temperaments, backgrounds and skills will instigate the creative thinking needed to anticipate new opportunities and threats. For the intelligence community, it becomes a critical determinant of success given the specter of asymmetric challenges. Most importantly, cognitive diversity within the workforce can lessen the possibility of homogenous "group think," or what Richard Haver, the Assistant to the Secretary of Defense for Intelligence, called a "poverty of expectations." Illustration 29 describes some notional examples of the types of cognitive disciplines the Defense Intelligence Agency will include in its workforce network.

Customer demand for intelligence from many different dimensions and disciplines will also

Category	Discipline	Value
Social Sciences	Anthropology – cultural	Understand the target's view of the world
	Crime – organized	Power center/organizing factor
	Economics – financial markets	Global economy impacts
	History – military	Operational predispositions
	Law	Political/military interaction
	Public Health	Peacekeeping missions
	Social Network Mapping	Political power structures
	Theology – world religions	Motivational factors/perceptions
Science and Technology	Artificial intelligence	Natural language queries
	Biochemistry	Future WMD threats
	Earth and atmosphere	Surveillance and vigilance
	Energy – sources and markets	Economic importance
	Quantum physics	Collection, cryptography, computing
	Space – satellite technology	Future battlespace
	Telecommunications	Key operational utility
	Wearable technology	HUMINT possibilities

Illustration 29: Notional examples of disciplines in the future Defense Intelligence Agency network

increase as the Agency becomes involved in planning more diverse military campaigns. Planners will increasingly seek privileged information to ensure decision superiority and leverage so-called smart weaponry. To meet this demand, the Defense Intelligence Agency will become increasingly involved at the planning stage, developing a more significant planning and audit role over time. As campaigns become more joint-service and include both destructive and constructive conflict, customers will call upon the Defense Intelligence Agency to provide context and planning support. And as weapon systems become more and more intelligence driven, the Agency will audit their effectiveness. All of these point to the need for developing a robust planning capacity within the Agency that can support these activities across a wide range of disciplines.

The need for cognitive diversity will lead to building a network based organizational structure composed of ad hoc teams, although some teams may remain in place for long periods. These teams will be multi-disciplined and focused around issues, not functions, and will use tools such as scenario planning techniques to derive new possibilities and solutions. However, the Agency will also recognize that an important role will continue to exist for the solo practitioner working outside a group context (either by choice or necessity). Our emphasis on interaction and group in this paper highlights a change in balance and process towards matrixed teams, not an abandonment of individual research.

An Open Market Culture Fosters Imagination

To unleash the full capabilities of the organization, the Defense Intelligence Agency will need a culture that supports and stimulates an open exchange of ideas across the workforce.

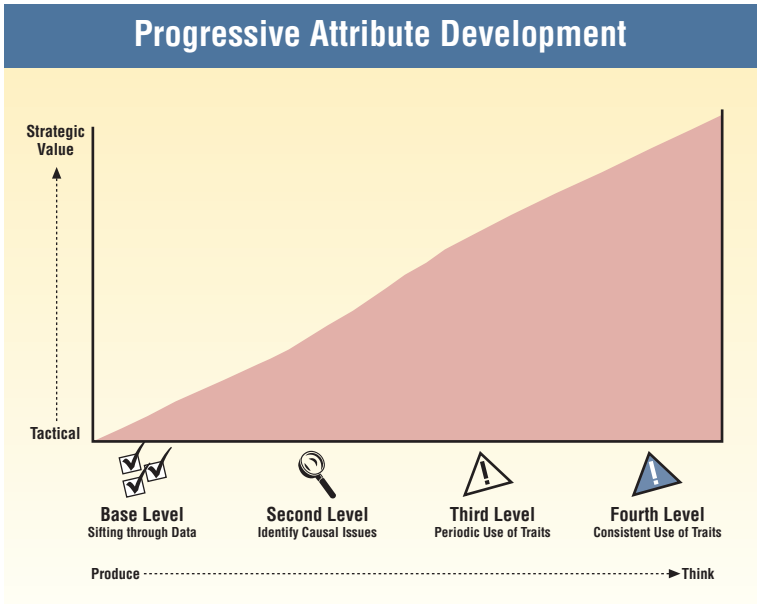


Illustration 28 — Progressive Attribute Development

"We can't think in terms of having a templated enemy."[78]

Bob Leonhard, Fighting by Minutes: Time and the Art of War

The culture of every organization has a direct impact on the product it produces. For the Defense Intelligence Agency, culture determines key interpersonal factors such as risk tolerance and a dedication to quality and innovation. For example, a sense of "safety" in the culture about the ability to question assumptions could have a direct impact on product content. Likewise, a culture of intense collaboration could result in development of new cross-functional processes, as well as support the sharing — versus hoarding — of information.

According to several people interviewed, the culture of today's Defense Intelligence Agency does not support and stimulate the open exchange of ideas across the workforce. The culture is one of risk avoidance and groupthink. "Analysts tend to align their recommendations with the institution's consensus. If they know what their boss wants and/or believes, they're much more likely to [gear their work] towards that outcome. It's an easier path than disagreement and potential confrontation"[80], said one person interviewed. While no organization can fully remove itself from self-protective employee behavior, it can lessen its pervasiveness.

The Defense Intelligence Agency will need to take highly visible steps to build a more open, proactive culture. The most important of these requires the leadership to "walk the walk." Leaders must lead by example, proactively modeling the behaviors they want to see in the workforce. Leadership by example sends a strong message because there is a proven natural inclination by the workforce (particularly by managers) to emulate what it sees — both good and bad. In addition, the Agency can support change by incentivizing collaboration and innovation. Rewards should flow to those who accept calculated risks, effectively work with matrixed teams and contribute to the open exchange of ideas. As an initial step, leadership could invite authors, scenario writers and foreign leaders to address the workforce. They could challenge conventional thinking and aid in "paradigm busting."

As one interviewee pointed out, "when you have people who are not belted into particular jobs by hierarchy but are encouraged organizationally (maybe by reward structures, but the rewards are not simply monetary) you will see people follow leads, inquire, build networks, and make linkages that are not necessarily apparent to others. These will be people who are totally comfortable working at the edge of chaos and who comprehend non-linearity."[81]

As the Defense Intelligence Agency moves to hire a more generalist population with new and diverse attributes, and builds a culture more congruent with its new mission, the sense of change will occur more naturally and become mutually supportive over time.

Future Training and Development Includes Structured Experiences

Many companies have long recognized that training programs can also serve as a mechanism for cultural change. GE's Jack Welch and his use of the company's Crotonville training facility provide the quintessential example. During the two decades he was CEO, Welch met with each graduating class of managers, using this opportunity to infuse his vision, values and priorities throughout the organization. Within a few years every important manager in the corporation heard directly from Welch what was important, and why. These managers, in true network fashion, spread the message to their subordinates. Through this forum, Welch spread his personal message throughout the corporation's decision-making staff.

As the Defense Intelligence Agency reconstitutes its training strategy, it can employ a similar strategy by using its extensive training programs to drive cultural change.

In fact, the Agency's training community will play a critical role in any possible cultural shift. Imparting the new imperatives will require more than speeches, memos and new wiring diagrams. Personnel need new tools to

"I hope the wild and crazy thinkers within the organization have a chance to thrive. You don't want to do things that suppress the wild and crazy thinker."[79]

Professor Daniel Hastings, MIT

perform in the new environment. The Agency's training system must help the workforce develop new sets of key attributes: cultural and cognitive diversity; teamwork; networked collaboration; customer service; pattern recognition; risk-benefit analysis; and scenario development. We outline several of those changes in Illustration 30.

The training community will also need new metrics to access success or failure. Since the expanded aim of training programs goes far beyond the teaching of specific skills, it will be difficult to measure the effectiveness of developmental programs — particularly using current tactical measures such as training hours. Thus, the training community needs to do more than just develop programs to convey these critical attributes. They must also devise outcome metrics for measuring their own effectiveness. Fortunately, such metrics emerge naturally from effective curricula. If the curricula are right, the metrics are obvious.

The Human Resource Function Changes With The New Workforce Design

The new design of the workforce shapes several changes within the human resource (HR) function of the Defense Intelligence Agency. Most importantly, HR will move significantly toward becoming more distributed. Activities such as record-keeping, database maintenance, physical records, cross-Agency policies and some recruiting, training and executive development will continue to be centralized (and possibly outsourced). However, many of the personnel normally assigned to a corporate HR office today will instead be forward deployed to work more closely with the business units they serve.

Additionally, roles within the centralized HR office will be transitional (versus permanent) with "sunset clauses" to move more of the traditional human resource functions into the business units. An executive committee will oversee these distributed functions and, with the advice of human resource policy professionals and general counsel, make the larger, strategic personnel decisions.

As the Agency continuously shifts and realigns itself in response to the dynamic operating environment, its support functions will do the same. This will create a need for continuous planning around every area of human capital investment, development, and utilization to ensure the workforce and its support systems evolve on a parallel track. A high level outline of the future forces at work and their anticipated impact on specific human resources activities follows. Illustration 31.

Human Capital Planning The progress of the Department of Homeland Security in its implementation of new approaches to human capital issues bears watching. The Department begins with a minimal number of job classifications, which changes the structure, introduces a pay for performance scheme to be more market oriented, and advances career specific developmental strategies for the workforce. These and other innovations "change the workforce planning conversation" as the Office of Personnel Management's Ron Sanders put it recently in an interview for this Paper.[82] This effort will likely provide numerous lessons that the Defense Intelligence Agency and others in the federal government will incorporate.

The workforce of the future's new design will drive many changes in the Agency's human capital planning efforts. Each piece of the workforce will have specific requirements. The generalist workforce will require a robust and sophisticated planning activity (linked to program management) that optimizes and develops staff across disciplines and projects. The contingent workforce will require recruiting, hiring, and maintenance activities not currently in existence. The specialist workforce will require "care and feeding" to ensure workers feel valued in a competitive marketplace for advanced technical skills. In short, the planning activity will need to be strategic — to

Current Development	Future Development
Information	Experience
Individual modus	Group modus
Group composition is serendipitous	Group composition is considered
Uniform demographics	Multi-service, function, background
Data imparting	Action learning
Fact based	Scenario based
Linear curriculum	Diverse curriculum

Illustration 30: Change in emphasis in future workforce development programs
Traditional

ensure it anticipates the needs of the organization, tactical— to ensure it develops and manages the workforce, and relationship oriented— to ensure it retains the best and brightest.

All of this ensures the Agency's access to the right people, ready for deployment to the areas of need on short notice.

On a high level, the human capital planning efforts of the Defense Intelligence Agency will need to harmonize with parallel functions inside the Department of Defense to ensure alignment and coordination. Without harmonizing with the Defense Department, the Agency runs the risk of failing to consider forces that will shape its future. It also runs the risk of making it more difficult to attract and retain top quality military personnel.

Recruitment The development of a diverse, multi-disciplined workforce in a competitive recruiting marketplace will require recruiters to become "human capitalists." They will need to be entrepreneurial, innovative and highly skilled at the art of developing and maintaining an extended network. The role, which is likely to be forward deployed into the business units, will require the ability to function successfully in a myriad of worlds — from academia to business — building relationships that will yield high quality candidates. A centralized administrative function manages the databases and support necessary.

Effective recruiting of military personnel will also be a critical factor in mission success, and therefore needs careful planning and nurturing. This would include cultivating relationships with those who help make decisions regarding personnel assignments to the Defense Intelligence Agency. The senior leadership of the military services must come to understand that the quality of personnel assigned to the Defense Intelligence Agency directly influences the quality of intelligence provided in support of military missions. Therefore, it is in the best interests of the services to ensure candidates are the best and brightest available.

Hiring During interviews conducted for this project, a consistent theme emerged of the need for greater speed in executing aspects of the Agency's intelligence mission. By extension, the same must be true for functions supporting the mission. This is particularly the case for hiring, where speed often determines whether the Agency wins or loses a valued candidate, especially scientists and technologists. As competition for superior human talent increases, and technology advances, the recruiting process must become leaner and faster.

The Defense Intelligence Agency will build its future hiring process with a bias for speed. To accomplish this, it will remove as many hiring layers and hand-offs as possible. A single point of contact can manage and close the process of hiring candidates. Recruiters will migrate into an account manager role, handling the process from inception to conclusion (supported by a centralized back office team handling administration). They would conduct this process in tandem with the business unit, ensuring that the offers extended meet the Agency's policies and the unit's needs.

Retention The drive for flexibility and agility, reflected in the new workforce design, will make retention a much more selective activity in the future. We strongly believe that "hire the best" extends into retention, and human capital planning must identify "critical need" positions into the future and plan to fill those positions. Once hired, leaders will identify the most valuable employees through use of social network analysis and make decisions on retention accordingly. For transitory, "one-off," or difficult to fill positions, the develop-

ment and use of a contingent workforce allows the strategic application of resources.

Retention will move from an effort to hold on to the workforce as a whole to an effort aimed at targeted parts and principal figures. The strategy becomes developing customized incentives that range from bonuses to work design (such as working from home), depending on the needs of the employee. A career vision and developmental plan that allow employees to see future opportunities for growth support these incentives, and help them understand how they fit within the larger vision, strategy, and values of the organization. The Agency will form a relationship with the individual, giving the employee a sense of importance, relevance, and shared commitment.

Performance Management The new workforce design also affects performance management processes. In the future, performance measurement will rely less on the boss-employee relationship, and make decisions based on judgments of teammates and customers. Project-based work and the contingent workforce will drive leaders to derive feedback from teammates, subordinates, customers, etc. After compiling regular feedback, the data becomes one of the bases for promotion, along with other mission-related outcomes. Contingent workers would receive formal feedback which would determine incentives.

The driver for promotion will be the perceived value of contributions by customers and colleagues, making it a highly outcome-based approach. As the value of the contribution and responsibility increases, position and compensation would follow. Consulting companies and other service businesses often use this model, which effectively aligns customer needs and workforce behavior. It requires self-reliance on the employee's part to take ownership of their career development, network relationships, and knowledge base. The Agency continues to offer a myriad of development activities as support, but ultimately the responsibility for career development lies with each individual.

Compensation Over the last several decades, the federal government has advanced a number of regimented compensation schemes. These approaches have limited the government's ability to be competitive in the marketplace, particularly when recruiting those with advanced skills in science or technology. While this is changing to some degree, the Defense Intelligence Agency will need to exploit available exceptions or pursue new reforms that allow for increased flexibility in compensation packages in the future.

Future Hiring Factors	Business Implications
Speed	■ De-layer processes ■ Limit hand-offs ■ Pre-authorize offers ■ Faster clearance processes
Competition	■ Customized role and schedule ■ Work/life balance supportive ■ Offers leading edge work ■ Offers unique work experiences
Relationships	■ Recruiters forward deployed ■ Single point of contact for process ■ Focus on key relationships ■ Field presence (e.g., Silicon Valley)
Compelling	■ Leading edge technology & tools ■ Joint work with external partners ■ Intra-preneurial opportunities ■ Positive, supportive culture
Developmental	■ Continual technology skills update ■ Multi-disciplined, stimulating offers ■ Offers lifelong employability ■ Leadership training (if appropriate)

Illustration 31: Future hiring factors and their implications for the Agency

Achieving transformational change will require moving away from the "billet" or "headcount" approach and instead creating a flexible "human talent" budget. For example, if an operating unit decided it needed to hire a leading expert at a high price (versus moderately priced employees that fit into a particular grade) it would have the flexibility to do so. To shape the workforce in a manner most advantageous to the future, the Agency will need to have the flexibility to hire competitively in the marketplace.

Training and Development Achieving a balance between competencies and attributes involves changes in the conception and development of future training programs. With the focus on

"Analysts are being given products from new sensors, but few analysts actually use these products. They don't understand them. If one analyst finds a new source that works, he or she spreads the word to others. But the process is slow. Only 10% of the guys actually use the new sensors."[83]

Intelligence Community Thought Leader

imparting experience over information, they will become more behaviorally driven than ever in the past.

Discrete and opportunistic training interventions will evolve into lifelong training over the continuum of one's career. The Boeing Corporation, for example, looks at development as providing life-long "employability" (not to be confused with life-long employment which they clearly state is up to the individual employee to achieve based on performance). This concept of the "Protean Career" drives the change toward multi-disciplined development approaches that allows employees to take on a variety of roles over the life of their career. This would work in tandem with a career vision and developmental plan and require all the elements of a good future training and development program as outlined earlier in the People section.

Two areas of training and development bear particular examination as the Agency looks into the future. These are Leadership Development and Technology Skills Development.

Leadership Development The future of the Defense Intelligence Agency rests in large part on the attributes and capabilities of its future leaders. Identifying leaders early in the process, and grooming them based on a clear development and succession plan is a critical component of the Agency's future. A haphazard succession plan jeopardizes mission.

Based on our understanding of the future operating environment discussed earlier, we know that future leaders will need broad-based experiences to succeed. The platform for leadership development will need to be multi-disciplined and ensure exposure to numerous social and technical, field and support experiences. The installation of cross-functional teams and a networked organization will require leaders that are relationship oriented and interactive. The development platform will need to be group based and contrive opportunities for interaction with a wide range of thinkers and practitioners. Finally, because leaders will need to understand cultures and thought patterns beyond their own, the platform should be international. This would argue for ensuring that leaders perform tours overseas in challenging assignments.

Continuous Development Of Technological Expertise

Because the Defense Intelligence Agency's future mission challenges will clearly be both techno-centric and techno-dependent, the Agency will need to develop a deep and robust technological knowledge and skill set. During interviews conducted by the Toffler Associates/Dove Consulting team, a variety of stakeholders expressed concern over the Defense Intelligence Agency's present level of technical knowledge and skill and the ability to build towards future strength. For example:

The nature of Defense Intelligence Agency's mission and the manner in which it conducts that mission inevitably ties people and technology. Failure in one negates success in the other. The increased complexity of technological advances, and the knowledge required to work with them, will be a competitive challenge for Defense Intelligence Agency.

Using the Joint Military Intelligence College (JMIC) to Advance a Broader People Strategy

While the JMIC clearly has a strong reputation as a provider of graduate level education within the intelligence community and military services, it will need to reconsider its positioning, mission, and overall contribution in light of the future operating environment and the transformation of the Agency.

"We are working to promote a culture in the Defense Department that rewards unconventional thinking — a climate where people have the flexibility to take risks and try new things."

Dr. David Chu, Undersecretary for Personnel and Readiness

The JMIC provides an important educational service, but has the potential to deepen and broaden its scope with respect to developing the intelligence community leaders of tomorrow and dealing with some of the difficult community issues of today:

Research and Development (Non-Technical) As JMIC sees itself in the vein of a small university embedded within the Defense Intelligence Agency, the development of a robust, directed "research center" — e.g. developing on-going, non-technical research and development to inform the future mission of Defense Intelligence Agency — would not be out of line with its vision. Closely focused on and tethered to the mission of the Defense Intelligence Agency, this has the potential to be a unique and valuable asset for ensuring the Agency continues to be forward looking in a thoughtful and considered manner.

Intelligence Community Platform The JMIC can serve as a platform for bringing together a fractionalized Intelligence Community and military service intelligence functions. The focus would be around the sharing of information and ideas that would move the overall community's workforce effectiveness to a higher level (and support Congressional demands for increased integration within the community). The JMIC is in a unique position to do this given its illustrious alumni who are in positions of leadership across the community.

Issue Advocacy Highlighting critical strategic and operational issues that are present in multiple intelligence community organizations is a role JMIC could fulfill well. The JMIC could serve as a voice for the community around universal issues that undermine effectiveness. These include: clearance related issues, human resource management, technology development, etc. The JMIC could provide a forum for study, advocacy, and resolution of these on a community-wide basis.

The Way Forward

The Defense Intelligence Agency will not undertake its transformation alone. The Department of Defense, individual services, the intelligence community, law enforcement agencies and numerous public and private sector organizations are all in the midst of some form of "transformation." This concurrency inevitably makes change even more challenging. Successes and failures in one area affect everyone. However, there is a silver lining. As Einstein observed, "In the middle of difficulty lies opportunity." The Agency's leadership may be able to seize the general commitment to transformation to reposition the Agency. It should start by articulating a new vision for defense intelligence for the decades to come.

We believe that the Agency must prepare for this future now by initiating a chain of events that shapes all of the Agency's human capital systems, departments, and various support apparatus to around two goals. First, hire, develop and retain personnel with demonstrated attributes needed for the emerging environment. Second, realign the workforce around

"His [the Director's] most pressing need, and the thing changing the fastest, is technology and the need for a workforce trained in…technologies. If you went through Defense Intelligence Agency today and asked what the chemical precursors to nerve gas are, not many would have any idea …this is a potential threat."[84]

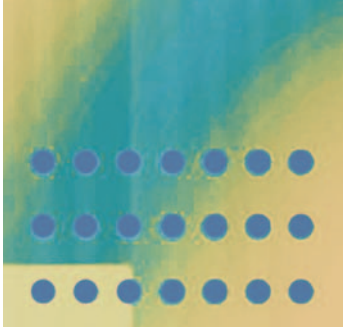
"Historically we've just made technology available to the people in our organizations, we haven't made it integral and helped the users make it integral in what they do every day, and we need to do more."[85]

"The attacks of September 11th make transforming the Department [of Defense] even more urgent because the military is not designed to fight the shadowy terrorist networks that operate with the support and assistance of terrorist states…"

U.S. Secretary of Defense Donald Rumsfeld

specialists, generalists and contingents, with the latter comprising the greatest number.

The rest, in intelligence parlance, is just noise.



STRATEGY

In the future, the Defense Intelligence Agency's achievements will result from a relentless focus on customers and continually assessing customer's needs and the quality of the services delivered to them.

"I've given up trying to be rigorous. All I'm concerned about is being right."

Stephen Hawking

The scope of the threats the United States faces in the global environment and the requirements for neutralizing those threats levy immense burdens on the Defense Intelligence Agency. From a radically changing environment, to the knowledge work the Agency performs, to the products and services and the decisions it enables in its expanding customer set, the Defense Intelligence Agency's leadership will help change the nature of world conflict.

Since its formation in 1961, multiple intelligence community reorganizations notwithstanding, the Defense Intelligence Agency has not had to significantly rethink its identity. The features of the nation's future require a fundamental shift in focus for the Defense Intelligence Agency. The Defense Intelligence Agency of the future seizes upon the opportunity, identifies the articulated and implied needs of its customers, and set out on a deliberate course of renovation. The Agency's external focus is broader, requiring new and closer relationships with DoD, the intelligence community, state and local law enforcement, commercial enterprises, as well as international partners and allies. Internally, DoD has rethought every aspect of operations to be more customer-centered, divesting itself of everything that does not provide tangible value to customers—helping them to make better decisions. Organizationally, it adopts a vigilant matrix analytic structure to avoid surprise.

The objective of preserving national security revolves around information superiority, and as a result, intelligence demands will continue to increase. Changes in the nature, number and magnitude of global threats and the availability of new sources of information place new demands on the Defense Intelligence Agency's customers and ultimately on the Agency.

The doctrine of preemption presents grave responsibilities too. It presumes that American intelligence can ferret out the most secret of foreign science with near infallibility, doing so not only to inform policy makers, but potentially to build a case for war. In effect, it posits a crystal ball.

Robert Gates, former director of central intelligence, notes, "It's not enough to say Iran is developing nuclear weapons. You need information specific enough to give policy makers options for acting against those programs. It's a very big challenge."[86]

The National Security Strategy of the United States, published in September 2002, addresses the challenge saying, "The U.S. has long maintained the option of preemptive

In a recent study, the General Accounting Office offered the following advice for successful transformation.

1. Ensure top leadership drives the transformation.
2. Establish a coherent mission and integrated strategic goals to guide the transformation.
3. Focus on a key set of principles and priorities at the outset of the transformation.
4. Set implementation goals and a timeline to build momentum and show progress from day one.
5. Dedicate an implementation team to manage the transformation process.
6. Use the performance management system to define responsibility and assure accountability for change.
7. Establish a communication strategy to create shared expectations and report related progress.
8. Involve employees to obtain their ideas and gain their ownership for transformation.
9. Build a world class organization.

From: "Highlights of a GAO Forum: Mergers and Transformation: Lessons Learned for a Department of Homeland Security and Other Federal Agencies," General Accounting Office, November 2002.

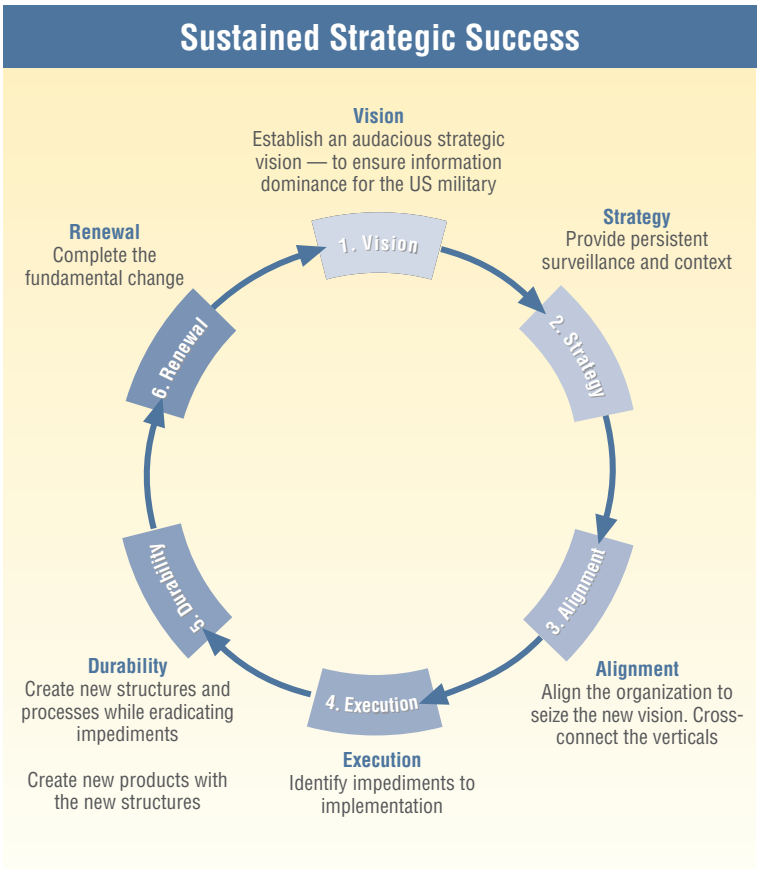


Illustration 32: The Strategy Cycle

actions to counter a sufficient threat to our national security. The greater the threat, the greater is the risk of inaction-and the more compelling the case for taking anticipatory action to defend ourselves..." The United States, as a result, will have to produce "better, more integrated intelligence" to find hidden threats and act against them and to address threats inspired by foreign governments and groups conducted inside the U.S, "we must also ensure the proper fusion of information between intelligence and law enforcement."[87]

A self-renewing process (Illustration 32) enables the Defense Intelligence Agency to develop a strategy, and deliver intelligence that is persistent (provides continual knowledge), denial resistant (resists adversarial compromise) and exquisite (contains all the required details necessary to checkmate an adversary) to respond appropriately to future customer needs.

Step One: Articulate a Compelling Vision

The strategy cycle begins with articulating an audacious and compelling vision of how the Agency accomplishes its mission and what it can become-in order to ensure the commitment of attention, energy, and resources from its many stakeholders. An audacious and compelling strategic ambition is an essential precursor to ensure the commitment of attention, energy, and resources from a broadening set of partners and allies.

Preemption: The Not-So-New Strategy of Prevention

There can be little doubt that "prevention" is a new strategy for the United States of America. However, it would be a mistake to think that such a strategy is in any respect "new". From the beginning of politics through the end of the 20th century, adversaries have used prevention and preventive war to ensure security. But never before has prevention been the stated policy of a democratic nation. And never before has it demanded so much of the people who make it possible.

Sun Tzu counsels, "What is of supreme importance in war is to attack the enemy's strategy." Sun Tzu refers specifically to strategy — not army, not cities, but strategy — because by upsetting an enemy's plans, the enemy cannot fight at all, and war will never occur.

Indeed, what Sun Tzu advocated thousands of years ago is what the Defense Intelligence Agency and its customers aspire to do in the future. Pervasive intelligence will change the environment in which nations function. By pervasive observation, the United States will change the enlightened self-interest of its adversaries, possibly persuading them to rule out war as a rational option.

Not surprisingly, the strategy of preventive war will demand new attributes from the Agency's workforce. Cognitively, Agency analysts and attachés will have to be global thinkers, able to imagine surprising permutations and reconstruct enemy plans. They must have sound judgment, and be able to take the calculated risks necessary to disrupt enemy strategies. They must be collaborative communicators, capable of real-time collaboration and facing their customer

Step Two: Craft An Engaging Strategy

As much of the world continues to struggle through industrial civilization into a knowledge era civilization, conflict is inevitable. An ancient Zulu proverb wisely observes, "War begins in the head, and goes to the mouth." That is, conflict begins when the unobservable "will" — the head — becomes hostile. By understanding the genesis of war, the Defense Intelligence Agency prevents conflict from developing into destructive conflict. In a future where information is the ultimate source of power, the U.S. can maintain its security by making better decisions through the development and application of intelligence. An audacious and compelling strategic ambition is an essential precursor to ensure the commitment of attention, energy, and resources from a broadening set of partners and allies. It means that by aggressively using and applying information, the Defense Intelligence Agency will help policymakers and human operators prevent most destructive conflicts and win those that they cannot prevent. In so doing, the Defense Intelligence Agency will render war a useless instrument of policy and make the U.S. a safer and more secure place.

In the second step of the cycle, leadership creates a strategy to achieve that vision that provides persistent context for policymakers and operators. In order to realize the vision of preventing destructive conflict, the Defense Intelligence Agency must ensure decision superiority by providing customers with persistent surveillance and context. Novel challenges require new ways of organizing and working, and serving a broadening array of customers with a tailored set of products and services. Future customers will be more intimately involved at every stage in producing the information they require, and the Defense Intelligence Agency must be able to provide access to the required information in the right period.

As discussed in detail in the Structure section, a customer-focused analysis function arranged in a matrix of regions and functional threats covers known threats and positions the teams to sense emerging threats. The regions relate to the geography and culture and demand an expert-area approach. The threat component supplies expert knowledge and imagination to assess how and why the geographies and cultures handle threat capabilities. The teams possess overlapping capabilities designed to anticipate and prevent threats from developing. The teams' focus areas shift as new threat areas emerge or combine. Although the teams overlap in their coverage, a "Global Warning" team articulates a global point of view and monitors emerging threats.

Defense Intelligence Agency executives lead each of the teams, but members may be full-time or part-time Defense Intelligence Agency employees, government employees from other

teammates in person. They will have to shape technology, and with it their future. And — above all else — they must be anticipatory and proactive, focusing not only on outcomes delivered to their customers, but the outcomes which their customers aim to achieve in their operations. Transformation is not about the changes the Agency makes for itself. Rather, transformation occurs when the Agency makes changes that allow its customers to transform their own operations.

The doctrine of prevention is not new, but it makes new demands. It must be executed seamlessly on the best intelligence to be successful. It demands that intelligence be both constant and pervasive. There is a mixed record for preventive war — some countries, such as the U.S.S.R. fared poorly by it, while others, such as Israel, used it to great effect. But preventive war results from the failure of a strategy of prevention.

One could argue that, in 1950, American national strategy was in a state of failure. Democratic Korea was in a dire situation. It was then that America considered preventive war: Secretary of the Navy Francis P. Matthews gave a speech in support of it late that August. At that time, American leadership judged that the nation was not capable of such a strategy, and summarily rejected it in favor of the strategy of containment. Now, they have judged differently. They have put their faith in those national capabilities upon which any preventive strategy must depend — intelligence and precision. The people of the Defense Intelligence Agency will not let them down.

agencies, contingent staff from think tanks, consultants, free-lancers, or academics or others. A smaller, more closely knit, Defense Intelligence Agency workforce may increase agility and response as each team member's responsibility level for tracking and reporting on threats increases. The analyst of the future works in a Contracting Officer's Technical Representative (COTR)-like role, contracting for or arranging for the acquisition of precisely the capabilities that his or team needs-and being accountable and responsible for the team's success.

Based on customer demand, the teams produce reports in a variety of formats on a variety of platforms. In broad terms, analysts produce two major categories of services: short, news-like, customer-tailored reporting for crisis support or for general information and awareness; and more in-depth studies that reflect deep understanding of potential threats by global experts and intelligence in each of the areas that enable customers to make informed decisions. The analyst teams continually update the in-depth studies as new information becomes available. A Global Warning team captures maintains global vision to report on emerging threats and to characterize current security risk and leads writing the "Annual Report".

The two broad categories of information benefit both of two broad categories of customers-policymakers and operators (Illustration 33). Customers include top Defense Department and other executive branch officials who will use the information to enhance their understanding and make better policy decisions regarding potential sources of danger or conflict. The Defense Intelligence Agency's knowledge of global cultures, technologies, and dynamics provides the advice Pentagon planners require as they anticipate future systems acquisitions.

Military operators at all levels rely on the information to enhance their own decisions at a tactical level to prevent conflict or to

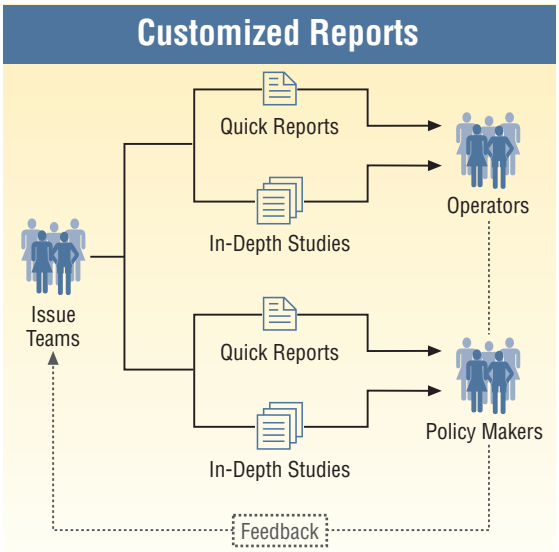


Illustration 33: The issue teams provide quick reports and in-depth studies for operators and policymakers, tailored to each customer's

prevail in existing conflict situations. The operator includes commercial suppliers to the Defense Department who use Defense Intelligence information to improve the products and systems they deliver. The Defense Intelligence Agency collaborates with customers at every level to understand their emerging needs and to provide them with the "persistent context" that anticipates their information needs and continually supports their ability to make better decisions.

Step Three: Align or Fail

Once the Agency creates the strategy — the implementation plan for the vision — it must educate the staff, align it with the processes, structures and technologies required to execute the strategy, and achieve the vision.

This issue management structure functions optimally with the support of a fully aligned leadership. Agency leadership models a global and intellectually diverse approach to intelligence. Operating executives work with the issue teams to set appropriate measures, and then apply those measures to continually improve performance. Advisory Board members import their global connections and strategic thinking to advise the director on innovative enhancements to Agency capabilities. The executive team ensures that the Agency maintains forward-looking focus and response to satisfying customer needs and removes obstacles to performance while adjusting the organization's focus as the environment changes.

A key to proper alignment of the issue management function is to ensure that executives fully support the model and communicate that support throughout the organization. New compensation programs focus attention by rewarding increased interdisciplinary collaboration to deliver on the strategy. Future threats will require an ability to focus on multiple changing priorities and to reassign priorities to respond to shifting environmental dynamics. Superior agility and adaptability allow the Defense Intelligence Agency to seize the opportunity to retain a competitive advantage over future national security threats.

Step Four: Execute With Discipline

Execution, where the first three planning steps result in tangible action, is arguably the most critical link in this cycle. It depends on having generated a commitment within the workforce to implement the strategy and achieve the vision.

An interviewee familiar with intelligence community strategies noted that although Defense Intelligence Agency articulates an appropriate vision, the Agency lacks a clear plan to execute it: "I've seen briefing decks from the Agency, they have good ideas, but they are not an Agency plan, they are missing a statement of the need for what technology is missing, and what the costs are. They need to articulate how the staff should be different in five years."[88] The executive leadership team should be accountable and responsible for the planning, execution, and assessment of the Agency's strategy.

The key to execution is careful planning, and the future Defense Intelligence Agency will have created a planning group that works closely with the issue teams to understand and map how the Agency must grow and change to remain ahead of customer demands.

The challenge of execution is critical to the success of any strategic ambition and most often the reason for failure. By methodically planning the "chunks" of changes needed, and ensuring broad understanding and engagement on the part of those responsible for achieving them, the Agency will deliver products that customers value and actively seek. By streamlining the core workforce and providing it with increased responsibility and authority for performing top quality detective work to uncover enemy secrets the Defense Intelligence Agency will unleash tremendous enthusiasm among its staff. No longer constrained by rules and standardized processes about every facet of work, employees will apply logic and intuition-using left- and right-brain-challenging and helping one another to identify and neutralize security threats before they imperil American civilian or military personnel or assets.

Step Five: Ensure Durability

In step five, the Agency ensures the durability of its vision, mission and processes to gener-

ate and sustain future value. As the Defense Intelligence Agency matures, it will focus increasingly on remaining agile in its approach to changes in its operating environment-continually adapting its structure, processes, products and services to the changing needs of its customers. The recruiting and succession processes will select for staff who demonstrate agility and adaptability. At the same time, the Agency will aggressively divest itself of those things that customers no longer value.

Step Six: Measuring Results Speeds Renewal

To ensure congruence with customer needs, in step six the Agency assesses value of work performed and adjusts accordingly, using a system of measurement and feedback. The future Defense Intelligence Agency will engage in continual assessment and renewal. The process of renewal springs from awareness of both the value the continually created by the Agency and opportunities for expansion. By measuring the value of its products and services, it will continually assess whether it is executing its mission and evolving to accommodate changing customer needs.

Ambitious strategic goals (e.g., Illustration 34) can indicate success and stimulate Agency staff to transform and improve the quality provided to its customers. These illustrative measures assume that the items assessed are significant, mission-relevant and demonstrate customer value. The executive team is responsible for establishing goals in cooperation with their areas of responsibility and for modifying the factors as customers' priorities change.

- Defense Intelligence Agency Policy Changes: Discovery leads to policy changes that better align present behavior with emerging future requirements. Transformation, "fundamental change," cannot occur without changes in policy.
- Introduction of New Processes: As executives discover process inadequacies, they rapidly introduce reformed processes. These processes might relate to human resource activities across the life cycle beginning with aptitude or skills identification, and running through recruiting, development, all the way to retirement. Or, they might relate to some element of product, service, production, channel, or relationship.
- Introduction of New Technologies: Technologies that take time and work out of production or management can increase productivity, improve quality, or enhance the workplace. Transformational application of technology can reshape reality for the adversary and provide strategic advantage.
- New Product or Market Identification: As the organization looks into the future competitive environment, it identifies opportunities for new products and new markets. In an environment of fundamental change, such as the changes the Defense Intelligence Community, is experiencing, every element in the value chain is changing simultaneously. Every change is an opportunity to grow in service.
- Community and Stakeholder Outreach: When an organization possesses critical intellectual property (new policies, new processes, new technologies, or insight into new markets) it owes the industry to reach out and give the industry this discernment. The degree to which the Defense Intelligence Agency becomes a model for the Intelligence Community is a measure of its success or failure. Knowing that the Agency will produce an "Annual Report to Stakeholders" helps motivate it to serve better.
- Salience and Portability of Recommendations: Discoveries made in one sector can be so valuable that the Agency exports them to other sectors, for the improvement and benefit of the system as a whole. For example, if a new approach works well for the Defense Intelligence Agency, the National Security Agency, the Department of Homeland Security or the Federal Bureau of Investigation could import it.
- Cost efficiency (ROI): This is the degree to which transformational efforts result in financial benefits, or return on investment in the form of positive effects produced per dollar expended.

- Divestitures: As the Agency identifies mismatches between the current state and the future state, it divests itself of low-value activities, processes, projects, investments, and structures. For example, administration, the management of the basic information technology architecture, or administrative aspects of the human resources function might all be outsourced.

With a clear path for creating, executing and renewing its strategic direction, the Agency will identify the critical strategies necessary to make violent conflict unnecessary and to prevail where force is required. It will methodically assess and subsequently align the capabilities of its technologies, processes, structure and people to support its strategic ambition. By articulating an inspirational vision, planning a motivational strategy, generating alignment across the enterprise, the Agency will be prepared to execute and overcome the expected resistance to major organizational change.

Measures of Transformation

	Criteria met	Some criteria met	Criteria not met
	🟢	🟡	🔴
DIA Policy Changes			
Introduction of new processes			
Introduction of new technologies			
New product or market identification			
Community and stakeholder outreach			
Salience and portability of product or services			
Cost efficiency (ROI)			
Divestitures			

Illustration 34: Stoplight symbols will indicate the level of transformational achievement in each area, each month. For example, if a policy change enables the Agency to move away from a billet-system that stoplight would be green for that month.

SUMMARY AND RECOMMENDATIONS

Be a partnership of highly skilled teammates helping prevent destructive conflict from erupting, and helping predetermine the outcome of destructive conflict in favor of the United States.

Plan Changes To Occur Epoch-By-Epoch

Time has run out for the "old" Defense Intelligence Agency. The Defense Intelligence Agency must pursue its re-invention immediately and earnestly, and finish the first increments of fundamental change before the end of 2007. We envision that change will manifest in five epochs, beginning in 2003 (Illustration 35), "The Epochs of Change" below, is a depiction and summary of those epochs and the focus of each. The focus is on work intends to attain a near-term goal in support of a longer-term goal.

Epoch 1: Build The Infrastructure For Good Growth

Epoch 1 has begun. The Defense Intelligence Agency rightly counts on people-human talent-to envision, implement, and master the necessary changes in end-state vision, strategy,

Epoch 1: Build the Infrastructure for Good Growth	**2003** ■ Know critical requirements for and attributes of the Analysts of the Future (AOTF) ■ Build the nformation infrastructure ■ Identify impediments for eradication
Epoch 2: Prototype AOTF	**2004** ■ Eliminate impediments ■ Create functional and regional teams to satisfy informational needs ■ Consolidate issues teams electronically ■ Publish initial annual Defense Intelligence Assessments from teams
Epoch 3: Structure for Strategic Effect	**2004-2005** ■ Hire the best, inspire and text, retire the rest to become all-source with effect ■ Change the Defense Attaché system and school
Epoch 4: The New DIA	**2005-2006** **Be a partnership of highly skilled people and leading edge technologies providing warfighters, policy makers, and planners with assures access to required intelligence.**
Epoch 5: New End State	**2006-2007** **Be a partnership of highly skilled teammates helping prevent destructive conflict nfrom erupting, and helping predetermine the outcome of destructive conflict in favor of the US.**

Illustration 35: Epochs of changes.

organizational alignment, technology, processes, and execution plans to usher in an era of renewal. The urgency of the need to close the gap between what the Defense Intelligence Agency is and what it must become determines what is necessary. The urgency of the need to close the gap also determines the scope and pace of change. For example, were the Defense Intelligence Agency to determine it needed more linguists, it might take the simplistic approach of hiring more foreign language speakers. On the other hand, it might take a more audacious approach by infusing funds into research and development for simultaneous translation systems. A third alternative would be to hire a contingent workforce of part-time linguists while investing in translation research and development. The urgency of the need to close the gap would determine the scope and pace of the response.

In all cases, in order to close the gap, a first step is self-awareness: base-lining the organization. Simultaneously, the organization must envision potential future environments and how it can best serve its customers and differentiate itself in whatever becomes "the future." This White Paper postulates that future environment and the strategies, process changes, technologies, structures, and people strategies necessary to command that future. Seeing the need to close the gap between where the Defense Intelligence Agency is and where it must go is the most difficult challenge in Epoch 1.

Why? This is a challenge because change impediments exist, and foremost among these may be the perception that the Defense Intelligence Agency is already successful, but understaffed. Policy, process, structure, technology, other organizations, and even the Defense Intelligence Agency's own people can be impediments to realizing or moving toward a different and more desirable future end-state. The less ambitious the end-state vision, the less urgent seizing it becomes.

Get The End-State Vision Right. We found little awareness of an end-state vision among the Agency workforce, and no awareness of one among key Agency stakeholders. Given the goal of fundamental change, and even appreciating how far the Defense Intelligence Agency must travel, its beginning end-state vision is modest: "Be a partnership of highly skilled people and leading edge technologies providing warfighters, policymakers, and planners with assured access to required intelligence." As one human resources and organizational development expert we interviewed put it, "No one will want to come to work 10 minutes early or stay 10 minutes late for a vision like that." Said another way, the present vision-however limited in its deployment-is descriptive of what the Defense Intelligence Agency should have been in 1990 and not what it should aspire to become at the end of the first decade of the 21st century.

Thus, to stimulate progress we offer a new end-state vision, faithful to what we see in the future: **"Be a partnership of highly skilled teammates helping prevent destructive conflict from erupting, and helping predetermine the outcome of destructive conflict in favor of the United States."**

To meet this vision by 2007 demands a new set of implementation strategies and actions that are more aggressive. A new matrix team structure, a new vision of "the analyst of the future," a new way to think of attachés, new products, and new services for new customers will demand new technologies aimed at producing an "all source knowledge overmatch." Given the requirement to create such knowledge, the Defense Intelligence Agency will be able to provide the knowledge and warning that allows it to help combatants and policy-makers prevent-to deter or preempt-conflict. It will have the capacity both to get inside the head and under the skin of potential adversaries. Should destructive conflict arise, the foreknowledge and analyses that the Defense Intelligence Agency provides helps ensure that the United States pre-decides contests in its favor.

Determining "what it takes" to close the gaps between the present and the future will consume much of Epoch 1. Doubtless, this phase will include policy changes, technology investment and deployment, training, the definition of customer-friendly and customer-demanded products and services, process and partnership and changes, and organizational structure changes. Defining the specific changes

and the integrated roadmap to affect them are integral to Epoch 1. Also integral is the assignment of a handful of trusted advisor coaches to the senior Defense Intelligence Agency executives responsible for change. Such coaches should have the actual experience of having led and managed large, complex organizations during change.

There Are Low-Hanging Fruit in the Technology and Process Arenas

Among the changes and attainments in the spheres of technology and process we consider urgent in order to support creating the workforce of the future are those listed in Illustration 36, "Low-Hanging Technology and Process Fruit," above.

Collection, Analysis, And Information Management Are The Core Businesses. In order to attain these objectives, the Defense Intelligence Agency must begin the process of identifying and targeting policies to change and plan for enhancements to each of its core business areas: collection, analysis, and information management. Simultaneously, it must support each of these by funded investments in the infrastructure.

Collection enhancements include the revitalization of Defense HUMINT capabilities and the integration of counterintelligence with Defense HUMINT, creation of better customer-provider partnerships, integration of national-global-theater capabilities to support the previously unassigned missions of the U.S. Strategic Command, and the preliminary definition of a portfolio of prioritized future technical capabilities and the direct liaison authority to work with Service and Federal laboratories and defense vendors to acquire and drive leading-edge capabilities and equipment.

Improvements to analysis includes identifying specialist functions (such as human resources administration, contracting, security, and information technology management) and regional expertise that can be "rented" from outside sources to shift organic Defense Intelligence Agency billets to the "Analyst of the Future" and the "Attaché of the Future." Other enhancements would include an increased focus on the carbon elements of future conflict (the human mind, human will, brain science, psychopharmacology, and the human vulnerabilities in decision-making) and the silicon elements (emerging adversary or rival "net-centric" capabilities, information operations at the molecule-, code-, machine- and network-level, and better understanding of the relationship between commercial communications and space capabilities and military communications and space capabilities for future conflict). Finally, improvements in access to data and control over when and how it is processed will yield future dividends.

To manage information better, the Defense Intelligence Agency's supporters must advocate assigning the Defense Intelligence information authority for information standards and protocols within Defense intelligence. As mentioned earlier, no intelligence agency is responsible for determining and enforcing data and metadata standards, search and access protocols, best applications, or best commercial practices for information management. Absent standards and processes for managing data across the commu-

Nine Immediate Opportunities

1. Begin shifting significant data integration to machine to avoid overloading analysts with information.
2. Exploit networking and encryption technologies to expand the pool of experts DIA can focus on emerging issues.
3. Focus conventional collection efforts on precision weapons, integrated sensor networks, stealth, and UAVs.
4. Educate DIA analysts on the newly emerging critical nodes in the American technological infrastructure.
5. Focus on bioterrorism as the most significant threat to US national sovereignty.
6. Increase HUMINT capability to ensure information superiority, warning capability, vet open source data and differentiate from media; rethink the role and processes of HUMINT personnel in the field regarding future information needs.
7. Rework the information classification system to increase sharing of information and knowledge: if the new competitive advantage of the U.S. military is information superiority or dominance, then that requires linked technology and sharing among U.S. intelligence, military, and policy making actors.
8. Use the opportunity of the new space construction to begin redesigning processes and interactions by creating a set of determined outcomes matched against the existing social network of the organization. For example, linking collection and analysis activities around customer requirements.
9. Create an Attaché in each customer space to vet requirements as a start to an aggressive set of actions aimed at proactively managing and prioritizing requirements, and use this as a means to link the overall transformation effort more closely to DOD's transormation efforts.

Illustration 36: Low-Hanging Technology and Process Fruit

nity, contemporary capabilities (such as fusion) and future capabilities (such as inductive analysis, visualization, and animation) are unattainable. Until content is manageable across the community, all source content cannot be integrated for rapid manipulation or display. Acquisition of access to continuous modeling and simulation capabilities also is a requirement.

Epoch 2: Prototype the Analyst of the Future

The demands of Epoch 2- beginning in 2003- deliberately drive the attainments required in Epoch 1. By the end of Epoch 2 in 2004, the Defense Intelligence Agency will reorganize into Regional and Functional Teams and use the physically and electronically collocated team structure to create a new family of predictive assessments. A contingent workforce of analysts, linguists, geographical area and subject matter experts will allow the Defense Intelligence Agency permanent workforce to shrink. The assessments of its Global Warning Team will begin to drive defense research and development investment.

Defining the first cadre of the "Analyst of the Future" and "Attaché of the Future" in 2003 will be critical to success in 2004. Selection for attitude, aptitude, and attributes will supplant selecting new hires merely for their basic skill sets. In addition to the polygraph, other measurement and screening tools will be necessary.[89] The team setting and matrix organization create "families" of cross-connected experts that help support the Department of Defense's top intelligence priorities. In order to create the first cadre in 2004, some policies and human resources recruiting, selection, accession, training, re-training, and release processes must be in place in late 2003 or early 2004. Empowering the analysts must be new technologies, and these must begin arriving in late 2003 or early 2004. Thus, the initiative shown in 2003 determines the success or failure of 2004.

Epoch 3: Structure for Strategic Effect

Epoch 3 begins in 2004 and cascades in to 2005. During this phase the workforce mantra is "Hire the best, inspire and test, retire the rest." in order for the Defense Intelligence Agency to become both "all-source" and "all-source with effect." Anticipating that some changes take longer than others do, changes to the defense attaché system and school do not occur until 2004-2005.

Epoch 4: The New DIA

By 2005 and through 2006, the Defense Intelligence Agency is in Epoch 4 of change. The alignment of vision, strategy, processes, technology, and the attributes and aptitude of its workforce move toward an ambitious end-state vision. By the end of 2006, the Defense Intelligence Agency will appreciate the more modest initial vision of its end-state. It will be a partnership of highly skilled people and leading edge technologies providing warfighters, policymakers, and planners with assured access to required intelligence. As products serve customers better, as the workforce is empowered to stretch its competence, as technologies help create foresight, the more ambitious vision of Epoch 5 moves within reach.

Epoch 5: New End State

Epoch 5 consummates when the Defense Intelligence Agency is a partnership of highly skilled teammates helping prevent destructive conflict from erupting, and helping predetermine the outcome of destructive conflict in favor of the United States.

Success Begins With Implementing These Recommendations

Attaining the vision for the Agency's more ambitious end-state begins in 2003. Before the end of 2003, implementation of the Workforce of the Future must have begun. An implementation plan is required for each of these early wins. Implementation plans should define the objective of "the chunk," the desired outcomes, and the success measures to attain the desired outcome by the time specified. As long as the Defense Intelligence Agency is alert to change fatigue, it can undertake multiple chunks at once. During this interval, the leadership of the Defense Intelligence Agency also must remain acutely aware of the distinction

between "activity" and "progress." They need to recognize the occurrence of numerous lower-value activities undertaken and disguised as progress.

For example, the introduction of tools or applications for better workforce management is progress to the degree that these activities support attainment of the future workforce or the futureend-state. One must recall that in 1939, for example, the U.S. Army research and development activity was pursuing creation of an effective but costly gas mask for horses. A transformation in warfare, the German combined arms Blitz, consigned that research and development to the category of "activity" while the effective coupling of the radio, the tank, and ground attack aircraft were authentic "progress."

The goal is to move forward with introducing fundamental change in the attributes and capabilities of the Defense Intelligence Agency workforce. The shoulders of the new workforce will carry the weight of authentic and valuable change. Figure 37, "Workforce of the Future First Fruits," identifies the progress possible in 2003.

The following five initial major muscle movements in the human resources sphere will help reshape the workforce so that it can envision, anticipate, and master the intelligence problems of the future.

Hire the Best, Inspire and Test, Retire the Rest

People — the right people — underpin the process of fundamental change. Not all the present workforce will be up to the challenge. Several years ago, we asked the leader of a large and complex Federal organization to assess what it would take to transform his organization. He replied, "We are an analog culture in a digital world. Figure out how I could pay 85 percent of my employees to stay in the parking lot and not come in the building and I could transform this organization."[90] This was not and is not a solution. Rather, the Defense Intelligence Agency must simultaneously hire the best and inspire the existing workforce and test its members for their ability to learn new things and work in new configurations.[91] Those who are unable or unwilling to be contributing members of the "new" Defense Intelligence Agency should retire, or be asked to leave to other endeavors.

Recognize And Reward New Behaviors, Dissuade Old Ones

Predictive and contextual intelligence requires insight, opinions, and, most of all, risk. Attaches gather and analysts assemble evidence to uncover knowledge of what adversaries are trying to hide. Expecting or demanding that they make perfectly precise forecasts or assessments is perfectly wrong. All hypothesis making is intuition. Accuracy in intuition supported by evidence ought to be the goal.

Scores of interviews show that today a form of organizational paralysis permeates the Defense Intelligence Agency. This paralysis manifests in the form of fear of not going out on a limb with analysis. Keen instinct and sharp analytical insights are lost when managers over-work intelligence products, take risk averse stances, or keep analysts separated from customers. Production cannot stop during the change process. Dissuading managers

1. Clearly articulate a more compelling end-state vision, durable and enduring core values, mission, and core competencies that the Defense Intelligence Agency will use to define its future.

2. Communicate and over-communicate the vision and the end-state to teammates, partners, customers, and critics.

3. Identify core skills and organic core competencies and plan to outsource or eliminate personnel requirements for obsolete skills.

4. Affirm the attributes required and identify a prototype cadre of Analysts of the Future and Attaches' of the Future and the training and development activities required to create them.

5. Selectively recruit for attitude and aptitude using existing new screening tools.

6. Identyify all known impediments to creating the Workforce of the Future and determine which impediments can be eliminated by policy changes.

7. Create an Advisory Board of "outsides"–CEOs, COOs, Vice Presidents, and mavericks – to help ensure openness in Defense Intelligence Agency leadership thinking.

8. Create an Information and Content Panel as a subordinate "outsider" council of advisors to the Advisory Board.

9. Enlarge the guiding coalition of change advocates into a diverse, multi-generational, "all-ranks" Change Leadership Council.

10.Chunk the change process into small, manageable, short-duration projects that lead progressively to the end-state.

Illustration 37: Workforce of the Future First Fruits

from creating fear, while working with analysts to acquire better communications skills and writing techniques, is a first step towards stabilizing and improving the Defense Intelligence Agency product.

Make Hiring "Decentralized Competitive" And "Centralized Supported"

In this construct, functional areas, specialist disciplines would have the authority and resource to recruit key knowledge workers from among those in the field with whom they have long-term, strategic relationships. The "masters" would select the "apprentices" and "journeymen" for each "guild family." The corporate human resources staff supports the guilds with broad policy and guidance and quick and flexible hiring processes that allow the Defense Intelligence Agency to be competitive with public and private entities. Policy changes should begin to move the Defense Intelligence Agency to a "human talent budget," and away from a "head count" and "head room" budget. If the budget allowed the Defense Intelligence Agency to hire more Defense Intelligence Senior Executive Service and Defense Intelligence Senior Level positions than present — and especially if these were recruited from the "outside" — that would not be undesirable.

Focus on the Building Of Technology Skills and Technology Capability

Among "knowledge organizations," the Defense Intelligence Agency is behind — both in terms of the operational availability of technology and in collection research and development. In the technology realm, in terms of people and equipment, we estimate that there is approximately a $2 billion shortfall between what the Defense Intelligence Agency has and what it needs to be an authentic "all-source" production engine. Technology shaped for specific purposes demands a cadre of technophiles within Defense Intelligence Agency passionate about improving the production and prediction capability of analysts and passionate about improving the system-as-a-whole. Hiring a new chief information officer would be a good first step, but budget, quality staffing, and creation of a network of experts are follow-on steps. We propose an Information Technology and Content Management Panel as a sub-council of the revitalized Advisory Board. This Panel would introduce the leadership of the Defense Intelligence Agency to "state-of-the-practice" and "over-the-horizon" technologies for information and content management.

We also suggest that the Defense Intelligence Agency begin to build relationships in knowledge centers as far apart as Silicon Valley and Bangalore. Many knowledge workers — especially more mature ones — are geography-insensitive. Opportunities for education with industry should be seized. These could provide an inspirational sabbatical for some Defense Intelligence Agency employees, and it is at least a network-extending initiative for the Agency.

Use the hiring of a chief training officer and the redevelopment of training to institute a group and individual training program that not only builds skills, but also builds the culture that the Defense Intelligence Agency strives for in the future.

General Electrics' "John F. Welch Leadership Center,"[92] in Ossining NY, also known as "The Crotonville Experience", and the 286-acre campus of the 120-residential room "Boeing Leadership Center" in Florissant, MO are fine models Illustration 38). Each focuses on training, executive development, and a corporate commitment to the lifelong learning that characterizes a learning organization. The Boeing Leadership Center, for example, has and offers training slots in most of its group development courses to customers, including the U.S. government. Among these courses are Strategy, The Strategic Mindset, Marketing, "Leading From the Middle," "Leading From Below," and Executive Development.

Group development is essential to inculcate the spirit and to create the culture of the "new" Defense Intelligence Agency. Group development links all staff to the mission — from finance to human resources to contracting to analysts — so all have a sense of purpose, importance, and relevance to the mission. Composing cross-functional, cross-

Illustration 38: "Harry's Place": The Two Hundred-Seat Dining Room of the Boeing Leadership Center

generational, Joint Service, and cognitively diverse groups helps the "new" Defense Intelligence Agency in developing resident attributes as well as discrete tactical skills.

Begin Building A Cadre Of Experts

The Defense Intelligence Agency needs "signature" people and "flagship" products. If the Defense Intelligence Agency seizes the vision to "Be a partnership of highly skilled teammates helping prevent destructive conflict from erupting, and helping predetermine the outcome of destructive conflict in favor of the United States," it will need a different cadre than a more modest vision would require. A more modest vision — "Be a partnership of highly skilled people and leading edge technologies providing warfighters, policymakers, and planners with assured access to required intelligence" — risks merely fixing what is judged broken.

- Recognize and reward new behaviors. dissuade old.
- Move hiring processes to be 'decentralized competitive' and 'centralized supported.'
- Focus on the building of technology skills and technology capability.
- Use the opportunity of the hiring of Chief Training Officer and the redevelopment of training to create a training program that not only builds skills, but builds the culture through group training processes.
- Begin building a cadre of experts. Start with the Advisory Board, but create expectations and opportunities analysts and other staff throughout the organization for a high degree of interaction with operators, journalists, regional experts, and others.

Illustration 39: Starting to Build the Workforce

Building the cadre begins with the identification of role models to mobilize the Advisory Board and the identification of a multi-tiered coalition of change advocates within the Defense Intelligence Agency. These role models — "signature people" — create behavioral expectations. "Signature people" also create opportunities for a high degree of interaction with operators, journalists, area experts, analysts, and other staff throughout the organization. This is a first step toward building the eventual contingent workforce that will magnify the Defense Intelligence Agency's capability. (Illustration 39.)

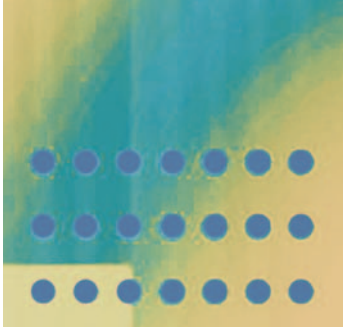
Summary: We Are Behind

In summary, as you read this we are nearly halfway through 2003. If fundamental change is the goal, our judgment is that we are behind. Our opinion is that we can — and should — both catch up and get ahead.

APPENDIX 1

External Interviewees for DIA Workforce of the Future

George Apostolakis	Director, MIT ESD Counter-Terrorism Program
Peter Baxter	Director, Jane's Information Group
Paul Bergamo	VP and CTO, Liberty Mutual
Brett Biddington	Space Initiative Manager, Cisco Systems
Scott Bradner	Senior Technical Consultant, Harvard University
Dennis Bushnell	Chief Scientist, NASA Langley Research Center
Scott Charney	Chief Security Strategist, Microsoft
Anthony Cicco	Chief Mission Support Officer, GAO
Joseph Convery	DIA Representative to NORTHCOM
MGen Dave Deptula	USAF, ACC/XP
Darleen Druyun	Deputy General Manager for Missile Defense Systems, Boeing
Carol Dumaine	Director, Global Futures Partnership, CIA
Bran Ferren	Co Chairman and Chief Creative Officer, Applied Minds
Jim FitzSimonds	Naval War College
Daniel Hastings	Professor, Department of Aeronautics, MIT
Rich Haver	Special Assistant to the Secretary of Defense for Intelligence
LtGen Daniel James, III	Director, Air National Guard
Lt. General Jay W. Kelly (USAF, Ret.)	Senior VP, National Security Solutions Group, ManTech Corporation
Penny Lehtola	Outreach Director, ARDA
Bob Leonhard	Military Theorist, Author, Fighting by Minutes
Wilson Lowery	Executive Assistant Director, Administration, FBI
Dennis McLain	Manager, Defense and Intelligence Operations, Sun Microsystems
David Moschella	Author, Customer-Driven IT
Col Jon Noetzel	OSD Air Force Military Assistant (Net Assessment)
Joseph Nye	Dean Harvard University John F. Kennedy School of Government
Michael Paige	Professor, Former Center Director, Xerox PARC
John Palguta	Vice President, Partnership for Public Service
Gene Partlow	Vice President, Boeing Corporation
Marsha Marsh	Vice President, Partnership for Public Service
Holger Mey	President and CEO, Institut fur Strategische Analyses
Proctor Reid	National Academy of Engineering
Sami Saydjari	CEO, Cyber Defense Agency
Howard Schmidt	Chair, President's Critical Infrastructure Protection Board, White House
Jeff Starr	Office of the Secretary of Defense, Special Operations Low-Intensity Conflict
Mike Tavik	NORTHCOM/J25
Alvin Toffler	Author, futurist
Craig Vroom	Special Assistant to NORTHCOM J2
CAPT Stu Yaap	Commander of the Combined Intelligence & Fusion Center
Stephen Younger	Director, Defense Threat Reduction Agency



APPENDIX 2

Critics of the intelligence community have been vocal.

Date	Publication	Author	Title	Comment
June 6, 1995	The Project on Intelligence Reform	John A. Gentry	A Framework for Reform of the U.S. Intelligence Community	The major reason for the nation to mandate reform of the Intelligence Community is that for many years it has not performed well. The reason is not the demise of the Soviet regime. Taxpayers have not been and are not getting their money's worth from this part of government. And, if history is the good guide it usually is, some people in uniform will pay heavy prices in blood one day for the errors of the Intelligence Community and its elected masters in the Executive Branch and overseers in Congress unless major reforms are promulgated soon. The ravages of years of bad leadership will take years to undo under the best of circumstances.
Fall 1997	Foreign Policy	John Deutch	Think Again: Terrorism	No combination of imaginable or affordable measures will give complete protection from terrorist threats. Nor should this be expected; after all, large armies do not stop all war, and effective police departments do not detect all crimes before they are committed. But it is reasonable to ask what protection can be employed against the range of threats. Not so long ago, the world endured a seemingly unstoppable sequence of airplane hijackings. The international community sought common ground, improved airline security, and found it possible to deter and limit such terrorist incidents. A disciplined and sustained international effort by intelligence and law enforcement agencies worldwide is required to impede terrorist threats.
1997	CIA Studies in Intelligence	Russ Travers	The Coming Intelligence Failure	Any huge bureaucracy has problems in various aspects of its operation, but, in this case, the most serious is the diminished ability to get the facts straight and to use them as building blocks for high-quality analysis. We are far ahead of any other institution in the world in terms of the ability to collect sensitive information. Corporately, however, the IC is getting to the point where in many instances we do not even know what we do not know. Generally speaking, fewer analysts have less time to read more traffic and still fewer can keep up with their part of an increasingly complicated world; analysts have little opportunity for reflection, much less longer term research (2). Consequently, they stand little chance of putting whatever analysis they do into context — a recipe for irrelevance, if not outright failure. Within our overall analytic effort, a lack of fusion and a lack of objectivity will be principally responsible for the IC failing the nation.
November/ December 1999	The Bulletin of Atomic Scientists	Craig Eisendrath	Needed: More intelligent intelligence	Assuming that Pickering's summary of how the United States came to bomb the embassy of the world's most populous nation was accurate, it was a jarring wake-up call. The bombing was simply one more destructive failure in a long string of U.S. intelligence failures. And again, it offered proof that the U.S. intelligence system is badly in need of reform. If the bombing had been an isolated incident, it could possibly have been considered merely a "mistake." But it was not an isolated incident. It was the product of the systemic error that characterizes U.S. intelligence.

Date	Publication	Author	Title	Comment
1999	RAND	John Arquilla, David Ronfeldt, and Michele Zanini	Countering the New Terrorism	The netwar perspective suggests that for the foreseeable future, various forms networked forms will emerge, coexisting with and influencing traditional organizations. Such organizational diversity implies the need for a counterterrorism strategy that recognizes the differences among organizational designs and seeks to target the weaknesses... Networked organizations rely on information flows to function, and disruption of flows cripples their ability to coordinate actions.
2000	Best Truth: Intelligence in the Information Age	Bruce Berkowitz	Chapter One: Providing Intelligence in a Changing World	Because the Soviet threat was predominant and enduring, intelligence planning became predictable and incremental. Intelligence questions involved issues with two or three decades of history behind them...In other words, questions were evolutionary, not revolutionary...The fundamentals of each field rarely, if ever, changed radically. The sources and methodologies for analysis changed incrementally too...much of the technology that is at the heart of the Information Revolution is already being adopted by the Intelligence Community. What has not occurred is the change in thinking that needs to take place in order to take full advantage of this technology. This thinking needs to consider both the technology itself and changes in the ways people consumer and interact with information today.
February 15, 2001	U.S. Commission on National Security	Sen. Gary Hart and Sen. Warren Rudman	Roadmap for National Security: Imperative for Change, Phase III Report	...the U.S. Intelligence Community is adjusting only slowly to the changed circumstances of the post-Cold War era. While the economic and political components have statecraft have assumed great prominence, military imperatives still largely drive the collection and analysis of intelligence. Neither has America's overseas presence been properly adapted to the new economic, social, political, and security realities of the 21st Century...it [the Intelligence Community] failed to warn of Indian nuclear tests or to anticipate the rapidity of missile developments in Iran and North Korea...Steep declines in human intelligence resources over the last decade have been forcing dangerous tradeoffs between coverage of important countries, regions, and functional challenges. Warfighters in the field are often frustrated because the granulated detail of intelligence that they need rarely gets to them, even though they know that it exists somewhere in the intelligence system.
July/ August 2001	Washington Monthly	Loch Johnson	The CIA's Weakest Link	In the aftermath of the Cole bombing, former Secretary of the Navy John Lehman criticized "the obscene failure of intelligence" to anticipate the attack. He dismissed America's intelligence efforts as a "$30-billion jobs program that takes the most wondrous products of space and electronic technology and turns them into useless mush." This kind of criticism — along with the litany of disasters that preceded it — recently prompted President George W. Bush to order a comprehensive review of the nation's intelligence capabilities. The review, due to arrive on the president's desk by summer's end, is designed to gauge how well equipped America's secret agencies are to cope with the complex array of new and lingering challenges that confront the United States in the aftermath of the Cold War. To judge from their recent record, the answer may be: not too well.
September 27, 2001	Jane's Defence Weekly	No Author Cited	Where does US intelligence go from here — and were they really to blame?	At the risk of stating the all-too-obvious, the terrorist attacks in New York and Washington are proof of very serious shortcomings in the operational methods and intelligence-gathering capabilities of the various US agencies...As one very well-informed source close to US intelligence told JID, "The main problem is not a lack of information — that comes in all the time — but that we simply don't have sufficient skilled operatives capable of analysing the intelligence we receive in a timely manner and identifying those who pose a real risk to our interests."

Date	Publication	Author	Title	Comment
November 9, 2001	Pacific Council on International Policy	No Author Cited	An exclusive interview with Dr. Gregory F. Treverton, Senior Fellow at the Pacific Council	Creativity is hard to legislate. But it seems to me we haven't done enough hard and systematic thinking about very different adversaries. We need to do a lot more of what the military calls "red teaming," in which you try to get inside the head of an opponent, imagine what the world looks like to him, imagine his operational codes, and then determine what tactics he might take. It also requires teams that bring to the task different specialties and different nationalities. I think we tend to treat adversaries as cardboard characters.
December 2001	National Defense Magazine	John Stanton	U.S. Intelligence Community Reaches Crossroads	The most widely voiced criticism of U.S. intelligence agencies is its over-reliance on high-tech surveillance, at the expense of human spying, known as HUMINT. Some critics observed that key U.S. intelligence agencies are organized under Cold War-era bureaucracies that no longer are suited to manage an asymmetric war against a worldwide network of nimble enemies.
2001	PBS Frontline Interview	Congressman Porter Goss (R, FL) House Permanent Select Committee on Intelligence	Why Did U.S. Intelligence Fail on September 11th?	We don't have enough analysts. We are hopelessly underinvested in analysts. These are again, the language people, the people familiar with the culture, the people who have actually been on the street in Khartoum or wherever you want to go, who understand a little bit what this means. Sitting in a chair one way might mean something to one person; it might be unremarkable to somebody else. If you know the culture and see the way a person is gesturing with his hands or his feet or something, you get a message that you might not get if you don't understand the culture. So it is critical that we have those people. We're horrendously underinvested in them. ...
March 4, 2002	Carnegie Endowment for International Peace Proliferation Report	Joseph Cirincione	Intelligence Failure	A major reason why the United States was so unprepared for the terrorist attacks of September 11 is that national threat assessments produced over the past few years have consistently pointed policy-makers in the wrong direction. Partisan political agendas distorted these assessments, and fundamentally misled and misdirected national security resources.
May 28, 2002	National Review Magazine Online	Mark Riebling	The Real Intelligence Failure	Spokesmen for both the FBI and CIA now insist the agencies are "communicating as never before." But that's what they say after every interagency snafu. And while they say it, our efforts to neutralize al Qaeda remain dangerously driven by attempts to both police and to spy. Unless Congress mandates one or the other approach, the road to future tragedies — as to so many intelligence failures in our past — will be paved with good but divided intentions.
September 20, 2002	Congressional Joint Inquiry	Eleanor Hill, Staff Director	The Intelligence Community's Knowledge of the September 11 Hijackers Prior to September 11, 2001	Our review has confirmed that... there were missed opportunities by the Intelligence Community. In each area, there were indications of larger, systemic issues that, at least in part, drove those missed opportunities. And finally,...there were individuals within the Intelligence Community who recognized the importance of what was potentially at stake and tried, though ultimately without success, to get organizations within the Intelligence Community to do the same.
September 25, 2002	Op-Ed The Baltimore Sun	Melvin A. Goodman, Center for International Policy	Intelligence Failure Demands a Shake-up	It turns out that [CIA] agents and operators in the field did their job, but that the bureaucrats at headquarters in Washington did virtually nothing. We had human and communications intelligence that linked the hijacking and weaponizing of aircraft and we had solid reporting from the field on Osama bin Laden's modus operandi. But we lacked analytical assessments of the likelihood that terrorists would use airplanes as weapons.

Date	Publication	Author	Title	Comment
October 8, 2002	Congressional Joint Inquiry	Eleanor Hill, Staff Director	Hearing on the Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993 to September 2001	The main intelligence agencies often did not collaborate. In particular, the absence of an effective system for "hand offs" between the FBI, CIA, and NSA led to a gap in coverage with regard to international threats to the United States itself, and that should have received particular attention...the intelligence community made several impressive advances in fighting terrorism since the end of the Cold War, but may fundamental steps were not taken. Individual components of the Community scored impressive successes or strengthened their effort against terrorism, but important gaps remained...the Intelligence Community did not fully learn the lessons of past attacks.
October 17, 2002	Congressional Joint Inquiry	Eleanor Hill, Staff Director	Joint Inquiry Staff Statement	While the specifics of the September 11th attacks were not known in advance, relevant information was available in the summer of 2001. The collective significance of this information, was not, however recognized. Perhaps as a result, the information was not shared, in a timely and effective manner, both within the Intelligence Community and with other Federal Agencies.
December 10, 2002	Senate Select Committee on Intelligence	Senator Richard C. Shelby	September 11 and the Imperative of Reform in the Intelligence Community—Additional Views of Senator Richard C. Shelby	As the Joint Inquiry Staff has noted in its presentations to the Committees, "despite the DCI's declaration of war in 1998, there was no massive shift in budget or reassignment of personnel to counterterrorism until after September 11, 2001... The IC's methods of information-sharing before September 11 suffered from profound flaws, and in most respects still do. In order to overcome bureaucratic information-hoarding and empower analysts to do the work our national security requires them to do, we need to take decisive steps to reexamine the fundamental assumptions that have guided the IC's approach to managing national security information.
December 10, 2002	Congressional Joint Inquiry	Joint Inquiry Staff	Final Report	Although relevant information that is significant in retrospect regarding the attacks was available to the Intelligence Community prior to September 11, 2001, the Community too often failed to focus on that information and consider and appreciate its collective significance in terms of a probable terrorist attack. Neither did the Intelligence Community demonstrate sufficient initiative in coming to grips with the new transnational threats. 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 before a direct connection to the hijackers could have been established. For all those reasons, the Intelligence Community failed to fully capitalize on available, and potentially important, information.
January 26, 2003	Washington Post	Vernon Loeb	When Hoarding Secrets Threatens National Security	Intelligence reformers have argued for years that the CIA and other major intelligence agencies are obsessed with guarding "secrets" and thus miss real intelligence that's all around them... The "all-source" analysts at the CIA weren't really doing "all-source" work because their own brethren on the operations side, not to mention the FBI and the National Security Agency, were holding out on them. Some of the hoarding occurred because they didn't have the technology to make sharing possible. Some took place because they didn't even know what they had in their own cases files and on their intercept tapes. And some came because they thought certain secrets were too sensitive to share, either to protect sources and methods, or preserve their own unique standing in the intelligence pecking order.

Date	Publication	Author	Title	Comment
2003	Cambridge University Press	Gregory F. Treverton	Reshaping National Intelligence for an Age of Information	Cold War intelligence lived in a world where information was scarce; it relied on secrets not otherwise available. Its business was those secrets. Now, though, it faces an era of information. Information and its sources are mushrooming, and so are the technologies for moving information rapidly around the globe. Given these circumstances, the business of intelligence is not longer just to provide secrets; rather its business is to provide high-quality understanding of the world using all resources.
January 2003	US Naval Institute Proceedings	Lieutenant Commander Mike Steadman, U.S. Navy		A fundamental problem of intelligence is that we do not exploit fully the body of material we collect. It is recognized widely all the way to the national intelligence level that we, the intelligence community, swallow far more data than we can digest. Valuable nuggets of information lay unprocessed on the cutting-room floor
			Pacific Faces Crisis in Intel Analysis	For military personnel at JICPAC, two years in one analyst job would be considered lengthy. Without historical references to consult, analysis tends to be based primarily on experiences during the tenure of the resident "expert."
February 10, 2003	Washington Post	Vernon Loeb	Rumsfeld's Man on the Intelligence Front: Interview with Rich Haver	"Current operations had received pretty much full funding... So the money was taken out of the future. We mortgaged the future to pay for the present. The only thing you [Cheney] should be surprised about in the next four years is if you're not surprised," Haver recalled. Underfunding the Intelligence Community for most of the previous eight years — personnel had fallen 26 percent since 1991. The intelligence agencies lacked analytic depth, they were standing still technologically, and they were suffering from serious morale problems. "If there was such a thing as an average person inside the intelligence community, in the year 2000, their attitude was, what they do isn't as important as it used to be," Haver said.
February 19, 2003	Christian Science Monitor	Stansfield Turner	Reforming Intelligence	It confirmed a lack of adequate communication among the 14 intelligence agencies that make up our intelligence community. None of us who have been associated with US intelligence were at all surprised that these agencies would place their parochial interests above those of the nation. Such inexcusably faulty performance cannot be risked again. All that has been done since Sept. 11 is official exhortation to correct the situation. The new Homeland Security Bill does nothing to straighten this out.
February 27, 2003	Hearing. Senate Armed Services Committee	Dr. Stephen A. Cambone	Answers to Advance Questions	The most pressing challenge facing the DoD is arranging itself to operate in an environment where surprise is commonplace. Defense intelligence has an important role to play in helping to avert surprise and mitigating its effects when it occurs. Defense intelligence is critical to enabling the Department to adjust its policies, structure, posture, and capabilities and plans to operate in this environment. Those activities need to be attentive to the possibility of surprise and will need to improve its ability to warn of impending surprises.
March 4, 2003	*Los Angeles Times*	Greg Miller	Military Wants Its Own Spies:	Congressional aides said intelligence committee members in the Senate and House have yet to see details of the plans. But they noted that there is broad support among lawmakers for expansion of the nation's ability to collect human intelligence — an area identified as a major shortfall by investigators of the September 11 attacks.
			Moving onto the CIA's turf, the Pentagon is seeking a cadre of operatives for global reconnaissance and the fight against terrorism.	Intelligence experts said the new program is a logical step at a time when the September 11 attacks and the ongoing terrorist threat have exposed inadequacies in the nation's intelligence capabilities.

Date	Publication	Author	Title	Comment
April 5, 2003	*Los Angeles Times*	No Author Cited	Intelligence On Iraq Seen As 'Weak'	...officials said intelligence out of Baghdad since the attack had largely dried up, despite expectations that the enormous military pressure bearing down on Hussein's regime would prompt a wave of defections and a flood of information by this point in the war. Pentagon officials this week expressed concern that intelligence on the Iraqi leadership was "weak" despite the daring work of CIA informants. One senior Pentagon official struck a blind pose — eyes closed, arms extended — when asked about the quality of intelligence that war planners were getting. "Nobody can tell us where anybody is," the official said. "Nobody can tell us what buildings they're in so that we can bomb them. I'd call that weak." Intelligence officials dispute that characterization but acknowledge that they have had limited success in locating Hussein and other high-interest officials inside Baghdad. They also stress that it is an exceedingly difficult assignment.
May 27, 2003	Op-Ed in the Berkshire Eagle (MA)	No Author Cited	Congress finds its voice	The administration assured Americans that Saddam Hussein was stockpiling chemical and biological weapons and was prepared to use them against U.S. troops, and the failure to find them will make it impossible for the White House to make a similar case against Syria, North Korea or other rogue nations. Americans need to know if this prediction was the result of the latest intelligence failure on the part of the CIA.
2003	Yale University Press	Lt. Gen. William E. Odom, US Army Ret.	Fixing Intelligence for a More Secure America	The events of 11 September 2001 cast a dark shadow over the Intelligence Community. Why was there no intelligence available to the war of the Qaeda attacks on the World Trade Center and the Pentagon? No intelligence failure since 1941 has been as great...Once again the United States found itself at war and ill-prepared to fight.

APPENDIX 3

Bibliography

"10 Emerging Technologies That Will Change the World," *Financial Times*, February 2003.

A.M. Best Country Risk Methodology," A.M. Best, A.M. Best Inc., November 18, 2002.

Ackerman, Robert K. "Imagery Agency Lends a Hand on Reach-Back," *SIGNAL Magazine*, January, 2003.

"Agencies can Improve Training on New Initiatives," Report to the Chairman, subcommittee on Technology and Procurement Policy, Committee on Government Reform, House of Representatives, Acquisition Management, Government Accounting Office, January 2003.

Alpert, Gary, "The Future of Recruiting," WetFeet.com, October 2000.

Ante, Spencer E., "From Desert Storm to Desert Swarm," Business Week Online, April 2, 2003.

"Are You Ready?" Strategic Assessments Group, CIA, 2000.

Armstrong, J. Scott, "Forecasting in Conflicts: How to Predict What Your Opponent Will Do," Knowledge at Wharton Online, February 13, 2002.

Aron, Ravi, Mukesh Kadab, and Ganesh Ramakrishnan, "Two Major Errors That Companies Make in Outsourcing Services," Knowledge at Wharton Online, March 12, 2003.

Arquilla, John and Ronfeldt, David, *Swarming & The Future of Conflict*, RAND Publishing.

Barabasi, Albert-Laszlo, *Linked, The New Science of Networks, How Everything is Connected to Everything Else and What it Means for Science, Business and Everyday Life* (Perseus Publishing, Cambridge, MA, 2002).

Barnett, Thomas P.M., "The Pentagon's New Map, It Explains Why We're Going to War, and Why We'll Keep Going to War." Esquire, March 2003.

"Battelle Forecasts Strategic Technologies for 2020," PRNewswire, November 30, 2002.

Berkowitz, Bruce D. and Allan E. Goodman, *Strategic Intelligence for American National Security* (Princeton University Press, 1989).

Berkowitz, Bruce D., Allan E. Goodman, *Best Truth, Intelligence in the Information Age* (Yale University Press, 2000).

Berkowitz, Bruce D., *The New Face of War: How War Will Be Fought in the 21st Century* (Free Press, New York, 2003).

Blank, Stephen, "A New Look at Peace, Stability Operations and Humanitarian Intervention," Journal of International Security Affairs, No. 4, winter 2003.

Bloom, Howard, "I Want My TIA: Total Information Awareness will Consign Google to the Stone Age," Wired, Issue 11.04, April 2003.

Borin, Elliot, "Feds Open "Total" Tech Spy System" Wired, www.wired.com/news/conflict/0,2100,54342,00.html, August 7, 2002.

Borin, Elliot, "Planning for the Next Cyberwar," Wired News, http://www.wired.com/news/technology/0,1282,58422,00.html, April 18, 2003.

Bossidy, Larry and Ram Charan, *Execution, The Discipline of Getting Things Done* (Crown Business, New York, 2002).

Boyd, Stowe, "Are You Ready for Social Software?," Darwin Magazine Online, May 2003.

Boyd, Stowe, "Get Real," Darwin Magazine Online, April 16, 2003.

Broad, William, "The Impossible Task for America's Spies." *New York Times*, May 11, 2003.

Buchanan, Mark, *Nexus, Small Worlds and the Groundbreaking Science of Networks* (W. W. Norton & Co., New York, 2002).

Burger, Kim and Michael Sirak, "Streetwise in Baghdad — U.S. Tests Urban Warfare Tactics", Jane's Defence Weekly, Vol. 39, Issue No. 15, April 16, 2003, pp 2- 3.

"Bye-Bye CNN," Arab News Editorial, March 22, 2003.

Cambone, Stephen A., Answers to Advance Questions, Hearing Senate Armed Services Committee, 27 Feb 2003.

"Careful Knowledge Management Planning is Key in Pharma Research, Industry, Reed Business Information-US, March 17, 2003.

Cebrowski, Arthur, Transforming Defense, PowerPoint presentation, 2003.

Chaudron, David, "The Nine Pitfalls of Organizational Change," Link & Learn Newsletter, October 2002.

Coil, Nina "The Management Imperative: Influencing in Three Dimensions," Link & Learn Newsletter, December 15, 2002.

Condit, Phil, "Shaping the workforce of the future," *Boeing Frontiers*, October 2002.

Cordesman, Anthony H., "The "Instant Lessons" of the Iraq War," Center for Strategic and International Studies, Third Working Draft: April 14, 2003.

Danzig, Honorable Richard, Secretary of the Navy, "NAPA Webb Lecture," National Academy of Public Administration Webb Lecture Series, presented on November 17, 2000.

Davenport, Thomas H. and John C. Beck, The Attention Economy, Understanding the New Currency of Business (Harvard Business School Press, Boston, MA, 2001).

Davenport, Thomas O., *Human Capital, What It Is And Why People Invest It* (Jossey Bass, San Francisco, 1999).

Dawen, Choy, et al, "Creating the Capacity to Change Defence Entrepreneurship for the 21st Century," Future Systems Directorate, MINDEF, POINTER, Journal of the Singapore Armed Forces, 2003.

"Looking Ahead," DCI Annual Report, 2002.

DeMaio, Carl D. and Patti Powers, "Strategic Recruitment for Government" Report of the Performance Institute, Washington DC, 2003.

Den Beste, Steven, "On the Battlefield — The Digital Warrior, A tribute to the men who make the Information Age military work," *Wall Street Journal*, May 19, 2003.

"DIA's Focus," *Washington Times*, December 27, 2002.

"DISTANCE EDUCATION: Growth in Distance Education Programs and Implications for Federal Education Policy," GAO, September, 2002.

"DoD Announces Mishap Reduction Initiative," News release from the United States Department of Defense, May 23, 2003.

"DOD Study Examines Asia's Reaction To Info Age, U.S. Transformation," *Inside the Pentagon*, December 19, 2002.

Drexler, Allan, David Sibbet, and Russ Forrester, "Team Performance Inventory System," Drexler, Sibbet, Forrester, Inc., 1999.

Eakin, Emily, "Connect, They Say, Only Connect," *New York Times*, January 25, 2003.

"E-learning Helps Companies Capture the Knowledge of Retiring Employees and Gain Competitive Edge," CMP Media Inc., March 11, 2003.

Ellig, Bruce R., Maureen Minehan, *Future Focus: HR in the 21st Century*, Society for Human Resource Management.

Emmott, Bill, *20:21 Vision: Twentieth-Century Lessons for the Twenty-First Century* (Farrar, Straus and Giroux: New York, 2003).

"Energy Official Outlines Measures to Combat Future WMD Proliferation, (Brooks says arms control is largely the agenda of the past"), Distributed by the Office of International Information Programs, U.S. Department of State, http://usinfo.state.gov, April 25, 2003.

Fallows, James, "America's Warlords — Up Close with the U.S. Military Commanders Who Run the World, Washington Monthly Online, March 2003.

Farber, David, "Fame, But No Riches for Cybersecurity," IEEE Spectrum Magazine, January 2003, pp 51-52.

Finley, Michael, "Think Narrative!," The Masters Forum, 2001.

Foley, John and Hayes, Mary, "Customers Are the Next Group to Benefit From Real-Time Information," InformationWeek, March 3, 2003.

Friedman, George, Stratfor Weekly. Stratfor, Inc.

Friedman, Stewart, "The whole story," *Financial Times*, November 22, 2002.

Friedman, Thomas, "Super Empowered Individuals," Excerpt From Longitudes and Attitudes: Exploring the World After September 11, 2000.

Friel, Brian, "Federal Retirements Fall Short While Hiring Booms," govexec.com, February 2003.

Friel, Brian, "IRS is human resources reform model, scholars say," govexec.com, April 23, 2003.

Gale, Stephen and Lawrence Husick, "From MAD to MUD: Dealing with the New Terrorism," Foreign Policy Research Institute WIRE, Volume 11, Number 1, February, 2003, Foreign Policy Research Institute.

Gannon, John C. "Intelligence Challenges Through 2015: Remarks by John C. Gannon, Chairman, National Intelligence Council, to the Columbus Council on World Affairs," April 27, 2000, CIA.

Gannon, John C., "Intelligence Challenges Through 2015," Remarks to the Columbus Council on World Affairs, 27 April 2000.

Garwin, Richard L., "The Technology of Megaterror," Financial Times, www.technologyreview.com/articles/garwin0902.asp?p = 0, September 2000.

Gladwell, Malcolm, "Connecting The Dots — The paradoxes of intelligence reform," *New Yorker*, Pages 83 - 88, March 10, 2003.

Global Risk Assessments series, Global Risk Assessment, Inc. Riverside, California.

"Global Technology Scenarios Through 2015: America's Game To Lose, Views from a Panel of Experts," Directorate of Intelligence, CIA, November 2001.

"Global Trends 2015: A Dialog About the Future With Nongovernment Experts", prepared under the direction of the National Intelligence Council, December 2000.

Goldsmith, Marshall, "Building Partnerships Inside and Outside the Organization," *Partnering: The New Face Of Leadership*, Segil, Goldsmith, and Belasco, eds. (AMACOM, 2002).

Gratton, Lynda, *Living Strategy, Putting People at the Heart of Corporate Purpose* (Financial Times, Prentice Hall, London, 2000).

Gruber, Amelia, "Defense Pushes For More Flexibility To Manage Civilian Employees," March 14, 2003.

Hart, Gary and Warren B. Rudman, co-chairs, "America Still Unprepared — America Still in Danger: Report of an Independent Task Force Sponsored by the Council on Foreign Relations," Council on Foreign Relations, 2002.

Heuer, Richards J., Jr., Psychology of Intelligence Analysis, Center for the Study of Intelligence (Central Intelligence Agency, 1999).

Hill, Eleanor, "Proposals For Reform Within the Intelligence Community," Joint Inquiry Staff Statement, October 3, 2002.

"HUMAN CAPITAL: Effective Use of Flexibilities Can Assist Agencies in Managing Their Workforces," GAO, December, 2002.

Hutchings, Robert L., "The World After Iraq," Chairman, National Intelligence Council, Presentation to the Princeton University Washington Seminar, Center for Strategic and International Studies, Washington, DC, April 8, 2003, with preface remarks by Steven Daksal.

IABC-Towers Perrin Study Finds Communication Professionals Still Failing To Measure Effectiveness," Business Wire, March 14, 2003.

"Implementation Update on President's Management Agenda e-Newsletter," The Performance Institute.

"Intangible Assets: What Do You Know?" Financial Times Limited, March 5, 2003.

"Intelligence On Iraq Seen As "Weak," *Los Angeles Times*, April 5, 2003.

"Interview: Vance Coffman, Chairman, Chief Executive, Lockheed Martin Corp.," *Defense News*, January 20, 2003, p. 22.

Isaacson, Jeffrey A. and O'Connell, Kevin M., Beyond Sharing Intelligence, We Must Generate Knowledge, Rand.

Jacoby, Lowell E., "Intelligence Support to Military Operations: Implications of Joint Vision 2010", Statement for the Record, Senate Select Committee on Intelligence.

Joint Chiefs Of Staff, Joint Vision 2020, US Government Printing Office, Washington DC, June 2000.

Judy, Richard W., and Carol D'Amico, *Workforce 2020, Work and Workers in the 21st Century* (Hudson Institute, Indianapolis, IN), 1997.

Kaplan, Lawrence F. and William Kristol, *The War Over Iraq — Saddam's Tyranny and America's Mission*, (Encounter Books, San Francisco, 2003).

Kaufman, Gail, "U.S. Defense Intel Shift Widens Cambone's Net," *Defense News*, May 19, 2003.

Kelly, Kevin, *New Rules for the New Economy, 10 Radical Strategies for a Connected World*, (Viking, Penguin Group, 1998).

Kessler, Glenn, "State-Defense Policy Rivalry Intensifying — Gingrich to Urge Overhaul Of Powell's Department," *Washington Post*, April 22, 2003.

Kirsner, Scott. "In software industry, a passage to India," *Boston Globe*, January 20, 2003.

"Knowledge Management/Best Practice Sharing Optimizes Limited Resources," Business Wire, March 19, 2003.

"Knowledge Management Excellence: Winning Ways to Create Best Practice Identification Systems," Business Wire, March 28, 2003.

"Kosovo Strike Assessment Final," Allied Force Munitions Assessment Team, October 14, 1999.

Krebs, Brian, "Cyber War Game Tests Future Troops," washingtonpost.com,

Lamb, Brian, "Interview with Dana Priest", C-Span Booknotes aired March 9, 2003. Ms. Priest is author of *The Mission: Waging War and Keeping Peace with America's Military,* (W.W. Norton and Company, New York, 2003).

Lathrop, Charles and Mackenzie M. Eaglen, "The Commission on National Security/21st Century: A Hart-Rudman Commission Primer," National Security Watch, Institute of Land Warfare, AUSA. April 6, 2001.

Lee, Christopher, "Survey Finds Federal Workers Are Restless, At Least a Third Are Considering Leaving Jobs," *Washington Post*, March 26, 2003, Page A15.

Leedom, Dennis K., "Final Report: Sensemaking Symposium", Command and Control Research Program Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, October 23 - 25, 2001.

Leonhard, Robert R. "Factors of Conflict in the Early 21st Century," ARMY Magazine, US ARMY, January 2003.

Lichtblau, Eric and James Risen, "Broad Domestic Role Asked for C.I.A. and the Pentagon," *New York Times*, May 2, 2003.

Light, Paul C., "The End Of the Civil Service?" Washingtonpost.com, May 9, 2003.

Lind, Michael, "'20:21 Vision': 2 1/2 Cheers for Capitalism," *New York Times*, February 2, 2003.

Loeb, Vernon, "Tactics Show Iraqis Learned Lessons Of War," *Washington Post* (washingtonpost.com), March 27, 2003.

Loeb, Vernon. "When Hoarding Secrets Threaten National Security," washingtonpost.com, January 26, 2003.

Lohr, Steve, "Scenario Planning Explores the Many Routes Chaos Could Take for Business in These Very Uncertain Days," *New York Times*, April 7, 2003, page C3.

Long-Term Global Demographic Trends: "Reshaping the Geopolitical Landscape," July 2001.

Mann, Charles C. and Farmer, Dan, "Surveillance Nation," *MIT Technology Review*, April 2003.

Markle Foundation, "Protecting America's Freedom in the Information Age — A Report of the Markle Foundation Task Force," The Markle Foundation, New York, October 2002.

McKellar, Hugh, "KMWorld's 100 Companies that Matter in Knowledge Management 2003," KMWorld, 2003.

"Measuring Knowledge and People," Financial Times Limited, February 12, 2003.

Metzl, Jamie F, "Network Diplomacy," *Georgetown Journal of International Affairs*, Winter/Spring 2001.

"MILITARY PERSONNEL: Joint Officer Development Has Improved, but a Strategic Approach Is Needed," GAO, December, 2002.

"MILITARY PERSONNEL: Oversight Process Needed to Help Maintain Momentum of DOD's Strategic Human Capital Planning," GAO, December, 2002.

"Military Wants Its Own Spies," *Los Angeles Times*, March 4, 2003

Miller, James Arnold, "Regional and Country Watch List No. 24," Interaction Systems, Inc., April 30, 2003

Moore, David T., "Species of Competencies for Intelligence Analysis," Defense Intelligence Journal, Volume 11, No. 2, summer 2002.

Moschella, David,"Semantic Application, or Revenge of the Librarians," Darwin Magazine Excerpt from *Customer-Driven IT: How Users Are Shaping Information Technology Industry Growth*, (Harvard Business School Press, Boston, 2003).

Naím, Moisés, "The Five Wars of Globalization," *Foreign Policy*, January, February 2003.

"National Strategy for Combating Terrorism," The White House, Washington DC, February 2003.

Negroponte, Nicholas, "Creating a Culture of Ideas," *MIT Technology Review*, February 2003, pp 34 - 35.

Odom William E., *Fixing Intelligence — For a More Secure America* (Yale University Press, New Haven, 2003).

Oudenaren, John Van, "What is "Multilateral?," Stanford University Hoover Institution Policy Review, No. 117, February and March 2003.

"Preserving National Security in an Increasingly Borderless World, Analytical Views from a Conference of Experts," Office of Transnational Issues, CIA, January 2001.

Proctor, Paul, "Building the 21st Century Work Force," *Boeing Frontiers*, October 2002.

"Quadrennial Defense Review Report," The Department of Defense, September, 2001.

"Range of Federal Agencies Will Offer Early Retirement in 2003," *Washington Times*, December 31, 2002.

"Results-Oriented Cultures: Modern Performance Management Systems Are Needed To Effectively Support Pay For Performance," Statement of J. Christopher Mihn, United States General Accounting Office, April 1, 2003.

"RESULTS-ORIENTED CULTURES: Using Balanced Expectations to Manage Senior Executive Performance," GAO, September 2002.

Ricks, Thomas E., "War Plan for Iraq Largely in Place," *Washington Post*, March 1, 2003.

"Risk Oversight: Board Lessons from Turbulent Times," Director's Monthly, volume 27, no. 1, January, 2003, National Association of Corporate Directors.

"Rumsfeld Issues Transformation Guide," Federal Computer Week (fcw.com), April, 14 2003.

"Rumsfeld Submits Report Calling For Sweeping Changes In Military," European Stars and Stripes, April 15, 2003.

Rumsfeld, Donald, "Defense for the 21st Century," *Washington Post*, May 22, 2003.

Schrader, John Y., Leslie Lewis, and Roger Allen Brown, "Quadrennial Defense Review 2001 — Lessons in Managing Change in the Defense Department," Publication of Rand National Defense Research Institute, Washington DC, 2003.

Shanker, Thom, "Rumsfeld Requests Power To Reorganize Services," *New York Times*, April 14, 2003, with preface by Steven Daksal, April 22, 2003.

Shelby, Richard C. "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," December 10, 2002.

Sherman, Howard and Ron Schultz, *Open Boundaries, Creating Business Innovation Through Complexity*, Santa Fe Center for Emergent Strategies (Perseus Books, Reading, MA, 1998).

Slywotzky, Adrian J., *Value Migration, How to Think Several Moves Ahead of the Competition*, (Harvard Business School Press, 1996).

Smith, R. Jeffrey, "Secretive Agency's Maps to Pave Way for Iraqi Relief; High-Tech Details That Aided Military To Be Released," *Washington Post*, April 22, 2003.

States Take Step Toward Sharing Cyberthreat Data," Post Newsweek Tech Media, 2/20/03.

Stephenson, Karen and Stephan H. Haeckel, "Making a Virtual Organization Work," reprinted from Focus no. 21, Zurich Insurance Group.

Stephenson, Karen, "What Knowledge Tears Apart, Networks Make Whole," Reprinted from Internal Communication Focus no. 36.

Sterling, Bruce, *Tomorrow Now, Envisioning the Next Fifty Years* (Random House, New York, 2002).

Stewart, Derek B., "DOD Personnel: DOD Comments on GAO's Report on DOD's Civilian Human Capital Strategic Planning," U.S. General Accounting Office, April 18, 2003.

"Swarm Strategies," *Defense News*, February 3, 2003.

Talisayon, Serafin D., "Knowledge Management and People," Financial Times Limited, December 19, 2002.

Tash, Jeff, "Business Intelligence Roadmap," Flash Map Systems, 1993 - 2003.

Tassell, Tony. "Retirement age will rise to 70 by 2030," *Financial Times*, December 11, 2002.

Terrorism Open Source Intelligence Report (TOSIR). Weekly bulletin by Interaction Systems Inc. for the Director of Central Intelligence's Counterterrorist Center.

"The Ecology of Warning: How the Organizational Environment Affects Strategic Intelligence", Conference Workshop Report May 29 - 30, 2002, Publication of the CIA Sherman Kent School, Washington DC, 2002.

"The Global Economy in the Long Term," Directorate of Intelligence, Office of Transnational Issues, Strategic Assessments Group, February 2001.

"The National Security of the United States of America," The White House, Washington DC, September 2002.

"The National Strategy to Secure Cyberspace," The White House, February 2003.

The Pentagon, "New DOD Intel Directorate Will Have Broad Policy, Program Influence," *Inside The Pentagon*, March 27, 2003.

"The Physical Protection Of Critical Infrastructure and Key Assets," The White House, February 2003.

Thomas, Timothy L., "Al Qaeda and the Internet: The Danger of "Cyberplanning," Parameters, 2003.

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

Toffler, Alvin and Heidi, "The War of Pyramids vs. Pancakes and How It Will Shape the Future," Los Angeles Times Syndicate International, 2002.

Toffler, Alvin and Heidi, *Powershift*, (Bantam, New York, 1990).

Huge and pyramidal structures worked for World War II. They worked in the Cold War when the United States opposed an even more bureaucratic foe. But attempting to fight the deadly, fast-flitting, flea-sized terrorist enemy with pyramidal bureaucracies is a blueprint for failure.

"When bureaucracies are forced to deal with a problem that fits into no one's existing cubby-hole, they behave in certain stereotyped ways. After some initial fencing, someone inevitably suggests setting up a new unit... This is instantly recognized for what it could easily become: a budget-eating rival of the older units..."

Transformation Trends, Office of Force Transformation.

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

Turner, Stansfield, "Reforming Intelligence," *Christian Science Monitor*, February 19, 2003.

Ulrich, Dave, Michael R. Losey, Gerry Lake, eds., *Tomorrow's HR Management, 48 Thought Leaders Call for Change*, (John Wiley & Sons, Inc., New York, 1997).

Using Scenario Planning as Weapon Against Uncertainty," Wharton Business School, Knowledge at Wharton Online, December 5, 2001.

Waldrop, M. Mitchell, "Can Sensemaking Keep Us Safe?" *MIT Technology Review*, March, 2003.

Walker, David, Comptroller General of the U.S., "Testimony Before the Subcommittee on Civil Service and Agency Organization, Committee on Government Reform, House of Representatives,

DEFENSE TRANSFORMATION, Preliminary Observations on DOD's Proposed Civilian Personnel Reforms," April 29, 2003.

Walker, David, US General Accounting Office, Responses to requests from Chairman Voinovich, Chairwoman Davis, and Senator Carper on "The Human Capital Challenge: Offering Solutions and Delivering Results," May 22, 2003.

Waller, Douglas. "The CIA's Secret Army: Because of past scandals, the agency had largely dropped its paramilitary operations. But the war on terrorism has brought it back into the business," TIME Magazine, January 26, 2003.

Ward, Andrew, "Reign Of The "Chaos-Maker": Interview With Yun Jong-Yong, Samsung Electronics, *Financial Times* (London), March 13, 2003.

Watts, Duncan J., *Six Degrees: The Science of a Connected Age* (W.W. Norton & Company, New York, February 2003).

Watts, Duncan, "Untapped Networks," MIT Technology Review, March 7, 2003.

Why Some Companies Retrain Workers, and Others Lay Them Off," Wharton School of the University of Pennsylvania, January 29, 2003.

Wire, Albert, "Science and Technology Reinvention Laboratory Personnel Management Demonstration Program," NewsEdge Corporation, April 3, 2003.

"Workforce Planning in the Federal Government" Corporate Leadership Council, February 2003.

Zack, Michael H., "Managing Organizational Ignorance," Knowledge Directions, Vol. 1, Summer 1999, pp 36 - 49.

END NOTES

[1] This Agency was the forerunner of the President's Foreign Intelligence Advisory Board, or "PFIAB" May 6, 1960.

[2] In testimony to the Senate Select Committee on Intelligence, February 11, 2003, the Defense Intelligence Community was defined as being composed of DIA, the Service Intelligence Centers, and the Combatant Command Intelligence Centers. The larger "Intelligence Community" now includes the Defense Intelligence Community, plus the CIA, the FBI, the NRO, and the National Security Agency.

[3] John P. Kotter, *Leading Change* (Boston: Harvard Business School Press, 1996), p. 16.

[4] Two examples: digital consumer photography and business unit transformation. Digital photography and cameras — and the multi-million dollar shoulder products industries that digital photography spawned — required a revolution in the industry. One or two providers could not introduce the revolution. Likewise, we know from our experience in business unit transformation that introducing fundamental and good change in a business unit is extremely difficult unless adjacent business units and the corporate staff align with the change. Unless there is horizontal and vertical alignment across and within the community, changes in the Defense Intelligence Agency are unlikely to be durable, if they succeed at all.

[5] Not for attribution interview with Chief Scientist, Fortune 500 Company conducted by Toffler Associates on 27 March 2003.

[6] The State of California, for example, has a GDP that already ranks it among the top 10 economies of the world.

[7] Will and Ariel Durant, *The Lessons of History,* (New York: Simon and Schuster, 1968), p. 19.

[8] Not for attribution interview with Chief Scientist, Government Agency conducted by Toffler Associates on 21 February 2003.

[9] Bruce D. Henderson, "The Origin of Strategy," *Harvard Business Review,* November 1, 1989. Reprint Number 89605.

[10] Qiao Liang and Wang Xiangsui, "Unrestricted Warfare: Assumptions on War and Tactics in the Age of Globalization" (Beijing: PLA Literature and Arts Publishing House, 1999), p.149. FBIS translation.

[11] Ralph D. Sawyer, translator and commentator, with Mei-chun Sawyer, "T'ai Kung's Six Secret Teachings," *The Seven Military Classics of Ancient China* [Wu ching ch'i shu], (Boulder: Westview Press, 1993), pp. 68-69.

[12] The Honorable Stephen A. Cambone, "Transformation Of The Submarine Community," April 26, 2003.

[13] "Rich Man, Wise Man...," *The London Observer,* March 10, 2002.

[14] National Strategy For Combating Terrorism, February 2003, p. 9.

[15] M-Day equals beginning of mobilization. C-Day equals beginning of hostilities. D-Day equals beginning of deployment. When all are the same day, the war started with no warning and the U.S. military was forced to mobilize, deploy and fight simultaneously.

[16] Not for attribution interview with SES conducted by Toffler Associates on 19 March 2003.

[17] See Hughes, Thomas, "The Cult of the Quick," *Aerospace Power Journal*, winter 2001.

[18] See "Are You Ready?" Global Futures Partnership, Central Intelligence Agency, July 2001.

[19] David Ronfeldt, "Beware the Hubris-Nemesis Complex: A Concept for Leadership Analysis," (Santa Monica CA: RAND MR-461, 1994), p. 31.

[20] Jeanne Kirkpatrick called the Soviet Union "Upper Volta with rockets." The rockets commanded our attention for three generations.

[21] Not for attribution interview with Chairman, US Government Board conducted by Toffler Associates on 11 March 2003.

[22] Not for attribution interview with Vice President, Fortune 500 Corporation conducted by Toffler Associates on 21 March 2003.

[23] 259 million online users worldwide by year-end 1999. 490 million Internet users by year-end 2002. See: http://www.interconnection.org/background/statistics.htm.

[24] http://www.aps.org/apsnews/1299/129914.html.

[25] MSNBC, "Cray Unveils Fastest Supercomputer," 14 November 2002.

[26] Admiral William A. Owens, USN, "Vision Force 2005: The Pending Revolution," VCJCS Briefing, 3/95.

[27] Not for attribution interview with DISES, Defense Intelligence Agency, conducted by Toffler Associates on 7 March 2003.

[28] Not for attribution interview with DISES, Defense Intelligence Agency, conducted by Toffler Associates on 20March 2003.

[29] Not for attribution interview with Major General conducted by Toffler Associates/Dove Consulting on 20March 2003.

[30] Not for attribution interview with DISES, Defense Intelligence Agency, conducted by Toffler Associates on 17 March 2003.

[31] http://www.fda.gov/cber/cntrbio/cntrbio.htm.

[32] Not for attribution interview with Group Manager, Fortune 500 Corporation conducted by Toffler Associates on 28 February 2003.

[33] Not for attribution interview with DISES, Defense Intelligence Agency, conducted by Toffler Associates on 27 March 2003.

[34] "Navy's New Affordable Cruise Missiles Ready For Use, If Requested," Inside The Navy, March 24, 2003, Pg. 1.

[35] But we can't be sure because the absence of observation, the only way to leave the target untouched, would also leave it unobserved. Hence, uncertainty.

[36] Not for attribution interview with Fortune 500 CTO conducted by Toffler Associates on 11 March 2003.

[37] Not for attribution interview with Chief Scientist, US Government Agency conducted by Toffler Associates on 21 February 2003.

[38] Clayton M. Christensen, *The Innovator's Dilemma* (Harper Collins, 2000), page xxvii.

[39] Thomas H. Davenport and John C. Beck, *The Attention Economy: Understanding the New Currency of Business*, Harvard Business School Press, 2001, pages 2 - 3.

[40] Not for attribution interview with IC member conducted by Toffler Associates/Dove Consulting on March 13, 2003.

[41] Dr. Dennis K. Leedom, "Sensemaking Symposium Final Report October 23-25, 2001," Command and Control Research Program (CCRP), Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, 2001, Page 27.

[42] Google.com web site: http://www.google.com/help/about_news_search.html, as check on May 12, 2003.

[43] Bob Leonhard, *Fighting by Minutes: Time and the Art of War*, from an interview conducted by Toffler Associates/Dove Consulting on February 14, 2003.

[44] Not for attribution interview with noted academic conducted by Toffler Associates/Dove Consulting on February 27, 2003.

[45] Not for attribution interview with media thought leader by Toffler Associates/Dove Consulting on March 3, 2003.

[46] Not for attribution interview with Intelligence Community leader by Toffler Associates/Dove Consulting on March 20, 2003.

[47] Not for attribution interview with Intelligence Community leader by Toffler Associates/Dove Consulting on February 24, 2003.

[48] Kees van der Heijden, *Scenarios: The Art of Strategic Conversation* (John Wiley & Sons, 1996).

[49] Art Kleiner, Karen Stephenson's Quantum Theory of Trust, *Strategy and Business Magazine* available at: http://www.strategy-business.com/press/article/?ptag-ps = LCShk0&art = 9056282&pg = 6#authors as of May 12, 2003.

[50] Adapted from a presentation by Dr. Karen Stephenson before the Conference Board May 2002, Strategy and Business Magazine, available at: http://www.strategy-business.com/press/article/?ptag-ps = LCShk0&art = 9056282&pg = 6#authors as of May 12, 2003.

[51] Thomas A. Stewart et al, "The 2003 HBR List: Breakthrough Business Ideas for Tomorrow's Business Agenda, *Harvard Business Review*, April 2003, Page 96.

[52] Not for attribution interview conducted with SES in federal law enforcement Community , conducted by Toffler Associates/Dove Consulting on March 27, 2003.

[53] The National Security Strategy of the Unites States of America, September 2002.

[54] Adapted from Thomas A. Stewart et al, "The 2003 HBR List: Breakthrough Business Ideas for Tomorrow's Business Agenda, Harvard Business Review," April 2003, Page 92.

[55] Toffler, Alvin and Heidi, "The War of Pyramids vs. Pancakes and How It Will Shape the Future," Los Angeles Times Syndicate International, 2002.

[56] Toffler, Alvin and Heidi, *Powershift*, (Bantam, New York, 1990).

[57] Reference to an article by Tom Peters, entitled "The Brand Called You", *Fast Company Magazine*, August/September 1997, Page 83.

[58] Second and Third Wave Economies are a reference to Toffler Associates model of the history and future of economies as symbolized by the predominant industry attributes of the period.

[59] Thomas A. Stewart et al, "The 2003 HBR List: Breakthrough Business Ideas for Tomorrow's Business Agenda, *Harvard Business Review*, April 2003, Page 96.

[60] Toffler, Alvin and Heidi, "The War of Pyramids vs. Pancakes and How It Will Shape the Future," Los Angeles Times Syndicate International, 2002.

[61] Not for attribution interview conducted by Toffler Associates with a Defense Intelligence Agency advisory board member on March 21, 2003.

[62] Toffler, Alvin and Heidi, "The War of Pyramids vs. Pancakes and How It Will Shape the Future," Los Angeles Times Syndicate International, 2002.

[63] HBR, pg. 93.

[64] Toffler, Alvin and Heidi, "The War of Pyramids vs. Pancakes and How It Will Shape the Future," Los Angeles Times Syndicate International, 2002.

[65] Rumsfeld, Donald, Report to the President, 2002.

[66] Not for attribution interview conducted by Toffler Associates with a Defense Intelligence Agency executive on March 7, 2003.

[67] Less, of course, the French Republic, which will continue the irreversible decline it began in 1870

[68] See Workshop Report, "New Warning Lessons Needed," The Ecology of Warning: How the Organizational Environment Affects Strategic Intelligence, Global Futures Partnership, Central Intelligence Agency, May 29-30, 2002.

[69] Adapted from Garratt, Bob and Robert A. G. Monks, *Thin on Top: Why corporate governance matters and how to measure, manage, and improve board performance* (Brealey, Yarmouth, Maine, 2003).

[70] Garratt, Bob and Robert A. G. Monks, *Thin on Top: Why corporate governance matters and how to measure, manage, and improve board performance* (Brealey, Yarmouth, Maine, 2003).

[71] Barabasi, Albert-Laszlo, *Linked, The New Science of Networks* (Perseus, Cambridge, MA, 2002).

[72] "The New Intelligence 'Order': A View from 2010," Global Futures Partnership, Central Intelligence Agency, April 22. 2003.

[73] ASD, C3I, 2003, http://www.c3i.osd.mil/homepage.html, 2003.

[74] Los Angeles Times, "Military Wants Its Own Spies," March 4, 2003, Pg. 1.

[75] Address by Under Secretary of Defense (AT&L) E.C. Aldridge, Jr., "Turning Point for Missile Defense," August 21, 2002. Emphasis in the original.

[76] From a meeting with the Deputy Director, Signals Intelligence, NSA, July 2002.

[77] Not for attribution Intelligence Community thought leader interview conducted by Toffler Associates on March 25, 2003.

[78] Bob Leonhard, *Fighting by Minutes: Time and the Art of War*, from an interview conducted by Toffler Associates/Dove Consulting on February 14, 2003.

[79] Professor Daniel Hastings, MIT, from an interview conducted by Toffler Associates/Dove Consulting team on March 31, 2003.

[80] Not for attribution interview with Intelligence Community Thought Leader conducted by Toffler Associates and Dove Consulting on March 17, 2003.

[81] Not for attribution private sector defense and space industry executive interview, conducted by Toffler Associates on February 28, 2003.

[82] Interview with Dr. Ron Sanders, Office of Personnel Management, for Defense Intelligence Agency Workforce of the Future Project, March 25, 2003.

[83] Not for attribution interview with Intelligence Community Thought Leader conducted by Toffler Associates on March 3, 2003.

[84] Not for attribution interview with Intelligence Community Thought Leader conducted by Toffler Associates on March 3, 2003.

[85] Not for attribution interview with Intelligence Community Thought Leader conducted by Toffler Associates on March 19, 2003.

[86] Broad, William, "The Impossible Task for America's Spies," *New York Times*, May 11, 2003.

[87] The National Security Strategy of the United States of America, September, 2002.

[88] Not for attribution interview conducted by Toffler Associates with an authority on creativity, management and DoD, March 28, 2003.

[89]These include the Myers-Briggs Type Indicator. Characterized as the "most widely used personality inventory in the world." According to http://www.cpp-db.com/products/mbti/index.asp , "the MBTI(r) instrument provides an accurate picture of a person's personality type. The MBTI(r) instrument determines preferences on four dichotomies:

- Extraversion-Introversion (describes where people prefer to focus their attention and get their energy-from the outer world of people and activity or their inner world of ideas and experiences)
- Sensing-Intuition (describes how people prefer to take in information-focused on what is real and actual or on patterns and meanings in data)
- Thinking-Feeling (describes how people prefer to make decisions-based on logical analysis or guided by concern for their impact on others)
- Judging-Perceiving (describes how people prefer to deal with the outer world-in a planned orderly way, or in a flexible spontaneous way)

Combinations of these preferences result in 16 distinct personality types. Understanding characteristics unique to each personality type provides insight on how they influence an individual's way of communicating and interacting with others."

Screening tools also include tests for creativity. According to Dr. Curt Bonk, of Indiana University, there are more than 20 of these available http://www.indiana.edu/~bobweb/Handout/cretv_6.html :

1. Exercise in Divergent Thinking (CAP Packet)

2. Exercise in Divergent Feeling (CAP Packet)

3. The Williams Scale (CAP Packet)

4. Wallas & Kogan Tests

5. Monitor Tests of Creative Potential

6. How Do You Think (Davis)

7. Structure of the Intellect: (SOI; Guilford Tests: Contents, Operations, Products)

8. Group Inventory for Finding Creative Talent: (i.e., Davis: GIFFI I/11, GIFT, PRIDE)

9. Torrance Tests of Creative Thinking (TTCT)

10. Adjective Check List

11. Getzels and Jackson Tests

12. Creative Attitude Survey (Schaeffer)

13. Thinking Creatively in Action and Movement (Torrance)

14. Thinking Creativity with Sounds and Words (Torrance)

15. Barron-Welsh Art Scale

16. Remote Associates Tests (RAT)

17. The Creative Reasoning Test: (20 items to assess creativity using riddles)

18. Biographical Inventory-Creativity

19. Instruments assessing creative products

20. The Creativity Behavior Inventory

21. Khatena-Torrance Creative Perception Inventory: tests for personal acceptance of authority, self-confidence, inquisitiveness, awareness of others, and disciplined imagination.

Finally, there are tests for psychological health. The most widely used is the Minnesota Multiphasic Personality Inventory (MMPI) http://www.pearsonassessments.com/assessments/tests/mmpi_2.htm and its successor the MMPI-2(tm). According to Pearson Assessments, a clinical and career testing firm:

"The MMPI-2 test's contemporary normative sample and extensive research base help make it the gold standard in assessment for a wide variety of settings. The test can be used to help:

- Assess major symptoms of social and personal maladjustment.
- Identify suitable candidates for high-risk public safety positions.
- Support classification, treatment, and management decisions in criminal justice and correctional settings.
- Give a strong empirical foundation for a clinician's expert testimony.
- Assess medical patients and design effective treatment strategies, including chronic pain management.
- Evaluate participants in substance abuse programs and select appropriate treatment approaches.
- Support college and career counseling recommendations.
- Provide valuable insight for marriage and family counseling

[90] Not-for-Attribution Interview, July 1999.

[91] See note 11 above.

[92] According to General Electric, the company has long been known for developing some of the best leaders in business and some of the most widely practiced business techniques. Worldwide, GE invests about $1 billion annually on training and education programs — from assembly lines to corporate classrooms to boardrooms. Over 30,000 students, including non-Boeing attendees, have graduated from the Leadership Center since it opened in March 1999. The Center has, according to press reports, a $30 million annual operating budget. According to Boeing: "The Leadership Center has three residential lodges, with a total of 120 private rooms, a dining room that seats 200, a commons area, and a workshop building. The workshop has two large classrooms, four medium classrooms, a lecture hall, and 21 breakout rooms. An underground ballroom, built in 1946, has been incorporated into the Leadership Center and is used as a meeting and dining place."