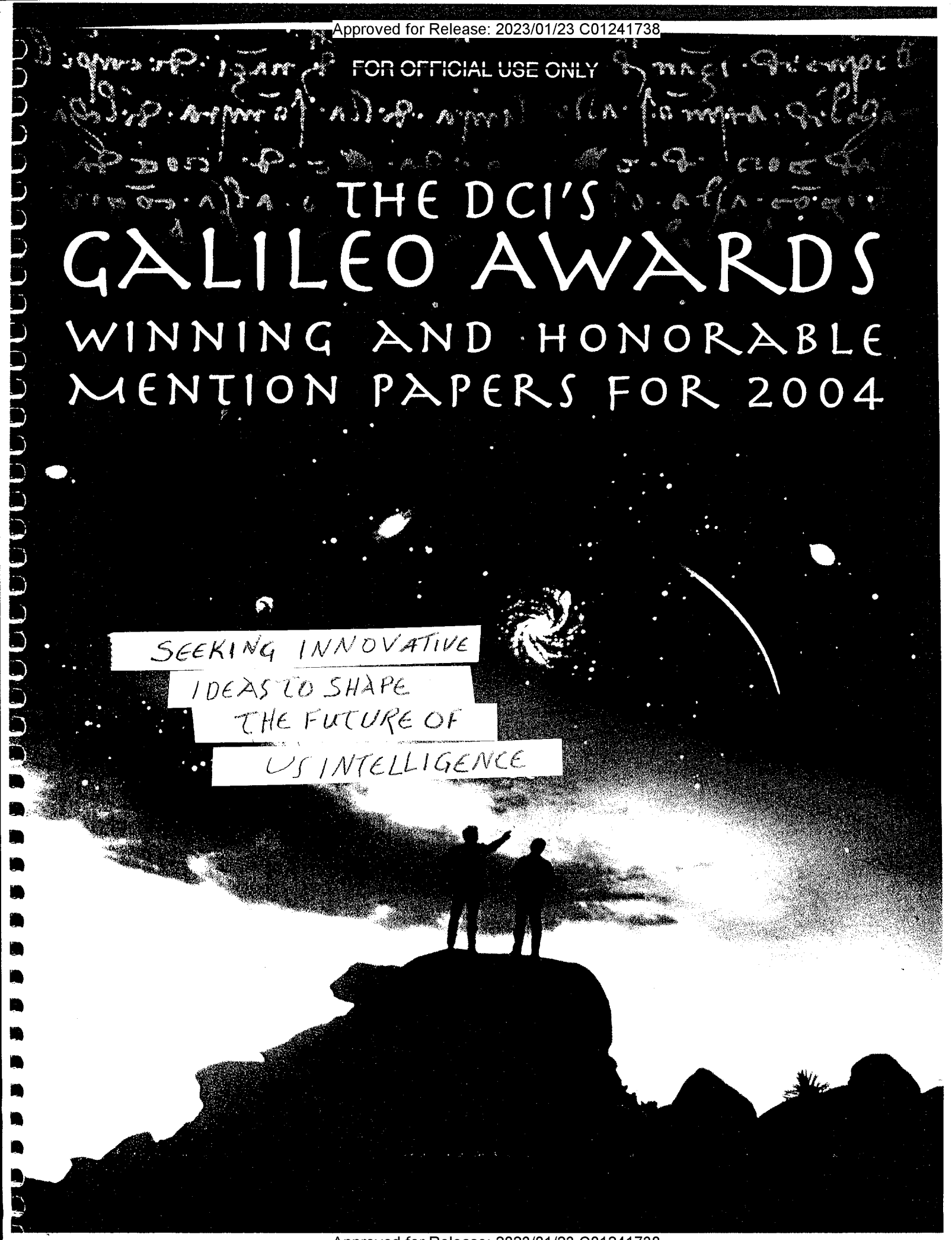
FOR OFFICIAL USE ONLY

THE DCI'S GALILEO AWARDS

WINNING AND HONORABLE MENTION PAPERS FOR 2004



From the Director of Central Intelligence

The Intelligence Community has always needed bold thinking. Today, we need it as much as ever to bring about transformative change. Thus, I am very pleased to present to the Intelligence Community the results of the first Galileo Awards competition for innovative ideas for the future of US intelligence.

The call for papers last summer prompted entries from all across the Community. The authors who submitted their works ranged from junior officers to senior executives, and their proposals covered the gamut of the intelligence business. The submissions offered suggestions relevant to every agency and every discipline.

The overall quality of the papers and their proposals was high, a factor that made it very challenging for the judging committee to award the final prizes. Indeed, the enthusiasm and creativity, which the Galileo Awards process generated, shows that the Intelligence Community employs no insignificant number of men and women who want to improve our institutions and methods to meet the challenges our nation faces.

Now, our task is to engage the best of the ideas presented in this collection – to discuss them, add to them, and find a way to integrate their creative value into the vital work of our Community.

Porter J. Goss
Director of Central Intelligence

From the Director Strategic Management Issues Office

(U) The creation of our office approximately one year ago reflected a recognition on the part of the senior leadership of the Intelligence Community (IC) that we need to seek bold, creative solutions to our nation's next national security challenges. Our charter is to promote a broad, thoughtful exchange of revolutionary change options for the future of US Intelligence: The Galileo Awards program has served as a powerful example of the outstanding potential of tapping into the wealth of talent and ideas that reside at all levels of seniority and responsibility in the IC.

(U) The DCI's Galileo Awards Program was conceived last spring as a call to IC officers challenging them to submit unclassified papers written on their own time with creative ideas for the future of our business. Instead of equating change with "reform" or "reorganization," we were looking for innovative ways to change how US Intelligence operates in all its dimensions. Our belief was (and remains) that the IC must establish a process for *dynamic reinvention* rather than implement one-time, overarching reorganization. We must transform the Community into an organization that continuously learns and adapts to accommodate change – and this kind of dynamic evolution cannot occur without the full participation and creative energy of all IC staff officers.

(U) By the September deadline, we received some 130 papers from officers all over the IC, and indeed all over the world. The papers were stripped of identifying information and were evaluated in two rounds of judging by experts from inside and outside of the IC using four criteria: subject matter, scale and scope, innovation and originality and literary quality. In November, I served as chair of a a five-member panel that selected three papers for awards, and identified ten papers for honorable mention. Also participating in the final panel were William Nolte (Deputy ADCI for Analysis and Production), Erv Rokke (Intelligence Science Board member and President of Moravian College), Joseph Keogh (CIA University) and Jeffery Cooper (SAIC).

(U) We are extremely pleased with the high quality of the papers included in the collection. They cover a wide range of topics and many points of view. They provide us a marvelous starting place for further discussions on many critical issues for our future. At the heart of the Galileo program has been the goal to promote a continuous dialogue throughout the IC about innovative ideas – not necessarily the championing of any specific solution or proposal. Our hope is that broad discussion of the ideas contained in these papers will inspire others in the IC to come forward with additional creative and well-considered ideas for how we can continue to build a successful future for US Intelligence.

Deborah G. Barger
Director, Strategic Management Issues Office

Contents*

The 2004 Galileo Award Winners

Honorable Mention

* The order in which the winning and honorable mention papers are listed was determined by a random process.

Honorable Mention
(continued)

The Wiki and the Blog

(b)(3)
(b)(6)

Problem Statement

US policymakers, warfighters and law-enforcers now operate in a real-time, worldwide decision and implementation environment. Information about a new development in Baghdad is known in Washington within minutes. Decisions about a response are made in Washington within minutes. These decisions are implemented in Baghdad within minutes of the decision. The total "intelligence – decision – implementation" cycle time can be as short as 15 minutes. While this is an extreme example, it highlights the tremendous compression of the response time required by all involved compared to previous generations. This severe compression not only affects the highest priority issues, it also ripples back into the most routine intelligence, decision and implementation processes.

It does so for good reason. The compressed response cycle gives the United States significant strategic and tactical superiority over our adversaries. Our national security is best protected when we operate more quickly than those who would do harm to our people and our freedom. This compressed response time allows us to disrupt, interdict, preempt and respond to injurious efforts before our adversaries can achieve their goals against us.

This compression is not just a preferred work style within the US National Security Community. It is a characteristic of the way the world works in the 21st Century. Thus, not only do we respond more quickly, but also the circumstances to which we respond—in and of themselves—develop more quickly. These rapidly changing circumstances take on lives of their own, which are difficult or impossible to anticipate or predict. The US National Security Community—and the Intelligence Community within it—is faced with the issue of how to operate in a security environment that, by its nature, is changing rapidly in ways we cannot predict. A simple answer is that the Intelligence Community, by its nature, must change rapidly in ways we cannot predict.

What was that? How can we change ourselves in ways we cannot predict? More directly, how do we modify our nature to enable such unpredictable changes? Before giving the right answer, there is a wrong answer that can be dismissed up front—reorganization. Any reorganization by its nature is both predictable and slow. By the time any particular reorganization has taken effect, the causes that spawned it will have been replaced by new and different causes. The reorganization is thus not suited to address these new and different causes. All major restructurings are based on the

assumption that we can take the recent past and predict the future. Such assumptions may have been reasonable in previous centuries, but not in this one.

The only way to meet the continuously unpredictable challenges ahead of us is to match them with continuously unpredictable changes of our own. ***We must transform the Intelligence Community into a Community that dynamically reinvents itself by continuously learning and adapting as the national security environment changes.*** Unless we, in the Intelligence Community, allow ourselves this ability to change, we cannot hope to fulfill our mission to ensure domestic tranquility, provide for the common defense and secure the blessings of liberty (U.S. Constitution, preamble) for our fellow citizens from those whose aim it is to deprive us of these values.

Theoretical Development

To describe a Community that "dynamically reinvents itself by continuously learning and adapting" in response to environmental changes harks to theoretical developments in the philosophy of science that matured in the 1990's, collectively known as Complexity Theory (Lewin, 1992). Complexity theory arises out of a rich and diverse intellectual heritage. Four significant theoretical building blocks undergird Complexity Theory. The scope of this paper only allows for a brief mention of these building blocks (though Complexity Theory itself will be treated in more detail over the next couple of pages). Briefly, the four building blocks are:

- General System Theory (von Bertalanffy, 1968). This theory was formulated in the 1930's and 1940's as a reaction to the then-popular theory of reductionism that asserted in order to understand a phenomenon, one only had to decompose it into its components. System Theory elevated the system itself as the subject of inquiry, independent of its parts.
- Information Theory (Shannon, 1948). This theory is built on the premise that no communication channel is error free—that is, random errors are always introduced into the message—in spite of error-correction routines. Shannon showed how to transmit correct messages in noisy channels. Moreover, he showed that the noise in the channel was information in and of itself and thus can be used to transmit messages. There is meaning in the noise.
- Chaos Theory (Lorenz, 1993). This theory dates from Lorenz's 1963 article in the *Journal of the Atmospheric Sciences*, where he showed that minor differences in the beginning of a weather pattern produced unpredictably large differences in how the weather pattern played out. He summarized this observation in the title of his 1972 address to the American Association for the Advancement of Science, "Predictability: Does the Flap of a Butterfly's Wings in Brazil Set off a Tornado in Texas?" The unpredictability of outcomes due to small changes in initial conditions has thus come to be known as "The Butterfly Effect."
- Fractal Theory (Mandelbrot, 1977). This theory took shape with Mandelbrot's 1968 paper entitled, "How Long is the Coastline of Britain?" He demonstrated that, as the

ruler got smaller, the length of the coastline increased. He also showed that, at ever-increasing smaller scales of observation, the coastline remained constantly jagged. He discovered this pattern in many natural phenomena, such as mountains. While a mountain rises from the surface of the earth into the third dimension, as we get farther out into space, it looks increasingly flat compared to the total earth's surface. From space, the mountain does not rise a full dimension from the surface of the earth, but just a fraction of a dimension. Something that exhibits this partial dimensionality is called a fractal. Fractals also exhibit consistent complexity regardless of the scale at which they are observed.

Four Examples

As an introduction to Complexity Theory itself, four examples of common phenomenon that express various concepts of Complexity Theory will be summarized below. Following the examples, an explanation of Complexity Theory will be given.

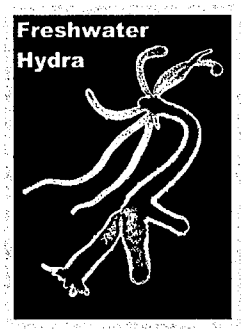
Example One: In one of the foundational treatises of modern Western thought, Adam Smith's (1776) *Wealth of Nations* describes how individuals, in pursuing their own economic self-interest, create a market for goods and services. This market has an "invisible hand" that decides which goods and services survive over time and which do not. It is "invisible" in the sense that no individual or group of individuals decides what the market should produce or consume. It just "happens" out of the aggregated actions of large numbers of individuals. The individuals are only trying to make their own lives better. Out of their collective and self-organized behavior, market behavior emerges. This market behavior is distinctly different from individual behavior. The market dynamically adapts prices in response to unpredictable supplies and demands. The market is able to do this because of continuous learning on the part of and information feedback to the individual purveyors and consumers of goods and services.

Markets are essentially bottom-up, self-regulated enterprises that become incredibly complex. Indeed, global markets emerge even when individuals behave locally. For example, German demand for bananas stimulates banana production in the South Pacific. Neither the German buyers nor the South Pacific suppliers need to travel to participate in the market (though some intermediary shippers do travel). The market price conveys information about the behavior of both the German consumers and the South Pacific providers. Moreover, billions of goods and services are supplied to people around the world, and no central authority is needed to manage a list of what goods and services are to be produced and delivered where at what price.

Two and a half centuries of experience with free markets teaches us, however, that markets are subject to manipulation, distortion and out-of-control spirals. We impose

rules on markets to ameliorate the worst of these effects. These take the forms of trade agreements, taxes and regulations with criminal and civil penalties. In sum, markets are complex adaptive systems with properties that emerge out of simple behaviors by a large number of self-organized individuals. The sum is greater than the parts.

Example Two: The mathematician Alan Turing is considered to be one of the fathers of the discipline of computer science for his work in formalizing algorithmic computation. He was also an intelligence officer during WWII, leading the effort to decrypt the German Enigma Machine. In the last paper written before his death (Turing, 1952), he addressed himself to the subject of the Freshwater Hydra and the leaves of plants. Turing worked out a mathematical model showing that relatively simple homogeneous sets of chemical agents following relatively simple rules generate quite complex biological structures, such as tentacles of the Hydra and the leaf patterns of plants. While guided by strict rules, these biological structures dynamically adapt to their changing and somewhat unpredictable environment of varying combinations of sun, water, nutrients and predators, etc. From the same chemical base, each hydra has a unique tentacle set. Similarly, from the same chemical base, each plant of a particular species has a unique placement of leaves—and each leaf has a slightly different structure. The important point is that, in the face of external changes, complex systems can change, albeit in unpredictable but adaptive ways.



Example three: Jane Jacobs (1961) shows that decisions by many individuals about where to locate their homes and businesses create neighborhoods with distinctive properties. These distinctive neighborhoods persist even though individuals are constantly moving in and moving out. Similar kinds of people are attracted to similar neighborhoods. Some neighborhoods do change over time in response to changes in the environment. Other neighborhoods (both exclusive and slum) resiliently maintain their character in spite of city planners' best efforts. For example, the silk merchants in Florence, Italy, have inhabited the same neighborhood for over 500 years. People, taking into account both the external environment and what the other people or businesses in their neighborhood are doing, decide to move or stay. This collective, self-organizing behavior determines how the neighborhood emerges and adapts.

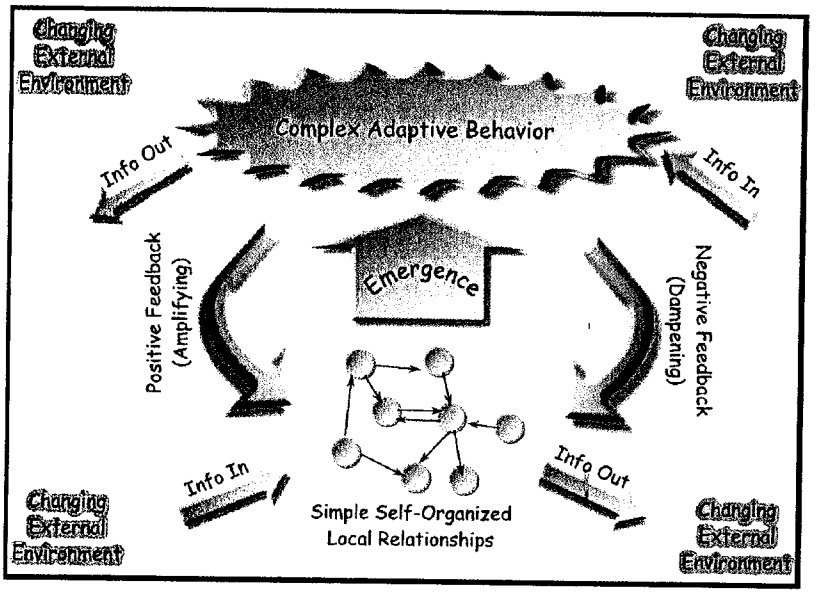
Example four: Deborah Gordon (1999) dispels the myth of the ant queen. For many years, entomologists thought the ant queen exerted a controlling, organizing influence over "her" colony. In fact, individual ants make individual decisions about what activities to perform (from a limited set of behaviors) based on what their nearest neighbors are doing. For example, if too many ants are cleaning a particular area of the colony, an individual ant will decide to go hunt food. Adherence to simple rules at an individual level allows ant colonies at the group level to respond to both strategic (seasonal) and tactical (predatory) changes in their environment. From a limited set of

individual self-organized behaviors, an ant colony emerges and survives for more than a decade.

Complexity Theory

The Santa Fe Institute (www.santafe.edu), founded in 1984, and The Center for Complex Systems Research, founded in 1986 at the University of Illinois (www.ccsr.uiuc.edu), have inspired a body of work (e.g., Johnson, 2001) that articulates a coherent framework of complex adaptive systems. The six critical components of a complex adaptive system are:

1. Self-organization – individuals (people, ants, chemicals) decide to act in similar ways in proximity to and in concert with each other, for their own reasons. For example, two boys independently shooting hoops decide to go one-on-one to 20 points. In addition, a critical mass of individuals is required for self-organization to happen.
2. Emergence – the whole is greater than the sum of the parts. For example, twelve Canadian Geese flying in a "V" is more than just 12 individual geese flying. The group behavior is distinct from the individual behavior.
3. Relationships – individuals look at their nearest neighbors to try and figure out what is happening so they can make decisions. For example, House Speaker 'Tip' O'Neil declared, "All politics is local." By this he meant that people vote for national leaders on the basis of what is happening in and around one's home. It doesn't matter what the national unemployment rate is, it only matters what the local unemployment rate is.
4. Feedback – information circulates in the system, is modified by others and then comes back to influence the behavior of the originator either as a positive (amplified) or negative (dampened) influence. For example, an ant crosses a pheromone trail it previously laid down. The ant says to itself, "I've already been here, so I'd better wander somewhere else." It is also important that the historical memory of the system be part of the feedback (amplifying or dampening) loop.
5. Adaptability – the system is open so that information (and/or energy) flows in and out of the system. This new information enters into the feedback loops and influences the behavior of the individuals, and thus the overall behavior of the system adapts to the external environment. For example, think of a group of kids engaged in unsupervised play in the basement as a self-organized system. When the dad opens the basement door and yells "everyone gets an ice cream cone when the toys are picked up" and closes the door, he adds new external information into the system. The kids adapt to the external influence by stopping play and putting the toys away. Systems that are 1) continuously open to new information from the environment, and 2) circulate the information within the system, will continuously change in response.
6. Non-Linearity – Small changes in the initial conditions or external environment have large (unpredictable) consequences in the outcomes of the system – also known as the "Butterfly Effect," cited earlier. For example, when the dad yells down the stairs for ice cream, the kids adapt by fighting over who made which mess. In the ruckus, they knock over a shelf that breaks one child's arm. The dad did not predict he would be going to the emergency room by offering ice cream to the children.



This graphic depicts these six characteristics. From simple, self-organized personal relationships emerges complex behavior. Information from the external environment enters the system and impinges on these relationships as either positive or negative feedback. The personal relationships are changed, and the complex behavior adapts.

Complex systems that under-adapt, such as snowflakes, present us with a model that is too staid for our use. Complex systems that over-adapt, such as the 1994 Rwandan massacres of more than one million people, are too chaotic for our use. The best complex adaptive systems are those that are poised on the edge of chaos. These vibrant systems thrive by continuously learning and adapting to the continuous changes in the environment. They have achieved a healthy circulation of positive (amplifying) and negative (dampening) feedback in the system.

Network Centric Warfare

There has been a recent attempt to apply the principles of complexity theory to government—specifically to the military services. The Department of Defense (DoD) is subject to the same response time compression as the Intelligence Community. The DoD understands that the command and control regimes that worked in the 20th Century do not serve as well in the 21st. In response, they are pursuing an effort called Network Centric Warfare (NCW) which is being championed by the Office of Force Transformation (OFT) and supported by the Command and Control Research Program (CCRP), both under the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I). While Network Centric Warfare has its detractors, it nevertheless does offer an example for the Intelligence Community.

Alberts, Garstka and Stein (1999, p2.) define NCW as:
. . . an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decisionmakers and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.

Wilson (2004, p.2.) identifies four main objectives of NCW:
1. Self-synchronization, or doing what needs to be done without traditional orders;
2. Improved understanding of higher command's intent;
3. Improved understanding of the operational situation at all levels of command; and
4. Increased ability to tap into the collective knowledge of all U.S. (and coalition) forces to reduce the "fog and friction" commonly referred to in descriptions of fighting.

The impact of NCW was seen in Operation Iraqi Freedom. Only about 250,000 US troops were deployed in Operation Iraqi Freedom compared to the nearly 500,000 US troops that were deployed a decade earlier in Operation Desert Storm. Individual units were smaller and moved faster. Because units knew the location of other nearby units without line of sight, they spread out in a "swarm" fashion. If one unit got into trouble, the other nearby units gave aid by converging on the enemy from all directions. Knowing the location of nearby units greatly reduced friendly fire accidents. Because the high-priority objectives were clear, there was no need to secure all of the rear. Units could hit the heart of the enemy command and thus disable enemy units on the periphery without having to engage them. When units encountered difficult obstacles, they could engage experts off the battlefield in real-time—sometimes as far away as Washington—to help solve problems. Moreover, units moved more quickly because damage and opportunity assessments were made and conveyed during the battle, rather than waiting for overnight analysis.

What were the key ingredients that helped make NCW a winning component in Operation Iraqi Freedom? The units were highly trained, professional warriors. Not only were they experts in the use of their advanced equipment and well practiced in the tactical art of battle, they knew the rules of engagement and the strategic and tactical objectives. Thus enabled, they were trusted to act on their own in the battlefield. From the thousands of deployed units—each pursuing their own tactical objectives—emerged an integrated land, air and sea force unparalleled in human history. No other military on earth can match the effectiveness of the US Military.

Application To Intelligence

The objective that was identified at the outset of this paper was that the Intelligence Community must be able to dynamically reinvent itself by continuously learning and adapting as the national security environment changes. Complexity Theory tells us that

we can only achieve this objective if several conditions exist. Enabling these conditions will be a big change for the Intelligence Community, but if we are serious about succeeding in improving ourselves, it is imperative that these changes be made.

1. Intelligence Officers must be enabled to act more on their own. Just as people in a market are empowered to make their own purchases, and individual ants in a colony can decide which task to perform, and military units are able to choose battlefield tactics in real-time, so too, intelligence officers must be allowed to react—in independent self-organized ways—to developments in the National Security environment.
2. Intelligence Offices must be more expert in Tradecraft. It is this expertise that engenders the trust required for independent action. Military units know the rules of engagement and are thus entrusted to engage in battle. Ants have a hardwired rule set, which enables the colony. Cities are built on the rules that govern property deeds, titles and liens. Expertise in tradecraft for each intelligence discipline must become a constant quest for each officer.
3. Intelligence Officers must share much more information. Just as military units in the field must know where other units are located in geographic space, intelligence analysts, for example, must know where their colleagues across the Community are located in intellectual space. This knowledge results from sharing information. From the previously cited examples, we understand that information sharing among individuals allows market niches to be filled, ants to fend off predator attacks and plants to distribute themselves in the ecosystem. Increased information sharing among Intelligence officers will allow these Intelligence officers to self-organize to respond in near real-time to National Security concerns.
4. Intelligence Offices must receive more feedback from the National Security environment. The only way to learn from and adapt to the changing National Security environment is to be in constant receipt of feedback from that environment. Just as zoo-raised animals cannot compete in the wild, intelligence officers cloistered in the Intelligence Community are not adapted to or fitted for the National Security environment.
5. Intelligence Managers must be more persuasive about strategic objectives. Quadrennial strategic directions are good, but these directions must become part of the everyday dialog at all levels in the Community. Many intelligence officers, with their noses to the grindstones, know little about the overall strategic intelligence objectives. One must know how one's own piece of work fits into the overall intelligence mosaic because the intelligence mosaic is constantly changing, and thus one's own piece must constantly change to remain well-fitted. Intelligence managers must be constantly communicating their constantly changing objectives. Intelligence officers will, in turn, adapt.

About 1843, the newest and largest western frontier city—larger than Chicago or St. Louis—was also the most orderly and well kept. A visiting dignitary asked the mayor of Nauvoo, Illinois how he managed so many people so well. He replied, "I teach them correct principles and they govern themselves" (Taylor, 1851). This sound bite encapsulates the spirit of what Complexity Theory suggests as a model for the

Intelligence Community. From intelligence officers who are allowed to share information and act upon it within a simple tradecraft regime will emerge an Intelligence Community that continuously and dynamically reinvents itself in response to the needs of the national security environment.

From intelligence officers who are allowed to share information and act upon it within a simple tradecraft regime will emerge an Intelligence Community that continuously and dynamically reinvents itself in response to the needs of the national security environment.

Self-Organizing Tools

At first blush—and in the context of how the Intelligence Community now operates—the five prescriptions seem almost ridiculous, especially the two most important ones about information sharing and independent, self-organized action. The good news is that in the last four years there have been technology advances that make implementing such prescriptions easier than one might initially think. There is a new generation of Internet tools that enable people to self-organize around shared knowledge.

The first of these self-organizing tools is known as "Wiki" (pronounced whicky) and is named after the Hawiian term *Wiki wiki*, which means fast. Wiki tools allow 1) any person to add content to a web site, and 2) any other person to edit the content. The most famous implementation of Wiki is the Wikipedia (www.wikipedia.com). This is an encyclopedia created and edited by Internet users. It has been in existence since 2001 and now has over 300,000 entries in over 100 different languages. By comparison, the 2004 edition of the 32-volume *Encyclopedia Britannica* contains just over 65,000 entries (see store.britannica.com). Other Wikis include dictionaries (www.wiktionary.com), books (www.wikibooks.com), quotations (www.wikiquotes.com) and document collections (www.wikisource.com).

The Wikipedia has an interesting and innovative 'tradecraft' or a rule set to which contributors and editors must abide. All content contributions are self-initiated. There is no editor-in-chief. Because all contributors are also editors, when a person notices an article that needs content revisions or does not abide by the rules, that person makes the edit. All previous versions of the article are available and all changes are attributable. Another wiki rule for the encyclopedia is that explicit or implicit points of view are out of bounds. These are edited out quickly.

There are privileged contributors with administrative powers beyond the normal contributor. They can adjudicate disputes among contributors. The existing administrators confer administrative powers to a person on the basis of the quantity and quality of that person's contributions. If a person disengages from performing administrative duties, the privileges are revoked.

The rules themselves are also subject to the Wiki process. Any person can introduce changes at any time. Disputes over the rules can be escalated to a board of administrators.

In sum, from the little bits of work by many, many people, following simple rules of content contribution and editing, the most comprehensive and authoritative, and bias-free encyclopedia in the world has been produced in three years. This is an encyclopedia that is dynamically and constantly changing in response to the world as the world itself is changing. The lists of medals received in the 2004 Athens Olympics were updated as the events concluded. No manager made the assignment. No editor-in-chief reviewed the accuracy. It happened, as if by magic. A person took the initiative to update the entries, and hundreds (or possibly thousands) of others reviewed the content for quality.

One of the Wikipedia's strengths is also a weakness—no points of view. Much of the self-corrective knowledge that exists in the Intelligence Community exists in personal points of view. Currently, there exists almost no official outlet for points of view in the Intelligence Community. A healthy market of debatable ideas emerges from the sharing of points of view. From the ideas that prosper in a market will arise the adaptive behaviors the Intelligence Community must adopt in order to respond to the changing national security environment. Not all good ideas originate at the top.

A second self-organizing information-sharing tool has matured in the last few years. It is called "blogging." The term comes from "web log" shortened to 'blog.' A blog is a journal or diary that is kept in the public space of the Internet. Individuals maintain their own blogs on an hourly, daily, weekly or periodic basis. They are their own editors. Current blogging technology makes it easy to manage one's blog (see www.blogger.com, for example). Most blogs take the form of citing a current event and offering a point of view about it. Often one blog will cite a comment in another blog and comment on it. The 'blogosphere' is truly a marketplace of ideas.

Enabling intelligence officers across the Community to express and share opinions may be one of the largest paradigm shifts for the IC. It will be uncomfortable for some because it will be in the blogosphere where the Community will ride along the edge of chaos. The blogosphere probably will obey the 99-to-1 Edison rule ("Genius is one percent inspiration and ninety-nine percent perspiration" – from wikiquotes.com). For every ninety-nine mediocre ideas, there will likely be only one brilliant idea. The few brilliant ideas, however, are worth the investment of many mediocre (and chaotic) ones. It is these few brilliant ideas that will provide the direction for the Community to adapt to the changing national security environment. The few brilliant ideas will survive in the market place of ideas. As individual blogs comment on each other's ideas, the brilliant ideas will spread as feedback throughout the Community. Individuals, recognizing the

brilliance, will respond. From this self-organized response will emerge the adaptive behavior required of the Community.

Three Wrapper Technologies

The Wiki and the Blog are complimentary companion technologies that together form the core workspace that will allow intelligence officers to share, innovate, adapt, respond and be—on occasion—brilliant. Blogs will cite Wiki entries. The occasional brilliant blog comment will shape the Wiki. The Blog will be vibrant and make many sea changes in real-time. The Wiki, as it matures, will serve as corporate knowledge and will not be as fickle as the Blog. The Wiki will be authoritative in nature, while the Blog will be highly agile. The Blog is personal and opinionated. The Wiki is agreed-upon and corporate.

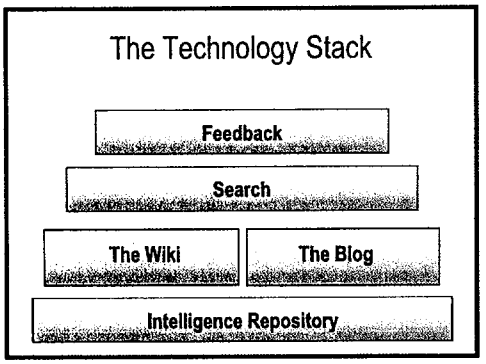
The Wiki and Blog, however, while standing together, cannot stand by themselves. Intelligence officers need a wellspring of intelligence from which to build the Wiki and about which to comment in the Blog. Such a wellspring would be a Community-wide intelligence repository patterned after DIA's SAFE or CIA's CIRAS. These repositories are largely disordered, out-of-context piles of cables. That is okay. The intelligence repository is like unrefined ore. (The repository could actually be many federated databases.) The Blog and the Wiki serve as successive refining processes for the unrefined ore in the intelligence repository. The Blog would vet, comment and establish context for the intelligence. This extracted intelligence knowledge from the intelligence repository would be placed in the well-organized Wiki. Both the Wiki and the Blog would link back to authoritative source documents in the repository.

While an intelligence repository is required "under" the Wiki and the Blog, two more technologies are required "above" them. One is a search technology and the other is a feedback technology. Part of the agility required in today's high-speed national security environment is to be able to quickly find information. One needs the ability to search for specific knowledge within or across the Wiki, or the Blog, or the Intelligence Repository in a Google-like (www.google.com) fashion.

While most intelligence officers are quite familiar with search technology, we are less acquainted with feedback technologies. These technologies are often in and of themselves self-organizing. For example, we might want to know which cables in the repository were most cited by the Blog over the last 24 hours. This feedback lets the visitor quickly know what the Community thinks is important. It also lets the originator of the cable understand its impact. Feedback technologies let visitors know what areas of the Wiki are changing most rapidly as an indicator of newly vetted knowledge. Feedback technologies can utilize subscription techniques such as "send me an alert when more than 10 people have read my blog." Wikipedia.com makes extensive use of these feedback technologies on its homepage. Another feedback Internet site (www.daypop.com) has dozens of real-time lists--from the top words to the top blog

postings to and the top sources cited. Its Top 40 list not only gives the current ranking but whether the ranking is going up or down.

Feedback technologies are an integral part of the solution suggested by Complexity Theory. As important as information sharing is to the success of the solution, it is even more important to know who is sharing what information. This allows intelligence officers to accurately understand where they are in the intellectual space of the Intelligence Community. It also allows intelligence officers to see what gaps exist and where changes need to be made. The feedback technologies allow an agile reading of the current state of play across the wide expanse of the Repository, the Wiki and the Blog.



Together, these five technologies (Repository, Wiki, Blog, Search, Feedback) would allow the Community to start down the path of implementing the five mission recommendations (self-organization, tradecraft, information sharing, feedback and strategic communication) suggested by Complexity Theory.

A Sharing Space

We need a space for change that is not organization dependent (remember, reorganizations are not part of the solution set). We need a space to begin implementing the five mission changes that is independent of organization. We need a space that is open not just to the Intelligence Community but also to other non-intelligence national security elements—to allow sharing and feedback. We need a space with a sufficiently large critical mass of intelligence officers. We need a space that is neither organizationally nor geographically nor temporally bound. We need a secure space that can host a corporate knowledge repository. We need a flexible space that supports tools for self-organizing (Wiki), information sharing (Blog), searching and feedback as previously mentioned. We need a place in which tradecraft procedures can be implemented. In short, we need a space that is always on, ubiquitously distributed and secure. We need an electronic network. We need SIPRNet.

SIPRNet (Secret Internet Protocol Router Network) is managed by the Defense Information Systems Agency (www.disa.mil). It is widely accessible by intelligence officers and other national security officers alike. It has been deployed to every Embassy and every Military Command. It is a more attractive experimental sharing space than the Top Secret Community Network (JWICS) because a critical mass accesses it, Policy Community officers access it, the tradecraft (security) rules are simpler and it reaches all organizations and geographic locations. Moreover, SIPRNet is designed to host the

Internet-based tools outlined above. Once the Wiki and the Blog processes and content mature on SIPRNet—that is, once the IC embraces the mission changes and becomes proficient in the use of the technology—the Wiki and Blog could be replicated on the Top Secret network.

Concept Of Operations

Lipnak and Stamps (1997), in their seminal work on virtual communities, identify four necessary conditions for success: a critical mass, trust, content and purpose.

- Critical Mass: Because the mission changes need to pervade the entire Community, the technology needs to be available to every officer in the Community. Because the Community must operate symbiotically with the Policy Community, Policy Community officers must also have access to the technology. For the feedback mechanisms to work, there must be sufficient numbers of participants from the various intelligence disciplines across the Community. To ensure the widest participation, the barriers to entry must be extremely low. This means the resources for deploying and operating these systems must be borne at the Community level and provided as a common service for all. All SIPRNet users must be allowed to search the intelligence repository, edit the Wiki, author a Blog, create links among these three and get feedback. This means not only must the software be easy to use, but also self-registration and self-authorization services must be trivial.
- Trust: As mentioned before, trust arises from tradecraft. Technical tradecraft has already secured the network. Technical tradecraft will also secure the tools and data. Procedural tradecraft in terms of the rules of use must be explicit and easily accessible. Security tradecraft has already cleared the users of SIPRNet. Applicable analytic and operational tradecraft principles must be identified and promulgated. For Complexity Theory to work, the procedural, analytic and operational tradecraft rules must be simple.
- Content: All intelligence organizations will need to identify content they can place into a Community intelligence repository on SIPRNet. The repository will likely be a number of federated databases. For hyperlinks to work, the objects in the repository must persist, and the address to the objects must be permanent. There will need to be some priming of the Wiki and the Blog so the content is sufficiently broad and deep to have value. In the beginning, some resources must be devoted on a full-time basis to bring the tools into full operational capability.
- Purpose: This is where Community leadership, as well as feedback from the rest of the National Security environment, plays a key role. There are strategic, intermediate and tactical purposes that must be communicated. A few Community seniors may want to author a blog. These would be sure to get high readership. Posting strategic directions into the repository would also work.

Conclusions

This paper identified a pressing Intelligence Community issue, namely that the Intelligence Community must transform itself into a Community that dynamically

reinvents itself by continuously learning and adapting as the national security environment changes. The paper elucidated the principles from an exceptionally rich and exceedingly deep theory (Complexity Theory) about how the world works and has shown how these principles apply to the Intelligence Community. These principles include self-organization, information sharing, feedback, tradecraft and leadership. The paper argues that from intelligence officers who are allowed to share information and act upon it within a simple tradecraft regime will emerge an Intelligence Community that continuously and dynamically reinvents itself in response to the needs of the national security environment.

Lipnack and Stamps (1997) make a case that a successful virtual community is 90 percent culture and 10 percent technology. The most profound culture change will be for Intelligence managers to let go of their officers the same way the battlefield commanders have let go of their battlefield troops. Managers must trust their officers to directly share with each other and directly with the Policy Community. Intelligence managers' role will become less command and control and more teacher of tradecraft and communicator of purpose and objectives. The Intelligence Community will need to put into place powerful incentives and rewards for managers to change. Indeed, Intelligence Officers must feel encouraged by their managers to spend their workday engaged in sharing activities. These changes will allow the dynamic learning community to emerge.

Recognizing that these changes in attitude and work processes will be challenging to implement, the paper recommended some first steps. It was suggested that recent self-organizing and information sharing tools from the Internet, **the Wiki and the Blog**, be deployed on the SIPRNet. Wrapping these tools in an intelligence repository, a search tool and feedback reporting would complete the technology package. This paper also suggested a few process principles (critical mass, trust, content and purpose) for success to be deployed along with the technology.

The Intelligence Community is under extreme political pressure in the wake of the 9/11 Report (National Commission, 2004) and the Senate's report on pre-war intelligence (U.S. Senate, 2004). If ever there was a time for the Community to re-examine its *modus operandi*, it is now. Our political leaders are now demanding these changes from us (Bush, 2004). The changes in mindset suggested in this paper are significant. Enabling intelligence officers to independently express their point of view in a Community-wide setting is groundbreaking. Equally avant-garde is letting intelligence officers create a body of intelligence knowledge without an editor in chief. Moreover, inviting our Policy Community counterparts at State, Homeland Security, etc. to be full participants in these information-sharing activities is breathtaking. If anything, however, these changes are timid compared to the changes required to bring the Community into the 21st Century. We must act, or we will certainly be acted upon. May we have the will to overcome our inertia and succeed in our efforts.

References

Alberts, David S., John J. Garstka and Frederick P. Stein (1999). Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition (Revised). Washington, D.C.: C4ISR Cooperative Research Program.

Bush, George W. (2004). Executive Order Strengthening the Sharing of Terrorism Information to Protect Americans. Washington, DC: The White House, 27 August 2004.

Gordon, Deborah (1999). Ants at Work: How an Insect Society is Organized. New York: The Free Press.

Jacobs, Jane (1961). The Death and Life of Great American Cities, Vintage Books Edition, 1992. New York: Vintage.

Johnson, Steven (2001). Emergence: The Connected Lives of Ants, Brains, Cities and Software. . New York: Touchstone.

Lewin, Roger (1992). Complexity: Life at the Edge of Chaos. New York: Macmillan.

Lipnack, Jessica and Jeffrey Stamps (1997). Virtual Teams: Reaching Across Space, Time and Organizations with Technology. New York: John Wily and Sons, Inc.

Lorenz, Edward N. (1963). "Deterministic Nonperiodic Flow." Journal of the Atmospheric Sciences, Vol. 20, No. 2, pp. 130–148.

Lorenz, Edward N. (1972). "Predictability: Does the Flap of a Butterfly's Wings in Brazil Set off a Tornado in Texas?" A talk given to the 139th meeting of the American Association for the Advancement of Science, as found in Lorenz (1993) pp. 181-184.

Lorenz, Edward N. (1993). The Essence of Chaos. Seattle: The University of Washington Press.

Mandelbrot, B.B. (1967). "How Long is the Coast Line of Britain? Statistical Self-Similarity and Fractional Dimension." Science, pp. 636-638. As cited in Mandelbrot (1977).

Mandelbrot, Benoit B. (1977). The Fractal Geometry of Nature, updated and augmented in 1983. New York: W.H. Freeman and Company.

National Commission on Terrorist Attacks Upon the United States (2004). The 9/11 Commission Report. Washington, D.C.: Government Printing Office. PDF version available from www.9-11commission.gov.

Shannon, C.E. (1948). "A Mathematical Theory of Communication." Reprinted with corrections from The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October.

Smith, Adam (1776). An Inquiry into the Nature and Causes of the Wealth of Nations, four volumes. Edinburgh. Original full text is available from the Adam Smith Institute at www.adamsmith.org/ and from the Gutenberg Project at www.gutenberg.net.

Taylor, John (1851). Millennial Star, Vol. 13, p. 339. As cited in the entry on Agency in Dahl, Larry E. and Donald Q. Cannon, eds. (1997). The Teachings of Joseph Smith, Salt Lake City: Bookcraft, as enhanced by Infobases, Inc.

Turing, Alan (1952). "The Chemical Basis of Morphogenesis." Philosophical Transactions of the Royal Society of London, Series B: Biological Sciences. Vol. 237, No. 641, pp. 37-72.

U.S. Senate (2004). Report on the U.S. Intelligence Community's Pre-war Intelligence Assessments on Iraq. Washington, D.C.: Senate Select Committee on Intelligence.

von Bertalanffy, Ludwig (1968). General System Theory. New York: George Braziller.

Wilson, Clay (2004). "Network Centric Warfare: Background and Oversight Issues for Congress, June 2, 2004." CRS Report for Congress. Washington, D.C.: Congressional Research Service.

Redefining the First Customer: Transforming Intelligence Analysis through Peer-Reviewed Publications

(b)(3)
(b)(6)

I. Introduction

Recently, two Congressional investigatory panels have criticized the U.S. Intelligence Community (IC) for a lack of quality and rigor in its analysis. It is possible that some fundamental cultural and procedural practices may negatively impact the IC's ability to analyze and produce foreign intelligence across the political, economic and military spectrum, including highly technical disciplines such as those associated with weapons of mass destruction (WMD). This proposal highlights the absence of a formal, internal, Community venue for presentation and discussion of alternate analyses as a vulnerability to the rigor of IC assessments. The proposal identifies an opportunity for the IC to address this gap through creation of an internal peer-reviewed periodical targeted to circulate alternate intelligence assessments throughout the Community

In the past two months, Congressional investigations into the terrorist attacks of 11 September 2001 and prewar intelligence on Iraq have noted a number of deficiencies within the IC that collectively contributed to two significant intelligence failures. Foremost among these deficiencies were the IC's propensity for group think, failure to communicate across organizational barriers and tendency to streamline intelligence assessments by removing necessary caveats and alternative perspectives from drafts as the texts progress through the coordination process.

According to the Senate Select Committee on Intelligence's (SSCI) Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq, "a series of failures, particularly in analytic tradecraft, led to the mischaracterization of intelligence."[1] Specifically, "the IC suffered from a collective presumption…this 'group think' dynamic led IC analysts…to both interpret ambiguous evidence as conclusively indicative of a WMD program"[2] and to discount information to the contrary. According to the committee, the presumption was so strong that "other types of alternative or competitive analysis were not utilized"; concurrently, analysts "did not give serious consideration to

[1] Senate Select Committee on Intelligence of the 108th U.S. Congress. Report on the U.S. Intelligence Community's Prewar Intelligence Assessments (July 2004): 14. Available at: http://www.realcities.com/multimedia/nationalchannel/news/070904_senate_report.pdf. Last accessed on 16 August 2004.
[2] SSCI Report, 18.

other possible explanations."[3] Clearly, the Senate report recognizes the absence of a management-endorsed mechanism for analysts to "question and challenge their assumptions [and] fully consider alternative arguments"[4] as a limiting factor in the quality of U.S. intelligence analysis.

In its July 2004 report, Congress' National Commission on Terrorist Attacks upon the United States (9/11 Commission) echoes many of the general findings of the SSCI investigation. The Commission further identifies a lack of transparency and communication among analysts across agencies as a key barrier to providing the agile joint intelligence required to combat threats such as terrorism and proliferation of WMD[5]. According to the 9/11 Commission, "the importance of integrated, all-source analysis cannot be overstated...without it, it is not possible to 'connect the dots'...no one component can hold all the relevant information."[6] The 9/11 report proposes significant modifications to the IC structure to facilitate the transparency needed for joint intelligence analysis. Although the SSCI report suggests no such restructuring, it does strongly imply that the IC needs to do a better job of enabling its analysts to interact in a forum that allows them to "fully consider opinions from other intelligence analysts"[7] and creates "a level playing field in which outside analysts fully participate."[8] To this end, a variety of academic communities that measure success based upon the discovery and communication of knowledge, such as those associated with the physical and social sciences, may provide some insight germane to current issues facing the IC.

On the surface, there appear to be strong parallels between intelligence analysis and scientific investigation. According to Dr. Donald Kennedy, Editor-in-Chief of the journal *Science*,

> intelligence as it is best practiced by experienced agents and agencies surely looks like a science...[a] problem is defined so that the right measures for dealing with it can be selected; relevant information is gathered and then analyzed, so that meaningful relationships can be uncovered and understood; and tentative conclusions are reached and then tested against possible alternatives. Finally, perhaps most important, critical review is sought.[9]

Kennedy cites discrepancies between the "unclassified" Iraq WMD National Intelligence Estimate released in October 2002 and the declassified version released in July 2003 as

---

[3] SSCI Report, 21.
[4] SSCI Report, 23.
[5] National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. (July 2004): 408.
[6] 9/11 report, 408.
[7] SSCI Report, 28.
[8] SSCI Report, 28.
[9] Don Kennedy. "Intelligence Science: Reverse Peer Review?" *Science*, vol, 303, (March 26, 2004): 1945.

evidence that the IC employed a "reverse peer review" of the classified document as it moved from the analysts and IC seniors to the policymakers. The result of this reverse peer review was that alternate hypotheses failed to be identified and caveats appeared to have been removed from the document. In the normal scientific peer review process, alternate hypotheses and assessments of data are often added to the final document as the result of a critical review from peers and senior experts in a field. Kennedy's editorial suggests that the IC would benefit from a tighter peer review process that incorporates alternate analysis and is modeled more closely upon that of the Scientific Community.

The fact that three independent reviewers (SSCI investigation, 9/11 Commission and Dr. Kennedy) of IC practices, policies and products came to strikingly similar conclusions regarding the failure of the IC to promote information sharing, critical review and consideration of alternate analysis in its assessments strongly suggests significant opportunity for improvement in these areas. Specifically, the IC needs (1) a balanced, objective, standardized, Community-wide peer review process that occurs on a level playing field, and (2) a "safe" forum within which IC analysts can develop, vet and communicate alternate assessments.

This proposal outlines how the establishment of an independent internal journal for alternative analysis could address existing shortfalls and enhance the Community's overall ability to ensure rigor, depth and quality of analysis by fostering critical discussion of analytic issues and promoting increased communication across the community of analysts. Moreover, incorporation of such a journal into standard IC practice and culture would reproduce the peer review process that currently benefits the Scientific Community and could serve to enhance the critical thinking, communication and collaboration skills of junior and midlevel analysts. The establishment of a journal for alternate analysis would help the IC senior leadership take a major step towards addressing the criticism of IC analytic methodology raised by the SSCI and 9/11 reports.

II. Understanding The Cultural Impediments To Alternate Analysis

There are at least three fundamental practices at work in the IC that tend to promote group think and restrict the formulation of alternate analysis. Yet, each of these practices deliberately has been established and maintained to produce a product that provides the busy policymaker with a clear and concise assessment of current threats and their implications for US security. These practices are: (1) the drive to seek consensus from within an organization and occasionally across the IC; (2) the focus on writing primarily for a non-technical audience; and (3) the constraint of crafting high-impact assessments for busy policymakers. Efforts to curb any of these tendencies are likely to meet with significant resistance because they are at the core of the IC's perception of the policymaker as the first and only customer for intelligence assessments.

1. *Seeking consensus in analytic products.* In an attempt to provide policymakers with a clear and consistent message regarding threats to national interests, intelligence organizations routinely seek to achieve analytic consensus and consistency during the internal coordination of intelligence products. This means that analysts focus on presenting a principal position, often at the expense of fully considering plausible alternatives. Although mention of dissenting opinions is occasionally included in finished intelligence products, these occurrences are deliberately kept to a minimum. While this effort to achieve analytic consensus arguably serves US policymakers by providing them with a concise and unambiguous assessment on which to act, it also can inhibit the full formulation, communication and evaluation of alternative assessments on complex issues. During the coordination process, assessments or statements, which are at odds with earlier products or the more pervasive views of an analyst's colleagues, tend to be minimized, reworded or cut altogether in order to present the Policy Community with a unified position.

2. *Writing primarily for a non-technical audience.* Another consequence of the IC's single-minded focus on writing for the policymaker is that the audience for these assessments generally lacks the time, expertise or inclination to critically review or challenge the underlying assumptions. As a result, many intelligence products fail to provide the reader with fully articulated and sourced arguments. Even though the underlying arguments and sources may have been thoroughly explored during the coordination process, they often do not make it into the final product, which tends to be concise and compact for the busy reader. Once in print, these assessments are less likely to be challenged or countered with alternate opinions because they are generally pitched at the Policy Community rather than one's analytic peers. Concise and devoid of footnoted sources, most IC assessments are intended to inform rather than provoke healthy discussion and debate among a community of experts. Because these printed documents do not retain references to primary sources, analysts are at pains to reconstruct and reevaluate the details of arguments presented by their predecessors or colleagues from elsewhere in the IC.

3. *Producing high-impact assessments.* Since most intelligence products are directed at high-level policymakers, emerging issues, which do not require the immediate attention of our leaders, get little, if any, formal attention and risk remaining unexamined until they are highlighted by current events. Because analysts are not given adequate venues to openly explore back-burner issues, the IC is often in the position of responding to unforeseen events.

III. Redefining The First Customer

Analysts take pride in crafting concise and clearly written intelligence assessments for busy policymakers. Within the IC, the President and other high-level intelligence consumers are occasionally referred to as the "First Customer" to emphasize their

primacy in the IC's mission. However, it is apparent from the procedures and practices mentioned above that the unique disposition of the IC's traditional first customers place certain constraints on the scope and content of intelligence products that ultimately degrade the quality of the analytic assessments. Even though the IC exists solely to inform the Policy Community, it is not evident that policymakers should be the first and only customers for most of the Community's analytic products. If one adopts Dr. Kennedy's view of intelligence analysis as a science—much like the other social sciences—and examines the publication model that has led to success in each of these disciplines, it becomes clear that the first customer for scientific scholarship is the Scientific Community itself and not the general public, even though the public ultimately benefits from scientific knowledge and expertise.

Intelligence analysis is clearly a compilation of many different sciences. These disciplines are as diverse as the academic backgrounds from which analysts are drawn and include political science, military science, economics, chemistry, biology and nuclear physics, just to name a few. However, when viewed as a whole, the challenges of intelligence analysis most closely resemble those of the historians who practice a form of social science. The primary goal of intelligence analysts and historians alike is to develop a refined understanding of remote events based on fragmentary and often biased information. Analysts and historians often have very little control over the limited data on which they depend. In many cases, the information is reported by individuals who may have indirect access to or imperfect recollection of the event in question. The sources themselves may be motivated to retell the story in a fashion that is beneficial to their interests.

Regardless of the particular field, scientific knowledge and theories invariably are expressed in two distinct genres, which are directed at separate audiences and serve very different functions. While distinct, both genres play important roles in the scientific tradition. These venues exist in the field of history as well as in the other social and physical sciences.

Peer-reviewed publications form the core of all legitimate scientific endeavors and are written by scientists to present their research and findings to other experts in their field. A strong tradition of peer-reviewed publications exists in each of the respected sciences, making the full and systematic exploration of alternate hypothesis possible. Peer-reviewed scientific publications are distinct from other forms of literature in a number of important ways. The primary audience for peer-reviewed papers is the body of one's technically competent colleagues. As such, these papers provide all the details necessary for knowledgeable readers to retrace the author's research and draw their own conclusions. Furthermore, peer-reviewed papers are valued for their unique contribution to scientific debate on a controversial issue. These papers generally are not intended to represent a consensus view, only the well-argued position of a small group of collaborators.

Popularized science is more journalistic in style and directed outside the Scientific Community to the general public. Popularized science papers are generally written to inform rather than debate. This form of writing has several important features, which set it apart from peer-reviewed work. Popularized science generally seeks to recognize trends in scientific research and consolidate a body of knowledge for non-experts—focusing primarily on the most relevant and predominant findings at work within the Scientific Community. Perhaps more importantly, this journalistic style casts scientific discoveries in a context the general public can understand and value. In this respect, those developments that have a direct bearing on the lifestyles and interests of the general public are more likely to find expression in this venue while more subtle findings tend to be ignored.

Although peer-reviewed and popularized publications each play important roles in scientific endeavors, legitimate sciences would not exist at all without the free exchange of ideas promoted by peer-reviewed papers. It is true that most sciences ultimately exist to serve the public good and must therefore interface with the public on multiple levels, including through the writing of popularized science articles. However, within the scientific tradition, the first customer for scientific writing remains the scientist.

In their commitment to presenting policymakers with concise, timely and high-impact intelligence products, analysts appear to have lost track of their preeminent obligation to develop a thorough understanding of complex issues through an open and formal written debate. Analysts have sacrificed the important peer-to-peer dialog for a relatively one-sided monolog with the busy, non-technical policymaker.

- The bulk of the IC's analytic publications are directed not at colleagues but at the policymakers who lie outside the community of intelligence experts.
- Publications to the policymakers resemble a popularized version of intelligence analysis in which positions must by pitched to a non-technical audience.
- Most intelligence assessments are not published be critiqued by the Policy Community or other members of the Intelligence Community.

The IC must not abandon the current array of policymaker products, which serve the critical mission of informing US decisionmakers in a concise and unambiguous manner. These products have been carefully developed over the years to meet the needs of the busy, non-technical Policy Community, which relies on the IC's consistent and well-reasoned assessments of critical events. However, efforts must be taken to promote the formal development and debate of alternate analytic assessments through the creation of a parallel peer review process similar to that which is at the core of all other scientific disciplines. Peer-reviewed papers are an essential component of every well-developed

science and would compliment and support existing policymaker products by overcoming limitations associated with the existing "popularized" intelligence product:

- Peer-reviewed intelligence products will permit the critical exploration of multiple assessments in a venue that does not require offices and organizations to present a consensus position on a particular issue.
- While peer-reviewed articles will be expected to inform debate on an issue, they need not bear the burden of presenting high-impact intelligence to a policymaker. In this way, emerging issues can be explored and understood long before they demand the attention of the Policy Community.
- Publication in IC-wide, peer-reviewed journals will ensure that alternate hypotheses and the supporting evidence become a part of the Community record. These publications will be easier to reference and retrieve than more informal mechanisms such as e-mails, memos and verbal exchanges, which are typically employed in the coordination process, are limited in their distribution and have a precarious existence.

The following sections describe the design and implementation of an IC-wide peer review Journal of Alternative Intelligence Analysis (JAIA), which is intended to promote the critical development of alternative assessments and thereby fuel the formation of well-considered popularized products for the non-technical policymaker. The JAIA achieves this by reducing the cultural barriers to publishing alternative assessments and making experienced and highly critical intelligence analysts across the IC the first customers for analytic products.

IV. The Journal Of Alternative Intelligence Analysis

Clearly, the need exists for an IC-wide publication to facilitate open and fair debate through a peer review process similar to that which has long been at the core of academic and scientific communities. Analysts must be encouraged to take ownership of alternative assessments and be given the opportunity to lay out an argument and present evidence in a forum free of bias. All too often, dominant opinions take precedence at coordination meetings and interagency working groups while alternative assessments are not given their due. The proposed JAIA will enable analysts with alternative interpretations of available intelligence to present their positions in well-articulated papers to their peers that are not encumbered by the constraints imposed by publications directed at the Policy Community.

The JAIA will be modeled after existing academic journals in fields such as public policy, history and archaeology. Contributors to the JAIA will be permitted to present independent interpretations of intelligence data, provided they use sound analytical reasoning and well-crafted arguments to arrive at their assessments.

The JAIA could be organized by geographic region as well as by topical issues. This format would sort articles in such a way that all stakeholders in the regions and topics of interest can consider the contributor's argument. For example, alternative assessments on proliferation issues in China that had been debated primarily by WMD analysts may now receive broader readership by regional economic, leadership and military analysts who can add substance to the debate as well as become more informed of contentious areas of analysis within their region of study. Additionally, the JAIA could sort the same article by the topic of proliferation, allowing WMD analysts who focus on other regions to weigh in on the debate and possibly apply novel analytical perspectives to their own accounts.

The main utility of the JAIA is in fostering healthy consideration for alternative analysis. This, necessarily, will involve more debate, and readers will be encouraged to respond to contentious articles either by submitting a letter to the editor or publishing an article of their own. Formal written discourse in this manner has an advantage over e-mails and verbal debates because it serves to document and publicize alternate perspectives, allowing analysts who otherwise might have been excluded from the coordination process to consider novel perspectives.

Authors' names should appear on JAIA articles in order to give analysts credit for their work and reinforce the point that their opinions, and not necessarily those of their colleagues, are being expressed. If necessary, pen names could be used to protect the true identities of analysts from inadvertent public exposure. Organizational affiliations should be noted as well to highlight the participation of analysts from different offices in collaborative assessments.

JAIA articles would be distinct from intelligence products intended for the Policy Community. Because the papers will be geared toward knowledgeable colleagues rather than busy policymakers, authors should be encouraged to strive for depth rather than brevity. Analysts would have less stringent space requirements in order to fully argue their points. Also, analysts will be encouraged to write more technically oriented papers that apply knowledge from one or more of the physical and social sciences to key intelligence issues. Typically, finished intelligence directed at members of the Policy Community avoids drawn-out explanations of technical data that could otherwise be used to support an analyst's argument. Since an author's goal in writing for the JAIA is to convince his fellow analysts of his position on a contentious issue, that analyst should be able to incorporate all appropriate technical arguments.

Properly formatted contractor studies should also be incorporated into JAIA articles to multiply the impact of government-funded research on IC-wide analysis and reduce replication of effort by different agencies. Often contractor contributions are overlooked because the results of their work are not circulated beyond the office that commissioned the study. While contractors are prohibited from writing finished intelligence for

policymakers, there is no reason contract-generated analysis could not be distributed via JAIA to IC analysts who may benefit from their research. Contractor studies, particularly in more scientific fields, may also lend credence to an analyst's argument, but may be overlooked by others because of unfamiliarity with the study. Similar benefits could be obtained by accepting qualified articles from experts in academia who are also prohibited from having a more direct role in crafting assessments for the Policy Community.

Some may be concerned that policymakers will mistake JAIA articles as coordinated intelligence products. Therefore, a clear disclaimer should appear on each article to prevent readers from mistaking the article for an agency- or IC-coordinated product.

Review of all JAIA articles will be carried out by a panel of peers selected from among the readership. A senior editor, who would be responsible for assigning reviewers, doing a final read-through of all articles and ensuring publication of accepted articles, should oversee the panel for each paper. Reviewers could be selected from all ranks throughout the Community, and attempts will be made to pull analysts with varying backgrounds from a range of participating intelligence agencies. Volunteers could be asked to review articles on a rotating schedule (perhaps only twice annually). This way, the review process will not require full-time service to the JAIA. Although substantive experts would be selected to review papers dealing with relevant accounts, non-subject experts who are also evaluating the paper could counter personal or career biases. If the argument is poorly articulated or the analytical reasoning flawed, the panel can opt to reject the paper or recommend changes that will make it acceptable for publication. All rejected papers should be returned with an explanation to the authors who can then appeal the panel's decision to the senior editor.

To aid in the peer review process and adequately inform journal readers, all articles must be fully sourced prior to submission, and sourcing will be retained in the published version. This would allow editors, reviewers and readers a chance to read the raw intelligence reports, if they are available, and check the validity of the author's argument.

V. Options For Establishing A Journal Of Alternate Intelligence Analysis

In addition to dedication of financial and material resources and personnel, creation of a journal for alternate analysis would require a fundamental shift in the IC analytic culture. Acceptance and use of the journal by IC analysts and managers as a forum for presenting, discussing and vetting hypotheses would likely be facilitated if its creation and employment are tailored to minimize the required culture shift. To this end, this proposal will outline a variety of options for leveraging existing resources, utilizing external entities and designing a responsive system for reviewing, publishing and disseminating assessments throughout the Community. The proposed peer review journal would be implemented within the existing intelligence culture and complement traditional policymaker publications.

To be most effective and useful to the IC, the journal will need to be highly responsive and permit rapid review and production of analyses; thus it will need to employ dynamic production methodologies that have significant flexibility. In this regard, a wholly digital production environment could meet the needs of the analytic community; such a format would naturally lend itself to rapid—perhaps even automated—nomination, review, publication and dissemination of analyses across the spectrum of community players. In this notional construct, the journal would serve as a daily product for IC analysts to read. Individual assessments could be crafted in a standard format, reviewed for general content and format by several individuals drawn from a pool of qualified analysts in a related discipline (biological warfare analysts for example) and published online in a classified environment as soon as the article has been approved for release. Secure Communities of Interest could be established to facilitate analyses containing information that requires additional dissemination controls. Ultimately, the journal would serve as a virtual "sounding board" for IC analysts where alternate assessments can be articulated, vetted and developed by the Community on a level playing field prior to being incorporated into more traditional products for the Policy Community.

Ideally, the implementation and daily execution of journal activities could largely be achieved by leveraging existing resources within the IC. For example, the Center for the Study of Intelligence (CSI) has a longstanding history of providing resources that promote study and debate of IC activities and assessments. CSI also has unique capabilities to support a journal of alternate assessments as it currently produces the peer-reviewed IC journal *Studies in Intelligence*. Thus, CSI likely already possesses much of the infrastructure and expertise needed to create a new IC-specific journal. Moreover, housing the journal at CSI would prevent it from being formally associated with any specific intelligence agency, promoting Community use of the periodical as a forum for engaging in discussion of pertinent issues. In addition, since much of CSI's publications are targeted towards the IC, its management of JAIA could serve as a buffer between the Intelligence and Policy Communities—a critical factor in protecting policymakers from assessments in the nascent stages of development.

In addition to the resources and benefits available via CSI, the IC could augment the Center's staff with support from a contract publishing agency. This may be a feasible fix for the potential problem of leveraging government resources that may be overburdened or insufficiently staffed to independently take on the mission of another IC periodical. In addition, experienced contract editors could help the IC define rules for submission, outline and implement an appropriate peer review mechanism and detail processes for editing and publication that will be acceptable to the Community and maintain appropriate security. Incorporation of contract support would likely not impact CSI's ability to preserve the membrane between this periodical and the Policy Community; if anything, the use of contractor staff in the journal's production would further dissuade policymakers from trying to access its publications, particularly since contractor staff

would not be affiliated with any specific intelligence agency. However, IC managers would need to be aware that contract support presents challenges regarding the clearance levels of the publisher staff; management would also need to help develop the infrastructure for coordination of review, editing, formatting and production via the contractor.

Ultimately, successful implementation of a journal of alternate analysis would depend in part upon IC management's ability to create an environment that both supports and promotes analyst use of the system. Restructuring of production and coordination processes to encourage preliminary publication and testing of hypotheses via the peer-reviewed alternate assessments vehicle could drive the analytic culture towards increased collaboration, critical review and broader discussion of substantive issues. In addition, realignment of analyst performance metrics to include their use of the alternate assessments vehicle could directly impact analyst attitudes and commitment regarding the process. Such actions, although requiring a concerted and longstanding effort on the part of IC management, could successfully impact analytic culture throughout the IC to address the criticisms that were raised in the SSCI and 9/11 reports.

VI. Conclusion

Congressional panels commissioned to investigate intelligence failures associated with the September 11 attacks and the Second Gulf War have recommended that the IC place a greater emphasis on alternative analysis. Building upon Dr. Kennedy's notion of intelligence analysis as a science, we believe that one way to systematically address Congress' recommendation is to promote a peer review process similar to that found at the heart of most academic and scientific enterprises. Such a peer-to-peer publication would provide a formal venue for analysts to articulate well-argued alternative points of view to be reviewed by their intelligence colleagues throughout the IC. We encourage IC management to endorse the creation of a journal of alternative analysis that will be broadly distributed to IC analysts in electronic format.

The peer review system has existed at the core of academic and scientific research for centuries. Peer-reviewed publications have assisted psychologists in their understanding of the human psyche, anthropologists in their search for our ancestors, engineers in building sturdier structures and pharmaceutical researchers in their quest to cure human diseases. Few can deny the importance of the peer review process in promoting a solid understanding of complex social and scientific issues by encouraging Community experts to work together.

The JAIA will help analysts who have well-argued and possibly dissenting points of view to share them with their peers and establish a Community-wide record of their debate. Because JAIA articles will be directed at peers working on related issues, there is a greater chance that alternative interpretations presented in this fashion will be understood

and either expanded upon or critiqued by their IC colleagues. Those who stand in disagreement will be encouraged to respond with independent articles that lay out evidence for their own points of view. Furthermore, by encouraging analysts from different analytic organizations and disciplines to coauthor JAIA articles, the journal will help lower boundaries that exist between organizations, subject matter specialists and regional analysts.

Given escalating terrorist threats to US populations and interests, deceitful use of dual-use technologies by state actors to evade international weapons conventions and innovative efforts of narcotics traffickers evade interdiction, the IC clearly has a need, as identified by independent investigators, to build a better system for promoting alternative analysis. The proposed peer-reviewed Journal of Alternative Intelligence Analysis provides a straightforward and cost-effective mechanism for promoting a more vigorous scientific culture of documented peer-to-peer debate within the Intelligence Community.

Dynamic Adaptation:
A Twenty-First Century Intelligence Paradigm

(b)(3)
(b)(6)

Introduction

The principal legacy of Galileo Galilei (1564-1642)—the introduction of a new paradigm in modern astronomy, and the scientific methods that brought it about—provided an empirically compelling case that the universe did not work as most people had imagined. Galileo demonstrated, through a series of systematic observations made through telescopes he had fashioned himself, that the sun rather than the Earth was the center of the (known) universe and anchored an entire system of planets, including the Earth, that revolved around it in roughly circular orbits.[1] This scientific breakthrough substantiated the controversial theory of Nicholas Copernicus that had lacked an empirical basis before Galileo, namely, that the heliocentric paradigm should supersede its geocentric predecessor. This "paradigm shift" created enormous controversy and intellectual disruption among key thinkers, and Church authorities, of his time.

A less-well-known legacy of Galileo's offers a keen lesson in adaptation: In spite of relentless Church pressure to repudiate his "heretical" positions, Galileo demonstrated uncanny flexibility in making temporary accommodations with the dominant authorities, while persisting with scientific integrity. In the end, he prevailed. Galileo's subtle lesson in adaptation is better understood through the work of another scientific giant who followed some two and-a-half centuries later. Charles Darwin (1809-1882) explained how species that survive the longest are not necessarily the fiercest or the strongest—rather, they are the ones that have demonstrated the best *capacity to adapt to changing environments*. Species that fail to adapt risk extinction.[2] Like Galileo's methods, Darwin's insights on adaptation have not been sufficiently appreciated by intelligence leaders.

Both Galileo and Darwin illustrate powerful lessons for US intelligence: Paradigm shifts are not easy, even if long overdue, and must be based on sound observation and evidence to justify serious advocacy. Further, attention to processes of adaptation is critical to survival. Such attention may reveal why US Intelligence is sometimes successful, and sometimes not. *Systematic efforts to better integrate a capacity for adaptation into key institutions and processes may better posture US Intelligence to warn or understand emerging, if unidentified, threats to US security in the early decades of the 21st century.*

[1] *Dialogue on the Two Chief World Systems: Ptolemaic and Copernican* (1632).
[2] *Origin of Species* (1859).

Thus, the key challenges facing US Intelligence are:

- to successfully transition to a new and more effective intelligence paradigm; and,
- to ensure that an intelligence paradigm shift fully integrates needed processes of adaptation. [3]

This essay explores both issues. It urges a new intelligence paradigm by focusing on three major kinds of needed adaptations for US Intelligence: *functional* adaptation, *cultural* adaptation, and integrating *adaptive mechanisms* within intelligence institutions. If successful, adaptive mechanisms would help ensure that important changes in the intelligence environment—as September 11th and Iraq's weapons of mass destruction illustrate—do not outpace needed change within intelligence itself. Taken together, these three types of adaptations will shape a new intelligence paradigm.[4]

Functional Adaptation

For US intelligence to succeed in the 21st century threat environment, significant adaptation is required within and across the principal *missions* of US Intelligence: Foreign Intelligence (FI, chiefly collection and analysis), counterintelligence (CI), and covert action (CA). Old and new paradigms are discussed. The key themes addressed here are those that illustrate US intelligence performance against the two significant issues at the center of public discussions about intelligence reform: the warning failure of September 11th, 2001,[5] and the apparent errors in estimating weapons of mass destruction (WMD) in Saddam Husayn's Iraq.[6] Neither issue is dissected in depth here, but both help illustrate key FI malfunctions, and thus frame the discussion much as they have shaped the current debates on intelligence reform.

Foreign Intelligence Collection: Old Paradigm. Significant failings are evident in both 9/11 and Iraqi WMD intelligence. In both cases, collection was insufficient, and analysis was inadequate. Both failed. Had collection been better, analysts arguably might have been more accurate, since successfully "connecting the dots" would have been more

---

[3] "Probably the single most prevalent claim advanced by the proponents of a new paradigm is that they can solve the problems that have led the old one to a crisis. When it can legitimately be made, this claim is often the most effective one possible." Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago: University of Chicago Press, 3rd ed., 1996), p. 153.

[4] A fourth type, *structural* adaptation, is already underway, and beyond the scope of this paper. Structural adaptation encompasses how the Intelligence Community is organized, and the range of DCI (or NID) authorities. Successful structural adaptation will empower the most senior intelligence official with unprecedented budgetary and personnel authorities, as well as significantly enhance needed authorities to protect intelligence sources and methods. It should also establish a fixed term for the DCI or NID of seven years, renewable for one additional six-year term.

[5] See *The 9/11 Commission Report* (New York: W.W. Norton & Co., 2004).

[6] US Senate Select Committee on Intelligence, *Report on the US Intelligence Community's Prewar Intelligence Assessment on Iraq* (Washington, DC: Government Printing Office, 2004).

likely had there been more or better dots to connect. The old paradigm of spotty collection and weak analysis will not well serve the Nation in the 21st century.

Both Galileo and Darwin exemplified innovative and relentless collectors. Galileo pioneered his own revolutionary sensor program (the telescope), while Darwin's "broad area search" aboard the *Beagle* enabled his study of flora and fauna heretofore unimagined by other naturalists. But both enjoyed one huge advantage that US collectors today do not have: Neither Galileo nor Darwin faced a target environment that *adapted* to their collection efforts in order to circumvent them.

In contrast, US intelligence collection failed in 9/11 largely because the terrorist target, in this case, al-Qa'eda, successfully evaded our current collection techniques, chiefly, traditional human (HUMINT) and signals (SIGINT) intelligence collection. Further, US imagery offered no appreciable warning help against the al-Qa'eda threat. Terrorist operatives conspired and conducted their operations, including those that preceded September 11th, in ways to avert timely detection by US intelligence. Similarly, Saddam Husayn's Iraq also successfully evaded US collection for largely the same reasons: US HUMINT generally failed to penetrate Iraq's WMD programs, as did SIGINT, and while imagery performed better against Iraqi WMD than it did against terrorists, it still provided too little of real value. We should ascertain why.

The best explanation for these major collection shortfalls is found in the depth and breadth of understanding that US adversaries bring to US collection techniques—and, by extension, the knowledge they use to defeat them. Many significant US collection failures are rooted in our failure to adapt to the fact that key adversaries—such as terrorists bent on mass killing of US citizens, and dictators who build, conceal, and proliferate WMD capabilities—have our playbook. Because they have a keen grasp of how we collect intelligence, they successfully implement denial and deception (D&D) countermeasures against known US collection techniques. This effectively blunts or neutralizes even the best of our major collection efforts.

Using D&D is how adversaries level the playing field—in some cases, tilting it in their favor. As a result, analysts (and policymakers) are left with insufficient—or worse, misleading—information about the major threats that face us. In short, in defeating US collection capabilities—often complex and costly ones—our key adversaries have demonstrated far better adaptation to our techniques than we have to theirs. Here, lessons from Darwin have worked to their advantage, while our failure to learn the same lessons has worked to our disadvantage. These collection failures are failures of adaptation.

New Paradigm: Adaptive Collection. US collection often fails because it does not defeat the countermeasures that sophisticated adversaries deploy to beat it. *It does not adapt to foreign D&D.* This must change. US collection efforts must defeat proven and emerging countermeasures by employing techniques that are not now known by

adversaries, and therefore, not yet countered. New collection—in HUMINT, SIGINT, IMINT, and MASINT—in short, must be developed precisely in ways that adversaries do not understand and cannot therefore counter. New collection techniques must be more agile, capable of defeating foreign countermeasures, and better protected from exposure. These adaptation attributes—agility, counter-D&D, and better protected sources and methods—must be integrated into all collection R&D and into all programs, including sensors, platforms, systems, and architectures. Otherwise, future US collection will not succeed against determined adversaries who learn to adapt to—i.e., outsmart—the old, much compromised, too transparent, and failing US collection paradigm.

FI Analysis: Old Paradigm. Notwithstanding the analytical burden of significant collection shortfalls, the essence of intelligence analysis is the ability to work successfully in an environment of ambiguous, missing, and even contradictory information. Better collection will improve analysis, but that is far from sufficient. Better analysis will mainly result from stronger analytical techniques, applied in ways to *generate* a wider range of hypotheses, and structured to *test* (evaluate, then accept or reject) the veracity of different (hence, competing) hypotheses.

Galileo's science prevailed in the same way that Darwin's did—through careful analysis of systematically collected data, making full use of new analytical techniques geared to evaluate multiple hypotheses. Neither Galileo nor Darwin was prepared to make claims that would revolutionize astronomy or biology until they were satisfied that their techniques were producing *reliable knowledge*. What techniques produced such knowledge? Science. But the scientific techniques that work so well in the physical world are often viewed as inapplicable to intelligence. Such views may be true to a point, but they are misleading, and paralyzing if fully believed. The issue is whether the analytical techniques (tradecraft) that we routinely use are adequate to produce *reliable intelligence*. The short answer is no, they are not.

A retrospective look at the production of intelligence on Iraqi WMD since about the mid-1990s, including the rushed National Intelligence Estimate on the subject, would reveal not only the impact of poor collection. It would also reveal a distinct lack of analytical rigor. This analytical failure is seen in the insufficiently critical acceptance of (now) questionable assumptions, and sources. It is seen in the lack of appreciation for missing information—that is, a failure to comprehend the impact on analysis of relevant data that we never collected—and in the woefully inadequate information base for the principal WMD inferences made. And it is seen in the unwarranted confidence in some key judgments that we now know cannot stand up to close scrutiny. *Analytical techniques that cannot discriminate between valid hypotheses and those that are not (i.e., between true sentences and false sentences) are not worthy of retention in the analysts' toolkit, nor in the intelligence production process.* Given their access to better information—and their professional responsibilities—intelligence analysts should be expected to outperform university scholars, think tank experts, and journalists.

New Paradigm: Reliable Analysis. What would a successful analytical paradigm use? The unique attribute of scientific investigation, when compared with other ways of producing knowledge, is that its techniques are *self-corrective*. (Epistemologists would cite *authority*, *habit of thought*, and *rationalism* as three alternatives to science, i.e., as different ways of knowing. Iraqi WMD analysis depended too heavily on these three). All four methods can produce truth and error. But science is self-corrigible. Of course, it may produce errors, but it also has intrinsic to its own methods the needed procedures to discover its errors. No other way of knowing can claim this significant feature. That is why the scientific method is the only way of knowing that consistently produces reliable knowledge. *We need to adopt similar self-corrective techniques in analysis if we want to produce reliable intelligence.*

Intelligence analysis, even if it cannot easily mimic analytical procedures used in the physical sciences, must seek comparably reliable knowledge-producing methods. Just as in Galileo's time, *a new analytical paradigm in intelligence must focus on developing self-corrective techniques.* Presently, the closest we get to them is the intra- or inter-agency coordination process. The best hope for developing analytical tradecraft with the intrinsic power of self-corrective techniques is, first, to ensure that it makes much greater use of such quasi-scientific techniques as the Analysis of Competing Hypotheses (ACH).[7]

Second, we must conduct the coordination process so that it will highlight potential error in the assumptions, facts, judgments, and conclusions of the analytical product. Fortunately, ACH is presently taught in CIA analyst training. But it is rarely used in practice, nor valued by managers of analysts who typically regard such techniques as time-consuming and cumbersome production delays. Moreover, the coordination process is often perceived as still another obstacle to production, and one to be accomplished as quickly and as painlessly as possible. (To meet its impossibly tight deadlines, the substantial October 2002 NIE on Iraqi WMD was coordinated in a single day!) While many appreciate the coordination process for its hypothesis-generating possibilities, too few appreciate it for its hypothesis-*testing* potential. As one of the critical steps in the analytical production process, coordination can—with ACH—*provide the self-corrective function in intelligence analysis* much as empirical techniques have served science so well since Galileo. We should do no less in intelligence.

A new analytical paradigm should also adopt a far more robust effort to improve and integrate reliable *forecasting methodologies* into routine intelligence work. Better forecasting of foreign political, military, technological, and economic trends is essential

[7] See Richards J. Heuer, Jr., *The Psychology of Intelligence Analysis*, (CIA: Center for the Study of Intelligence, 1999), chapter 8; and Heuer's "Limits of Intelligence Analysis," forthcoming in *Orbis*, Winter, 2005. With Heuer, in emphasizing the importance of better "structuring" in analysis,

(b)(3)
(b)(6)

to a more effective warning function; to a better understanding of new and emerging threats and opportunities; to the development of required new approaches to collection; and to the adaptation of US intelligence capabilities. This is essential so that 21st century threats do not overpower our intelligence and surprise an unprepared nation.

Counterintelligence: Old paradigm. Arguably, counterintelligence (CI) has been the worst performing discipline in modern US intelligence. Its failures have had a far greater impact on Foreign Intelligence than is commonly appreciated. Careful study of the worst US spy cases (e.g., Ames, Hanssen, Hall, Pelton, Chin, Kampiles, Pollard, and Montes), and other major penetrations of US human and technical operations, would reveal that the quality of FI has been significantly degraded by the poor performance of CI. Many of these failures were preventable—or their damage could have been reduced—through better CI. It is not well understood that our CI failures have caused incalculable damage to FI capabilities in all collection disciplines, and even to the analytical process.

US counterintelligence has been crippled by numerous *systemic failures* over the years. These include the failure to overcome such negative *legacies* as the excesses of CIA's Angleton and FBI's COINTELPRO; the failure to function as a *Community* due to long-standing FBI, CIA, and DOD bureaucratic parochialisms; and the failure to successfully transition from a HUMINT-centric activity to an *all-source* discipline. CI has also failed to incorporate *analysis* as a key function of the profession. It has failed to command the needed *resources* to accomplish its vital mission, and to integrate itself into the dominant (FI) *culture* of the intelligence professional. It has also failed to develop effective *leaders* owing to the lack of career services and other debilitating CI career disincentives in all agencies. And CI has failed to comprehend its extraordinary importance to the *effectiveness of the FI mission*.

Effective CI: New Paradigm. While durably fixing CI ranks among the toughest challenges of intelligence reform, few are discussing it today. *Major structural CI changes are required.* The present CI Community organization, the National Counterintelligence Executive (NCIX), must be significantly strengthened to exert real authority over the CI activities of the FBI, CIA, the DOD intelligence agencies, and others such as DOE and the national labs. The senior CI Community official (today, NCIX) requires dramatic new budgetary, personnel, investigative, and operational authorities. It should be brought directly under the new NID (or whatever new senior FI official emerges in the present reforms) with the rank and organizational wherewithal comparable to the major intelligence agencies. Significant new authorities for CI—spanning domestic intelligence as well—must be crafted in legislation and executive orders. The future role of CI must be re-conceptualized not only to address its critical relationship with FI, but also its imperative to overcome the key systemic failures and adverse legacies discussed above. Perhaps most importantly, the new CI must take responsibility for significantly enhanced protection of intelligence sources and methods.

In *counterespionage*, urgent new attention must be given to the insider threat, guided by substantial new psychological work.[8] Significant improvements in *operational CI* will result from a much-enhanced priority for asset validation, including information validation—which both require greater analyst engagement, and clearer authority over FI operations—and from a much-elevated role for *offensive* counterintelligence.

Covert Action: Old Paradigm. Covert action (CA) suffers the negative legacies of the Bay of Pigs, Iran, Guatemala, and other instances popularly understood as CA failures. A strong disinclination to use CA, especially if lethal, within both the policy community and relevant agencies, has hobbled US ability to forcefully address the threats that face us in the 21st century.[9] Overcoming this legacy requires a new appreciation for the power and potential of successful CA, especially given the nature of the terrorist and WMD proliferation threats to US security and the range and depth of the growing anti-US attitudes increasingly prevalent among the populations of the Muslim countries.[10] CA does not require a whole new paradigm, only the renewal of an earlier tradition. Less broken than CI and FI, it can learn as much or more from past successes as from failures.

Effective CA: Renewed Paradigm. No intelligence capability generates more controversy than covert action. But to succeed in the 21st century, US intelligence will require a much more effective CA capability than it has had before. It is impossible to evaluate the long-term effects of major CA programs to turn public opinion, shape popular attitudes towards a governing regime, galvanize opposition groups, or even topple governments. But arguably, some CA-capable nations have enjoyed some success at this.

Soviet "active measures" against the United States during the Cold War, for example, enjoyed a high priority from its top political leadership and commanded considerable resources within the KGB. According to KGB archivist Vasili Mitrokhin, the Soviets conducted vigorous CA programs worldwide to destabilize the CIA through operations—largely successful—to expose roughly 2000 Agency officers, and also used forgeries to "expose" hostile CIA operations *that never existed* against Third World governments. Other major Soviet CA operations focused on penetrating European peace movements to forestall US INF deployments in the early 1980s; stirring up racial tensions within the United States during the 1984 Olympics; spawning a worldwide disinformation campaign that the AIDS virus was a creation of US biological warfare efforts; and the incredible

---

[8] The preliminary efforts begun in Project SLAMMER some years ago should be revisited and much improved.

[9] See Richard Shultz, "Showstoppers: Nine Reasons Why We Never Sent Our Special Operations Forces after Al Qaida Before 9/11," *The Weekly Standard*, 26 January, 2004; and Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (New Brunswick: Transaction Publishers, 2001), pp. 64-65.

[10] See the Pew Global Attitudes Project, *What the World Thinks in 2002* (Washington, DC: Pew Research Center, 2002), and Pew's *Views of a Changing World* (2003).

"baby parts" fabrication. This story alleged that rich Americans were butchering Third World children in order to harvest their organs for transplants. These outrageous allegations even resulted in a successful motion in the European Parliament, introduced by a French delegate in September 1988, condemning this trafficking in baby parts.[11]

According to a Western scholar of intelligence, Roy Godson, covert action is an essential policy tool. While its effects can never be measured precisely, Godson argues that CA, at a minimum, has fared no worse than other instruments of statecraft such as public diplomacy, economic assistance, or military force. Further, "US covert action programs in Western Europe after World War II seriously challenged the notion that covert action is of little value." More recently, the Soviet military withdrawal from Afghanistan and the demise of communism in Eastern Europe were almost certainly hastened by US efforts, secret at the time, but now largely acknowledged by key players. Specifically, the "slow-drip" effect of Radio Free Europe and Radio Liberty in weakening communist ideology has been cited in testimonials in 1990 by such East European leaders as Czech President Vaclav Havel and other senior counterparts from Poland, Hungary, Romania, and the former Soviet republic Estonia.[12]

To succeed, covert action should be conceived as a very long-term proposition and part of a well coordinated policy. CA, moreover, cannot substitute for bad policy nor provide an excuse for foreign adventures. It requires opportunity, of course, but also timing, creative leadership, coordination, and plenty of self-evaluation.[13] In sum, the ingredients of CA successes necessitate a long-term, highly-classified, sustained program with clear strategic objectives, sound infrastructure, adequate resources, and the political will to carry it out. These features should provide the foundation for a well conceived and substantial effort fashioned to address the present and emerging terrorist and WMD threats to the United States. Nothing less will do. We need to apply the lessons of past CA successes as well as failures. In light of 21st century threats, US policy and intelligence officials must learn to re-appreciate the considerable potential that well-conceived and properly executed CA programs represent.

---

[11] Christopher Andrew and Vasili Mitrokin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999), pp. 230-245. See former DCI Robert M. Gates, *From the Shadows* (New York: Simon and Schuster, 1996), pp. 260-261 for discussion of the Soviet's anti-INF campaign throughout Western Europe.

[12] Roy Godson, *Dirty Tricks or Trump Cards*, p. 26 and 267-268 (note 70). For elaboration, see Gates, *From the Shadows,* pp. 358, 450-451 on Poland, and pp. 319-321 and 348-350 on Afghanistan. Ferment in Eastern Europe, especially Poland, was also feared as contagious by Soviet leaders at that time. As early as 1983, the Soviet leaders privately expressed great concern—justifiably, we now know—about possible spillover effects of the Solidarity movement within the USSR. *Dimensions of Civil Unrest in the Soviet Union*, National Intelligence Council Memorandum, 83-10006, April 1983, p. 20; declassified 25 Feb. 1994.

[13] Godson, *Dirty Tricks or Trump Cards*, p. 121-127.

Cultural Adaptation

There is no discernible professional culture—an aggregate of supportive attitudes, values, and beliefs about the intelligence profession—in the Intelligence Community. There should be. Presently, there is only a collection of the different cultures of different agencies, and subcultures within them, that may episodically help—but more often impede—the common goals of the Intelligence Community. A common culture of professionalism across the Intelligence Community will much enhance individual and component performance within and across the FI, CI and CA professions. All three of these mission areas require extensive interagency engagement. Performance levels in all three can be enhanced, or degraded, depending on how specific agency cultures and subcultures may support or impair cross-cultural (meaning, cross-agency) cooperation.

Old Paradigm: Agency-centrism. If there is a dominant theme in the diagnosis of the 9/11 warning failure, it is the crippling deficiencies in information-sharing among agencies. If some of the key, however fragmentary, pieces held by several agencies had been assembled earlier, possibly analysts might have imagined a preview of that terrifying September 11th puzzle.[14] This kind of breakdown was also at the heart of the 1941 warning failure at Pearl Harbor.[15] The subsequent creation of the *Central* Intelligence Agency was intended precisely to improve information sharing that had been impaired earlier by the deeply rooted institutional reluctance within the US Army and Navy. At bottom, that was a cultural problem in 1941 that was largely solved for a generation with the creation of the new CIA. The fix wasn't permanent.

Cultural barriers between FBI and CIA, for example—traceable to the J. Edgar Hoover era and remarkably persistent over the years in both agencies—impeded vital FI information sharing in 9/11. They are also often cited as a major factor in the notably poor CI investigations of the Ames and Hanssen cases and in others as well. Such agency-centric parochialisms have been notoriously resistant to change, in spite of top leadership exhortations for many years to mend them at both agencies. These are only the most egregious examples. *All* intelligence agencies are afflicted with deep cultural parochialism, in varying degrees, and efforts to build a *community* of intelligence organizations can never succeed without a corresponding national effort to build a community culture. Such a cross-agency culture can never be built unless specific agencies are willing—or are forced, as the Goldwater-Nichols solution clearly established for the US military—to cede key authorities and prerogatives to some central governing or overarching supra-organization (the Joint Staff, in the case of the military).

New Paradigm: Community Professionalism. *US intelligence sorely needs a culture of the intelligence professional.* Intelligence is a bona fide profession, but it lacks the

[14] See *9/11 Commission Report*, (note 5), chapter 8.
[15] Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962).

culture necessary to develop and sustain the required professionalism. All agencies hire experts—language, country, and regional specialists; technical and technology specialists; lawyers, and contract and budget specialists; and countless others. None is hired as an *intelligence* professional, but each is expected to become one in due course. Some succeed. Many do not. The expectation seems to be that, over the years and with a little training, people hired into the intelligence profession as experts in something else will *also* become experts in intelligence, and their requisite intelligence skills and values will follow later. This expectation is naïve and remains unfulfilled.

In order to establish a culture of the intelligence professional, the Community requires a program fashioned to build the necessary attitudes, values and beliefs. Such a culture should supersede the narrower cultures of the individual agencies. It should emphasize the uniqueness and importance of the intelligence mission as *the acquisition and analysis of secret (i.e., denied) information by secret means*, and the unwavering ethic of *protecting intelligence sources and methods*. It should stress the necessity of combined interagency efforts, including information sharing, to succeed in all missions, and the achievement of excellence (as DCI Casey tried to foster in his time) and the intolerance of mediocrity. And it should seek to learn from previous intelligence failures—and successes—experienced throughout the Intelligence Community. The overwhelming majority of intelligence officers suffer from a poor understanding of the history of their own profession. This must change. A smart culture learns from its past.[16]

Establishment of a real community culture of the intelligence professional will require a massive, long-term, education and training effort of unprecedented proportions. This can be accomplished through the establishment of an *Intelligence Community University.* Such a university will not have separate agencies as its constituent elements, but rather a *functional* organization defined by mission. Addressing expert and cultural training for the three basic missions, its three colleges would be Foreign Intelligence (large), Counterintelligence (medium-sized), and Covert Action (small).[17] The FI and CI Colleges should also "cross-train" each other's students. This would help ameliorate the unacceptable levels of CI illiteracy now found throughout the FI population, as well as prepare CI specialists for a much expanded role in support of FI operations and activities.

---

[16] "The study of paradigms," notes Thomas Kuhn "is what mainly prepares the student for membership in the particular scientific community with which he will later practice." Kuhn (note 3), p. 11.

[17] Each college would have separate schools to address its principal mission areas. For example, schools in the FI College would include Collection, Analysis, and Support (such as TPED: tasking, processing, exploitation, and dissemination). It should also have several target-area schools such as Counter-terrorism, and Counter-proliferation. The CI College schools would include Counter-espionage, CI for FI operations, and Offensive CI Operations. The CA College would include schools for Political-psychological Operations, and Paramilitary Operations. The next level down would be departments. For example, the FI Collection School would staff departments in each of the four collection disciplines; departments in the Analysis School would include Political Analysis, Military, S&T, and so forth.

A key idea in the IC University concept is the organizational absence of agencies per se, and the combined interagency training of intelligence professionals by mission area, not by agency. The University should train for unequalled expertise in all the intelligence professions. It should teach and train from a rich history of intelligence successes and failures. Perhaps most importantly, it should nourish and transmit the values and ethics of a culture of the true intelligence professional, much as the scientist descendants of Galileo and Darwin learn the values of their own professions.

The University should also conduct a kind of "boot camp" for new entrants at all agencies before the new entrants report aboard their agencies. This training should help imbue the next generation of intelligence professionals with the appropriate values and ethics for the new Community culture requisite for the highest professionalism. Through training and over time, The IC University's alumni will assimilate the values of the intelligence professional, broadly defined, not the parochial identity of separate agency employees. Its graduates will be intelligence professionals *first*, then regional or technical specialists secondarily. Their intelligence professionalism will be Community-focused, not agency-centric. To succeed, a drastic reform in career services must follow.

Institutionalizing Intelligence Adaptation

In order to achieve needed intelligence adaptation for the 21st century, the Intelligence Community must establish a process of *dynamic reinvention* as the sine qua non for future effectiveness. Broadly, such a process requires three essential elements:

- Effective *forecasting* of emerging threats, opportunities, and major developments—the most likely and least likely security environments for the 21st century.
- A process for *identifying needed intelligence capabilities and resources* that will provide the best match for the range of security environments forecasted.
- An institutionalized mechanism *to formulate and implement sound intelligence policies* to achieve the most effective Community capabilities, optimally postured for a changing security environment.

The first requirement—effective forecasting—can best be achieved through a substantial, dedicated, futures-forecasting effort. Yearly analytical products should seek near-term (1-5 years), mid-term (6-15 years), and long-term (more than 15 years) forecasts. They should combine methodological rigor with genuine imagination and make extensive use of non-intelligence experts and resources. Save for the fledging Futures effort at the Sherman Kent School, and the NIC 2015 and 2020 products, this kind of forecasting is—astonishingly—almost non-existent in the Intelligence Community. It should rank among the Community's most important processes and products. The principal customer for these forecasts should be intelligence policymakers first, and national security policymakers secondarily.

The second requirement—linking needed IC capabilities with forecasted security environments—is currently addressed among disparate components, including the Community Management Staff, here and there in the Community. But this essential function must be much more focused and explicitly integrated into capabilities planning. Presently, future capabilities planning, to the extent that it actually occurs, seems mostly ad hoc, is too decentralized, and does not benefit from systematic forecasting.

The third requirement—an IC policymaking process that actually formulates and implements IC-wide policies—would be an entirely new function. The current policy bodies (e.g., the IC Principals Committee, IC Deputies Committee, and the more narrowly focused National Intelligence Collection Board and National Intelligence Analysis and Production Board) are chiefly advisory and have little teeth. The new NID (or whatever the new top intelligence chief is titled) will need a real policymaking mechanism to govern the Community. Whatever IC policy mechanism emerges will attend to day-to-day management issues, but the adaptation function—dynamic reinvention—will require a dedicated policy body, with clout.

In order to achieve these goals, the Community should create a new *Intelligence Adaptation Council* to monitor its posture and preparedness for threat warning, and for understanding future security environments. Its mission should drive *the adaptation cycle*, that is, ensure that the adaptation piece of intelligence policymaking is fully functioning as an integral feature of the Intelligence Community policy and planning process. Unlike Darwin's evolution, intelligence adaptation does not happen naturally.

The Intelligence Adaptation Council should have senior representatives from the principal agencies and centers within the Community, from the Intelligence Community University, and from academe and industry. It should meet yearly to review and assess the year's forecasting products (near-, mid-, and long-term) and to evaluate the match-up between forecasted environments and planned or needed capabilities. It will recommend to the top intelligence official any new needed capabilities or program course corrections (redirections, plus-ups, or terminations) that are out of synch with sound intelligence adaptation for the emerging security environment. *All major Community budgetary, strategic, planning and policy guidance decisions will conform to the Intelligence Adaptation Council's recommendations, or have to justify the departures.*

Conclusions

Bureaucracies are better at resisting change than leading it. Not everything in US Intelligence needs to be changed. But much of it does. Without significant structural, functional, and cultural adaptation to 21st century requirements, the Intelligence Community will be hopelessly ill-equipped to identify, warn, and characterize the complex and elusive threats we will face. Failures are assured. To ensure needed adaptation—and to maximize the potential for greater success—adaptive mechanisms

such as the Intelligence Adaptation Council must be *integrally* built into intelligence institutions and processes. To be fully effective, the Intelligence Community needs nothing less than a full-blown paradigm shift, analogous to what Galileo and Darwin accomplished. Neither astronomy nor biology has been the same since.

Lacking comparable intellectual giants in intelligence, our paradigm shift will be less dependent on visionary scientists than on sound decisions and processes. To succeed, we must:

- Prioritize *adaptive collection techniques* that will defeat adversary denial and deception and will provide analysts and policymakers with the unique value-added that only intelligence can—the successful collection of denied information on such security threats as terrorism and WMD that cannot otherwise be acquired.
- Fully integrate *self-corrective mechanisms* into analytical processes so that intelligence products are maximally reliable, and that intelligence can be fully trusted as a basis for the Nation's most important policy decisions.
- *Re-conceptualize counterintelligence* for much-enhanced support of FI—especially the vital, and tragically neglected, protection of sources and methods—with significantly greater capabilities in counterespionage and intelligence validation enabled by greater CI centralization and much expanded authorities.
- Establish a *key role for covert action* in the global war on terrorism and in counter-proliferation, especially targeting regions where anti-American sentiment is strong and growing, but can hopefully be reshaped through soundly conceived CA programs.
- Engineer a comprehensive *cultural adaptation* throughout the Community through a new professional culture, facilitated by a new IC University structured to nourish the values, ethics, and expertise worthy of the 21st century intelligence professional.
- Institutionalize dynamic reinvention through a new *Intelligence Adaptation Council* that will ensure an IC adaptation cycle geared to learn and to acquire the intelligence capabilities that the United States requires for its security in the 21st century.

Individually, accomplishment of any of these proposals would be significant. Taken together, they could provide the basis for a paradigm shift in US intelligence. Even as they fall short of an intelligence counterpart to Galileo's and Darwin's respective impacts on science, they will still better posture US intelligence for the responsibilities it must shoulder as new threats and uncertainties unfold. The dynamic adaptation paradigm as outlined here could minimize surprise, better support national security policymakers, and even help shape the environments to come. This paradigm should also help fashion a new community of intelligence professionals who would elevate US intelligence effectiveness to unprecedented levels.

The 2004 Galileo Awards

Honorable Mention

Constellation

(b)(3)
(b)(6)

(kŏn´stə-lā´shən) *n.* … A brilliant gathering or assemblage.
[*American Heritage Dictionary*]

I. Concept

As the national leadership wrestles with how to reinvent the country's intelligence apparatus and whether or not to rewrite the provisions of the National Security Act of 1947, one alternative reform offers continued innovation of the Intelligence Community (IC), *by* the Intelligence Community, and with little disruption to the daily functioning of the IC during a time of war. The Constellation concept envisions establishing a second tier to the IC comprised of approximately a dozen small, interagency teams mandated by the Director of Central Intelligence (DCI) and National Intelligence Director (NID) to marshal the country's resources against the most difficult intelligence missions while drawing support and expertise from the existing IC agencies. Some of the most talented IC officers would assemble for a brief period – no more than 18 months – to devise an operational and collection strategy to address a specific challenge and to task the IC to carry it out. Deliberate IC use of transitory, task-oriented teams would overcome the Community's biggest hurdle to dynamic reinvention: the wiring diagram.

Temporarily removing select IC officers from their bureaucratic components and placing them into Constellation teams to tackle specific intelligence challenges is analogous to the "skunk works" project undertaken by International Business Machines (IBM) in the late 1970s that resulted in the invention of the Personal Computer. "Skunk works" consisted of a handful of IBM's brightest and most creative employees cloistered on Long Island, New York to create a revolution in technology. The Constellation concept seeks to produce similar innovations in the intelligence business by removing the barriers that divide the Community's brightest and most creative officers and placing them in an environment to reinvent the US approach to specific threats.

The Constellation concept also resembles the DCI Task Force of the mid-1990s that addressed the Balkans crisis and North Korean nuclear revelations, as well as Hard Target Board Tiger Teams that continue to pursue approximately 10 hard targets worldwide today. The critical difference between the DCI Task Force or the Hard Target Board model and Constellation, however, lies in when and why the interagency teams coalesce. The Constellation concept seeks to spur the IC at the first sign of an emerging threat so that the Community can establish a creative and coherent plan to maximize IC resources *before* the threat rises to the level of a crisis. The Constellation model further

differs from the Hard Target Board concept in another important way – in its authority to task the IC agencies with specific actions based on its newly devised strategy.

The Constellation concept views an emerging threat as an opportunity to readdress the IC's approach to intelligence challenges. The Constellation team would harmonize the capabilities of CIA, DIA, NSA and the military intelligence centers like NGIC, with the FBI, the Department of Homeland Security, DOE and other agencies, much like a conductor would conduct an orchestra – ensuring a seamless and synergistic approach to the challenge. In this sense, the Constellation team would be the agent for dynamic change within the Community.

Constellation teams would best serve specific, non-traditional missions that cut across many disciplines and agencies in the IC, and especially against hard targets – where traditional IC efforts may have fallen short. They would not, however, serve well against broad, strategic threats like global terrorism or the spread of nuclear technology. Instead, Constellation would be more tactical in focus. Examples of threats that met threshold would include a specific al-Qa'ida plot against the United States, terrorist insurgent activity in one of the oil-producing nations, or efforts by a single rogue nation or non-state actor to acquire weapons of mass destruction (WMD). By focusing on this level, a newly created Constellation team would devise a plan to task, direct and orchestrate the intelligence agencies – *and all of their assets* – to penetrate the hardest targets, expose the most elusive plans and attack the most dangerous enemies.

The Constellation model does not advocate reorganizing the intelligence agencies. Such reforms would risk replacing current bureaucratic inefficiencies with new ones. Rather, it seeks to harness the strength of the IC in mission-specific teams to address intelligence challenges *as they emerge*. By creating these mergers on an ad hoc, mission-specific basis – and disbanding the teams when the challenge has been met or the team's strategy successfully has been adopted and implemented by the IC – Constellation will instill within intelligence officers a higher standard of performance and a strong sense of purpose.

II. Justification

A Community Divided

A close look at the wiring diagram of any agency within the IC illustrates how it is divided against itself in its efforts to protect US interests. Officers that share similar areas of responsibility are separated from each other by teams, branches, offices and directorates. But the Community is further divided into a multitude of agencies, all ostensibly sharing the same areas of focus. To respond to our nation's most pressing security challenges, the IC needs to rethink its current organization – which will mean

redefining the concept of "team," and ultimately redefining the concept of "intelligence officer."

Consider, for example, how some of the most dangerous threats to our national security – terrorist groups and proliferation networks – are organized. In general, the most prominent terrorist and proliferation networks are organized loosely and are highly opportunistic in their behavior. The symbiotic arrangement that al Qa'ida is establishing with mujahedin and insurgent groups, and that proliferation networks enjoy with each other, represents a *competitive advantage* over our national security apparatus.

By comparison, the IC generally can be rigid, compartmentalized and parochial. The notion of coordination within the IC does not always engender images of cooperation and synergy. Instead, the term "coordination" can conjure thoughts of friction, resistance and even intransigence. Reorganizing the agencies within the IC, or creating new ones, will not eliminate parochialism or coordination problems. Rather, the United States needs to capitalize on its many specialized intelligence agencies by orchestrating their disparate capabilities into a congruent, synchronized response to emerging threats. By realigning the IC around the Constellation concept, the United States can enjoy the same synergy as its adversaries and an enhanced ability to counter threats.

The Need To Redefine "Team"

Currently, the friction that can be experienced between various teams in the IC often results from the phenomena of "turf" and the "stovepipe." Any number of teams within and among the agencies may claim a given threat as their purview ("turf") and bring widely divergent approaches to bear in countering it based on their particular skill set or job description ("stovepipe"). This friction frequently results in a waste of government resources and a haphazard response to each intelligence issue. Constellation, however, would alleviate the friction suffered in the IC by centralizing the government's resources into one team that provides a coherent response.

For one intelligence problem that surfaced in December 2003, there were as many as 15 teams throughout the IC attempting to tackle the issue – six teams within CIA, four teams at NSA, three at NGA and one each at DIA and ONI. Although several teams worked together collegially, the disagreements and coordination difficulties between others routinely were enough to delay warnings to the President despite an impending threat. Without perseverance, the team spearheading the effort to warn the White House might have lost heart from the grinding coordination and abandoned its effort. Alternatively, the other, dissenting teams involved might have simply overruled the lead team's assessment of the problem and prevented coordination from occurring. In either scenario, the IC eventually would have been tarred with another allegation of "intelligence failure."

Ultimately, the lead team's efforts were validated, and it provided highly accurate intelligence to the President and the NSC. But those accomplishments could have come to the White House more quickly in a Constellation team. A Constellation team addressing the same issue would have been comprised of officers from all five agencies (CIA, NSA, NGA, DIA, ONI) and, as the mission leader within the IC, the Constellation efforts would have been streamlined because coordination over the nation's response would have occurred within the one team.

The Need For A New "Intelligence Officer"

By creating within the IC a small group of interagency, task-oriented teams, Constellation would help to develop a new breed of intelligence officer. Officers that have reached the full-performance level and have distinguished themselves among their agency peers would be given the chance to serve as more than operations officers, reports officers, analysts or branch chiefs. When called to serve on a Constellation team, they would step beyond their narrowly defined role to work with their community peers on *all aspects* of an intelligence issue to achieve specific national security objectives.

In a sense, Constellation would allow IC officers to enjoy the latitude and involvement in the national security mission that some intelligence officers have in smaller services. For example, an intelligence officer in a smaller country may be involved in clandestine operations to counter threats to national security, but he/she may also be involved in drafting reports and analyses of his/her work for the Policy Community. The officer may even help to position other intelligence assets to complement the operational, reporting, analytic or law enforcement aspects of the mission.

Within the IC, the opportunity for such a well-rounded intelligence experience is uncommon. Instead, the relevant components of each agency tend to divide the national effort into its component parts. Officers provide their contribution to the mission based on their job description – much like workers on an assembly line. The level of engagement for the individual officer, therefore, may be no greater for a critical task than for a routine intelligence issue.

The benefits and disadvantages of each model are clear: in the United States, we have been able to afford a complex, highly specialized officer corps, but each officer has a very small role to play in safeguarding national security. In a smaller country, an officer may be more of a generalist but play a much larger role in protecting his/her homeland. In a Constellation arrangement, the IC officer can enjoy the benefits of both models – a highly specialized corps of officers focused on a specific threat to US interests, with a broad mandate to ensure national security.

The *mission-oriented officer* is the kind of officer America needs but cannot develop through top-down agency reorganizations. Instead, by creating a fluid and dynamic array

of task-oriented teams that spans the current IC structure, Constellation will encourage officers to hone their skills within their home agencies to eventually serve a higher calling. An intelligence officer that is encouraged to think in terms of his/her mission in the broadest possible sense rather than in terms of a specific, routine set of duties, is more likely to be engaged, highly motivated and creative in his/her approach to meeting the intelligence challenges facing America today.

A Two-Tiered System Is Customer-Focused...

In addition to creating a highly focused, highly motivated and more *mission-oriented* cadre of intelligence officers, Constellation makes good business sense from a customer-focus perspective. When the NSC Director for Nonproliferation requires information on the national response to Country X's suspected nuclear weapons program, he or she needs a coherent and up-to-date picture of the tactical situation. Most importantly, he/she needs to be able to make one phone call to get a complete answer. The current IC structure requires the director to make multiple calls or levy multiple taskings, often requiring days of waiting for a response to all of his/her questions.

In the new model, the Constellation team that is charged with attacking that specific threat could provide answers to all of the director's questions virtually immediately. Namely, the Constellation team would provide the policymaker:

- its operational and collection plan,
- any operational or collection achievements,
- an evaluation of its available assets,
- and its current analysis of the issue.

It is important to note that the existing agencies would still have a vital role to play in the Constellation model as the country's institutional knowledge base and repository for expertise. Although the NSC would direct mission-specific inquiries to the Constellation team, it would look to the agencies to address some of the broader, related issues. The IC agencies would provide assessments of:

- the competency of Country X's scientist cadre,
- the level of popular support for the regime,
- its current military readiness and alert status,
- and plans and intentions regarding the use of nuclear weapons.

Most important, the existing agencies would have highlighted indications of the emerging nuclear weapons program, triggering the creation of a Constellation team to counter it.

The two-tiered system, then, would encourage much of the strategic effort to reside in the existing intelligence agencies while the tactical response to a specific threat or emerging issue would come from a Constellation team.

...And Maximizes Our Greatest Resource: Our Officers

Constellation would reclaim the value of the IC's most important, yet currently inefficiently utilized, resource. The highly motivated, imaginative and patriotic officers that comprise the IC currently cannot serve their country as much as they would like to because of bureaucratic impediments. A Constellation of interagency teams tackling specific national security missions would allow intelligence officers to prove that they are truly capable of full performance.

III. Implementation

How Constellation Would Work

Upon IC identification of an emerging threat to national security, the DCI and/or the NID would order the creation of a Constellation team to address the threat. The DCI would choose a Constellation team leader from one of the agencies based on the nature of the Constellation team's mission and the agency best suited – in terms of specific focus, resources and assets – to lead the mission. The Constellation team would enjoy a mandate from the NID to task the agencies with any operational or collection requirements, involving clandestine or national-level assets, to support the mission. The team would consult regularly with the DCI and NID to ensure that its approach met the needs of policymakers.

The length of a Constellation team assignment would vary according to the nature of the mission and the accomplishments required of it by the DCI and the NID. Some missions may be highly tactical in nature and require only a few months to complete. Others may be more complex and last for a year or more. A longer mission – one that approaches 18 months – eventually might devolve into a matter for the IC to accomplish provided the Constellation team had successfully realigned the focus of the agencies and orchestrated their efforts to handle the task.

Dissolution of the Constellation team would occur when the team leader notified the DCI that:

- the threat had dissipated or had been defeated,
- the intelligence warning of the threat no longer remained valid,
- the team's action plan successfully had realigned the IC to address the threat,
- or the threat had reached crisis level, meriting creation of a DCI Task Force.

In the event that the mission devolved to the IC, the leader of the disbanded Constellation team would serve an ombudsman role, floating between the agencies to ensure the

mission continued to proceed according to the Constellation plan and the wishes of the DCI and NID.

How It Would Look: Small Logistics Tail

The size of a newly created Constellation team would depend upon its mission and the assets required to fulfill the mission. Because each team can task the IC with specific collection, operations or analysis to supplement its work, and because each mission would be specific in focus, most teams probably would require no more than two officers from each of the relevant agencies. A team of 20-25 officers, therefore, should be more than enough to handle any mission and allow for staffing issues that arise during longer assignments – like when an officer takes leave, travels or enrolls in training.

Housing the new team may prove a challenge because of the scarcity of office space in the IC. However, because most teams probably would be 25 officers or less, finding space to house the team may be mitigated somewhat. Another mitigating factor could be the ability for some members of the team to participate virtually, especially if their contribution to the Constellation team requires intensive involvement of their home agencies. The DCI would have the discretion to place the team based on availability of space and the needs of the DCI and NID to maintain close contact with the team.

Training The Mission-Oriented Officer...

With a team of 25 officers or less, the division of labor would be unconventional. A Constellation team would emphasize removing the "stovepipes" that currently define most officers' careers. Instead, a Constellation team would encourage an open-minded approach to the problem by having reports officers help with the team's analysis, by having collection specialists help plan the team's operations strategy and by having analysts help review and validate available assets. This crossbreeding of officers would include, time permitting, a smattering of one-day to one-week-long training courses, which already are available to IC officers according to their discipline.

As officers found the time during longer Constellation assignments, they would enroll in brief training courses to polish the new skills they developed while on the team. Although each officer still would bring his/her own specialized skills to bear on the team's mission, a technical collection specialist might be encouraged to take a course in HUMINT targeting, a reports officer might enroll in a course on spotting denial and deception in imagery analysis and an all-source analyst might enroll in an asset validation course. One exception to the team's training opportunities would be the clandestine service trainee curriculum, which is too involved and specialized for the purposes of cross training. Instead, a brief tutorial in the principles of field operations would suffice in exposing the non-case officer to the clandestine service. Through this exposure to

other disciplines, officers that serve in Constellation teams ultimately would develop the skills to become truly full-performance intelligence officers.

...And Creating A Tighter-Knit Community

The professional experiences and values shared by Constellation team members would help to foster enduring personal relationships that would bring the IC closer together. After a team had disbanded, officers would follow related issues from their home agencies but would be more likely to contact their former Constellation teammates and team leader to confer on further developments. The Constellation experience, therefore, would further encourage officers to shed the narrowly defined "stovepipe" approach to intelligence and would integrate them into a more holistic security network over the course of their careers.

Smashing Rice Bowls

Just as Constellation would help to remove the phenomenon of the "stovepipe" by encouraging team members to handle all aspects of the intelligence mission, it also would remove the notion of "turf" by holding primacy within the IC on mission-specific issues. Because of the charter from the NID, all tasking originating from a Constellation team would carry the same weight as a direct tasking from the White House. Field officers, managers of collection platforms and headquarters officers alike would be subject to NID-level scrutiny in their support of the mission. This arrangement would streamline the archaic processes involved in tasking national-level collection platforms, it would focus agency priorities and resources, and it would ensure movement in the field.

Constellation In Action

Small, interagency teams would be able to focus IC resources on the most intractable and immediately challenging intelligence problems far more effectively than the individual agencies would through normal coordination. Constellation teams, therefore, would best serve non-traditional missions that cut across many disciplines and agencies in the IC.

Indications of a sale of North Korean long-range ballistic missiles to Syria might be one example of where a new Constellation team would take the lead. Counterproliferation officers and other experts from CIA and DIA would contribute their experience on the North Korean and Syrian accounts to identify targets for collection, while NGA and NSA representatives to the team would use their intimate knowledge of national collection platforms to propose innovative collection strategies for both countries. Military representatives would help to coordinate airborne and shipborne collection efforts off the coast of each country and, if necessary, support interdiction operations. ONI and SOCOM officers may also be seconded to the team if a shipment appeared imminent and interdiction remained an option. Meanwhile, clandestine service officers would

orchestrate efforts to recruit sources with access to both countries' missile programs to collect HUMINT to further guide the Constellation operation.

All of the IC agencies' contributions to the action plan would occur in unison under the Constellation team's direction.

Another mission might involve pursuit of an al-Qa'ida affiliated terrorist cell purportedly extracting uranium from mines in Africa. Counterterrorism officers and African specialists would help the Constellation team identify the parties involved as well as their vulnerabilities. Clandestine service officers and all-source analysts could help decide how best to attack the problem and provide "ground truth" once the site of the activity had been located. Depending on the Constellation team's approach, SOCOM officers may be part of the team to coordinate a joint military-intelligence operation to disrupt the activity. NSA and NGA officers could assist in the operation by providing continuous, real time – or near-real time – operational intelligence on the intended target. FBI officers and Department of Homeland Security officials would contribute to the mission by ensuring the cell did not have a presence in the United States.

Several other potential missions undoubtedly exist for Constellation teams to pursue – some of them perhaps more dramatic or immediately threatening to US interests. For those missions, a "business as usual" approach could fall woefully short of ensuring national security. In the post-9/11 world, the synergistic power of a Constellation-style approach to security threats is a force our country should not hesitate to employ.

Courage Of Conviction

A critical element to the successful implementation of a Constellation mission will be the courage of all intelligence officers – including the DCI and NID – *to pursue aggressively the national security mission based on imperfect information*. None of the most important national security challenges facing America today involve clear-cut intelligence or ready-made solutions. Our adversaries are increasingly more sophisticated in their attempts to hide their activities. As such, our leadership will need to act on *indicators* vice explicit intelligence. The DCI and NID will need to be forward-leaning in establishing Constellation teams *before* Country X develops a nuclear program or Arms Dealer Y sells fissile material to al-Qa'ida if the United States is to counter such threats sufficiently. About a dozen such teams – analogous to the Hard Target Boards – should be sufficient to address the IC's most urgent missions without taxing the IC infrastructure. But the transitory nature of the Constellation team should encourage the DCI and NID to lean forward in pursuing the missions that merit focused IC attention.

The advantage to the Constellation model of IC reform is that once a threat to national security has diminished – either because the IC has realigned its assets in accordance with the Constellation team's strategy, or because the indicators that triggered the formation of

a team no longer remain valid – the team can dissolve with no disruption to the IC. But the country's leadership must be willing to allow pursuit of specific missions to counter perceived emerging threats *at their inception* in order for it to maximize the value of the Constellation model. Ultimately, effective leadership of the IC will depend upon the will to pursue the mission before all the intelligence has been gathered and to see the mission through until its officers are satisfied that the challenge is being, or has been, met.

IV. Conclusion

Constellation Is Nothing New...But Long Overdue

The concept of fusing the strengths of different components into a hybrid unit is nothing new. We see the technique applied in agriculture through genetic enhancement of crops, in epidemiology through the use of live viruses to create vaccines and in businesses that create project teams under managing partners. Most importantly, however, we see it in the organization of our most treacherous enemies and the most insidious threats to our security.

The establishment of a fluid, flexible array of interagency teams that spans the Intelligence Community would allow the most talented and creative officers the space to depart from their bureaucratic stovepipes and reinvent the IC's approach to the most important intelligence missions. In so doing, America would arm itself with a powerful tool to immediately address threats to national security and would instill within the intelligence officer corps a newfound sense of purpose.

From Stovepipes to a Web: Adapting Intelink's Gated Communities for the Networked World

(b)(3)
(b)(6)

The World Wide Web has given us astonishing communication abilities. We can meet people from across the world that share our interests. We can get news information from thousands of sources, all of it current to the minute. In under a second, a modern search engine like Google can scan billions of documents to find exactly what we're looking for and then make suggestions for related material. Intelink was built to do for the Intelligence Community what the Web has done for the world: electronically connect its members to information and to each other. But ten years after Intelink's inception, finding analysts at other agencies is still a chore. Many of the official assessments on Intelink are outdated soon after publication. Its search engines give users seemingly arbitrary results that have little to do with their search terms. The information management tools used by the Intelligence Community are years behind free technology available to the whole world.

Intelink is managed by layers of technical directors, systems administrators, Web designers and editors. The placement and contents of each document are approved by several people. The network is as neatly organized and regimented as a modern military. You would think that this devotion to order and centralization would make it a more user-friendly version of the Web, which is a tangled mess of pages with no managed method of publication or cooperation. Users can publish anything they want in almost any format they choose, without going through middlemen. They can remove content as quickly as they can publish it. It is anarchy.

But this anything-goes culture is what makes the Web so much more powerful than Intelink. Many analysts agree that the open Web gives them more research power, a more intuitive organization scheme and more communication capabilities than does Intelink. This is unacceptable. If Intelink is to have the advantages of the Web--dynamic, easily located information and a lively, interconnected community--its managers must instill in it the culture that has given the Web these qualities. We must give analysts the same thing that Internet users have: their own personal space on the network, where they are free to write and publish their knowledge, ideas, thoughts and questions to personal home pages. Only then will Intelink begin to benefit from the technical and sociological benefits of the Web.

Intelink's Hierarchical Culture

Intelink's technical standards are appropriately managed to stay up-to-date with the World Wide Web's (which are set by its own standards body, the World Wide Web Consortium). New technologies and programming languages are making information much more manageable, and the Intelink Management Office sees that these are implemented properly by site managers. But adopting the Web's technical standards is not enough. Intelink must embrace the Web's fundamental democracy idea before it can take full advantage of the technologies it implements.

Both Intelink and the open Web are organized into virtual communities of information. Links are the critical pieces that determine which "neighborhood" a page belongs to. On the open Web, contributors freely place links to any page they like. These pages likely have related content, thereby creating a set of links and nodes--a web--connected by common interests. Its chaos is a result of its democratic, decentralized governance: each person with Internet access has a right to publish and link to anything they like. They can belong to as many neighborhoods as they want. They can contribute expert knowledge, learn from others or just watch in silence. The result is the most dynamic community of people and information in the world: an American florist and a Russian gardener can become business partners after meeting through their chess newsgroup. A Canadian photographer learning about snorkeling can give a Jamaican scuba diver advice on underwater cameras.

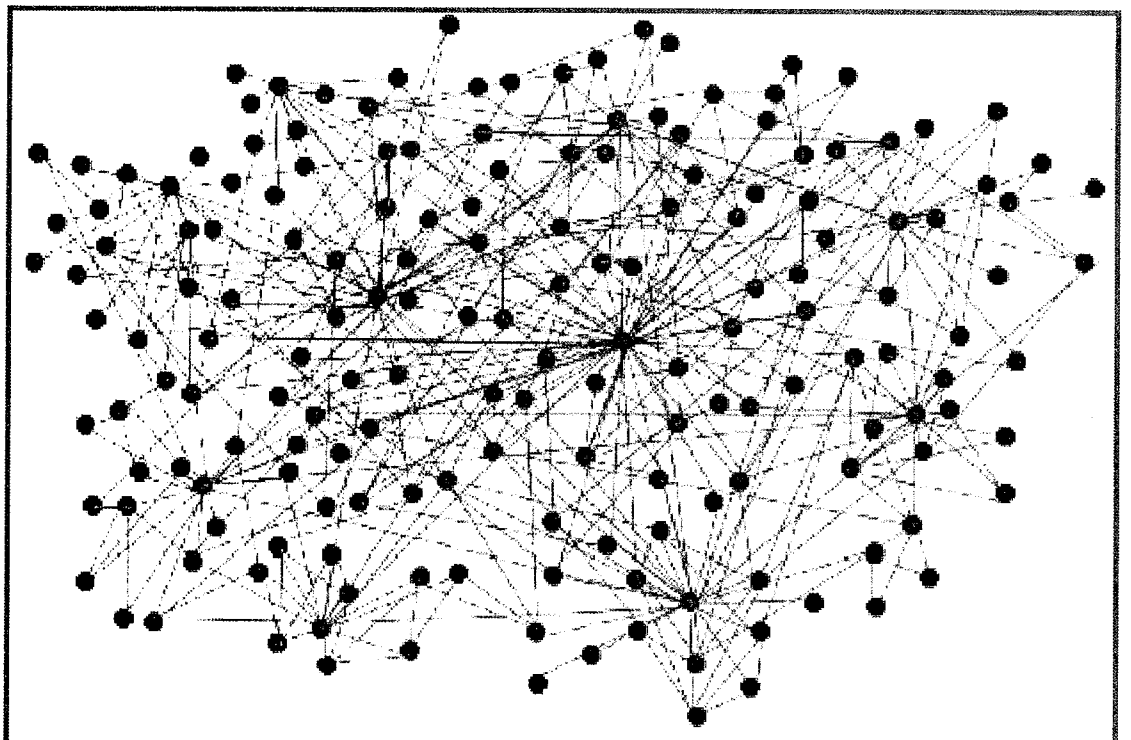


Figure 1: A figurative view of the World Wide Web. Users are allowed to link to any page they want but will naturally build communities of information with similar pages. The better sites receive votes of approval (in the form of links) from many pages.

Intelink, however, is a "branched network." (1) Instead of a web of pages, the network looks similar to the organization charts of the agencies involved. Finished intelligence products are designed, coded and uploaded by nonanalysts unfamiliar with their content and their place within the grander scheme of the Community. The result is a branched network with very few "deep links" that cross agency domains--for instance, a DIA analysis that links to an NSA source document. There might be more physical bridges between DC-area intelligence agencies than there are deep links between their ic.gov domains. So instead of being organized into communities of like content--a terrorism neighborhood, a biological weapons borough, et cetera--Intelink is rigidly divided into sectors of pages seen mainly for the agencies and offices that own them (Figure 2). And the lack of deep links makes them more like several gated communities instead of an urban cultural capital. This practice perpetuates the image of U.S. intelligence as a group of competing agencies instead of a true community of analysts and collectors. But Figure 2 is more than just a symbol of the communication gap. It also has a serious impact on how our computers make sense of data.

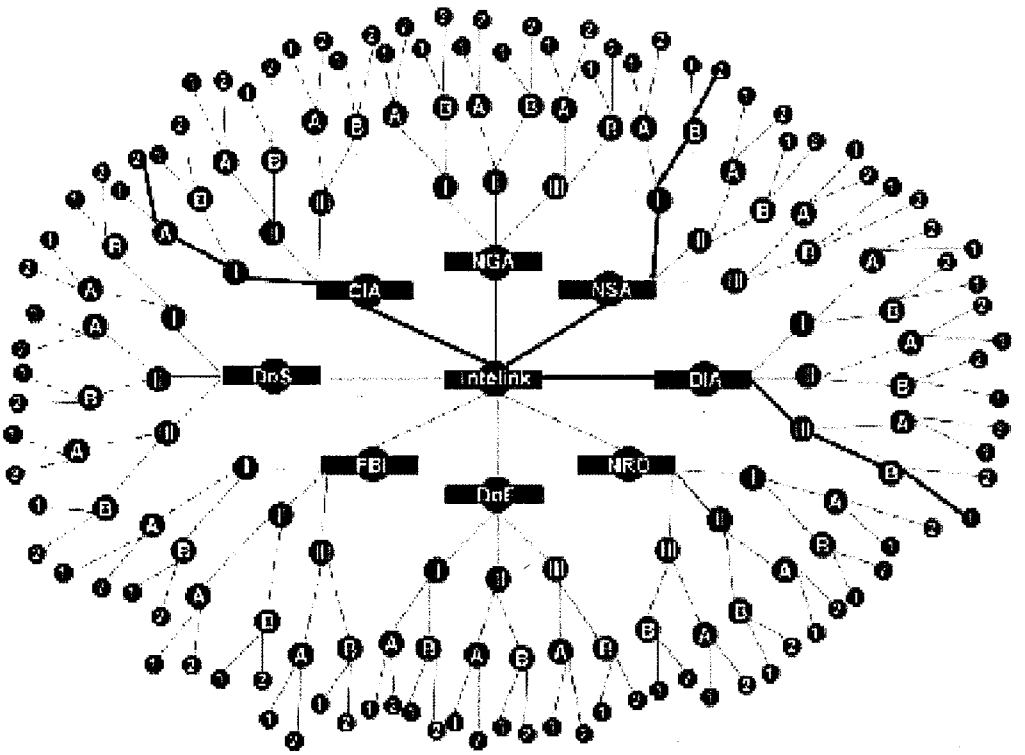


Figure 2: A figurative view of Intelink-SCI. Roman numerals, letters and numbers represent directorates, offices, etc. **Red Lines** show how distant like pages are on Intelink, making it harder for analysts trying to find a page buried deep within a site. It also keeps search engines from building logical communities.

Disconnected Data...

Deep-linking is what gives modern search engines like Google their ability to make sense of the Web and find what you're looking for. Links mean relationships. Modern search engines judge a page's value and relevance to search queries based largely on links. When one page links to another, a search engine's crawler assumes that the two pages have something in common. The number of links to a certain page, the text of the link itself, the words surrounding those links and even the number of times those links are clicked all factor into Google's formula. Try searching for "NRO" on Intelink. You will get the home page of the National Reconnaissance Office as the first hit--not because that's what the page claims to be, but because many other pages on Intelink have "voted" for it by linking the letters "**NRO**" to http://nro.ic.gov.

When the web of pages becomes as complex as the one shown in Figure 1, Google sees each page as a composite of not only its words, but of the words on all of its linked and linking pages as well. On the Web, two communities that might seem completely unrelated can easily find something in common. Inspired by the "six degrees of separation" theory, which hypothesizes that every human on earth is separated by just a few acquaintances, researchers at Notre Dame University found that the "diameter" of the web--the maximum number of clicks to get from any Web page to another--was about 20. (2) Just like people, the closer two pages are to each other, the more they have in common.

The lesson is that once the virtual dots are connected, it becomes much easier to connect logical ones. When an analyst is a few logical steps from solving a terror plot, it helps if his web page knows the web page that knows the web page... But because of Intelink's "gated communities" structure and lack of deep links, its search engines cannot draw relationships between similar reports from different agencies. The link path between them is too long for a search engine to see what they have in common (Figure 2). Computers cannot see the connection between an FBI report on an Arizona flight school and CIA report on student pilots in Florida--a connection that humans can only recognize in hindsight. For the same reason, a DIA document on North Korean nuclear proliferation will have more relevance to DIA's profile of Kim Jong-Il than to NSA's own WMD assessment.

...And Disconnected Analysts

Intelink's structure has social implications as well. Before Google and the World Wide Web, the Internet was used solely as a way for people to directly communicate with each other and among large groups. It cultivated communities that became as close-knit as a suburban neighborhood. This camaraderie is nonexistent on Intelink. Its social culture is decades behind the one available through your home computer. While sociology and

economics professors have projected the Web will mean the end of the nationstate, the borders between Intelligence Community agencies are still strong.

The problems of analyst-to-analyst communication are more tangible than the abstract information theory discussed above. They start with a difficult interface. Finding your way to a page is reminiscent of a maze. It usually involves guesswork as to which links to follow, as there is often only one correct route through many pages. An incorrect guess means retracing your steps.

Sometimes it seems like you're intentionally being sequestered from outside analysts. Unlike World Wide Web pages, which usually offer an easy way to e-mail their authors, most finished intelligence products provide nothing more than an obscure office acronym; sometimes there's a phone number, which may or may not have a name. E-mail addresses are rare. Even then, the address given may be for the agency's internal system, leaving outside analysts frustrated when their e-mails are returned as undeliverable: another dead end in their research. As for online directories, some agencies let you search for analysts by name only, which doesn't help when you're trying to meet new people. Others let you search for obscure office acronyms that have an indecipherable connection to their analytical focus, but rarely does a site let you drill down by regional and functional specialty and pinpoint an expert. After two years at my agency, I still run into new people from across the community that share my focus. When I first realized that there were probably dozens of unknown analysts writing reports on my subject without ever asking for my opinion, they felt like competitors instead of teammates.

What are we achieving by electronically segregating our agencies? Although exaggerated, Figure 2 makes it easy to understand why the entire Intelligence Community has a communication problem. Intelink's pitfalls are most obvious during crises. Scenarios change quickly, meaning that by the time an assessment has gone through the edit and posting process, the information is already outdated. One of the problems with a finished product's Intelink presence is that it *is* "finished." The situation could change drastically in the days, months and years following its posting, but intelligence law requires that the document's content remains the same. Analysts deserve an opportunity to amend their past assessments, and customers should not be relegated to outdated information. A personal home page where an analyst can write thoughts and comments on past assessments and current crises would solve both problems. A bit of self-rule is vital if Intelink is to be as dynamic and agile as the World Wide Web. Our analysts must have a network that opens doors instead of locking them, and one that values an intelligence product for its words, not the agency that owns it.

Your Counterparts, One (Virtual) Cube Over

As an analyst, some of your teammates are in neighboring cubes. You can roll your chairs into circles and discuss breaking news and coming challenges. But most of your

teammates are on opposite sides of the beltway at different agencies. The only way to share your thoughts with the whole group is to meet every several months for a midmorning conference. This does not cultivate teamwork. Daily communication is essential for a cooperative spirit between agencies. The best (but impossible) solution would be to stick your counterparts into the next cube. On the other hand, analysts could build their own online communities if given the chance. All they would need is permission and a few megabytes of server space. Linking their products to source documents, similar analyses and the home pages of their counterparts would let this subcommunity of Intelink evolve into a true web of information, connecting both related data and like-minded analysts.

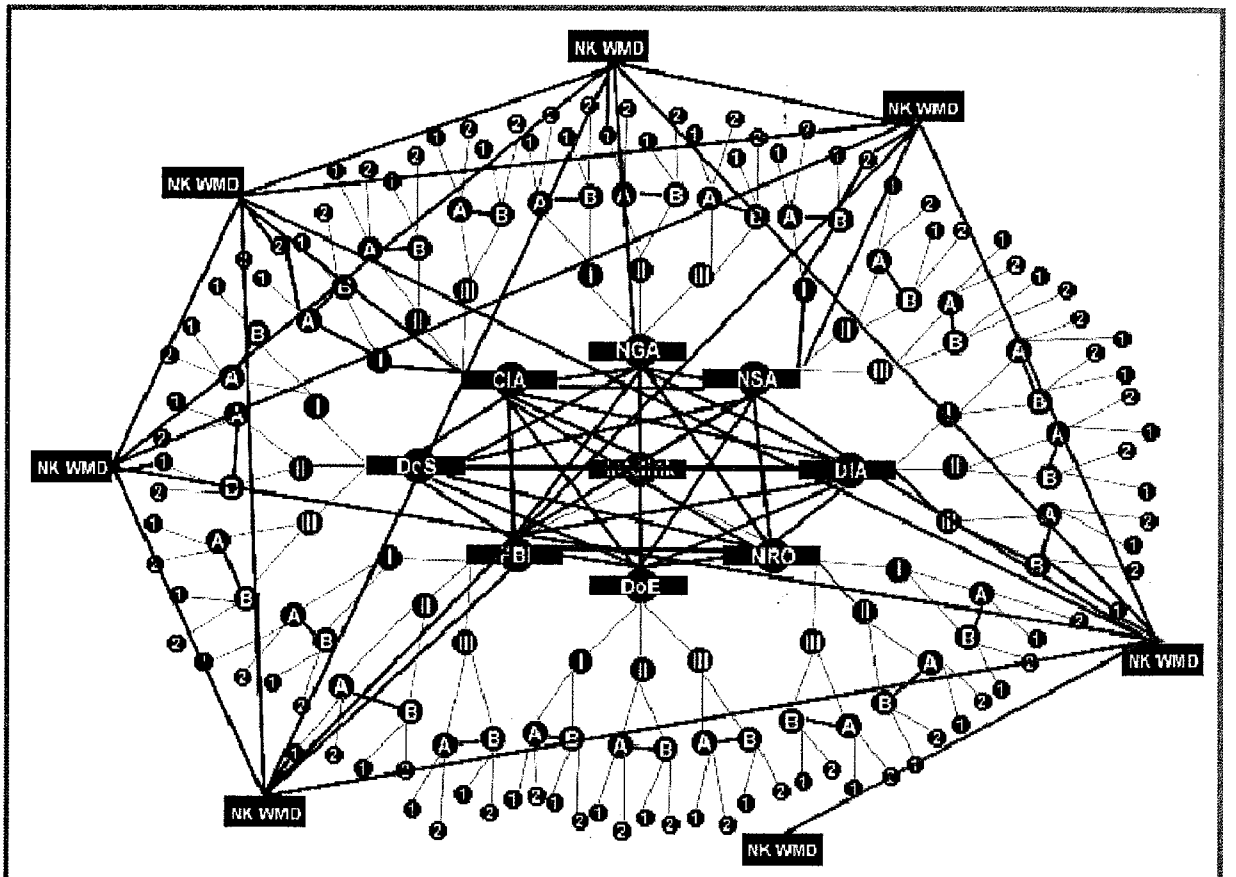


Figure 3: Intelink-SCI with the beginnings of a hypothetical online community. North Korean counterproliferation analysts have developed their own home pages and are now interlinking with counterparts' pages and analyses, making information on the subject easier to find for both humans and search engines. Even with just one link established, analysts at DoE are much closer to dozens of other analysts throughout the community. Agency home pages are also linking to each other.

A fundamental rule of any information management plan is that it will work only if the primary users support it. This is achieved by giving them tools that they're comfortable with and use on a daily basis, and by giving them a bit of control over their information. But past Intelligence Community programs have involved new software, training sessions and thick instruction manuals along with costly layers of codewriters, image editors and web designers. (3) Implementing this proposal would be so cheap and simple, it seems closer to a policy than a project. The infrastructure and staff for an online community already exists. All that is lacking is permission. The average analyst will require only a few megabytes of space, allowing every analyst in the country to store their information on a single Web server (which would ideally be under the control of a neutral body such as the Intelink Management Office). Some agencies already provide HTML editing software to all analysts; for the rest, word processors can easily convert documents into HTML. When the current generation of bloggers and Instant Messagers grow up to become the core of the Analytical Community, a self-publishing capability will not only be expected. It will be their most comfortable form of communication. If given permission to use it, the only thing dividing the Intelligence Community of their day will be the Potomac River.

Endnotes

1. Watts, Duncan. *Six Degrees: The Science of a Connected Age*. New York: W.W. Norton, 2003:39.
2. Albert, Réka, Hawoong Jeong and Albert-László Barabási. "Diameter of the World Wide Web."*Nature*. September 9, 1999, Volume 401: 130-131.
3. Martin, Fredrick. *Top Secret Intranet: How U.S. Intelligence Built Intelink--The World's Largest, Most Secure Network*. Upper Saddle River, NJ: Prentice-Hall, 1999.

Intelligence Information System Audit Log Analysis: Transforming IC Mission Performance and Collection Evaluation Processes

(b)(3)
(b)(6)

Executive Summary

Exploiting auditing software in intelligence information systems (IISs) can multiply the productivity of Intelligence Community (IC) decisionmakers and dramatically change the way the IC does business. Audit log software captures detailed information about analyst-document transactions in the IIS—in effect converting the IIS into an automated transaction processing system (ATPS). When combined with analyst demographic data and document metadata in the IIS, audit log data can generate a host of new performance metrics of value to operations, planning, programming and budget personnel throughout the IC. Because audit log data is objective, behavioral data generated by analysts in their daily work process about the value of documents in the IIS, it can be used directly in resource allocation processes—unlike subjective opinion survey and value scale rating data. Widespread availability of audit log metrics opens the door to greater use of modern quantitative management techniques, including benefit/cost analysis, operations research and mathematical optimization approaches developed since World War II for addressing resource allocation and investment decision problems. Use of audit log metrics in the IC should expand dramatically because of their high value and low cost. CIA's ongoing audit log pilot project has already established the feasibility and practicality of such applications to intelligence problems. Similar opportunities abound within the IC and the Community Management Staff. This paper outlines the benefits to be derived from IISs through the use of audit log software. These benefits are real and substantial as demonstrated in CIA's pilot audit log program. Together, the audit log technology and its applications constitute a paradigm shift, a major change in collection evaluation, resource allocation and future investment activities in the IC.

The Transformative Power Of Audit Log Data

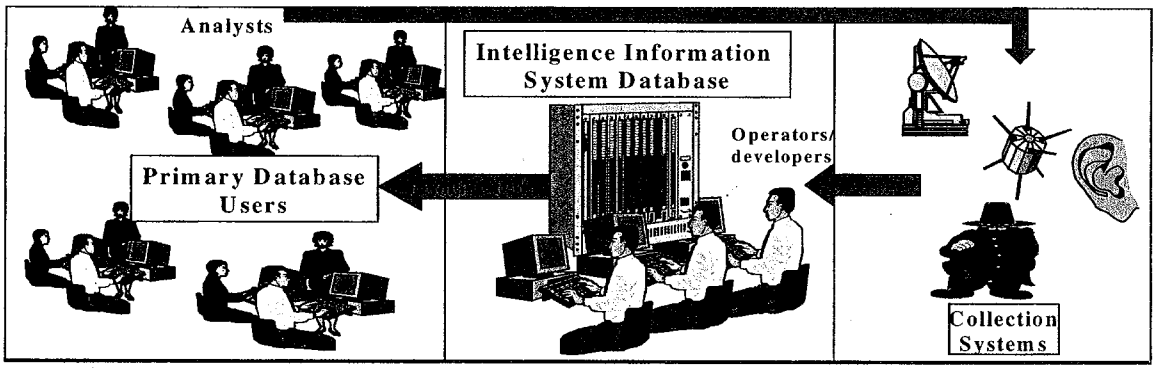
Security auditing software can transform an IIS into an automated transaction processing system (ATPS). (See box below.) A product of the information technology revolution of the 1990s, ATPSs have been rapidly proliferating in the private sector and provide a model for the application of audit log analysis to IISs. Figure 1 shows a typical IIS, with the collection systems that provide the data, and the intelligence analysts who use it. The green line from the analysts to the collection systems indicates direct feedback from analysts to collectors about information needs and collection

requirements. This figure illustrates the intelligence cycle in which analysts review IIS information, refine their information needs and provide feedback to the collectors who adjust their activities accordingly. The information flow focuses on substantive intelligence problems, including plans, intentions, actions and activities of key world political figures and their countries.

Automated Transaction Processing Systems (ATPS)
Icons of the Information Technology Revolution

ATPSs have become ubiquitous in American commercial society. Supermarket ATPSs capture essential data about a customer's interaction at the checkout counter: number of items, amounts, prices, supplier names, customer and sales person identities, payment methods, discounts, etc. This information is stored and forwarded to corporate data warehouses where it is analyzed for a multitude of purposes—inventory control, product mix and profitability studies, assessing advertising program effectiveness, new product features evaluation and design, pricing policy, market segmentation, etc. Similarly, ATPSs in hospitals, libraries and salesrooms capture essential information about products and services provided at the level of individual transactions. ATPSs have not seen widespread application in the Intelligence Community, but their application has the potential to substantially change the way the IC does business.

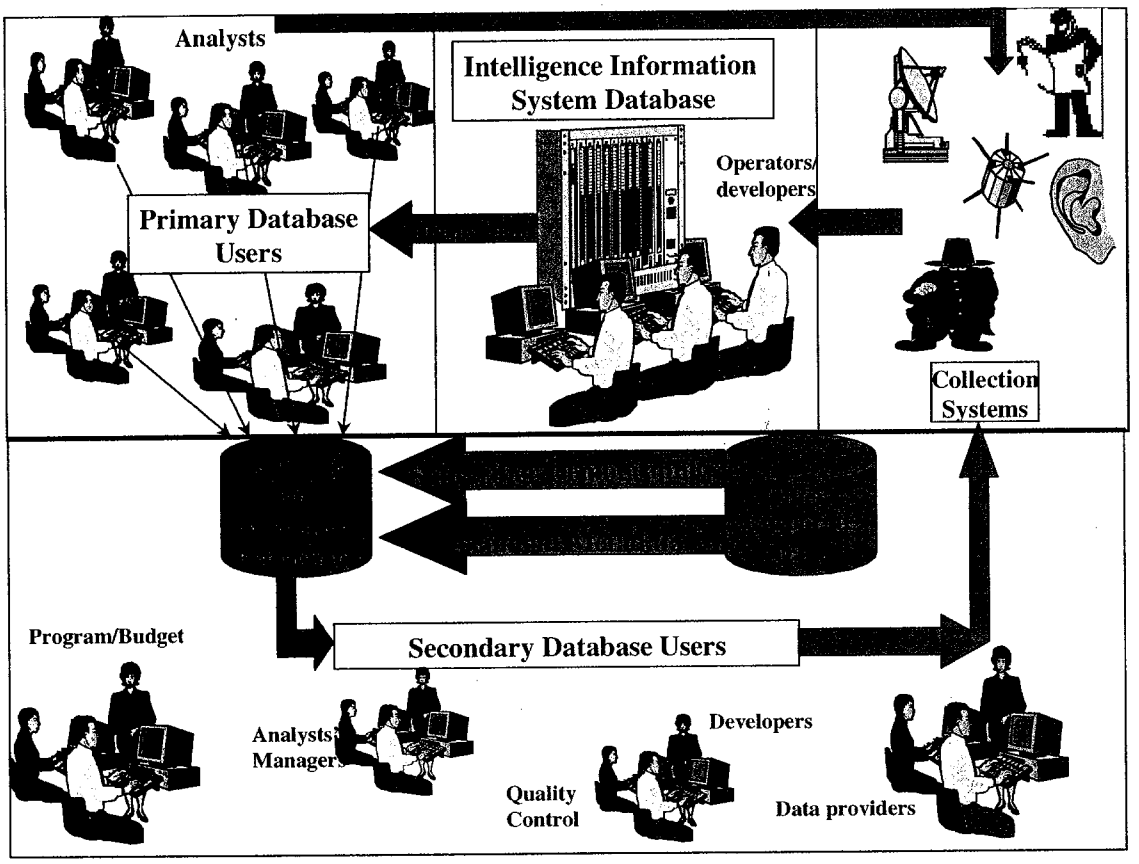
Figure 1: IIS Showing Collectors and Primary Database Users



ATPSs Create High Value Data For Entirely New Customers

Figure 2 shows the operation of same IIS but with audit log data analysis fully integrated as part of the overall system. The audit log software creates data that can generate objective metrics on intelligence issue support and collection performance. The audit log software automatically monitors and records individual analyst transactions

Figure 2: IIS Showing New Class of Customers Exploiting Audit Log Data



with the documents in the IIS. Transaction records are date/time stamped and include information about the analyst, the document and the document actions taken by the analyst.[1] Figure 2 also shows audit log data--combined with analyst demographics[2] and document metadata[3]--going to an entirely different set of "secondary" database customers including operators, managers, planning, programming and budget personnel of both database subscribers and data providers. The information flow depicts *analysts' use of the data* in the IIS. This information flow constitutes an additional feedback loop from analysts to collectors.

[1] Audit log records contain the user name, document identifier, type of user-document transaction and the date/time of the analyst transaction on the document.
[2] Including user office/team, intelligence issue, analytic specialization, grade and years of experience.
[3] Including collection agency, collector type, document originator, publication date, date of receipt by the IIS; classification and document length.

Intelligence Value Metrics Available From ATPS Data

Because an intelligence analyst's time is at a premium, the time expended, the number and type of transactions he/she makes with an IIS document reflects the value of that document. The number of transactions an analyst makes on a document correlates strongly with the likelihood he/she will cite it in finished intelligence. Audit log metrics are available for every analyst and every intelligence report in the IIS and can be used to derive a measure of the intelligence value for each report. Unlike most collection metrics that measure only the quantity of reports generated by a collector, the audit log metric identifies and counts those reports that are highly valued and identifies the analysts who benefited from those reports. Other metrics of interest include (a) two measures of document display time, (b) number of documents saved, (c) total number of analyst transactions—including send, export, print or annotate transactions, and (d) the number of revisits to a document. Averages per document, analyst, analytic group or time period may also be of interest.

Why Audit Log Data Is So Valuable

Audit log data is highly valuable because of its distinctive characteristics and attributes:

- Audit log data extraction is non-intrusive, it does not interfere with analysts' daily work processes, and it is inexpensive to generate compared to other evaluation methods.
- Audit log data is objective, behavioral and customer-generated. Customer based, "value-of-output" measures like those derived from audit log data are the "holy grail" of program/budget analysis and resource allocation processes. Audit log data provides a solid basis for estimating document use, value, quantity and timeliness from individual data providers.
- Audit log data has numerical qualities that permit mathematical operations essential to program/budget and resource allocation decisions. Unlike ordinal subjective, categorical assessments, audit log data can be used directly in benefit/cost and resource allocation calculations, in contrast to opinion survey data that merely "informs" resource allocation decisions.
- Audit log data is voluminous[4] and readily available for every issue, analyst and

Intelligence Collection Evaluation Has Traditionally Relied on Subjective Opinion Data of Limited Value to Decisionmakers

Intelligence collection evaluation efforts have traditionally centered on labor-intensive, intrusive surveys, questionnaires, focus groups and interviews which tend to provide subjective, anecdotal evidence or categorical ratings of system use, value, timeliness and responsiveness to requirements. These methods rely primarily on analyst memory or on impressions of what was relevant. The rating scales employed are highly non-linear which severely limits their use in cost-benefit, resource allocation or investment decision processes.

(b)(3)
(b)(6)

document associated with the IIS. Timely document-by-document value metrics present new opportunities for collectors to improve their responsiveness to customer information needs and a new opportunity to reduce the intelligence requirements-to-reporting cycle time.

Audit log systems can now provide metrics and market research data to the IC that have traditionally been available only to industry and commercial enterprises, including:

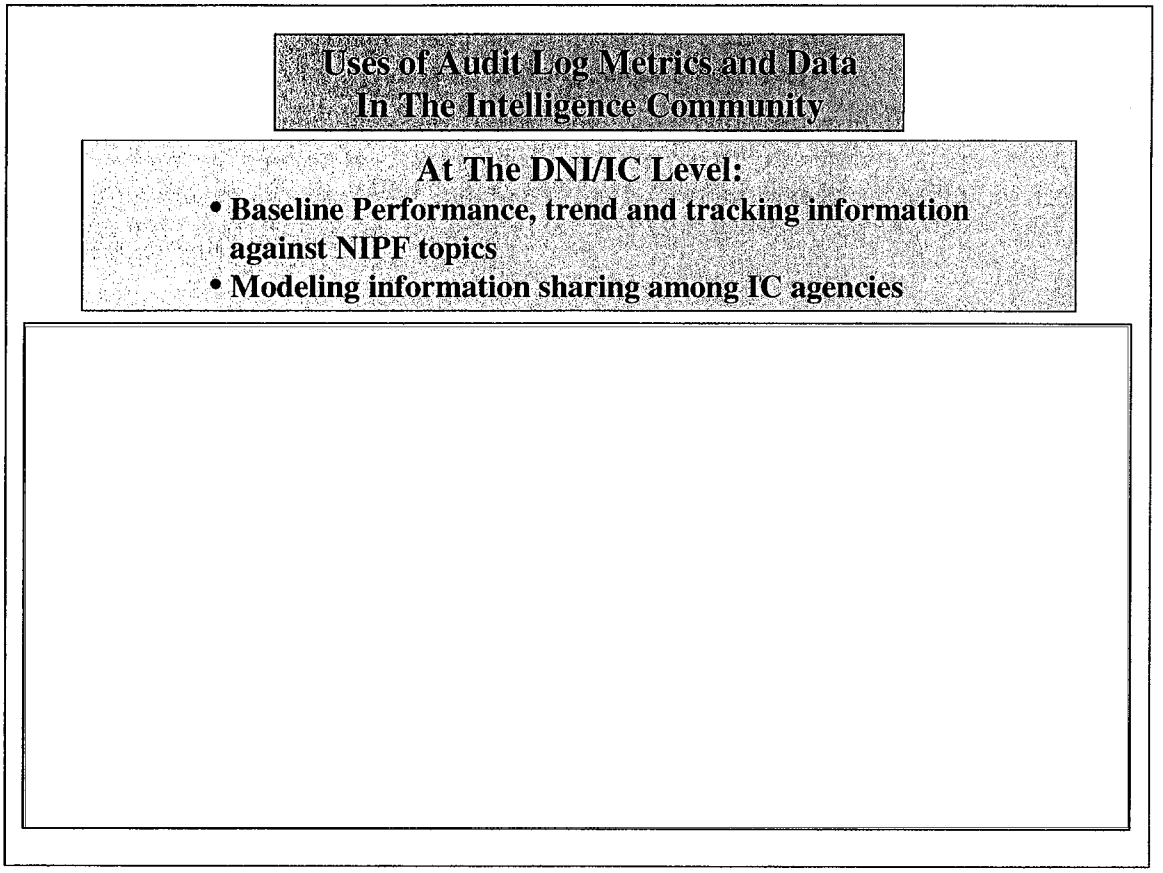
- Which groups of customers are using the IIS and data from specific providers?
- When and for how long are they are using the IIS and each of its intelligence reports?
- What they are using the intelligence reports for?
- Which intelligence reports are most valuable?
- Which intelligence reports have very low usage or are not being accessed at all?

Audit log records represent a key untapped resource for increasing collector and decision-maker productivity without presenting an additional workload for intelligence analysts. IT program managers, intelligence collection managers and senior intelligence officials who gain experience in the use of this data will find it increasingly useful to support decisionmaking on mission and collection performance, collection system utilization and general resource allocation. For many purposes, audit log data can supplant labor-intensive, questionnaire-based evaluation methods. Substituting audit log analysis for these evaluation methods, where possible, can improve the productivity of the analytic workforce.

Uses Of Audit Log Metrics And Data

As shown in Figure 3, audit log data has a number of applications important to the Intelligence Community at multiple levels.

Figure 3: Uses of Audit Log Metrics and Data in the IC



(b)(3)
(b)(6)

At the DCI/IC level **these applications include:**

- **Performance baseline, trend and tracking information** on Intelligence Issue and National Intelligence Priorities Framework (NIPF) mission accomplishment. (See Figure 4 for one of many audit log metrics that can be used as baseline information.)
- **Modeling the effectiveness of information sharing programs/**policies among agencies. A comprehensive audit log database could provide an objective basis for assessing the effectiveness of information sharing and policy/legal compliance.

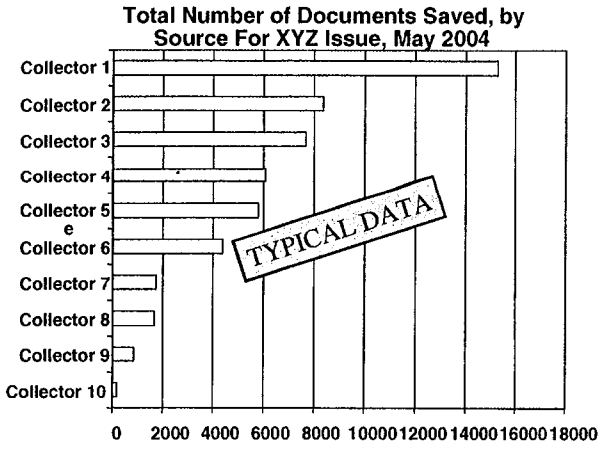


Figure 4: Baseline Example

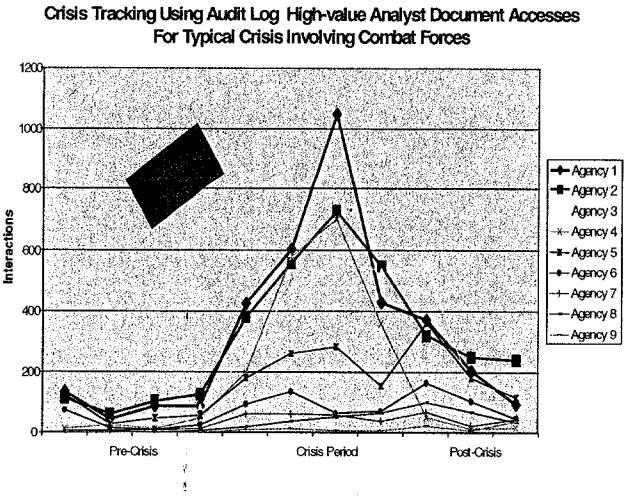


Figure 5: Trend/Tracking

At the Agency/Collector Level, audit log analysis has a large number of applications, including:

- **Baseline, trend and tracking information** on the quality, quantity and timeliness of collection agency support to NIPF mission areas and intelligence analysts working those issues. (See Figure 5 above for an example of tracking the number of high value analyst/document accesses over time for a typical crisis.) Audit records can be analyzed for long or short time periods to discern trends, look for anomalies in usage patterns or focus on a unique series of reports or documents. Audit log analysis can also provide collectors with insight into source productivity, product use and value and changes over time—especially during surge efforts and periods of crisis. Audit log analysis of IIS audit records during international conflicts, for example, can be used to assess peaks or declines in usage as well as peaks or declines in reporting.
- **Generation of timely feedback to data providers** about analyst utilization and value of their products on a report-by-report basis. If provided daily, audit log data could significantly reduce the intelligence cycle time and improve collector responsiveness to requirements. Audit log record analysis can likewise be targeted to specific intelligence producers, categories of documents and groups of users. Specialized reporting for clearly defined time periods can also be subjected to audit log analyses. Such analyses would allow producers to focus on potential problem reporting areas and initiate corrective actions in a timely manner. For high volume intelligence collectors, such as open source, with a wide array of sources, audit log data may, for the first time, provide objective measures of the value of their products to their users. This information could greatly enhance the ability of high volume collectors to focus on customer needs, reduce marginal and unread reporting and enhance their responsiveness to customer requirements.

- **Market research data** characterizing the customer base to database providers in terms of numbers of analysts, their intelligence specialization, issue affiliation and degree of interest in their reporting.
- **Determining which IIS reports are not used** by any analyst. Audit log data permits documents not accessed by any IIS user to be easily identified and called to the attention of the data provider. The percent not used is an important measure of collector performance. (See Figure 6.)
- **Estimating analyst workload** devoted to information search, retrieval and review functions on data in the IIS.
- **Hypothesis Testing:** Audit records can be seen as a vast new source of objective data with which to test hypotheses, myths, conventional wisdom and commonly asked questions about many aspects of the intelligence enterprise. Using appropriate aggregate statistical techniques[5], audit log records can be used for: assessing the relative value of different product lines, the relative importance of different sources, the productivity of different production processes and detecting changes and trends over time. Audit log analysis can provide valuable data to intelligence collectors seeking to assess the impact of their products. For example, are analysts reading their products and, if so, which ones? Does the reporting appear to be of value to the users? This information can be critical to intelligence-production organizations facing serious resource constraints in meeting their responsibilities.

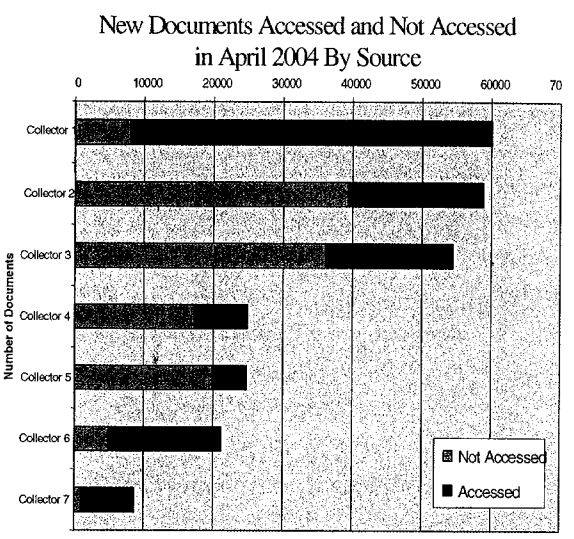


Figure 6 Documents Not Used Analysis

- **Enabling benefit/cost methods:** Perhaps the most important application of audit log data is enabling greater use of benefit-cost methods in IC decision making and investment analysis regarding future collection and processing systems. For example, the value metrics available in audit log data can be combined with incremental cost data to generate a set of "willingness to pay" guidelines for use in evaluating alternative investments in future collection systems, collection architectures and system expansion/improvement alternatives. Audit log metrics can play an important role in anchoring subjective intelligence value judgments elicited in decision conferences for building integrated, cost effective intelligence, surveillance and reconnaissance programs. The abundance of objective intelligence value metrics from audit log data should also facilitate increased use of decision-analysis and operations research methods in the IC.

[5] Chi-squared analysis, regression analysis, analysis of variance and covariance, dynamic modeling and other data analysis techniques.

Audit Log Data Security

The utility of audit log data ultimately relies on the data security procedures employed by the audit log project managers. A well-designed and executed security plan that addresses audit log data usage, data storage and the types of manipulative strategies that will be employed is critical to the success of any audit log data analysis program. One key element of any security plan is identity protection. IIS audit log data normally contain sensitive user identification data, that should be sanitized by substituting numbers or codes for true analyst names. Audit log data on individual users should never be released to managers or supervisors for individual user evaluation or for performance assessment purposes. Such actions would carry the inherent risk of creating a marked change in analyst behavior that could severely compromise audit data integrity.

CIA's Pilot Project --Pioneering ATPS Application In The Intelligence Community

(b)(3)
(b)(6)

(b)(3)
(b)(6)

Future Applications Of CIA's Audit Log Project

(b)(3)
(b)(6)

- **Analyst Training**

(b)(3)
(b)(6)

substantial delays. Audit log data can be used to assess the relative value of sources cited in finished intelligence, important because cited intelligence documents differ significantly in value and are often used for the partial or incomplete information they contain.

ATPS Potential Applications In The Intelligence Community And Homeland Security

(b)(3)
(b)(6)

- ***The Community Management Staff Should Establish Audit Log Standards for the IC.*** Because ATPS applications are in their infancy in the IC, the Community Management Staff should take the lead in establishing minimum audit log application software standards. This would encompass the use of robust and flexible auditing software in existing as well as new IISs within the IC. Without IC-wide standards, many of the benefits of audit applications outlined below will not be fully realized because of data incompatibilities. Auditing software, carefully designed, integrated and tested to IC standards, will provide maximum value to senior IC leaders.
- ***The Community Management Staff should propose an IC-wide audit initiative to facilitate the rapid exploitation of security auditing software as a way to improve IC decisionmaking and the productivity of IC IISs.*** Not all IISs will merit the investment, but for those larger systems that do, it would be reasonable to expect significant improvements in the responsiveness of collectors to all-source analysts' needs as well as the effectiveness and efficiency of collection systems. Audit log initiatives at NSA and NGA, for example, would provide objective measures of the utilization, value and timeliness of products generated by their systems. Audit log initiatives for IMAGERY, SIGINT and HUMINT should be seriously considered.
- ***The Community Management Staff should establish an IC-wide database consisting of the audit log data from every all-source analyst in the IC.*** Such a database would enable collection evaluation and feedback data to collectors from the totality of all-source analysts in the IC and would be extremely valuable to collection managers, program developers and resource allocation/investment decision personnel. The widespread use of such a database to support program initiatives and budget requests would be expected to increase the objectivity of intelligence decisionmaking and resource allocation processes while de-emphasizing the role of organizational politics.
- ***The Community Management Staff should establish a government-wide database of audit log data on policymakers' use of finished intelligence reporting from all-***

source analysts. Audit log records from finished intelligence reporting delivered electronically to policymakers and intelligence consumers would be of continuing interest to issue managers and all-source analysts.

- ***The Community Management Staff should establish a pilot initiative to use IC audit log data in the production of long-term Strategic IC Studies.*** Often criticized for its lack of long-term historical, and strategic, future-oriented analyses, the IC could benefit from the integration of audit log record databases from key agencies for the production of large-scale cooperative studies. Such studies could provide the basis for a "big picture" look at information flow, information usage and the value of the reporting to various analytical units within the IC. It is conceivable these studies could also provide an objective basis for future changes to improve IC information handling, sharing, analysis and the IC organizational structure.

Audit Log Applications For Homeland Security

Audit log analysis has significant applications for information systems deployed to enhance homeland security and improve the effectiveness of US defenses against the threat of terrorism. With the current emphasis on increased information sharing for Department of Homeland Security (DHS) based networks--including the Federal Bureau of Investigation (FBI) and other key Federal agencies--a robust audit log data analysis program could provide valuable insights into overall system usage patterns. Given the wide variety of data available to DHS--including databases, media reporting, analysis, mapping/imagery and the large number of data recipients (state, regional, local and selected private-sector organizations)--a proactive audit log program would facilitate selective targeting of key user populations to ascertain the value of online offerings. Audit Log analysis for a variety of homeland security systems would be particularly beneficial in view of difficulties inherent in (a) conducting valid survey or questionnaire studies (which may often have marginal response rates), and (b) accurately polling the diverse and geographically dispersed customer population for homeland security information. Audit log analysis would generate data on the value of publications and reporting, as well as provide a validated methodology for testing the usefulness and value of new or modified offerings with selected user groups. Newly proposed homeland security systems or those undergoing substantial hardware/software upgrades should be designed and deployed with enhanced auditing capabilities. To be effective, homeland security information must be accurately and effectively disseminated to those at the state, regional, local and private sector organizations who are best equipped to act upon it. Audit log data analysis for homeland security information systems could provide system administrators and senior-level agency managers and policymakers with the same types of usage and customer transaction data available through [redacted]

(b)(3)
(b)(6)

Conclusion

Use of audit log record analysis, as outlined in this paper, represents a new opportunity for IC agencies to take full advantage of rapidly accelerating advances in computer technology. The benefits of this methodology are real and substantial as demonstrated in the CIA pilot project. Audit log analysis and its associated applications will result in a clear paradigm shift sparked by what we believe to be a technologically innovative approach to collection evaluation, resource allocation and future investment activities in the IC. The wide variety of information systems in the IC will provide a unique test bed to further validate this methodology and to expand the technology on which it is based. While we recognize that changes of this magnitude in large organizations often occur slowly over time, we look forward to future Community-wide initiatives that will provide the resources and the high level visibility to begin to foster the development of IC prototype efforts that can be transitioned into production level mainstream programs.

Rethinking Analytic Tradecraft

By a CIA [redacted] Officer, serving undercover overseas

I. Proactive National Security

Current foreign policy exigencies and national security threats mandate a review of US intelligence analysis, procedures, and objectives. Today's concerns are markedly different than those that faced many senior policymakers when they were working at the functional levels within the Intelligence Community (IC) or the broader United States Government (USG). Developing, deploying, and exploiting technical means to monitor known or suspected activities by specific adversaries — often with predictable modus operandi — are very different than global threat and warning coverage against asymmetric threats and heretofore unknown entities. For example, tracking a specific Soviet "boomer" submarine is very different than trying to determine if a violent, anti-American cell is forming in a basement somewhere in the world, communicating via the Internet or transferring economic value through intangible and untraceable means.

In short, the international security playing field has changed; so must our team and its game plan. The 1980 United States (US) gold-medal ice hockey squad probably would not win this year's Wimbledon tournament. Those decisionmakers who trained with slide rulers or studied communism may not be the best suited to assess tactical operations in a world of microprocessors or events in the Horn of Africa; rather, their intellect and foreign relations experience should be leveraged in concert with the relevant, contemporary knowledge of their highly-qualified subordinates. Regardless of the epithet used (e.g., "group think", received wisdom, tradecraft, tradition, standard operating procedures, etc.), just because the USG did it that way yesterday does not imply that it is the best plan for today.

While no USG component can be appropriately blamed for wholesale nonfeasance or malfeasance in connection with the tragedy of 11 September 2001 (9/11), some lessons can be learned from that harrowing experience. The Federal Bureau of Investigation (FBI) was not trained or mandated to conduct ex ante intelligence collection on foreign nationals or US persons. The FBI's expertise lay in post hoc, investigative skills that were second to none, but the law forbade them from being employed without court orders or probable cause — or possibly the lesser legal requirement of reasonable suspicion — that a crime had been committed or was imminent. Central Intelligence Agency (CIA) and National Security Agency (NSA) officers, on the other hand, had strict prohibitions against collecting information about or studying US persons and purely domestic activities. In essence, the al-Qa'ida operatives training in the US could not legally be monitored by any USG intelligence or law enforcement entity prior to 9/11.

Some of those shortcomings have been rectified by the Patriot Act, and others are sure to be remedied as a result of the 9/11 Commission's report and Congress's intelligence reform bill. But those findings and their subsequent impacts will not be realized for years to come. Reorganizing, funding, staffing, training, and mobilizing a new national or homeland security apparatus will take years. Perhaps by 2007 or 2008, the recommendations of the 9/11 Commission will be fully implemented and functioning. Is one to believe that the international security playing field will not have changed again before that time? With what certainty can Congress say that the terrorist threat will be the primary security concern in 2010? By the time the US retroactively prepares to meet the exigencies of 2001, the game will likely have changed again ... and the USG will be "ready" to react once again (i.e., our revamped Wimbledon players will march onto the pitch for a World Cup soccer game).

The last three years' experiences have shown one thing clearly: the USG is reactive in its national security posture and thinking. The current IC structure is the result of the National Security Act of 1947 and the Central Intelligence Act of 1949 that were passed in the aftermath of World War II as a reaction to the Japanese attack on Pearl Harbor. The future IC structure will be the result of new policies or statutes adopted in the aftermath of 9/11 as a reaction to al-Qa'ida. Why does it take a new catastrophe for the IC to contemplate and guard against such new threats? Is it a lack of intellectual creativity or stifling bureaucratic hierarchies that prevent proactive national defense? (By proactive national defense, let it be understood that this author does not refer to preemptive military strikes, but to intelligence and security measures that safeguard against the next rather than the last threat.) Why not start preparing for the unforeseen exigencies of 2010 today?

Clearly the IC and the defense establishment have a long way to go in reinventing themselves to be one step ahead of the next adversary. If the patriotic sacrifices and selfless determination of our public servants in and out of uniform are a testament to this nation's resourcefulness and capabilities, however, then there is no doubt that the necessary objectives could be accomplished — provided that the IC's sights are pointed in the right direction.

Such a transformation of the US security posture will require a new approach to intelligence analysis as well as an attenuation of the American time horizon for foreign policy and intelligence planning. Too much emphasis is placed on yesterday's failure, the next Gallup poll, tomorrow's press briefing, and daily fluctuations of the Dow Jones. Most Americans only think in terms of 90-day fiscal quarters, and US politicians rarely look beyond the next presidential election. Such cultural (i.e., social, economic, and political) limitations poorly suit a nation that is embroiled in strategic competition with

adversaries whose time horizons transcend future, or even past, generations and centuries.[1]

II. Getting It Right

In order to maintain US hegemony in the global arena, the IC must systematically embrace change, maintain a proactive posture, and reward foresight. First and foremost amongst the necessary changes is developing a professional culture that values rectitude above procedure. As open public discussions have illustrated, recent assessments about (a) the existence of weapons of mass destruction (WMD) in Iraq, (b) the imminence of nuclear conflict between India and Pakistan in late 2002, and (c) the gravity or nature of al-Qa'ida plots against US interests in 2001 all proved wanting. The first two issues are Boolean in nature and logically exposed to verification or falsification. The third proposition is more complicated, but one can presume that few would argue the IC got 9/11 "right."

Received wisdom in the CIA's Directorate of Intelligence (DI) is that it is acceptable to get the wrong answer for the right reasons. In other words, analysts are not at fault if established tradecraft procedures and available intelligence reporting lead to inaccurate assessments. The predominant focus in the DI is placed on official chains of review, inter-office coordination, templates for analytic products, institutional writing style, etc. In this author's humble opinion, nothing could be more wrong. The American public does not pay its intelligence analysts to follow any pre-ordained playbook. Nor does it care how many supervisors review an assessment or what rank those reviewers hold. In many cases, additional reviewers are only farther removed from both the analytic details and the kind of atmospherics that cannot be articulated, but which lead to useful analytic judgments.[2]
What the taxpayers care about is whether or not the IC gets it right. That begs two questions: (1) "How often is it possible to get intelligence questions right?" and (2)

---

1 For two examples of this cognitive incongruity, consider (i) the lack of inflective tenses in the Chinese language and that nation's historically irredentist foreign policies, and (ii) the way in which many Arabic males define themselves in terms of their progeny — using the moniker "Abu" — as compared to the Western patronymics that are so prevalent in America and Europe.

2 For example, in order for IC managers to substantively review an intelligence assessment, they need to know everything that the primary analysts read and did not read over the last few years. What they chose not to include in the paper could be as important as what they did include. In fact, omitted reports that may never be read by any manager could run counter to the thesis of any assessment. Second guessing the people with the deepest knowledge on a topic can be dangerous. It leads to "group think" and static judgments. Of course, mentoring and teamwork play a role in developing good intelligence analysts, but the DI needs to trust its talented employees — or else hire different employees whom it is willing to trust. Further discussion under Section III entitled "Analytic Accountability" will assuage concerns about very inexperienced analysts being given too much authority.

"What methods lead to the most accurate results?" On the first point, the public must understand that intelligence analysis is an art and not a perfect science. It deals with (a) refining past or present truth from limited, conflicting, and often deceptive data, usually without the opportunity to perform controlled experiments or measurements, and (b) making predictions about the future.[3] More realistic expectations — coupled with vigilant efforts to produce ever-improving assessment capabilities — would go a long way towards helping policymakers use intelligence wisely.

Switching to the second question regarding analytic methodologies, it does not matter how you get the right answer, but it does matter if you do not get the right answer. Indeed, the exact inverse of the DI's approach holds true. Neither the White House nor the American public would complain if the CIA consistently and accurately predicted future world events with a crystal ball, yet they do complain when all of the DI's formal tradecraft procedures produce critical, wrong answers.

Clearly, a preoccupation with process turns the question upside down. Why not focus on results? Does one deposit one's retirement savings with an investment manager who promises to follow certain research methods, or with the one who has consistently achieved the highest return for his investors? Does one even ask what analytic methods the several brokerage houses' analysts use? No, most people look for a track record of success. By eliminating attribution, and hence accountability, on most products, the DI has lost its ability to monitor the most important metric of all, namely who is getting it right?

What the DI really needs is a way to determine what methods or individuals produce the most accurate assessments or predictions over time. Some commentators would counter that that is exactly what established DI methodologies are: tried and true ways of getting the most accurate intelligence assessments possible. Unfortunately, not only is the current track record for those methods unsatisfactory, but the "paths not taken" are rarely, if ever, recorded for comparison in a post hoc review. Nearly always, resource and time limitations lead to a single course of action being selected, with all competing operations proposals or analytic approaches being sidelined and eventually forgotten. Comparative statistics do not work, or even exist, in the DI's monopoly environment.[4]

---

3 Perhaps .300 is a good batting average in the intelligence game, just like in baseball. Boolean questions would obviously demand a better than .500 average that could be achieved through random guessing; however, issues such as "Approximate the date for a possible coup in country X within one month" may not lend themselves to very high success rates but may nonetheless be critically important to US policymakers.

4 Several interesting CIA programs exist — such as red-cell analysis and the Strategic Assessments Group in the DI's Office of Transnational Issues — which try to provide avenues for counter-culture viewpoints or subject matters that are "over the horizon." This author lauds those initiatives and proposes that such strategic and "outside-the-box" thinking be incorporated into mainstream DI intelligence assessments.

Disagreements over substantive assessments should be resolved in favor of those with the best record for accuracy, not based on seniority, political will or other procedural machinations. In certain instances (e.g., computer hacker events), a 23 year-old analyst just may have more apposite knowledge than the DCI himself. Reviewers can help ask the right questions and improve analysis, but they should not trump analytic judgments regarding fields in which they are not pertinent intelligence experts at that time. Analytic expertise stems from proximity to the first-order data and a proven ability to grasp and accurately predict substantive developments in that field.[5]

The rampant conflation of substance and process is the DI's greatest woe. Most of a new DI officer's analytic training covers computer databases, templates and formats, writing styles, chains of review, organizational diagrams, interagency communications, and the President's Daily Brief (PDB) process; in lieu of logic, decision and game theory, rational choice modeling, probability, statistics, Bayesian reasoning, human psychology, and other heuristic methods for turning incomplete information into probabilistic inferences. Today's world does not produce many bright line rules and red flag intelligence reports. IC analysts should be trained to leverage the most rigorous epistemological tools for augmenting human inference (i.e., deduction, induction, and abduction) in order to analyze today's intelligence problems.[6]

III. Analytic Accountability

Placing an increased focus on getting it right will entail more of an onus on junior officers to respectfully engage reviewers on issues of substantive concern. For example, many IC assessments sink to the least common denominator of agreement amongst all coordinating parties and are caveated into uselessness by the ambiguous words "could," "may," "might" or "possible." As the intelligence analysts responsible for a portfolio, and most intimately familiar with the current all-source reporting, those individuals have an obligation to resist substantive claims that they disagree with — even if there is not "smoking gun" evidence to prove their belief. Too often junior analysts themselves equate lack of experience or rank with lack of relevant knowledge. Too often they quietly defer to senior administrators or operational colleagues who claim a monopoly on

5 Some commentators might contend that intelligence analysis does not or should not involve predictive inference. This author would refer those critics to the overwhelming prevalence of terms such as "likely," "possibly," and "probably" in most DI products. The questions "What happened yesterday?", "What is happening today?", and "What [in your expert opinion] will happen tomorrow?" are inextricably linked in the intelligence profession. Pericles queried the oracle at Delphi; the President of the US turns to the IC.

6 To give just one recent example, the logical distinction between implications and biconditionals was apparently lost on policymakers when certain "evidence" of nuclear weapons development in Iraq surfaced. The identification of dual-use technologies that were necessary but not sufficient for WMD production was somehow misconstrued (i.e., a logical proposition does not always imply its converse).

wisdom through either past experience or compartmented information. In the end, though, all-source intelligence analysis is a unique profession with its own purpose, duties, and required skill sets that are not fungible. Ignoring that link, or trying to replace that specialist with a reports officer or manager, only weakens the entire intelligence chain.

The other side of that matter, however, is that the junior analysts had better do their homework because a track record should be kept of their assessments. Analysts should perform analysis, not mere compilation and presentation of myriad intelligence reports produced and vetted by others. That means making a substantive determination and taking personal responsibility for it — just like any other skilled professional. Producing an intelligence assessment should be taken every bit as seriously as prescribing a medication, issuing a legal opinion, certifying an engineering survey, etc. IC analysts must be relied upon to reach determinations about the state of affairs of the world and be respected in their professional judgment. If the IC's management or USG's foreign policy decisionmakers are not willing to rely on them, then that proves the irrelevance of the analysts and argues for either (a) not employing them any more or (b) replacing existing analysts with expert analysts who can be relied upon for their good judgment and who are willing to stake their professional reputations — and their jobs — on those judgments.

Looking back to the discussion in Section II above, one must question how one could hold analysts accountable for assessments that are so inherently difficult. If one agrees that intelligence is an imperfect art, then how can one expect even the best analysts to get it right most of the time? The answer comes to us from decision theory and probabilistic mathematics.

In cases of uncertainty, probabilistic judgments are themselves valuable decisionmaking inputs. Accurately assessed, the simultaneous pursuit of two independent courses of action that each carry a 50 percent chance of accomplishing the same objective should yield a certain result. In terms of intelligence analysis, the IC should expect its expert analysts to be able to assess uncertain states of affairs with a probability coefficient. Analysts should be judged based not on whether something happens or does not happen but on their track record of applying correct probabilities to possible events — past, present or future. Any event adjudged to be 100 percent likely should be expected to happen; one-half of the events adjudged to be 50 percent likely should come to fruition.[7]

7 Assessments could be divided into tiers, perhaps in increments of ten percentage points, and the respective percentage of the total number of propositions assessed to be in that tier should come to pass if the analyst is correct. Alternatively, if not enough propositions are adjudged to make tier-wise evaluation statistically sound, then every assessment made by each analyst could be multiplied by its associated probability and summed in one algebraic equation. In that case, the final outputs most closely approximating the number of all events under consideration that actually occurred could help identify the superior analysts; although, this method of evaluation would also be imperfect due to the possibility of

Analysts over- or under-assessing the likelihood of events should be equally criticized because accuracy is what is most important to a decisionmaker. Risk and uncertainty can be mitigated or hedged, but inaccuracy cannot.[8]

Unlike intelligence collectors or analysts, the policymakers' purview is to weigh options, consider the utility of different outcomes, and select courses of action. Rational choice theory has incontestably shown that incomplete information (i.e., multiple, uncertain outcomes that carry individual probabilities) is not an obstacle to effective decisionmaking, provided that the probabilities are assessed as accurately as possible.

Despite our psychological preferences, we live in an uncertain world where few things are known absolutely without qualification. Even the best natural scientists will admit that their method of hypothesis, experimentation, and abduction infers models of reality that are subject to future changes as additional information becomes available.[9] If intelligence has the objective of divining truth about world events, why does the IC not embrace the methods that have proven most useful and won dominance in all other fields of human study?

Let it be the role of the intelligence analysts to assign probabilities to selected propositions and let policymakers add the utility values to the various outcomes in the decision function. In that way, experts in the field can speak definitively about what is or what can be without being politicized, while elected leaders can decide what should be and take the necessary courses of action. And in every instance, the intelligence analysts should be professionally judged, and compensated, based on how often their assigned probabilities match reality in retrospect. Any analyst who could consistently and accurately state the percentage chance of events occurring would be worth her weight in gold in Las Vegas, on Wall Street or in Washington, D.C. Good decisions do not mandate certainty, but a good foreign policy decision calculus does mandate accurate probability assessments.

Many intelligence officers equate their warning role with imminent danger and "FLASH" cables; but surely, proper installation of smoke detectors is every bit as important as, if

---

offsetting errors. Nonetheless, the two simplified schema discussed here illustrate the type of mechanisms that could be used to evaluate analysts' probability assessments.

8 Using this method of accountability will discourage conservatism by analysts who might otherwise underestimate all probabilities to avoid being penalized for claiming something that later does not come to fruition or is not verified ex post.

9 The best historical example of the evolution of imperfect models was the pre-Copernican effort amongst geo-centrists to explain anomalous planetary locations through increasingly complex series of epicycles. Finally, a much simpler heliocentric model was adopted in accordance with the principle of Ockham's razor.

not more so than, a last-minute call to the fire station. The IC comprises highly educated experts, but their judgments on future threats are rarely acted upon in tangible ways. True, finite resources and ongoing crises mandate attention, but this author is not convinced that several hundred thousand well-placed dollars today could not avert the need for several million tomorrow. The ultimate questions become: (1) "Whose opinion about the future do you listen to?" and (2) "How much credence do you put in — or resources do you direct towards — their distant warnings?"

This Section has preoccupied itself with exploring a new method for determining an answer to the first of those two questions. The second is a matter of public policy based on the policymakers' aversion to the probable impact (i.e., the product of the trusted analysts' probability coefficient multiplied by its potential negative value). An intelligence analyst should be judged and rewarded based on her ability to accurately assess extant or future scenarios.[10] Elected politicians, on the other hand, should take action to avert the outcomes that their constituencies find the most undesirable, if such is indeed possible.

Analytic methods that worked in the 1980s may not be what works best today, so why not use empirical evidence to prove what does work best? One can be certain that even good strategies have finite terms of applicability (i.e., "dominance" in game theory parlance). By holding analysts individually accountable, evaluating their assessment records, and placing preferential value on the future assessments of those analysts with the best performance, the IC could ensure an adaptive mechanism for producing the best inputs for each critical decision calculus at the policy level.

Analytic accountability would also provide significant and indisputable opportunities for performance-based compensation. One can even imagine a situation where an analyst who had a "batting average" of .750 in the IC and saved millions of US lives could be publicized and lauded — even under a pseudonym if necessary for security reasons — as much as someone who can hit, throw or catch a spheroid with distinction. Until analysts are ready to be accountable, they do not deserve that level of respect, compensation or acclaim. Until analysts are made accountable, the IC will not get it right as often as the American citizens deserve.

---

10 The actual timing of the event is immaterial for the cognitive processes involved, since, in the absence of adequate information, something happening today about which one will only later learn is intellectually equivalent to something that will happen tomorrow. At any point in time, an intelligence analyst is trying to infer a truth within the present state of information, regardless of whether the subject matter is an event in the past, present or future. Only with complete information (e.g., eyewitness accounts in the absence of denial or deception techniques) does the tense of the proposition under study have operative value to the analyst.

IV. Meta-Level Analysis

Once the procedural focus has given way to accuracy and accountability, the question arises as to what propositions the analysts should study and assess. Clearly, top-down assignments from policymakers and IC managers should be included. Additionally, analysts should review the bottom-up intelligence that is derived from HUMINT, SIGINT or other collection channels. Finally, analysts themselves should generate some of their own taskings for, as the foremost experts in the field under scrutiny, they may have the best understanding of imminent concerns. What makes the New York Times' front page or a CNN sound bite is not always the most critical issue for national security. Diverting analytic resources to respond to media claims or the political issue du jour may, in fact, be dangerous in some cases.

Intelligence failures are the result of one of four possibilities: (1) errors in inductive or deductive reasoning in the presence of sufficient, valid information; (2) errors in vetting inaccurate information, potentially from denial and deception efforts or genuine ignorance by the reporting source; (3) insufficient access to accurate information; or (4) inabilities to apply the necessary resources to matters. Items (1) and (2) obviously represent analytic failures that are addressed by Sections II and III above, and (3) might be mitigated if analysts placed better requirements with collectors. Depending on the circumstances and the nature of the target, overcoming (3) may be very difficult; however, analysts could still try to assist in devising new human and technical collection methods. Item (4) seemingly rests beyond the realm of analytic failure, but it actually forms the crux of the IC's current challenge.

In a world of global information that is propagated, reproduced, and transmitted far faster than intelligence resources — either human or financial — can be applied to process it, failures to optimally allocate analytic resources are essentially analytic failures. The IC needs to find ways to cut corners, otherwise it will never keep pace with tomorrow's national security threats. There are simply not enough intelligence operatives or analysts to assign even one minder to every potential threat. Failures to ask the right questions due to a preoccupation with existing or past concerns can prove a fatal error.

Indeed, the very first analytic intelligence question must be "What intelligence questions should the IC be asking?" Rather than persisting in an exclusive study of historical targets or recent catastrophes, the DI needs to revamp its analytic tradecraft to detect the next question that needs to be examined more closely or investigated through additional collection efforts. The US's previous intelligence posture for warning can be likened to a distant observer with a looking glass and a copy of Jane's Fighting Ships. He knew what he was seeking and had a point of reference; his job was to identify the first glimmer of the adversary's mast on the horizon. Today's world mandates a new approach more analogous to a cadre of seismologists, chemists, biologists, physicists, economists,

statisticians, etc. — all with very sensitive instruments — standing motionless in an open field and observing in every direction. Their objective would be to detect each and every anomalous event and then endeavor to explain its occurrence.

America's adversaries have leveraged technology to conceal their basic actions, but they still leave higher order — or meta-level — "footprints" of their nefarious activities. Communications, financial transactions, and operational logistics all necessarily leave some trail in a modern economy, and the more esoteric the activity, the more likely it is to stand out against the background patterns (i.e., baseline data). Mathematical functions can be analyzed to determine rates of change and other patterns, and so too can human activities in the aggregate. Just as derivatives in calculus permit the Newtonian mind to greatly expand its knowledge of how the natural world functions, meta-level analysis permits the intelligence analyst to rigorously study global phenomena without even requiring specific, first-order data (i.e., the substantive content of any particular intelligence datum). It is time for more IC analysts to move beyond the conceptual equivalent of arithmetic and algebra and embrace advanced methodologies in order to detect statistical anomalies that may highlight criminal, terrorist, military, or espionage activities. The second- and third-order derivatives of intelligence data are very difficult to obscure in an increasingly networked world.

Interestingly, much of the desired data is already collected and processed — just not by the IC. Investors, service providers, industry analysts, management consultants, public relations firms, and government regulators all study the critical sectors in a modern economy. While we live in a world that is uncertain in its specific events, we live in a world that is highly predictable in its patterns of events. The insurance industry produces actuarial tables on systemic events, and research scientists rely on probabilities in the form of standard deviations.[11] The time has come for intelligence analysis to make better use of similar methods, and what is most required to permit such exploitation of meta-level data is an understanding of the baseline values and states of human activity on a global scale. As stated above, much of that information is already generated and recorded in the private sector.[12]

If an anomaly were detected but not easily explained, then meta-level analysis would suggest that the IC explore the issue further. Perhaps then, the analysts would find a

11 If anyone doubts the efficacy of these inductive methods of inference, he need merely consider the profitability of most insurance companies and casinos.

12 Ironically, the USG trails far behind the average credit agency, insurance company, brokerage house or online merchant in performing the role of "Big Brother." Through a combination of monetary incentives and service-oriented tracking methods, the private sector already has far better monitoring capabilities. Just consider the security feature offered by some credit card issuers that proactively declines charges to a card that a would-be thief is trying to utilize in a country or region where the real customer has never traveled before — all in real time.

sufficient explication for the anomaly, but if not, the investigation would need to continue and more resources would need to be applied to it. This analytic posture, however, presumes a commitment to be proactive (as discussed in Section I above) rather than merely reactive. It means studying items of interest before they become the foci of problems; otherwise, there will be no baseline measures and, hence, no way of detecting anomalies when they do occur.

Meta-level analysis offers a wealth of opportunity for determining where best to apply IC resources in an era where full-time, global coverage is simply not possible. Information is produced, replicated, and transmitted so quickly that analysts will never again be able to keep pace with all first-order developments. The human mind has finally become the slowest link in the information chain. The IC must abandon its old models that proved satisfactory in a finite information environment and adopt scientifically proven means of analyzing inordinate amounts of data about the world.

V. Personnel Structure

The observations in this Section may not resonate with senior IC managers who do not, or no longer, directly participate in meetings and labor on specific projects at the functional levels within their organizations. That is because the very presence of senior management itself necessarily dictates the nature of the meeting and restricts the likely participants to other senior or mid-level managers. Very rarely, if ever, are senior managers direct witnesses to the quotidian activities and basic assessments that ultimately determine both (a) what information the senior managers themselves receive and (b) the course of their organizations' actions and impact — or lack thereof — on US foreign policy and world events.

The single greatest denial and deception success within the IC is the "handling" of senior managers by division, office, and group chiefs. Many scholars of information sciences will identify the greatest epistemological challenge as, "We do not know what we do not know."[13] Upward information management and non-existent checks and balances permit managers to filter the very evidence that senior management uses to assess lower-level decisions. Hence, the opportunity costs of pursuing one avenue over another — or not pursuing any avenue at all — will never be reviewed as a matter of ordinary business. This shortcoming is most harmful in areas where competing components have incentives to quash each other's programs or recommendations in order to obtain increased funding and recognition for themselves.

In the business of intelligence, making the correct assessment or choosing the right operation to run is critical. The CIA, however, is so preoccupied with its antiquated procedures that it

13 See, for example, the work of Professor Anthony Oettinger at Harvard's Program on Information Resources Policy. Dr. Oettinger is also the Chairman of the DCI's Intelligence Science Board.

regularly overlooks the important substance at hand. For example, only a fraction of any DI analyst's time is actually spent making intellectual assessments. She is primarily held accountable for properly following bureaucratic procedures and stylistic preferences, while very little attention is paid to checking or recording the rectitude of her actual judgments.

The institutionalized inefficiency in the DI is nothing short of astounding. The extensive rhetoric about Information Age technologies and real-time intelligence simply cannot be reconciled with month-long coordination processes for products, habitual photocopying by Ph.D. engineers or operational timeframes that conspicuously diverge from any normal business activity. Although it once shared technological parity with the private sector, the CIA is now only competitive with equally obsolescent foreign intelligence services. As our national security threats increasingly come from non-state actors who capitalize on real-time technologies and require operational responses from the USG that are active on a similar timetable, the CIA's dilatory procedures will prove fatal.

The unnecessary multiplication of professionals actually further inhibits productivity by requiring additional procedures to keep them all informed of relevant activities. This syndrome is best exemplified by the superfluous referent and liaison positions that separate professional working groups and impose even further delays. By comparison, few doctors, consultants or accountants feel the need to hire go-betweens to manage their communications with their own colleagues or clients.

The DI's inefficiency runs far deeper than bureaucratic red tape or understandably burdensome security requirements. A brief examination of the DI's structure reveals an organization that is almost the perfect inverse of any other professional services provider. Most investment banks, consulting companies, engineering companies, accounting firms, law firms, medical offices, and think tanks all strive to maximize the productivity of their professionals by offering them every assistance and maintaining a support staff which significantly outnumbers them. If the DI's value-added functions are researching, writing, and briefing, then the individuals responsible for those activities should be encouraged to spend as much time as possible doing them — not filing, photocopying, and filling in on-line forms.

Spending more resources on skilled support staff would both increase the productivity of case officers, analysts, and engineers and also reduce the number of expensive professionals that are required to perform the CIA's mission. Many private sector entities realized this economic truism and streamlined their organizations in the 1980s. The CIA should not persist in paying computer scientists or Chinese linguists to perform clerical tasks that a well-trained secretary can do better and more cost-effectively. Hiring highly trained secretaries and research assistants — even at high salary levels — would significantly increase the productivity of the expert analysts in any group. It takes both good management and good support to render the most honey from the worker bees (i.e.,

the analysts in this case), yet the DI under-hires and under-compensates those essential support roles.

VI. Conclusion

Analytic tradecraft should consist of identifying future strategic threats, and added emphasis should be placed on substantive accuracy, not process. In order to do the preceding, those analysts with the best track records should be acknowledged, rewarded, and more highly regarded in their future assessments, particularly on issues where differing views are present. Moreover, many cognitive tools and methods exist that could serve as "force multipliers" for intelligence analysts, but they require a command of logic, mathematics, and statistics. The powerful advantages of those means should not be underestimated or eschewed simply because they may be arcane to the bulk of intelligence analysts who have liberal arts backgrounds. Few individuals fully understand the intricacies of atomic fusion or fission, but most can recognize their efficacy and impact.

By rethinking the very premises, purposes, and procedures of intelligence analysis, the DI could regain the strategic initiative and guide the CIA and IC to a new position where it presages new threats and prepares the USG to defend against them — all before the next tragedy occurs. The DI must constantly evolve in order to remain a relevant and valuable national asset.

Ironically, the DI fails to avail itself of many of the advantages of the very same liberal democratic ideals (e.g., a free market for ideas, competition, etc.) that it espouses to safeguard and foster around the world. The CIA's historical culture and organizational precepts deny it the full benefits of American ingenuity and determination, even where the inherent secrecy of the intelligence business does not mandate such limitations.

Not every question can be answered or every outcome predicted, but US intelligence analysts should aspire to be more than a cadre of clandestine journalists. An analyst's true value and purpose lies in her ability to correctly solve puzzles with incomplete information and to foresee implications. While much effort is being spent to analyze intelligence failures at present, little mention is made of the ongoing failure to ardently pursue new intelligence successes. Inevitably, today's failure to achieve strategic intelligence successes will manifest itself in tomorrow's acute intelligence failures.

Science and Intelligence Analysis: The Requirement for "Critical Thinking" Training in the Intelligence Community

(b)(3)
(b)(6)

Slowly, the satellite slews to the next target and begins a sequence of exposures. Information is sent swiftly to the ground station and transferred to an analysis facility where the data are converted into a format humans can understand and then archived to be analyzed when convenient. The information contained in the data files is significant to our understanding of the target of the observation.

Another day observing targets of intelligence value in a denied country? Not quite. In this case, the telescope is observing a distant galaxy, and the analyst is an astrophysicist. But the initial guess was a good one.

Pure scientific research—and in particular astronomical research—is, interestingly, very similar to what the intelligence professional does on a daily basis. I first discovered this after a very short time working on my account in the Directorate of Intelligence. I began my professional career as a Ph.D. astrophysicist (an activity I continue today). Having had an interest in science from an early age, the scientific method has been ingrained deeply in my psyche.

I guess I shouldn't have been, but I was startled at how similar the analysis I was doing for the CIA was to scientific research, and even more so to astronomical research. Even the DI writing style is close to what we do for our scientific journals, in the "outside world" of academia.

The Scientific Method And Critical Thinking

The scientific method is a process for understanding the universe around us that has been developed over more than two thousand years of trial and error. The scientific method as we know it today first started making an appearance about 350 years ago.

A thumbnail sketch of the scientific method is the following. An observation is made, and then a hypothesis or theory is proposed to explain the observation. The theory leads to predictions, and experiments are designed with the intent of ***disproving*** the hypothesis and exploring the predictions. It is a common misconception that science and scientists try to ***prove*** their hypotheses. Indeed many scientists do this—I certainly have. It is the easier route to follow. Nonetheless, the pure scientific method is all about *disproving* a theory. The experiments are planned—sometimes over many years—and are often

accompanied by rancorous debate. But observations are eventually made and data obtained.

If the theory is disproved, a new and better one is put forward, one that must explain **all** the observations. In practice, an entire theory is rarely thrown out completely, just modified to explain the new observations.

Ideally, many independent scientists or groups of scientists are working the same issue, attempting to obtain data and advance knowledge. This competition is good, as it keeps everyone moving forward and honest. Also, an observation that proves or disproves a hypothesis needs to be validated by independent researchers to ensure that no coincidences or errors have occurred. Only after repeatedly performing the same experiment multiple times, in multiple independent ways, can we be certain that the experiment is correct.

In addition, competition also means that there are multiple hypotheses advanced to explain the same phenomenon. This is good too, as it means that the **best** theory wins out over other, less successful ones. While an issue is being worked, a scientist will always prefer multiple theories over a single one as a way to determine truth, even though it may mean that the originally preferred theory does not work in the end and must be thrown out. A researcher may be disappointed when a favored hypothesis is disproved, but in the end, this is okay because the goal isn't to be right—it is to determine truth. A correct theory trumps an incorrect one and is usually more interesting as well.

In the end, after numerous cycles of theory, observation/experiment, correcting the theory and repeating this process, a number of theories may appear that explain things quite well and have survived the brutal process of attempting to disprove them. How do we choose which one will become *the* accepted theory? Well, scientific-method pioneers thought of that too. Actually, William of Ockham, a 14th-century British Philosopher and Franciscan monk, thought of that: *Pluralitas non est ponenda sine necessitate,* or, "Plurality should not be posited without necessity."[1] This principle is now known as 'Occam's Razor.'

What this means is that, if there are two (or more) competing theories to explain a given phenomenon, and both (or all) of them explain the phenomenon—and everything associated with it—equally well, the *simplest* theory is preferred. Or, as stated by Isaac Newton: "We are to admit no more causes of natural things than such as are both true and sufficient to explain their appearances."[2] This is a very useful concept in science—

[1] From, e.g., http://skepdic.com/occam.html

[2] Newton, Isaac, Rule 1 of 'The Rules of Reasoning in Philosophy,' from *The Mathematical Principles of Natural Philosophy*, trans. A. Motte (London, 1729), cf. http://www.fordham.edu/halssall/mod/newton-princ.html

and intelligence analysis—because without it, you can formulate Byzantinely complex theories that explain every aspect of an observation but are so convoluted they have no basis in reality. An example is given in Text Box 1.

So that's the scientific method in a nutshell. To be complete, however, I should add that what I have described—**observation**, theory, experiment, correction of theory, new experiment and repeat the cycle—while being what almost all scientists perform daily, is not the ideal of the scientific method. The purest way of employing the scientific method is **theory**, observation, experiment, correction of theory, new experiment, repeat cycle—that is, the theory comes first. In practice, this is extremely difficult, however, and this pure form of the scientific method is really only left to the geniuses among us. Einstein, for example, postulated the Theory of General Relativity three years before his predicted observations were made, vindicating the theory. (Another interesting thing about geniuses is that their theories rarely need to be corrected!)

Text Box 1: Occam's Razor – An Example.

An example of Occam's razor is the debate between the heliocentric (sun-centered) and geocentric (earth-centered) models of the solar system. From the Greek astronomer Ptolemy, in the Second Century of the Current Era, to Nicolas Copernicus around 1500, the accepted view of the solar system was that the sun and all the other planets revolved around the earth. This model explained the observations quite well, but to get it to work required an enormous amount of complexity.

Copernicus proposed a different model, one where the sun was the center of the solar system around which everything else revolved. This heliocentric model was much simpler than the geocentric one and thus became the accepted model. Problems due to the fact that Copernicus assumed circular orbits (instead of the true, elliptical ones) were corrected in the following centuries by Johannes Kepler and Isaac Newton, among others.

An example of the scientific method—using General Relativity—is given in Text Box 2. (What is provided is a very general summary of an enormous subject.) An example of the scientific method employed for intelligence analysis is in Text Box 3.

Making a habit of employing the scientific method in analysis also encourages the use of critical thinking—that is, not to accept observations at face value but to think actively about them and how they fit in with the bigger picture. (It was the key to solving the mystery of the TWA Flight 800 "missile sightings," as discussed later.) Critical thinking

should be employed constantly, particularly in our everyday lives. It affords the user an open mind, able to change and spot opportunities that wouldn't normally be apparent.

Text Box 2: Einstein's General Theory of Relativity (1915): An Example of the Scientific Method.

Foundation/Background: Non-Euclidean geometry, studied by Riemann, was thought not to be appropriate to the real world; Newton's theory not wholly applicable in some conditions; frames of reference; Michelson-Morley experiment in the late 19th century showed that the speed of light was uniform in every direction; experimental observations showed that inertial (acceleration) and gravitational masses are equivalent.

The Theory: Gravity and acceleration are different perspectives of the same thing (Equivalence Principle); space/time curved (by matter and energy); some reference frames must obey non-Euclidean geometry.

Predictions: Space/time curved by matter and energy; changes in the orbit of Mercury around sun (Newton only explains some of changes, not all); moving clocks have to be corrected for gravitational effects; path of light beams changed by gravitational fields; light coming from strong gravitational field should have its wavelength shifted (gravitational redshift); gravity waves, and many more.

Confirming Observations: First confirmation in 1919, starlight bent by gravitational field of sun; later observations confirm this and gravitational redshift; moving-clock effect; theory is foundation for much of modern life, as well as other theories; 1916, Schwarzschild develops the mathematical solution to Einstein's equations, defining the intense gravitational field of an extremely compact object, and the field of Black Hole astronomy is born.

Sources: http://en.wikipedia.org/wiki/general_relativity;
http://csep10.phys.utk.edu/astr162/lect/cosmology/gravity.html
http://www-gap.dcs.st-and.ac.uk/~history/HistTopics/General_relativity.html

Intelligence Analysis Versus Astrophysics

Back to astronomy (which is the surrogate for the scientific method in this discussion) and my surprise at how similar it is to intelligence analysis. Research is research, so why was I surprised? What struck me most was the "quality" of the similarity between intelligence analysis and astronomical research. Not only is the substance of research the same, but so are the details.

Figures 1 and 2 show the scientific method and the Intelligence Cycle. Note the similarities. For Figure 1, the alternate path is shown with dashed lines. The goals of both are to determine truth and disseminate knowledge. For the Intelligence Cycle, Figure 2, the 'Planning/Direction' bubble most closely corresponds to the 'Theory/Hypothesis' bubble of the scientific method. Similarly, 'Collection' corresponds to 'Observation.' The Intelligence Cycle includes a 'Processing' bubble that is implicit in both 'Experiment' and 'Observation' in the scientific method.

Table 1 below shows these areas of similarity. The most important point is that, for both astronomy and intelligence analysis, the researcher does not have *direct* access to the sources of data (in all cases for astronomy, in practically all for intelligence analysis). This is what makes astronomy different from almost all other sciences, yet so similar to intelligence work.

In addition to analysts not being able to interact with the data, there are very few data available in most cases for both astronomy and intelligence analysis. Astronomy's limited data result mostly from technological constraints. Intelligence analysis is affected both by technology and human/social-scientific factors. Limited data also means 'holes' in the analysis in both cases. And the data that one obtains are not always "perfect," but can be "noisy." The signal is not always clear (in a literal sense and also figuratively, especially for intelligence analysis). There also may be "false" information present in both cases.

All of these issues make determining truth challenging: Limited, missing, noisy data make interpretation difficult and more than one interpretation possible. And everyone working the particular issue probably holds at least a slightly different view. It is in such cases where the scientific method works best. When multiple scenarios are possible, the scientific method allows workers in the field to explore all the possibilities, cogitate over them, discuss and debate, perform new experiments and develop new techniques to obtain more and better data. Often repeating this cycle multiple times is the only way to obtain consensus regarding what is being observed.

In intelligence analysis, like astronomy, a perennial goal is to obtain more and better data. Sometimes we get it, sometimes we don't. But new and better data don't always enlighten us. Usually we can refine our knowledge—or the new data show us that we

were wrong all along and must make new hypotheses. We must be prepared for this outcome and be willing to change our views, even if they are long-held and comfortable.

Table 1: Similarities between astrophysics and intelligence analysis.

Activity	Astrophysics	Intelligence Analysis
Indirect access to target.	Distant objects.	Distant; in denied areas; covert collection.
Limited amount of data.	Telescope time is expensive.	Competing collection priorities; no access.
Data can be "noisy."	Weak signals, interference.	Sparse/conflicting data make interpretation difficult.
Lack of data leads to best guesses (based on informed judgment).	Many times the only possibility is a guess.	Many times the only possibility is a guess.
Multiple scenarios possible.	Available information may mean that multiple interpretations/hypotheses are possible.	Available information may mean that multiple interpretations/hypotheses are possible.
Multiple viewpoints held.	It's how science gets done. Consensus is reached to give the most likely possibility.	It's how intelligence analysis *should* be done. Consensus is reached (in NIEs, for example) to give the most likely possibility.
New data make new hypotheses necessary.	New and better data may indicate that the initial hypothesis is wrong or needs to be modified. This is the scientific method and how 'truth' is determined.	New and better data may indicate that the initial hypothesis is wrong or needs to be modified. This is how intelligence analysis *should* be done in order to determine 'truth.'
New, more and/or better data don't always clear things up.	Absolutely the case here. Usually they make things murkier.	Can make understanding murkier.

Figure 1: The Scientific Method Cycle.

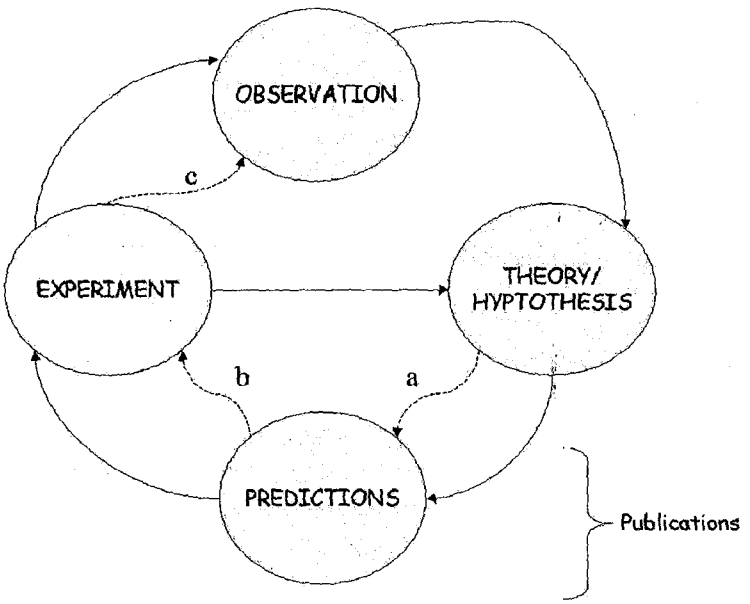
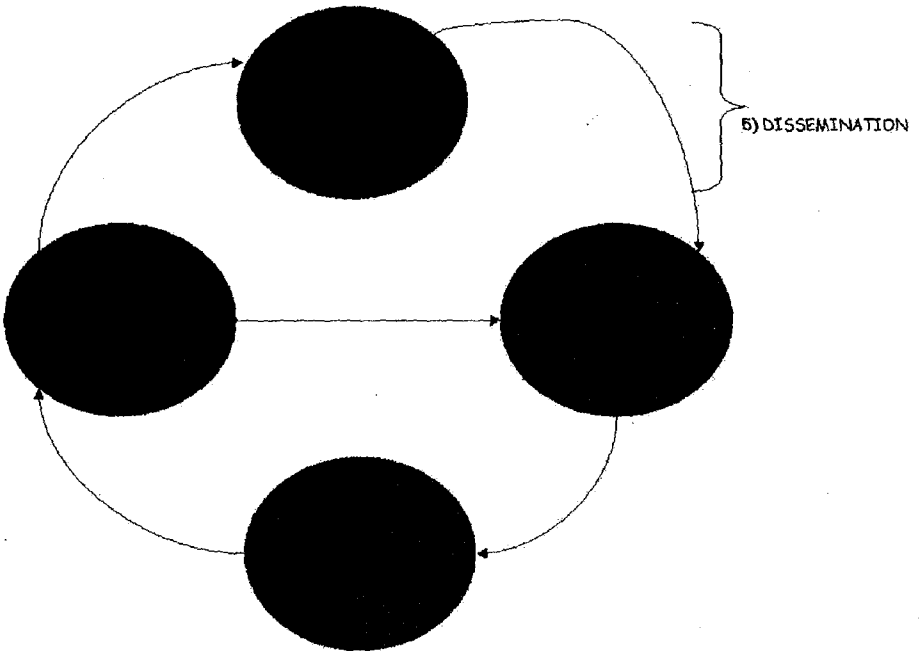


Figure 2: The Intelligence Cycle.



Text Box 3: Analysis of the TWA Flight 800 Crash: A Scientific-Method Case Study.

The crash of TWA Flight 800 off the coast of Long Island on 17 July 1996, potentially one of the most lethal international terrorist acts perpetrated against the United States up to that date, touched off the most extensive, complex, and costly air disaster investigation in US history. Had it been the result of state-sponsored terrorism, it would have been considered an act of war.

Early in the investigation, the possibility that a missile downed the plane was considered highly likely because of reports from dozens of eyewitnesses in the Long Island area who, on the evening of 17 July, recalled seeing something resembling a flare or firework ascend and culminate in an explosion. Even FBI investigators and CIA analysts focused much of their early (and costly!) work delving into this theory, often to the exclusion of other theories that didn't seem to have the "preponderance of evidence" afforded by the independent eyewitnesses.

It wasn't until the scientific method was applied rigorously to this investigation that it was demonstrated that the eyewitnesses had not—indeed *could* not—have seen a missile attack the plane (see *"The Crash of TWA Flight 800 – Solving the Mystery of the Missile Sightings,"* Studies in Intelligence, Volume 44, No. 2, 2000). What they had seen was the burning aircraft in various stages of crippled flight *after* it had undergone an initial explosion in its center fuel tank.

Ultimately, the FBI used CIA's work to suspend their criminal investigation. What is less-well-known is that the accolades given to CIA by Congress and others following the suspension of the FBI's criminal probe were the direct result of CIA analysts applying the scientific method and critical thinking to their work.

So What?

I've described at length the scientific method and how intelligence analysis is similar to science. I hope I've convinced you that the scientific method is important and science and intelligence analysis are similar. And I hope that it is becoming clear that intelligence analysis can be treated as a hard science—that it can, and should, employ the scientific method in all its forms and nuances.

Moreover, for the intelligence analyst (and thus the DI and Intelligence Community), research is **the most fundamental thing we do**—a fact, I think, which is often overlooked. It is the goal of all those operations we can't discuss, and the motivation for

developing technology many thought couldn't exist. Research is what provides material for the products we churn out daily, and for all the briefings we give.

So you can imagine my surprise when I realized that the scientific method, as such, wasn't being taught at CIA, nor elsewhere in the Intelligence Community. This oversight, I believe, has enormous consequences for how intelligence work is done. And I'm not only talking about science/technology analysis, but *all* forms of intelligence analysis; S&T analysis of course, but also political analysis, leadership analysis, economic analysis and so on. At their most fundamental level, they all should employ the scientific method.

What To Do?

In order to make sure we are doing research properly, we need to inculcate the scientific method and critical thinking in all analysts within the DI, and ultimately the Intelligence Community. This process *must* start early in an analyst's career, particularly if he/she doesn't have a scientific background. If we do not initiate a relatively straightforward and simple scientific-method training process, our analysis, products and, ultimately, reason for existence suffer.

Lack of understanding this fact, and failure to employ the scientific method rigorously in our work, has caused failures in our past and will lead to failures in our future. (See Text Box 4 for another potential problem.) Other organizational changes currently underway will be perfunctory if we fail to fix this fundamental process.

Text Box 4: The Scientific Method and Collection.

One of the key components of the intelligence cycle is 'collection' (see Figure 2). Collection is driven by the analyst because of a need for data to answer a question or help address a hypothesis. Failure to employ the scientific method can proscribe collection in a way that skews results. Collection requirements based on faulty premises may provide information that is incorrect, leading us to potentially false and dangerous conclusions. In addition, we may be wasting resources by "barking up the wrong tree."

In the early stages of the TWA Flight 800 analysis, one leading theory was that a missile had destroyed the aircraft. Collection was tasked—such as searching underwater for a discarded portable missile launcher—based on this premise. Such collection needlessly cost the US Government millions of dollars.

Note that, even when analysts employ the scientific method properly, sometimes our hypotheses lead to wasted collection efforts or useless data. We try to limit such cases, and using the scientific method is one of the best ways to do this.

Courses

My suggestion, then, is for a two-pronged approach. First, we need to teach formally the scientific method and critical thinking. Proper use of the scientific method takes years and comes from employing it everyday, in the real world. So, over a new analyst's first five years, there should be a series of courses dealing with these important issues. However, to begin, an in-depth course on the scientific method and how to apply it is vital. These cannot be one-size-fits-all courses. For example, if a new analyst comes in already knowing the scientific method, they would only be required to take agency-specific courses.

Current analysis courses and sections of other courses deal, in some way, with these topics. But—and this is surprising given how crucial research is for what we do—there exists no single course that teaches the scientific method and critical thinking, and how to apply them to the everyday world of intelligence analysis. As Heuer states, "most training of intelligence analysts is focused on organizational procedures, writing style and methodological techniques...More training time should be devoted to the thinking and reasoning processes involved in making intelligence judgments...."[3]

Again, the concepts will not be developed in a single one-week, one-month or six-month course. But a course that introduces and defines the concept is vital. Preferably, this course would be provided to new analysts almost as soon as they arrive. It would complement—but be distinct from—courses that explain our specific work in the Intelligence Community (how to write, brief, etc.). Text Box 5 sketches a possible syllabus for such a course, which would be anywhere from two weeks to one or two months in length.

A course such as the one outlined would be a good introduction to scientific-method concepts, providing theory and practice. This intensive course could be followed by a series of "literature survey" courses, designed to study the scientific method in action, as well as in-depth case studies of failures caused by not using the scientific method, discussing how the outcome could have been different if the scientific method *had* been used properly.

[3] Heuer, Richards J., Jr., 1999, 'Psychology of Analysis,' p.178 (CIA, Center for the Study of Intelligence).

Text Box 5: A Draft Syllabus for a Course on the Scientific Method and Critical Thinking.

- *Critical Thinking*

  This section will evaluate a variety of grandiose and exceptional claims made in legitimate science and pseudoscientific realms to see how critical thinking is employed, and what happens when critical thinking is lacking.

- *The Scientific Method*

  This section will explore the scientific method, study its historical development and learn how it is applied to scientific and intelligence analysis.

- *Analysis*

  This section will apply everything presented in the previous two modules to teach how to analyze data properly. This will be the largest part of the course. Alternative analytical methods and processes will be explored.

- *In the Everyday World*

  This final module will tie all the theoretical learning into how the material is applied to the everyday world of the analyst. Many courses present excellent material that is never used by the student. Since the goal for this course is the continual application of the material learned, this module will explore how the analyst can incorporate these practices realistically in their work (and home) environments.

Existing employees obviously will have a strong background in research and the analysis we do. However, since employing the scientific method is a lifelong endeavor, refresher courses will ensure that staff aren't falling into ruts and/or cutting corners. I believe a selection of three or four such courses, designed for employees of differing abilities—presenting critical thinking and the scientific method at a higher level and perhaps more anecdotally—should suffice in these cases. These refresher courses would be offered at various times throughout an employee's career: at 5, 10, 15 years, etc.

More Scientists

The second prong is important, but not as vital as the first. Nonetheless, it will help limit the requirement for extensive scientific-method, in-house training. What I propose is the accelerated hiring of scientists—and physicists, in particular. These new scientist-employees won't be just for science and technology accounts, but for *everything we do.* Would they assent to this? Yes! In fact, most physicists don't "do" physics, but rather participate in other varied fields.

But why physicists? A physics background is a well-rounded one. Physics teaches problem-solving skills and the ability to synthesize information. It is one of the most popular degrees for managers looking for highly skilled labor in areas as diverse as finance and industry. According to studies by the American Institute of Physics (AIP), surveys of managers with physicist employees (not doing physics) spoke highly of them, and more often than not would rather go to them than employees having other backgrounds (including more specialized, job-specific ones) because of the physicists' problem-solving abilities and approach to problems.[4]

According to another study by the AIP, a physics education provides students with a set of skills that are important, including cognitive skills such as critical and analytical thinking, and expertise regarding how to define a problem (half the battle!).[5] Moreover, such an education provides students with experiences that develop important traits: diligence, creativity, meticulousness, persistence and self-confidence. And, of course, physicists have a strong background in the scientific method. These are all skills necessary for the intelligence analyst and the work we do in the Intelligence Community.

Thus, I would like to see more physicists in *every* area we pursue. That is because the skills and traits listed above are fundamental. Other skills such as leadership analysis, political analysis and economics can be learned on the job—and much faster if the employee already has the fundamentals. Just ask the vast number of physicists and astronomers who have gone to work for Wall Street in New York and the City in London. They quickly rose to the top in their fields, surpassing economists who had been in these firms for years.[6]

Of course we need other experts, too. But we need more scientists than we currently have—throughout the Intelligence Community. In fact, having physicists on the team will nicely round out and complement the analytical force available to be brought to bear on the problems we face.

---

[4] Physicsweb, 5 June 1998, http://physicsweb.org/article/news/2/6/20

[5] Czujko, Roman, 2004, American Institute of Physics, presentation notes, available on http://www.aip.org/statistics/trends/reports/bachpass.pdf

[6] New Scientist, vol. 158, issue 2132, 02 May 1998, p. 54; Author's private communications with colleagues and students (1990-2004).

Table 2: An approach to reinvigorating research and analysis in the Intelligence Community

Prong 1 – Teach critical thinking and the scientific method.	
New Employees	Extensive course(s) on critical thinking, the scientific method and how to do analysis in general; specifics for intelligence analysis.
Existing Employees	A series of refresher courses designed for differing employee abilities and length of service.
Prong 2 – Recruit and hire physicists as all-source analysts throughout the DI and Intelligence Community.	

Summary And Conclusions

Research is the most fundamental thing we do at the Agency and in the Intelligence Community. Data collection provides the fuel—and our briefings and papers the product—of analysis. Yet we are not providing the proper background for our professionals conducting research.

A straightforward solution is to provide a strong and aggressive course structure, teaching new employees how to conduct research and refreshing the concept for existing staff. Reinforcing critical thinking in employees would be a side benefit of these courses, enabling students to better confront the world around them and to make better decisions in everyday life. Bringing in new employees who already possess many of these skills, such as physicists, will be beneficial as well.

In the scheme of things, these suggestions are relatively simple and cheap to implement, compared to other things we do. The process *does* take time—as do all educational and recruitment endeavors—so it must start soon. But since it affects our most fundamental activities, the consequences of not pursuing this course of action could have a significant detrimental impact on our work that will only increase over time.

Starting Over

By Carmen Medina (CIA)

In this, the season of intelligence reform, recommendations for change are coming fast and furious. Everyone has their favorite theory—the Intelligence Community needs to use more technology, it needs more centralization, it would benefit from more competition, it needs more accountability, it could use more HUMINT, it requires greater exposure to outside views. In perhaps the most curious recommendation, the 911 Commission notes (on p. 344) that the challenges of today and tomorrow require that we find a way to routinize, even bureaucratize the harnessing of imagination on behalf of national security. (We would indeed be fortunate if bureaucratic processes could be counted on to generate imaginative concepts.) Many of the recommendations, certainly the ones that form the framework for Congressional and Presidential action, stress the importance of organizational change. The restructuring even threatens to eliminate entire organizations, such as the CIA.

Perhaps one of the reasons for the many recommendations, and why they so often manifest themselves as contradictory pairs, is that most deal with the externalities of the intelligence discipline, rather than its essential core. It would be analogous to a hospital, desperately trying to fix alarming fatality rates on its operating tables, concentrating its reform efforts on the administration of the hospital, and ignoring the doctors and nurses who do the work. While it would be foolish to overlook the context in which the medical staffs operate, it would also be negligent to assume that the processes used by doctors and nurses are without blame. Only the most wrongheaded of organizational approaches would interfere with the work of talented, motivated professionals employing optimum processes well-suited to the problems they face. But even the best organization in the world will not save professionals who misdiagnose cancer for heart disease and apply chemotherapy when bypass surgery is called for.

So, why is it so difficult to spot the process issues behind the organizational curtains? Part of the answer no doubt is contained in the phrase "intelligence reform." All significant current proposals start from existing conditions. They intend to build upon (or in some cases, build down) from the status quo. They all assume, to one extent or another, that many, if not most, of the processes that define the intelligence discipline remain sound. These processes are just being executed incorrectly, and the solution to that is new and better management and oversight.

To gain a different perspective, indeed, to compile a complete picture of what must be done to prepare for the challenges of today and tomorrow, we need to approach the problem with a fresh mindset. Instead of assuming that the existing Intelligence

Community needs to be reformed, why don't we imagine the National Intelligence Community away? What if we pretend, in the autumn of 2004, that the US Government faces a dangerous and fluid world without a defined intelligence discipline, let alone a national community? How would policymakers approach the problem then? Based on a diagnosis of the challenges we face, what would they think are the best things to do? To prepare well for our future national security, we must first expunge our past.

Starting With A Blank Page

If policymakers were tasked today with creating the US's first-ever national intelligence capability, they would start by assessing the environment in which the USG will be operating—what threats and opportunities will the world present to the US? Probably one of the first things policymakers might notice is that the US in the future is unlikely to face a single peer competitor. (This, of course, is in marked contrast to how the policymakers would have assessed their environment in the late 1940s.) Instead, the world of the future is likely to consist of several important countries or groupings that wield significant, and in many cases, growing power. We are entering a new era of history, where an unprecedented number of countries will hold important shares of effective power. Among these would be China, the European Union, India, Indonesia and Brazil. Russia would be an interesting case because if our policymakers approached Russia without the conceptual hangover of the Cold War, would they focus more on its nuclear weapons or on its status as a somewhat unstable country with vast energy reserves? What would dominate their thinking?

The world would also be noteworthy for both its jagged sociocultural schisms and the transformative phenomenon of globalization. Policymakers would likely be concerned that these two dynamics might be among the factors sustaining terrorism, or at least creating the conditions that cause some individuals to engage in violence, often against the West. Most world governments would share the desire to prevent such violence and terror attacks. They would also want to prevent proliferation of weapons of mass destruction, particularly to renegade countries or superempowered individuals. But the status of a particular country as a renegade would be the topic of debate.

The policymakers designing the first Intelligence Community would almost certainly want to take advantage of all the technological capabilities available to them. They would understand the vulnerabilities of computer networks and wireless communications, but they probably would be hard-pressed to imagine how an Intelligence Community could operate without these tools, particularly given how essential modern technology had become for the military and for industry. They would be unlikely to think it a good idea to have a National Intelligence Community that is less capable technologically, in some respects, than the neighborhood grocery store. Indeed, the thought would probably never cross their minds.

Once they had reached some conclusions about the context for their new Intelligence Community, the policymakers would probably settle on some key processes which would be familiar to the intelligence professional of today. The first Intelligence Community would need some capability to *collect meaningful information*. Our policymakers/designers would want some ability to *analyze this information for meaning* so that their new community could help them make sense of this dynamic world, and given its volatility, provide an occasional heads up on what might happen next, particularly concerning terrorism and proliferation. Finally, the first Intelligence Community would need to *communicate its findings* to policymakers already accustomed to getting their information quickly and whenever and wherever they needed it.

Collecting Meaningful Information

A collection system designed from scratch would be quite different from the one we have today. As we think about how to change the Intelligence Community, we tend to lose sight of the fact that many aspects of the current collection system were designed to gather the specific information needed in the 1950s and 1960s, i.e. during the height of the Cold War. We also take it as a given that most of the protocols and processes conceived forty-plus years ago still get the job done today and tomorrow. We are probably mistaken.

Some of the most fundamental and familiar aspects of our collection systems include:

- Clandestine and/or secret mechanisms.
- The targeting of important officials likely to know critical government secrets.
- The assumption that we can generally anticipate what we need to know, i.e. the concept of requirements.
- The ability to limit collection to a discrete set of issues; in other words, we don't need to collect information on the entire world.

What is less well-known and appreciated is how each of these qualities is linked to the Cold War environment that led to their development. Do they still help us grapple with the issues of today, let alone future challenges?

Most legacy collection methods rest on the principle of secrecy, but this characteristic is particularly acute for HUMINT. Individuals serve overseas in capacities intended to disguise their principal motives for being there.

It is important to note how this element of secrecy is linked to the requirements of the Cold War era. The individual collectors operate clandestinely because they are key targets of the host government, which doesn't particularly welcome individuals who seek to gather its secrets. It is well-known that the US and Soviet intelligence services were each other's principal targets during the Cold War.

But our policymakers starting from scratch, given the threat environment they anticipate, probably would not immediately assume they need a completely clandestine collection service. They would want to collect secretly against some individuals no doubt, but they would also place a significant premium on understanding how societies worldwide are evolving. They would be interested, not just in the views of elites, but also in the views of ordinary men and women who might be tempted to support a terrorist organization. Their collection priorities would call for getting some sense of how café society is evolving in Cairo and how university students think in Djakarta. In this context, access would arguably be more important than ability to operate in a clandestine nature.

Our policymakers would also be unlikely to assume their HUMINT collectors could somehow divine ahead of time most of what they need to know. The fluidity of the modern world and the increasingly globalized culture of the future would lead them to stress flexibility and a nimble intelligence culture. They would be reluctant to invest billions of dollars in collection platforms that could become obsolete overnight, given rapidly changing technologies and evolving fortunes of countries. These policymakers would understand that a country such as India could seemingly go overnight from poor, planned economy to booming globalization hub. They would want collection systems to shift almost organically to new priorities; in fact, their collection capabilities would so easily track the changing world dynamic that they would serve as a subtle early warning system. Indeed, our policymakers would worry that, in the future, trouble or opportunity could emerge from anyplace in the world. They would want a collection strategy that would afford them the greatest coverage of the planet at the lowest cost, including minimal infrastructure.

One more characteristic of the future world would influence the shape of their collection systems. Our policymakers would worry that the increasing use of identification technologies designed to capture terrorists, such as biometrics and linked databases that could be accessed almost immediately by the most harried of customs officers, would also make it problematic in the near future for individuals to operate under assumed identities. The new collection officers would have to operate under the caveat that secrecy is so expensive and difficult to maintain that it should be used in exceptional circumstances against high-value targets.

A Collection Solution

Given these strictures, the very first collection system might look something like this. The USG Intelligence Community, along with the intelligence services of many key allies, would maintain informal but still official contacts with a range of individuals all over the world who would report on general developments they observed in their respective societies. These individuals would be vetted but lightly managed—they would post their reports to protected Internet sites, and on occasion, be asked to respond to specific questions. Rather than validating each individual report, a time-consuming and

expensive process, the Intelligence Community would depend upon the multiplicity of sources to cross-check their accuracy. Some of these individuals might be employed by organizations, such as RAND, with contractual relationships with the government.

Is there an existing model for such a collection approach? The financial risk analysis firm The Eurasia Group, based in New York City, collects information using a very similar model. They maintain a network of stringers around the world—individuals from many professions who are known to be keen observers of their societies. The Eurasia Group, by the way, is one of the most admired firms in the New York financial community for the accuracy and insight of its future analyses.

Some might argue that the type of high-fidelity information needed by our new Intelligence Community could not be gathered by a group of enthusiastic amateurs, no matter how talented. For many issues, we would need a more reliable group of professionals, with near-constant on-the-ground experience, reporting on the societies in which they operate. This objection has its merits. Luckily for our policymakers, there exists already a worldwide group of dedicated professionals with the capability to observe societies almost continuously—the policemen and women of the world. These individuals today are charged mostly with maintaining law and order, but they could also be asked to report what they see in their societies, particularly at the non-elite level. They could, appropriately organized and provided with the right questions, tell us about the mood on the street, the level of economic activity in neighborhoods, the cohesion of cities, the appeal of inflammatory leaders.

As farfetched as this model may seem, elements of it are already apparent. Police in Israel, for example, are trained to do more than fight crime; they are taught to be keen observers of the communities they patrol to help detect early indicators of terrorism. In January of last year, police leaders from 34 countries went to Israel to learn lessons on "Law Enforcement in the Era of Global Terror."[1]

With most of its information collected through pervasive and relatively inexpensive observation processes, the new Intelligence Community would be able to reserve clandestine and more expensive collection methods for those problems that required them. Among these would likely be issues such as proliferation of WMD and the specific plans and intentions of known terrorist groups. But the new collection strategy would be of particular help in understanding when societies enter into a pre-terrorism stage, a stage when the options available to US policymakers can often be more effective and positive.

---

[1] Website of the Global Jewish Agenda, a Publication of the Jewish Agency for Israel WWW.Jafi.org.il/agenda/2001/english/week4-5/3)

Analyzing Information For Future Meaning

Our policymakers designing the US's first National Intelligence Community would now turn to the question of analysis. Again, they would want an analytic tradecraft well-suited to the world of today. Concerned with the rapid pace of change (and not obsessed, as they were in the 1940s, with understanding the Byzantine Kremlin), they would want a tradecraft that was well-oriented to understanding the future.

How does this contrast with the analytic tradecraft employed by most intelligence agencies today? Most observers would estimate that 90% of the tradecraft of analysis concentrates on how best to understand what just happened and its significance. Analysts are quite experienced, if not always proficient, in writing instant histories. In their first assignments, they are usually provided with a stack of cables—almost all of them describing an event in the past—and asked to write a concise piece describing the development and its import. The analytic profession has never devoted as much attention, nor has it developed as much technique, to address the future. In fact, many expert practitioners, such as former Deputy Director Dick Kerr, have often said that the primary job of the analyst is to explain, not predict, in large part because prediction is so difficult and risky. When the future is discussed analytically, it invariably takes one of three forms:

- A linear projection of current trends forward into the future. (Interestingly, the word trend—which sounds like it's about the future—is really only reliably a description of the past.)
- A scenario trio that borrows heavily from Goldilocks and the Three Bears: too hot, too cold and the ever popular just right.
- Or, if analysts are familiar with the scenario process developed by the Global Business Network, a set of four possible futures, each of which describes an extreme outcome so removed from the present day as to offer no obvious guidance to current policymakers.

The designers of the first Intelligence Community would not find this tradecraft well-suited for much of the analysis they would need. After all, they would already perceive that, on many issues, such as the policies of West European governments or the persistence of state failure in West Africa, they could obtain much of what they needed to know about current events from the media, or their NGO contacts, or their business acquaintances. As they set about to design the first national analytic capability, it wouldn't make sense to them to create yet another source of current information. Instead, they would probably be seeking some unique, analytic value-added that they couldn't reliably obtain from existing information networks. Even though they would recognize the difficulty, they would want analysts to understand the future, to identify when countries or societies are in danger of entering the pre-terrorism phase and to give them a

heads-up about new threats to national security, and not just provide a running commentary on today's problems.

An Analytic Solution

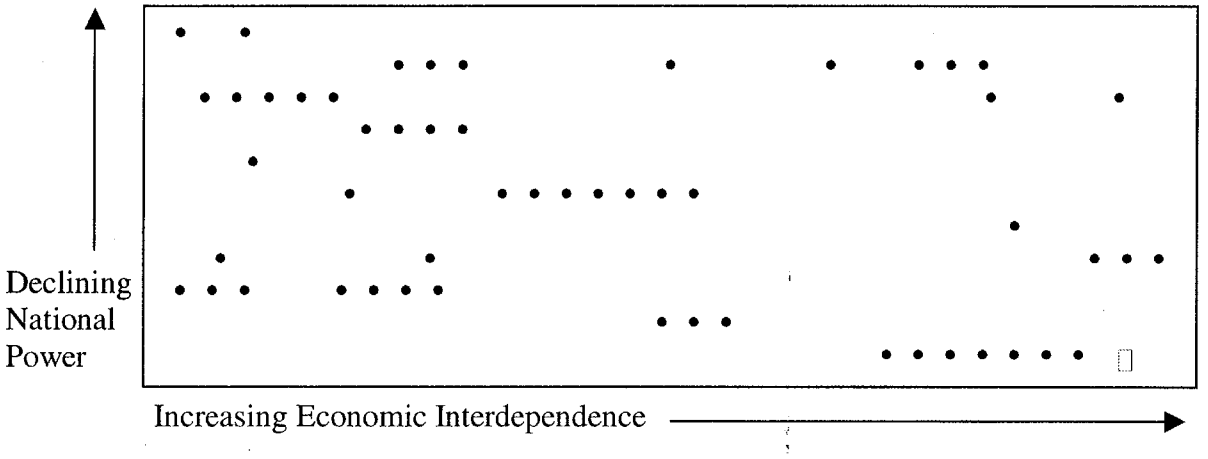
Given this goal, the first analytic capability might look something like this:
A group of analysts would be specifically charged with developing and refining a more effective tradecraft for thinking about the future. The mandate for our intrepid analysts would be clear but demanding: they were not just being asked to think about the future or gather expert opinions about possible outcomes. Their job was to combine every possible approach, from human creativity and imagination to advanced software techniques such as agent-based modeling, into a coherent, systematic process that would improve US prospects of identifying and understanding emerging issues and thus avoid strategic surprise.

As the first analysts approached this problem, they would find that some of their initial steps, while not that difficult, would yield measurable improvements. For example, the analysts might begin by assembling and keeping up to date a master list of scenarios concerning all relevant international and national security issues. This list could, in fact, serve a clearing function for government agencies wanting to plan strategically for the future. Policymakers, concerned that the US should always be optimally positioned to deal with emerging threats, probably would prefer to turn to a common resource for a more complete picture of contingencies.

But our first analysts could probably do more than just maintain a list of scenarios. They could also develop ways to categorize and organize these scenarios. Using either collaborative analytic approaches or perhaps some automated process, analysts could create "landscapes" that sorted the scenarios based on defined parameters. The analysts would probably develop not only a master landscape of scenarios but also landscapes that organized future scenarios dealing with a particular country or issue.

Starting Over

A Landscape of Future Scenarios



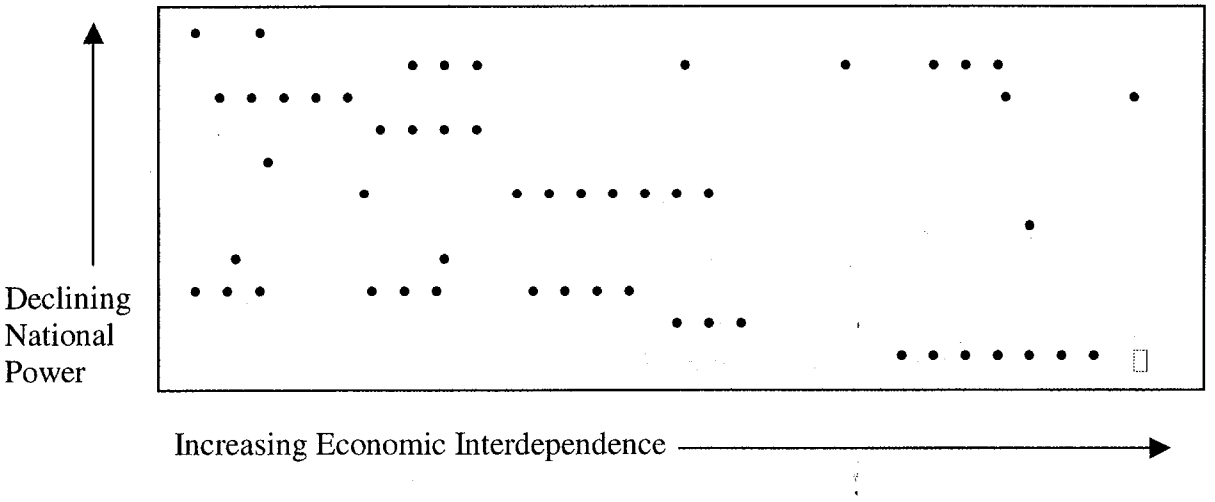
• • • Each dot represents a scenario arrayed against parameters

In the example above, the center of gravity for the scenarios, arrayed by the assumptions they make about the future power of nations and the interdependence of the world economy, is located in the left half of the landscape. This would indicate to analysts and policymakers alike that most scenarios about the world economy anticipate only modest future integration and that the level of integration is not particularly dependent on the power of nation states. Landscapes could be developed on a periodic basis, allowing analysts and policymakers alike to observe important shifts. Analysts could also compare a scenario landscape developed from the thinking of US Chinese scholars with a landscape depicting the views of Chinese nationals on the same issues. The differences would be instructive.

As useful as this approach could be, our analysts might be even more ambitious. Using content analysis and categorization software, they might be able to map sets of information, for example one year's worth of relevant New York Times articles or reporting gathered by the worldwide web of policeman/observers, against the same scenario landscapes. Over time, this technique might allow analysts to contrast the assumptions behind their scenarios against incoming information. Significant discrepancies might suggest that it was time to rethink the assumptions behind their scenarios. In the example that follows, for example, the yellow highlighting indicates how a particular set of information might map against this landscape of future scenarios. This discrepancy warrants analytic investigation.

Starting Over

A Landscape of Future Scenarios



• • • Each dot represents a scenario arrayed against parameters

Communicating Meaningful Findings To Policymakers

Finally, our policymakers would want to ensure that they had easy and timely access to the work of their new Intelligence Community. If they were starting with a clean slate, how would they want the Intelligence Community to communicate with them?

The policymakers might be motivated to develop a communications process based on a few simple principles.

Intelligence should be timely. There should be as little delay as possible between its completion and its availability.

Intelligence should be interactive. Policymakers should be able to quickly ask follow-up questions of analysts or delve more deeply into topics that interest them.

Intelligence should be persistent. Once the information is communicated, it should remain available and convenient so that policymakers and their staffs can refer to it when necessary and track significant changes in analysis.

Intelligence should be shareable. Given the worldwide nature of many of the emerging threats and opportunities, policymakers would want to know right away what information could be shared to rally allies and coax demurring governments. Their expectation would be that most information is in fact shareable.

A Communications Solution

Given these goals, the first capability to communicate findings to policymakers might look something like this.

While one is tempted to place the emphasis here on information technology that would no doubt meet all the policymaker goals, our new Intelligence Community would be better served by first deciding upon a classification and document-handling regime that was designed around the policymakers' objectives, and not around the interests of the collectors and analysts. Without a customer-focused protocol, any information system would be slowed down by the persistent requirement to reconcile the policymakers' needs with the unrelated logic of the classification regime.

Classification and other document markings for our first Intelligence Community would easily show:

- Whether a particular item of information could be made available on secure, wireless networks. This category might include information up to the level we now describe as Secret Noforn.
- Whether an analytic team was available to answer follow-up policymaker questions.
- Whether the information would remain available in a policymaker repository and for how long. Particularly sensitive information would protect itself through automatic purging software.
- Whether information was shareable, as is, with other governments.

At all times, the markings would make the status and further use of the information immediately evident to policymakers. The classification regime would facilitate, not impede, their timely use of intelligence.

Escaping Our Past

The way to developing an Intelligence Community capable of meeting future needs is to begin anew. As long as we let ourselves be restrained by structures and practices that were created many decades ago for a very different world, we will fail to adequately protect future US national security interests. The National Security Act that created the CIA and established our national community was enacted in 1947, or 57 years ago. To gain some perspective on how potentially misleading it is for us to accept decisions made then with anything other than grains of salt, we need only to consider the world 57 years before 1947. If President Harry Truman had made his decisions about the first National Intelligence Community with 1890 on his mind, our country and the world would have been poorly served.

Some of the suggestions in this paper may seem farfetched, alien to how we think analysts, collectors, or for that matter policemen, should work. But the professionals who began the Intelligence Community in the 1940s were courageous enough to take significant leaps of faith. They, too, imagined activities and jobs that had never been done before. But they accepted that the times required bold imagination. We should do the same.

Avoiding Intelligence Failure: An Approach to Recurring Self-Diagnosis by IC Senior Managers

By [redacted] (CMS)

(b)(3)
(b)(6)

Summary

The elements of intelligence reform alone are not sufficient for the Intelligence Community to make progress in avoiding future intelligence failures. There is a significant role for the IC's senior managers to conduct recurring self-diagnoses of their organizations. These self-diagnoses should be framed in terms of at least four factors: centralization versus decentralization for specific issues and tasks, the extent to which theories are used as guides to data, the organizational approach to handling uncertainty and the openness to lessons learned.

Background

The US Intelligence Community is potentially on the verge of one of the most sweeping reorganizations in its history. Expectations are high that the reorganization will correct deficiencies and ultimately pave the way for significant improvements in avoiding future intelligence failures. However, even at this late date, after extensive analysis of 9/11, it is not obvious how the elements of proposed reform by themselves will help avoid future intelligence failures. It is clear that changes in authorities and reporting relationships are intended to promote information sharing and "breaking down stovepipes." What is less clear is what mechanisms will be put in place so that more information sharing and fewer stovepipes help avoid intelligence failure. What else is needed?

This paper will make the case that the desired results of intelligence reform, including more information sharing and fewer stovepipes, are necessary but not sufficient conditions for helping avoid failures: More attention by senior IC management is needed, in a specific dimension. Even a complete overhaul of the Intelligence Community does not obviate the need to conduct repeated self-diagnoses over time. IC managers need to be continually exploring the trends and features in IC processes that have the most potential to lead to intelligence failure in the future. Such recurring assessments have the potential to support incremental organizational changes that will in turn improve the IC's ability to understand trends and complex phenomena signaling coming events.

What Are We Trying To Fix?

A huge part of the current debate over intelligence reform emphasizes the importance of information sharing between elements of the Intelligence Community and the related need to break down organizational stovepipes. What the current debate tends to miss, for most commentators, is that there are always trade-offs between intensive effort within a given domain of expertise and activities that work across domains. A complex organization with massive information flows in, within and out will always be trying to seek a delicate balance between intensive work within a stovepipe and lateral work to communicate with other areas of expertise, sources or needs for information.

To simplify the analyses of the House/Senate Joint Inquiry and the 9/11 Commission, 9/11 might have been avoided if, within the IC, FBI, INS and others within the US Government, there had been:

- More information sharing, including sharing across security classifications.
- Better recognition of the importance of particular pieces or "nuggets" of information.
- Better passing of "nuggets" up the chain of management.

The massive challenge, of course, is identifying which characteristics to pay attention to: share what information with whom? what are my criteria for recognizing importance in information? when does a "nugget" merit passing up the chain of management? When these kinds of questions are answered in a specific context, it amounts to successfully "connecting the dots."

With the benefit of hindsight and the painstaking analyses of chronologies, cable traffic and "who knew what when" by the both the Joint Inquiry and the 9/11 Commission, many commentators now see 9/11 as avoidable. For them, it should have been sufficient that the information to "connect the dots" was "somewhere in the system." For those responsible for helping to avoid future intelligence failures, the 9/11 analyses present a sobering lesson about how a great many individual lapses add up to systemic failure. However, the 9/11 analyses alone do not offer a definitive way forward. The factors that may have helped avoid 9/11 will likely not be the factors that will help to avoid the next, or after-next, challenge. Breaking down the specific barriers cited in the 9/11 reports certainly has merit and will improve the IC's posture in the future for a specific kind of threat.[1] Beyond that, a general exhortation for more information sharing, or better recognition or up-chain passing also is not very helpful for practitioners.

There is simply no formula that applies across the complex range of activities across the IC to identify what to share, with whom, the criteria for recognizing importance and so on. From this perspective, mandating information sharing and breaking down stovepipes

[1] Cordesman, Anthony, August 2004, The 9/11 Commission Report: Strengths and Weaknesses, Center for Strategic and International Studies

as part of intelligence reform can be only part of the solution in helping avoid intelligence failure.

The Organizational Roots Of Information Sharing

To provide guidelines for IC managers trying to grapple with future intelligence failures, it is necessary to go beyond the last, worst example. One way to do this is to try to relate the elements of "connecting the dots" to organizational factors. IC senior managers need to be asking more often: What are the organizational roots of more information sharing, better importance recognition and better up-chain passing of information for my own and other relevant elements? This paper offers no definitive answer to the question. To do so would require more insider knowledge about how organizational factors influence information flows across the IC and in individual elements. Such knowledge probably does not exist in a single spot anywhere in the Community. This paper, however, does suggest that four broad organizational factors are major influences on information sharing and the other elements of "connecting the dots." This is one way to begin to give some meaningful content to the notion that there is need for a change in "IC culture." The four factors in summary are:

- How centralized or decentralized an IC element is: how much is the element focused internally to meet mission and taskings? How much access do senior managers have to information brokers from other organizational elements? How much access and influence do such brokers have? Are such brokers only from adjacent elements or also from those far away in the organizational landscape?
- The extent to which an organizational element encourages or tolerates use of theories or alternative explanations of adversary behavior or events: To what extent is there tolerance for coherent speculation on motives, unseen connections or communications, causes of behavior? Is debate of competing theories encouraged or discouraged in the interests of a more straightforward message or nuggets of new, solid information?
- An organizational element's approach to measuring and monitoring uncertainty: How much do managers force themselves to think above the substantive complexity of an activity to ask themselves about sources of uncertainty? Are managers focused on the right time dimension: days – weeks – months – years for the intelligence problem under their purview? To what extent have the sources of uncertainty changed?
- Openness to lessons learned: How does an element exploit the lessons of recent operations, crises or salient activities to get insight into "the good, the bad and the ugly"? How widespread are solicitations of lessons learned? How honest are lessons learned?

A key point here is that, for each of the factors, there is no "right answer" for all time and all elements. The IC cannot complete reform and declare: "we have arrived." Rather, the "right answer" will vary even for a single organization over time. Getting to the "right answer" has to be the result of continual assessment in the light of the element's mission and tasks, the nature of the threats and where the element fits in the rest of the US

Government landscape. The "right answer" for a given set of circumstances has to be determined based on the judgment of senior managers, based on their recurring diagnosis. The thesis of this paper is as follows: If IC senior managers get used to seeing their own organizational elements in these terms, and acting on their judgments to vary these factors, it will open the way for incremental adjustments and contribute to avoiding intelligence failure. This approach, if institutionalized, would recognize that avoiding intelligence failure is a "game of inches" of hundreds of incremental judgments. Such recognition would be a major innovation in the way the IC does business.

Each of the four factors below is considered in more detail.

How Centralized Or Decentralized Is An IC Element For A Specific Issue?

The injunction of some commentators on intelligence reform to "break down stovepipes" involves complex trade-offs. To a great degree, a "stovepipe" is where expertise, sometimes highly specialized, is recruited, developed, rewarded, managed, funded, advocated and tasked. Centralization of people and effort around an issue, for example North Korean WMD, allows for expertise to exist and grow, and forms the precondition for information sharing with others. At the same time, some degree of decentralization, including lateral or horizontal coordination, is mandatory. The consumers of intelligence tend to live outside the stovepipes. Cross-talk with people in adjacent or related areas of expertise can cause people within stovepipes to get a better grasp on what is actually happening, relationships that they might not be aware of and other benefits. The key point is that eliminating stovepipes is not a true option. Rather, across the entire set of IC issues, regions or interest and tasks, there is a shifting mix of centralization and decentralization that needs to be adjusted.

Some of the trade-offs bearing on centralization/decentralization are as follows:

- Cultivating and maintaining subject matter expertise calls for specialization but specialization can result in parochialism, inter-unit rivalry, blockage in information sharing and concealment of dissent and alternative interpretations.
- The need to motivate and control personnel requires hierarchy, but hierarchy can result in filtering in upward communication, the perceived need to keep substantive experts "in their place" and isolated, and a "groupthink-oriented" emphasis on loyalty to the sub-unit.
- Proper coordination (many experts, many overlapping subject matters, many trade-offs for attention and resources) calls for centralization, but centralization can result in top management layers that are overloaded and out of touch.
- Classified sources and methods, often highly vertically-oriented, can penetrate "real secrets"—things that adversaries are actively trying to hide—but can create a sub-culture of ideas that sharing is always on a case-by-case basis, secret sources are superior, and that limiting access is a way to stifle dissent on interpretations.

In some circumstances, more specialization or vertical orientation is needed: to sharply increase specialized expertise, to pursue covert activities, to encourage candor within a limited group, or for other reasons. Some organizations can become so "coordination-oriented" that they cease to have any real expertise in a given domain. In contrast, over time, or in other circumstances, more lateral contacts, or involvement with "out-of-channel contact people" are needed to broaden perspectives, share concerns, calibrate information sources, introduce skepticism, cross-fertilize views of narrower experts and other reasons. How centralized or decentralized, vertically or laterally oriented an organizational element should be at a given time is a matter of judgment.

How Are Theories Or Alternative Explanations Of Behavior Or Events Factored In?

What information is shared, deemed important or passed upward in particular cases is likely to be driven in part by an organization's attitude toward theory or alternative explanations of phenomena or behaviors. For example, different theories on the level of cooperation between different Iraqi insurgents and the extent to which ideological or sectarian difference matter could serve to help air opposing viewpoints, develop coherent views of conflicting data and promote sharing of concerns on anomalies. Another possible example comes from the Senate's report on the IC's prewar assessment of Iraq WMD[2].

The benefits of attention or openness to theory are various:

- Automated or web-based forms of information flow, access and storage create efficiencies but can also create an implicit doctrine of "more is better," to the detriment of interpretation or theories as guide for organizing or seeking information.
- Especially in an environment where there are massive volumes of inflowing information, theories can be powerful tools to organize information and to prioritize information needs. Theories can be used as guides to data collection, data needs, data organization and interpretation and analysis. Development of theories can help people fit disparate data into a coherent picture, highlight the need to bring other data into the picture and serve as the basis for further posing of questions, even if there is a risk that the theory is wrong.
- Theories also can be a major dimension of cross talk between people from diverse elements of Community. The different theories could serve as the basis for asking questions and discussion among people from diverse parts of the IC and US Government.

[2] Senate Select Committee on Intelligence, SSCI# 2004-2940, 7 July 2004, Report on the U.S Intelligence Community's Prewar Intelligence Assessment on Iraq, (redacted version) pp. 21

Like centralization and decentralization, there is no single, once-and-for-all balance between use of theories and its opposite, relying on raw and interpreted data and "connecting the dots" with yet more data.

The aspect of no "right answer" on the use of theory is well recognized in one of the classics on intelligence art, *Psychology of Intelligence Analysis*. In that book, Richard Heuer notes:

> "There are both advantages and drawbacks to applying theory in intelligence analysis. One advantage is that "theory economizes thought." By identifying the key elements of a problem, theory enables an analyst to sort through a mass of less significant detail. Theory enables an analyst to see beyond today's transient developments, to recognize which trends are superficial and which are significant and to foresee future developments for which there is today little concrete evidence."[3]

Heuer also notes some of the problems caused by relying on theory:

> "Theoretical propositions frequently fail to specify the timeframe within which developments might be expected to occur. ..if theory enables the analyst to transcend the limits of available data, it may also provide the basis for ignoring evidence that is truly indicative of future events."[4]

The use of theory as way of organizing data and thought bears on the 9/11 Commission's critique of the IC needing to institutionalize imagination[5].

As before, reducing the risk of intelligence failure requires IC managers to get used to thinking in terms of varying the factors for their organizational element and others in current and projected circumstances.

What Is The Organizational Approach To Handling Uncertainty?

A third major factor bearing on the potential for distortion of information in the IC is the general approach by which the IC writ large, and IC organizational elements handle the uncertainty of information. Organizations can be more or less attuned and willing to revisit the major uncertainties that underlay the information coming into and leaving the organization, and the kinds of factors, internal and external, that affect the uncertainty of the information. Lack of use of mechanisms such as red teams, devil's advocacy and

---

[3] Heuer, Jr., Richards J., 1999, Psychology of Intelligence Analysis, Center for the Study of Intelligence, pp 35

[4] ibid, pp 36

[5] The National Commission on Terrorist Attacks Upon the United States, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2004, pp. 339-348,

competitive analysis were a prominent part of the Senate's assessment of the IC for Iraq WMD[6].

A classic thinker on the sociology of information in private sector companies, Arthur Stinchcombe, provided insight into what managers need to pay attention to:

> "The maintenance of the quality of the flow of information is in general achieved by constant minding by people who know what uncertainty is to be analyzed, where the news about it is to be got, what causal units are subject to that uncertainty, how to make the trade-off between currency of information and noise reduction, what temporal span the decisions cover, what degree of uncertainty different sorts of information are subject to, who is motivated to distort the system, what auditing or control procedures will work and who are the other experts to consult on all these questions."[7]

> "Many of the sources of untrustworthiness of information are faults in the incentive system for providing accurate information and accurate estimates of how one is likely to be wrong."[8]

This way of thinking about uncertainty in manufacturing also could apply to some aspects of work in the Intelligence Community. It poses the question: To what extent do which IC managers take the time to raise themselves above the fray of tasks and process to assess the sources of uncertainty affecting their element and seams with other elements?

Attention to the sources of uncertainty likely varies across the elements of the IC. Elements involved in HUMINT, for example, are likely to be highly tuned to diverse sources of uncertainty. Other elements may be less attuned. In the effort to produce daily usable product, for whatever kinds of intelligence function, there can be a tendency to become complacent about the sources of uncertainty or to focus attention to uncertainty to the inherent unknowns in the intelligence. An alternative approach is to give periodic attention not just to the inherent unknowns but also to the uncertainty in the "factors of production"—the characteristics of the process and people involved in producing the intelligence. Thinking in terms of the more abstract "factors of production" may come naturally to many IC senior managers and may require a deliberate focused effort to achieve.

---

[6] Senate Select Committee on Intelligence, SSCI# 2004-2940, 7 July 2004, Report on the U.S Intelligence Community's Prewar Intelligence Assessment on Iraq, (redacted version) pp. 19-28

[7] Stinchcombe, Arthur L., 1990, Information and Organizations, University of California Press, pp 17

[8] ibid, pp. 15

What Is The Level Of Openness To Lessons Learned?

Efforts to eke out lessons learned from prior activities, assess them honestly and reasonably disseminate and debate the results can be a major tool of organizational self-diagnosis. In an important sense, efforts on lessons learned can knit together the preceding three factors: experience from prior efforts can show where centralization versus decentralization worked well or poorly, how the use of theories did or did not contribute and help clarify if organization's approach to uncertainty was sound.

Such lessons learned activities are particularly important for war or crises. To paraphrase a dated public service advertising spot for the United Negro College Fund, but applied to war or crises: "Data is a terrible thing to waste." In war and crisis situations, the organizational element is stressed, the users of intelligence are stressed and the pace is typically much higher. The potential for information distortions to arise is multiplied: information not shared, information not recognized for its importance, information not passed appropriately up the chain and others. After the fact, it is critical to develop chronologies on who knew what when, conduct candid interviews with intelligence consumers to determine what happened and how could it have been done better. Not to collect and assess such real-world data, such as is available from Afghanistan and Iraq operations, is a waste because it misses a relatively painless chance to self-correct.

Part of openness to lessons learned is the willingness to take a 360 degree view of events, including interviews with participants at the worker analyst level and up and down the chain of management, within the scope of an organization. For example, the conclusion that an analytical misjudgment was the result of bias in analyst assumptions is unlikely to have been based on a 360-degree assessment.[9]

Extent Of IC Self-Diagnosis

This paper has outlined four factors that could link organizational features to the elements of "connecting the dots" in the IC. As noted above, this approach requires IC managers to get used to thinking and making adjustments in terms of what the "right answer" is for their organizational element and others in the current and projected circumstances. To what extent does the IC today conduct and act on self-diagnoses of kinds described above? This is probably a topic requiring another paper, and it is difficult to generalize across the entire Community, but some preliminary judgments are as follows:

- Since 9/11, there has been significant growth in the number of organizational elements increasing their lateral contacts. The decentralization dimension has received major attention as a means of facilitating information sharing.

[9] In a given case, analyst assumptions may or may not end up being the major problem, but only after an honest assessment of the role of management, the position the analysts were put in, and other factors.

- The senior management of the Intelligence Community seems to lack the ability or mechanisms to get organizational assessments on a recurring basis without the intervention of outside commissions and panels.
- There seems to be an IC bias against theory in favor of solid bits of new data, volume of data and better means of categorizing and tagging data for ready access. A symptom of the disfavor in which theories are held may be the relative lack of debate in the Community over competing broad interpretations.
- The IC's approach to lessons learned varies by organization, but outside the activities of the Inspectors General, it is generally at a depressed level. Community-level lessons learned efforts tend to be rare. Where lesson learned efforts are undertaken, they sometimes serve the function of marketing good outcomes, not serving as an input to self-diagnosis.
- The more formal mechanisms for self-diagnoses in the Intelligence Community tend not to direct attention to the organizational factors at work that could cause or contribute to distortions. The two leading examples are the means for measuring effort against the National Intelligence Priorities Framework (NIPF), and the performance measures that are put in the IC's President's Budget submissions. The NIPF is a major improvement in the way the IC tracks investment of effort over time toward major issues, regions and threats. However, in directing attention toward the trends and patterns of effort across priorities, the NIPF has less relevance toward the potential for information distortions in any specific priority. The organizational pathologies that may exist between priorities also get relatively little attention in the NIPF. The performance measures system that the IC is now including in Congressional Budget Justification Books is only a point of departure for more attention to organizational factors. The system stipulates goals and putative measures of progress toward those goals but does not provide a framework for linking to organizational behaviors.

Conclusions And Recommendations

An approach to avoiding future intelligence failures that relies only on macro-structural changes in organizations (missions, reporting relationships, authorities) is intellectually suspect: such an approach cannot easily explain how the intended result is supposed to work. A successful approach needs to explain what mechanisms will be put to work to cause increased information sharing, for example, of the right kind, at the right time, with the right content. The approach taken in this paper is to recognize that structural reform can help greatly, but that the burden of helping avoid failures is with IC managers, and making improvements is an incremental "game of inches." One way to guide managers is to focus on a set of factors bearing on how the IC writ large and individual elements organize and process information: centralization versus decentralization for specific issues and tasks, the extent to which theories are used as guides to data, the organizational approach to handling uncertainty and the openness to lessons learned. The

course correction that might be needed at any given time will vary, but the thesis of this paper is that the kinds of factors that need attention remain more or less the same.

The following table shows how the four organizational factors may contribute to the behaviors that more directly help avoid intelligence failures.

Relevance of selected organizational factors to behavior to help avoid intelligence failures (X indicates relevant contribution of row to column)

	Information sharing	Importance recognition	Passing critical info up-chain
Centralization versus decentralization	**X**		**X**
Use of theory	**X**	**X**	
Approach to uncertainty	**X**	**X**	**X**
Openness to lessons learned		**X**	**X**

For example, use of theory has the potential to allow for more coherent cross talk across subject matter domains and increase the chances of information sharing and recognition of information importance. Openness to lessons learned is a means for IC senior managers to communicate priorities, as well as giving people a sense of can go awry, thereby contributing to importance recognition and passing information up-chain.

In one important sense, for IC managers to adopt this perspective, they would have to recognize that, in complex organizations, to include the IC, distortion of information or intelligence is inevitable. In a given circumstance, factors such as centralization versus decentralization, the extent of use of theory and the approach to uncertainty can be at the wrong setting—leading to information distortion. Even openness to lessons learned can become excessive if people become too backward-focused or risk-averse.

To adopt the approach discussed in this paper would require IC managers to take risks. Adjusting an organization's operating features in the absence of external direction, based on judgment on potential beneficial effects, requires going out on a limb. In addition, there are inherent difficulties in making IC organizational elements agile enough to respond to the results of repeated self-diagnosis: constraints involving budgets, personnel policies, security policies and inertia stand in the way. However, if avoiding intelligence failure is in fact an incremental "game of inches," achieved or not at the level of hundreds of IC managers, then it is imperative to change. The senior management of the Intelligence Community should be in a position to ask, and answer, questions about what

factors in their organization or in seams with other organizations may affect their ability to "connect the dots" successfully at a given time, even if IC agility initially appears to be limited.

Beyond "cultural change" with the content discussed above, some specific actions could be taken, as follows:

- Formalize a discussion of the appropriate degree of centralization versus decentralization for a sample of high NIPF priorities, or CTC or TTIC areas of expertise. Develop actual graphic maps of the extent and access of lateral "information brokers."
- Undertake an effort to graphically map out the IC's contacts with elements of the Department of Homeland Security.
- Establish a small NIC-like entity in each relevant organization as means to (1) stimulate and solicit debate on theories and alternative explanations for major open analytical issues, and (2) conduct reviews of draft outputs for the factors affecting uncertainty.
- Use the ADCI/C and ADCI/A&P forums to stimulate and solicit debate on theories and alternative explanations for major open analytical issues. Pose questions to Issue Teams to describe the leading alternative explanations for major areas where there are conflicting data.
- Establish a small Community-level organization to initiate, guide, consult on and review lessons learned efforts. Coordinate closely with relevant DoD and Service lessons learned activities. Seek to hire people with DoD or Services experience in lessons learned development.

References

Cordesman, Anthony, August 2004, The 9/11 Commission Report: Strengths and Weaknesses, Center for Strategic and International Studies

Etheredge, Lloyd S., 1985, Can Governments Learn? Pergamon International Library

George, Alexander L., 1995, Bridging the Gap-Theory and Practice in Foreign Policy, US Institute of Peace

Heuer, Jr., Richards J., 1999, Psychology of Intelligence Analysis, Center for the Study of Intelligence

The National Commission on Terrorist Attacks Upon the United States, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2004

Senate Select Committee on Intelligence, SSCI# 2004-2940, 7 July 2004, Report on the U.S Intelligence Community's Prewar Intelligence Assessment on Iraq, (redacted version)

Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attack of September 11, 2001, Dec 2002

Stinchcombe, Arthur L., 1990, Information and Organizations, University of California Press

Wilensky, Harold L., 1967, Organizational Intelligence, Knowledge and Policy in Government and Industry, Basic Books, NY

Wohlstetter, Roberta, 1962, Pearl Harbor, Warning and Decision, Stanford University Press

It's Not Rocket Science: The Limits of Analysis and the Requirement for a "Synthetic" Complement

(b)(3)
(b)(6)

Summary

This paper argues that it is a deeply ingrained Newtonian "analytical" mindset that causes intelligence analysts to unconsciously but continuously misapply a linear behavioral template to their assorted subjects (nation-states, non-state actors, etc.) – subjects that are in fact inclined to "nonlinear" behavior. This, in turn, promotes the illusion of predictability, and consequently, the likelihood of surprise. Given this, the article considers the basic behavioral characteristics of nonlinear systems – especially their inherent unpredictability and dynamism -- and explains how the prevailing linear mindset and metaphors are less than ideal for dealing with those characteristics. Subsequently, the article explores how more applicable nonlinear perspectives might be cultivated so as to more realistically account for and accommodate that fundamental unpredictability.

> For decades, the U.S. Intelligence Community has propagated the myth that it possesses analytical methods that must be insulated pristinely from the hurly-burly world of politics. … The C.I.A.'s scientific pretensions were established early on by Sherman Kent. In his 1949 book, "Strategic Intelligence for American World Policy," Kent argued that the truth is to be approached through a systematic method, "much like the method of the physical sciences." This was at the time, just after the war, when economists, urban planners and social engineers believed that human affairs could be understood scientifically, and that the social sciences could come to resemble hard sciences like physics.
>
> -- David Brooks, The C.I.A.: Method and Madness, The New York Times, 3 February 2004

An Uncomfortable – But Fundamental – Truth

"Gibberish." "A rant." "Brooks just doesn't understand what we do."

These comments are a representative sampling of the responses elicited by the posting of the above-quoted passage on the DI discussion database. And to be fair to the respondents quoted, Brooks is indeed wrong on several counts, not the least being his assertion that the Intelligence Community/Central Intelligence Agency (hereafter referred

to as the IC) has "scientific pretensions." For the fact of the matter is that what the IC does is indeed "science." It may be empirical/soft (social) science vice experimental/hard science, but it is science nonetheless.

That said, however, it is in this distinction that Brooks comes very close to an uncomfortable truth – namely, that the IC does tend to approach its task as though it were a hard science. The reason it does this is (or ought to be) obvious: the IC is expected to be able to predict events, and hard sciences lend themselves to predictability.

Not Kent – Newton

For all Kent's lingering influence on the IC, Brooks exaggerates when he says that it is due to Sherman Kent that the IC tends to apply hard science – particularly linear – approaches to its problem sets. For the real culprit behind this tendency is more the lingering influence of Isaac Newton whose laws of motion have exerted such a fundamental grip on the Western worldview.

Given this observation – and the fact that recognition must precede remedy -- this paper will begin by arguing that it is a deeply ingrained Newtonian mindset that causes intelligence analysts to unconsciously but continuously misapply a linear behavioral template to their assorted subjects (nation-states, non-state actors, etc.) – subjects that are in fact inclined to "nonlinear" behavior.[1] Second, it will examine how this mindset promotes the illusion of predictability. Third, this article will consider the basic behavioral characteristics of nonlinear systems – especially their inherent unpredictability and dynamism -- and explain how the prevailing linear mindset and metaphors are less than ideal for dealing with those characteristics.[2] Fourth, and finally, this article will explore how more applicable (i.e., less bounded) nonlinear perspectives might be cultivated so as to more realistically account for that fundamental unpredictability.

---

[1] This largely unconscious application of a simplifying behavioral template is an excellent example of "bounded" or limited rationality, a concept first advanced by Herbert Simon. "Because of limits in human mental capacity," he argued, "the mind cannot cope directly with the complexity of the world. Rather, we construct a simplified mental model of reality and then work with this model. We behave rationally within the confines of our mental model, but this model is not always well-adapted to the requirements of the real world." From Heuer, Richards J., *Psychology of Intelligence Analysis*, Center for the Study of Intelligence, Washington, DC, 1999, pp. 3.

[2] What this article refers to as a "nonlinear" system is more commonly, and perhaps more accurately, referred to as a "complex" system. The reason for this use of nonlinear vice complex is that most people tend to confuse the distinct scientific meaning of the term complex (i.e., having many interactions that can lead to untold changes in behavior) as it would be used here, with its more common usage that is synonymous with complicated (i.e., having many components).

Square Peg, Round Hole

The term "linear," when applied to a system – any grouping of components that together interact according to some "rules" so as to form a larger whole -- describes behavior of the whole which is *additive*, that is to say equal to the sum of its parts.[3] By extension, a linear approach to understanding a system holds that once a system's component pieces' behaviors are understood individually, it is merely a matter of adding them all together in order to understand -- and consequently predict -- the system's behavior as a whole. This analytical methodology (from the Greek *analyein* meaning "to break up"), often termed "reductionism," "linear reductionism" or "Newtonian reductionism" (after Sir Isaac Newton) is, by and large, the default Western – and certainly American -- approach to information processing.[4]

The main limitation of this approach, as the term reductionism suggests, is that it only works well with systems that are genuinely reducible. Since the components of linear systems do not change or adapt their fundamental behavior as interaction occurs, the components of such systems, and consequently such systems as a whole, can be readily understood via reductionist approaches. Moreover, as a result of this "constancy of behavior," linear systems also tend to be susceptible to prediction and manipulation. For example, mechanical systems, such as the solar system or ballistic missile systems -- "rocket science," as it were -- tend to be highly linear. Consequently, the movements of the planets and the trajectories of ballistic missiles are theoretically, if not always practicably, predictable and pliant.

However, as a means for understanding (i.e., predicting) the behavior of nonlinear systems -- those systems in which the behavior of the whole is not necessarily equal to the sum of the parts -- linear reductionist approaches offer significantly less utility. For one thing, nonlinear systems are not readily reducible. In nonlinear systems, the behavior of the various components changes, evolves and adapts as interaction occurs, and consequently, the components of such systems cannot be realistically considered absent or removed from one another. For the purposes of this article (and in marked contrast to what the prevailing mechanical metaphor -- balance of power, tension, inertia, etc. -- might lead one to believe), a good example of a nonlinear system is the international system. In that system, the various components (supra-national organizations, nation-states, non-state actors, etc.) are also systems in themselves, and their unique sub-

[3] Plotted on a graph, these types of equations form smooth lines – hence the name linear. For an understandable discussion of this that is particularly useful to the lay reader, see Waldrop, M. Mitchell, *Complexity: The Emerging Science at the Edge of Order and Chaos*, New York, Simon and Schuster, 1992, pp. 64

[4] Although reductionism is usually associated with Newton since he effectively "codified" it with his laws of motion, its roots go back to the ancient Greeks – it was Aristotle who emphasized "illumination through disaggregation."

components (nation-states, individuals, families, social/political/commercial organizations, etc.) are often systems as well.

As a result of this "system of systems" character and the interactivity, dynamism and adaptability that it leads to, nonlinear systems tend to be "messy" and resistant to thorough understanding via excessively neat, linear, reductionist approaches. Rather, what is required is a *complementary* (not necessarily substitute) approach that is based on developing a broader, big-picture perspective -- what Nobel Prize-winning physicist Murray Gell-Mann has termed a "crude look at the whole" or, in a word, a synthesis.[5]

That said, the development of such a "synthetic" perspective is usually more easily said than done. Since synthesis is the antithesis of analysis and most Americans lack a well-developed nonlinear/synthetic intuition, the intuitive response when confronted with significant complexity (numerous components, interactions and feedback loops) is to default to the artificial but comforting simplicity (read predictability) of linear reductionism. And it is this resulting application of linear approaches and perspectives to what are essentially nonlinear systems that is a recurring theme of America's foreign policy analysis in general, and its intelligence analysis in particular.[6]

Illusions Of Predictability

In addition to *additivity,* linear systems also demonstrate *identifiable cause-and-effect* relationships, *repeatability* and *proportionality* between inputs and outputs – properties that together render linear systems susceptible to prediction.[7] And since prediction, as mentioned earlier, is expected of the IC, a linear prism is inherently attractive to intelligence analysts shouldering those expectations. Nowhere is this more apparent than in the choice of terminology/metaphor that analysts tend to employ than when talking about the future.

The Newtonian term "trajectory" almost invariably attaches itself to *any* American discussion that involves prediction. Formally defined, the term describes smooth, evolutionary, continuous – and thus predictable – movements over time, such as those of the planets in accordance with Newton's laws of motion. By contrast, the term does not apply to the abrupt, revolutionary or discontinuous perturbations that inevitably – but

---

[5] Gell-Mann, Murray, "The Simple and the Complex," *Complexity, Global Politics and National Security*, Washington, DC, National Defense University, pp. 19

[6] This reductionist mindset is clearly illustrated in the terms with which foreign policy tends to be discussed. For instance, one often hears of foreign policy *analysis* or intelligence *analysts*, but rarely, if ever, of foreign policy *synthesis* or intelligence *synthesists*. Moreover, when synthesis is mentioned, it is usually subsumed within the analytical context of organizing and summarizing information, and not as a distinct intellectual approach or perspective.

[7] Czerwinski, Thomas J., *Coping with the Bounds: Speculations on Nonlinearity in Military Affairs*, Washington, DC, National Defense University, pp. 8-9

unpredictably – occur in nonlinear systems. Given this, it can be argued that the extensive use of this term is a manifestation of the constant (mis)application of a linear behavioral template – a template that allows for a system's past behavior to be projected continuously into the future. Indeed, this use of this term is really just another way of *predicting continuity* and, in common practice, these terms are often used in conjunction, as the following quotation both explains and illustrates:

> ". . . knowledge of why and how things have gone as they have day after day for years naturally inclines the analyst to estimate that developments will **continue** along the same **trajectory**. It is always a safer bet to **predict** that the situation tomorrow will be like it has for the last dozen years than to say that it will change abruptly."[8] (Emphasis added)

Terminologically consistent with the mechanical "trajectories" mentioned above, America's foreign policy debate has long been framed in the largely linear and mechanistic terms of linkages, levers, inertia, momentum, tension, etc. In this context, nations and such tend to be discussed as if it were a physical object that can be pressured, pushed, pulled or propelled. An excellent example of this was apparent in the flurry of commentary that surrounded the collision of an American surveillance aircraft and Chinese fighter in April 2001. Take, for instance, this editorial from the *New Republic*:

> Also abounding was the bizarre notion that the United States has little or no leverage over China. . . . This is nonsense. The United States buys 33 percent of China's exports. China buys 1 percent of the United States' exports. This looks like a lot of leverage to us. There is also the matter of China's membership in the World Trade Organization, and of the Olympics that Beijing fervently desires to host and of the sophisticated weaponry that Taiwan wishes to acquire from America. Levers, levers, levers.[9]

For all its passion and apparent sensibility, this passage's emphasis on leverage and levers is particularly useful for illustrating how linear templates, when erroneously applied to nonlinear systems, provide the illusion of predictability. In particular, this passage provides an excellent illustration of how, when looked at through a linear prism, a nonlinear system tends to take on the mechanical character that permits it to be discussed – however artificially -- as though it were a ball of clay whose behavior can be predicted a la Newton's laws of motion.

---

[8] Betts, Richard, "Fixing Intelligence," *Foreign Affairs*, January/February, 2002, pp. 49
[9] *The New Republic*, April 23, 2001

In the aggregate, although these linear processes have their own logic, the fact is that they really only provide their practitioners with arguments for a single *possible* scenario – not the much wider array of *plausible* outcomes. Thus, in the broader sense, the problem with such linear prisms is that they directly contravene Gell-Mann's requirement for a "look at the whole" and in doing so, completely, but artificially, wash out the complex dynamism (with its alternative outcomes, unexpected effects, etc.) that is inherent in the behavior of nonlinear systems.

Complex Characteristics

Based on the unrealistically predictive illustrations above, it should be clear that the characteristics of linear systems (additivity, evident cause-and-effect, repeatability and proportionality) discussed earlier have limited utility when one is trying to think about – predict -- the future behavior of a nonlinear system. Consequently, before the American debate over China can reasonably reflect reality, it is necessary to illuminate the nonlinear complements of those linear characteristics. These include:

Synergistic, not additive. First and foremost, a complex system's essence lies in how the components interact, not in any individual component. These interactions can be direct or indirect, obvious or subtle. From an intelligence perspective, this makes for a daunting and often messy challenge. Take for instance the regional analytic divisions within the IC. Sensible as it might seem for any number of reasons – from simplicity to manageability to political expediency – to impose such separations, any such separation is unavoidably artificial. In other words, actions in Europe have consequences in Asia and to consider them distinctly is, however understandable, also artificial.

Uncertain cause-and-effect. This expansive interconnectivity and interaction makes cause-and-effect relationships in complex systems ever-changing and often uncertain. While cause-and-effect tends to be predictable in linear systems (it's usually a safe bet that pressing the accelerator will result in an increase in acceleration), this is often not the case in nonlinear systems. In fact, in nonlinear systems – probably 95% of the systems watched by the Intelligence Community – cause-and-effect is only clearly identifiable in retrospect. This fact, in turn, helps explain why the IC, with its predominantly linear lenses, tends to focus on (and excel at) explaining what has already happened – not what might happen.

Not repeatable. The dynamics of any particular complex system are unique to its own specific combinations of components, initial conditions, interactions and timing. Consequently, the exact re-creation or repetition of such dynamics in other instances is impossible. From an intelligence perspective, this is important because policymakers commonly seek policy precedents and the validation that they believe such precedents bestow. This is dangerous; in complex systems, *exact* circumstances do not repeat

themselves.[10] Therefore, it is important that analogies not be over-stretched. In practice, the benefits to be derived from the consideration of historical precedent often derive more from the recognition of contextual differences (contrasts) than from the illumination of apparent similarities (comparisons). This is especially problematic in a warning context since the dynamics of events that we take as our lessons simply do not repeat themselves. Perhaps no better example of this danger exists than the 9/11 Commission Report which is so fixated on preventing *a repeat* of 9/11 that it almost ensures that we will be surprised when the next attack emerges from a different operational dynamic.[11]

***Disproportionate input and output.*.** In order for any impulse, especially one introduced from outside a complex system, to prosper and ultimately reveal and/or sustain its effect on a system's behavior ("tipping" is the usual mechanical term applied to this), it must at some point be reinforced by the system itself. Without positive feedback on at least some level, an impulse will not survive, much less flourish or "emerge" in the face of systemic resistance. Sometimes this process takes a significant amount of time. This said, the confluence of circumstances and timing cannot be emphasized enough. No matter how carefully crafted or brilliant a particular policy might be, both the moment and conditions must be opportune – ripe – if the desired effect or outcome is to result.[12]

Changing The Metaphor, Changing The Mindset (And The Reverse)

Evolution, adaptation, side effects, interactions, ripeness, etc.; these are the terms and concepts of biologists, psychologists and medical doctors – not mechanics, physicists or engineers. This noted, it ought to be clear that the ingrained mechanical metaphor is ill-suited to accurately reflecting, and consequently dealing with, nonlinear systems. Instead, what is required is a more apt metaphor that is firmly rooted in the life sciences. For foreign intelligence analysts this means learning to think, converse and act more like the professionals in those fields. For instance, just as doctors need to think about *interactions* (drug combinations), *side-effects* (allergic reactions), *particularity* (patient specifics: age, weight, blood type, etc.) and *timing* (stages of a particular illness, age of patient, etc.), so must intelligence analysts. Moreover, and perhaps most importantly as a starting point for analysts to build upon, the prevailing mechanical lexicon (trajectories, leverage, inertia, momentum, tension, etc.) needs to be supplanted – consciously to start, unconsciously in time (hopefully) -- with a more biological idiom.

---

[10] As a philosophical basis for this assertion, nonlinear systems theorists often point to the Greek philosopher Heraclitus and his observation that "it is impossible to step in the same river twice." For an excellent side-by-side comparison of Heraclitian and Newtonian metaphors, principles and terminology, see Andrew Ilachinski's *Land Warfare and Complexity, Part II: An Assessment of the Applicability of Nonlinear Dynamic and Complex Systems Theory to the Study of Land Warfare*, Center for Naval Analyses, Alexandria, VA., 1996, pp. 52-53

[11] See Nassim Nicholas Taleb's "Learning to Expect the Unexpected," *The New York Times*, 8 April 2004

[12] "Ripeness" in a foreign policy/strategic context receives exceptional treatment in Steven R. Mann's "Chaos Theory and Strategic Thought," *Parameters*, Autumn, 1992, pp. 54-68.

This issue of metaphor is bound to be controversial, as many who read this will undoubtedly be inclined to dismiss it as much ado over what are merely figures-of-speech or semantics. After all, mechanical terms and concepts like trajectory, leverage, momentum, tension and such are now so infused into the foreign policy lexicon as to seem unassailable. Such a dismissal, however, would be a mistake. Metaphors are extraordinarily powerful in that they both reflect and reinforce the mindset from which they spring – no matter how unrealistic that mindset may be. Therefore, as a second step – after first recognizing the problem -- it is critical to get the metaphor as realistic as possible.

Toward A "Synthetic" Complement

Metaphors are only one way of "modeling" a complex system, and changing them is only one step toward a more "synthetic" mindset. Another type of modeling that is particularly well-suited to explaining the behavioral patterns of complex systems is "agent-based modeling" (ABM). ABM uses computers to build models around multiple autonomous actors or agents (nations, companies, individuals, etc.) that are programmed to interact, learn and change their behavior as a result. Although still a relatively nascent field, such models tend to be quite effective at explaining nonlinear behavior.[13]

In addition to modeling (metaphorically-speaking and/or agent-based), a fourth step toward a more synthetic approach will involve a dedicated effort to educate intelligence analysts to think "complexly/nonlinearly." This point cannot be emphasized enough since too much analytic training within the IC is focused on writing, and nowhere near enough is focused on thinking. Perhaps the assumption is that college educated employees already know "how to think." And while that may be true, the fact of the matter is that the university system in the US is structured to merely reinforce linear thinking – everything is divided into neat little departments, and specialization is encouraged, if not required. Given this, it is crucial that analysts be taught to think differently – like synthesists. In particular (after learning the fundamentals of linearity/nonlinearity and complex systems), would-be "synthesists" need to be taught the "7 principles of strategic thinking":[14]

1. Look at whole systems, not just their parts. (The system is always bigger than you think.)
2. Complex adaptive systems are self-organizing and pattern-forming. (What are the "attractors" that pull the system in question together?)

---

[13] For an excellent discussion of this field, see Jonathan Rauch's *Seeing Around Corners*, The Atlantic Monthly, April, 2002

[14] This formulation is from T. Irene Sanders' *Strategic Thinking in a Complex World*, Washington Center for Complexity and Public Policy, www.complexsys.org.

3. Small changes can create big results – the so-called "butterfly effect." (What's perking at the edges, on the horizon?)
4. Maps, models and visual images make it easier to see connections, relationships, patterns of interaction.
5. Scanning across disciplines, forces, agencies, etc...is key to seeing subtle changes, emerging conditions (multiple perspectives, integration of knowledge).
6. Nonlinear thinking is critical to recognizing clues about changes in the environment.
7. Perspective is important. You have to know what you're looking at and place it in context.

Fifth and finally, in addition to educating analysts, it is imperative that policymakers be educated as well – to both the complex nature of the problem sets (after all, they are "Newton's children" as well) and to what can/cannot reasonably be expected from intelligence. To do this will require an integrated, comprehensive and dedicated effort involving all four components (recognition, adoption of nonlinear metaphors, use of ABM for illustrative purposes and appropriate education) mentioned above.

Conclusion: It's Not Rocket Science

In conclusion, it is not unfair to expect the cultivation of nonlinear perspectives to help alleviate (but not eliminate) the periodic blindsides that an excessively linear mindset has helped make all too common. And while that alone would be an extraordinary accomplishment, it is nonetheless important that the potential contributions of such perspectives not be oversold. At the end of the day, nonlinear systems such as those in the purview of the Intelligence Community are messy and inherently unpredictable. That is a fact, and nonlinear perspectives are, quite simply, not going to change it. In the final analysis (or hopefully, synthesis) then, perhaps the most that can be hoped for from nonlinear perspectives is a more "blurred" but nonetheless greater understanding of the many patterns, possibilities and scenarios that the future may present.

Or, to sum it up differently, when it comes to thinking about innovation within the Intelligence Community so as to ***better anticipate*** – not predict -- complex issues, the first imperative must be to understand: it's not rocket science.

The Intelligence Community of the Future

(NSA)

(b)(3)
(b)(6)

These days, the world seems like a smaller and smaller place. And yet, the challenges to the US Intelligence Community (IC) only grow larger. Today's unpredictable security environment is constantly evolving, and the IC must adjust by reinventing itself as the Intelligence Community of the Future, one that is flexible, dynamic and adaptable. Presented here are three major areas in which the IC must fundamentally change in the coming years: technology, communication and demographic transformation. Although each area is discussed separately, they are interdependent, and changes in any one area will affect changes in the other two.

The first section deals with the challenge to the IC of technically savvy targets in a rapidly changing technological environment. It makes arguments for: realigning resources based on a division between technologies in which the IC must lead and those in which the IC may follow; eliminating duplication of effort by relying on commercial and open source solutions; implementing a system in which technology is a primary driver of the intelligence system; and changing internal system design methodology to promote organic and interconnected systems.

The second section discusses ways in which to strengthen communication within the IC and between the IC and outside elements in industry and academia. It makes arguments for: harnessing emerging technologies for internal and external use; creating a public space of knowledge; building a culture in which job movement is the norm; and nourishing a strong and capable middle management.

The third section addresses the impending and necessary change-over in the workforce from one dominated by those near retirement to one heavily represented by those in their twenties and thirties. It makes arguments for taking advantage of the shift in population demographics; accommodating a future workforce with a high turnover rate; sustaining retention by fostering job flexibility and increasing the influence of young people and new hires; and developing support services aimed at the younger generations.

Technology

An analyst sits at his computer, combing through the data he receives daily through his regular requests. For awhile he's been noticing that the information about a particular target has been slowly dwindling. Today there is no information at all. As the target seems adaptable and technologically savvy, he ponders the possibility that the target may be using a new type of technology that escapes the current intelligence system.

Just down the hall, a researcher studies a new technology that is rapidly gaining worldwide acceptance. She has tried to encourage the intelligence system to adapt to this new technology by adding capabilities for it. However, she has been constantly met with stiff resistance, being told that there are no available resources for a new technology that doesn't have any proven intelligence value.

The described parable of the analyst and the researcher illuminates a major shortcoming in current practices: namely, that the system is driven by customers who may have no knowledge about new and emerging technologies. Even when customers learn about a new technology, they may be unwilling to devote resources to it, as it has an unknown intelligence value. These problems only stand to grow worse as technological development accelerates.

Over the past fifteen years, both the nature of U.S. adversaries and the worldwide technical environment has undergone revolutionary change. Meanwhile, the IC has looked to a tradition of incremental change to adapt. This is no longer sufficient. Technology has metamorphosed over the past decade, completely changing the playing field on which IC operations are conducted. Cellular phones, text messaging, satellite phones, instant messaging, email, voice over the Internet, chat rooms and the world wide web have become ubiquitous the world over. The combination of quantity and diversity of technology now and in the future threatens to overwhelm the IC.

While the IC tries to maintain a tradition of being at the forefront of technology, it must adopt a new perspective on its place in the technology world. If the IC continues to try to be at the bleeding edge in all technical areas, it will fail to keep up in any of them. There are simply not enough resources to do so.

In addition, the IC relies on monolithic processing systems and tools, which require extended development cycles. It commonly takes more than a year to incorporate systems and tools for newly identified technology into standard baselines. In some cases, the new technology is so revolutionary it requires the redesign of entire systems. These unwieldy, inflexible systems stand in the way of producing timely intelligence.

The IC faces a daunting task in the years ahead. It must address the internal strains that novel technology puts on current methodologies. It must strive to understand all new and emerging technologies. And it must develop a practice to incorporate major changes to internal systems and tools in timeframes measured in days and weeks instead of months and years. Here are four proposals to do so:

The first major change that must occur is that a **system of recognizing new and future technologies must be put in place – and the system must be a primary driver for intelligence gathering**. The problem with the target-only driven system is a chicken-and-

egg problem when it comes to technology. The earlier example of the analyst and the researcher is a classic case.

Thus, a system of recognizing new and future technologies must help drive the intelligence system alongside the traditional target-driven approach. This can only be done with a strong amount of risk-taking – after all, there may be no intelligence value in a new technology, or not any for a while. Resources must be available for trying the unknown.

Secondly, the IC needs to **make a distinction between two types of technology: the ones for which it must remain a leader, and those for which the IC can follow at a close distance**. Resources for technologies in which it must lead should be directed towards promoting further advances in such technologies, whereas resources for technologies in which the IC may follow should be directed towards partnering, conferences, education and training.

An example of the former would be the realm of cryptography. The IC needs to be ahead of other nations, ahead of industry and ahead of academia in its codes to maintain information superiority. Even here, however, it must be acknowledged that the Internet has spurred an interest in cryptography outside of the IC and academia based on the profitability of e-commerce. And so, even with technologies for which the IC must be a leader, it must not turn a blind eye to developments on the "outside."

An example of a technology in which the IC can follow is that of cellular technology. The IC must understand cellular technology to garner the most intelligence possible from the medium. But it can learn as much or more about cellular systems from experts in industry than by building its own cellular network and creating its own experts. It is imperative that the IC partner with industry and academia to the fullest extent possible to save money and manpower for the missions that can only be accomplished within the IC. Classification systems with regard to technology knowledge need to be reassessed to enable the fullest amount of sharing possible.

The third major change that needs to occur with regard to technology deals with internal processing systems and tools. The IC needs to **stop duplicating effort that is already being carried out in industry, academia and the open-source community**. Currently, it is common for technical offices within the IC to develop new systems and tools in response to each new technology that comes along. It has always worked this way, and indeed, until recently there has been little other choice. Now there is a choice, and the IC needs to actively make the decision to rely on commercial and open-source systems and tools.

The advent of the Internet has given rise to online criminals – and to a community of companies, academic institutions and individuals who have developed uncountable

systems and tools for tracking and stopping them. These very same systems and tools could easily be put to use in the IC for developing intelligence. In addition, the open-source community, which advocates the spread of unlicensed (i.e. free) software, continues to write high-quality systems and tools that are easily modifiable and quickly available. The utility of such free and versatile technology should not be overlooked, and indeed, the IC needs to actively encourage such partnering.

The switch from a "build-it-yourself" mentality to a "buy it, trade for it or get it for free" mentality will not be an easy one. One of the biggest concerns will be in the area of risk. A product that is created on the "outside" has the potential for malicious content beneath the surface. However, the risk is a necessary one, and it must be actively managed. The bigger risk is to fall further and further behind the technology curve.

The fourth major change must be a change in the design of internal systems. The classic approach to designing any sort of technical system in the IC has been a top-down, large-scale design process. This approach is not only slow and expensive, but also it just doesn't work for the dynamically changing technical environment that today's world has become. **Designs for future internal systems must be organic and functional, piece-wise limited and interconnected.**

Current systems are monolithic and unwieldy. They often perform current tasks well but are unmodifiable for future tasks. A better system implements many pieces that fit together like Lego blocks. Each piece is self-contained and performs a limited task. Each piece also contains interfaces in order to fit together with any number of other pieces. Thus, a new task can be performed by taking several old pieces, developing perhaps a new piece or two and putting them all together. This is an organic system, allowing easy, inexpensive development of new pieces and quick response time to new technologies.

In implementing such an approach to systems design, it is necessary to give up a few of the strengths of older, top-down-designed systems in exchange for new strengths. The new systems won't be perfect; they will have flaws, but these flaws will become less over time as the flawed pieces are discarded and better ones created. Control over the system by one office will be almost non-existent, as the new system will encourage others to create and modify pieces. But the new organic system may be migrated to over time. It is imperative that the technological underpinnings of processing intelligence be made to run in a modular, organic way so that it can keep up with the pace of technological innovation.

Communication

Deep in the dark recesses of a government building sits an employee busily working on her widget. She knows that the widget will be of great use in gathering intelligence and is growing excited as she nears completion on it. She has spent the past six months getting

the details just right with help from her coworkers and support from her boss. They all believe it will be a wonderful creation as well. It's just too bad that none of them realized that a very similar tool had been built a year ago in another building, in another agency.

While the public and the press harp about the lack of information sharing and an inability to "connect the dots" in regard to intelligence product, the barriers to information sharing run across all disciplines in the IC. Not only does intelligence product face all sorts of legal, policy and classification issues, but also technical information about the systems and tools used to collect and process intelligence remains unshared.

It is inexcusably difficult to find Community experts in all fields, to find papers and reports and to discover if duplication of effort is taking place. When technical information isn't shared, the IC ends up with many systems and tools that don't fit together very well. The result is that the IC as a whole doesn't know what it knows. And, worse, it doesn't know what it doesn't know.

The world has produced new technologies that make it ever easier to communicate, and yet the IC sits idle, filled with anxiety of the unknown risk of using them. Companies are continually experimenting with new organizational structures and practices to increase communication amongst employees. Yet the IC balks at such unproven ideas, not wanting to offend a workforce that is accustomed to stable work life. But the risk to national security of not overhauling the Community's internal communications is too great. The IC must harness these new powers of technology and innovative workplace practices. Here are four proposals to do just that:

First, the IC must **take advantage of new and future technologies to promote better communication within the IC, and between the IC and the rest of the world**. Today, communication in the IC, for the most part, relies primarily on internal networks of telephones and email – the technology of ten years ago. But communication can be vastly improved by taking advantage of newer innovations that are already standard in the "outside" world, and by increasing access to the "outside" world in the workspace.

Such real-time communications tools such as instant messaging and chat rooms would allow easy collaboration between elements at physically different locations. Online forums focused on one topic could bring together people who would never otherwise interact, spurring creativity and insight. Already online-learning has begun and could be expanded even further to provide training to employees around the globe.

Access to the outside world must be increased and encouraged. Internet terminals, while remaining separate from internal networks, need to become ubiquitous. In today's world, the Internet is a fundamental tool, like a pencil. It is a powerful research implement, facilitating work in all job descriptions. It is also a primary medium through which to stay connected to outside partners and contacts. As previously described, these partnerships

must increase in quantity, and the Internet provides the communications link with which to create, maintain and strengthen them. One or two Internet terminals amongst fifty people are insufficient, just as one or two pencils amongst fifty mathematicians are insufficient.

Secondly, the IC must **create a public space of knowledge** within its walls. Being a traditionally compartmented organization, the IC has always relied on one-on-one contacts to pass information from one place to another. But as the necessity to increase intra-employee communication grows, these limited strings of access will not be enough.

One common problem in today's IC is that of finding an expert in a given area. Today this problem is solved by networking with one's colleagues until finding someone who knows someone who knows an expert. In industry and academia, experts are known not just through personal contacts but also through publishing. The IC has no means of allowing Community-wide publication, wherein the paper is available to – and discoverable by – anyone possessing a high enough security clearance. Scattered libraries exist throughout the IC, but the need to bring disparate information together is going to require that some sort of universal digital library be established. Imagine an "Amazon.com" of the Intelligence Community, where papers are searchable, ranked by previous readers on quality, and instead of a dollar amount, appear with a reader's required classification level. The paper can then be received in hardcopy or else downloaded as a digital version.

The third major change with regard to communications is to **make movement a regular part of an employee's assignment**. Individuals must be encouraged to break away from their normal routines and offices to meet new coworkers and spread ideas. It is critical that the IC not spend resources on constantly reorganizing the workforce. The workforce must be able to, and willing to, dynamically rearrange itself according to necessity.

New and innovative ideas, indispensable for confronting today's target set and technological environment, do not originate with people working alone doing the same job day-to-day. Innovation comes from people exposed to new ideas and information, who then apply them to what they already know or do. It is therefore imperative that people be constantly exposed to new ideas and practices. An outsider has the ability to question overlooked assumptions and suggest ideas that are "outside the box" of traditional thinking.

Different people are comfortable with different working styles, and so a mixture of techniques will be necessary to encourage movement within the workforce. One simple possibility is outlined here; there are many others.

Encourage flexibility in employees' weekly working schedules. As an example, consider an employee who normally works in office X, doing the same job, day after day. Now,

allow this employee to spend Tuesdays in another office, perhaps in another building, perhaps in another component of the IC. These Tuesdays will be spent as an intern, learning about another aspect of the intelligence system. Allow the same employee to spend Thursdays in a different office, as a visiting expert on the information and methods of office X. This employee is now acting as a pollinator, bringing fresh perspectives to all three offices. The employee is also increasing the communication amongst the offices, building new contacts and increasing his own knowledge base. Office X's manager may see the loss of the employee for two days a week as a detriment to the office. But the benefit to the IC far exceeds the loss to the individual office. If there are many such flexible employees, then no individual office loses out, and the IC as a whole gains tremendously.

Fourthly, in order for the workforce to sustain dynamic change as part of its basis of operations, the IC must **create and sustain an incredibly capable middle management.** It may seem obvious, but the managers directly above the average employee are the key to the employee's use of technology, the employee's communications and the employee's flexibility and adaptability. Mid-level managers should be brought in and trained specifically for their positions. Employees should never be forced to decide between stalled upward mobility and a management track. Conversely, lower-level employees with strong management potential should be identified early and encouraged to (formally or informally) apprentice with an accomplished mid-level manager.

Demographic Transformation

In a small village somewhere in the Middle East sits a house. The young man, whose parents own the house, has been fortunate to learn a fair amount about technology and has set up several computers in a front room, which connect to the Internet. He charges a small cash fee for the locals – and for anyone else stopping through – to use these computers to keep in touch with the rest of the world. Right now, in fact, another young man is using one of these computers to chat with an associate in another country. They're planning on blowing up a western embassy.

Although this is a made-up example, the challenges to the IC it demonstrates are all too real. Who are the best people to address these challenges? They're not the career intelligence officers who know all about cold-war targets and strategy. The ones to face tomorrow's IC challenges are currently studying for their semester midterms. There is no better training ground for understanding the possibilities of today's communications technology than the college campus. And there's no one more suited to a fast-paced dynamically changing work environment than young people.

The new adversary relies on a range of strengths: resourcefulness, flexibility, adaptation to change, mobility, risk-taking and creativity. America's youth also encompass all these strengths, in addition to being extremely technologically competent. The technology that

older employees need to work hard to master comes like second nature to students who have been immersed in it from grade school. The Internet has revolutionized the skill sets needed to be a capable IC officer, and it can be disconcerting to realize that in some cases, those just out of college are more qualified to deal with today's challenges than those who have spent a career in the IC. Fortunately, the next decade presents a golden opportunity to hire a great many of these youth.

Too often the focus of demographic transformation is on "knowledge transfer" from the retiring generation to the younger ones. But as the target set and technological environment continually change, it is just as important to sustain a workforce that can continually learn. The focus of the upcoming demographic shift should be on molding the new working culture into one that takes the most advantage of the change, on managing a constantly changing employee base and on retaining the best young minds through both procedural changes and redesigned support services. Here are four proposals for doing just that:

Firstly, the IC must **take advantage of the unprecedented opportunity to hire a largely youthful workforce**. As large numbers of 1980's-era hires retire in the next decade, a void is created, which as it's filled, can drive a change in the Community culture. This massive loss of people, and therefore knowledge and skill, has largely been seen as an upcoming obstacle. But this obstacle may be overestimated; new cultural norms in retirement and increasing longevity are encouraging retirees back to work. This allows for a pool of knowledge and skill to continue to be available long after the employed population has transitioned to younger generations.

In addition to hiring a youthful workforce, the IC must make major changes in order to retain the next generation of employees. In fact, retention will prove to be more difficult than recruitment. In today's post 9/11 country, patriotism is at a high, and the IC has seen record numbers of applications. However, with an improving economy and new norms for career paths, patriotism alone will not be enough to retain the necessary number of young people more than several years.

Secondly, the IC must **acknowledge and accommodate the new paradigm for working careers** that comes with the next generation of employees. The IC – and the government as a whole – has always been a haven for those who like comfort and security, who desire to spend their entire careers within one agency or branch. This has been beneficial to the IC in creating experts in intelligence matters and maintaining a core knowledge and skills base that lives within the minds of the employees. That is all about to change. The youth of today does not envision a career with one company or government entity; rather, today's careers are a series of varied jobs, each a stepping-stone along a career path that changes many times over the career.

The implications for the IC are considerable and must not be ignored. The IC must learn how to adapt to a workforce with a higher "churn" rate than in the past; core knowledge and skills must be preserved, while allowing for a steady stream of new hires and resignees. There are three possible benefits to be gleaned as well from an ever-changing workforce. For one, new ideas and perspectives will continue to flow into the IC. Ties with outside entities will be strengthened as employees move between the IC, academia and industry. And lastly, the new career paradigm also permits employees to leave one job and return years later after having worked elsewhere; the learning that takes place outside the Community can be of great benefit when an employee returns.

Thirdly, the IC must **change internal procedures and traditional practice to encourage retention of youth**. The top-down hierarchy, which leaves new hires and youth squashed at the bottom, presents a challenge. Recent hires are rarely heard because of the overwhelming and intimidating size and complexity of the IC. And traditionally one must "climb the ladder" before making an impact or introducing a new idea. In a dynamically evolving IC with considerable changeover in personnel, this is especially undesirable. The leaders of the IC must make a concerted effort to solicit the thoughts and views of youth and recent hires.

The IC must also open its internal doors and allow employees much more flexibility in career movement. As stated, the emerging work ethic is one of regular change, and today's youth expect to be continually challenged, continually learning and continually experiencing novelty. One obvious way to increase retention will be to encourage rotations through the various components of the IC, overseas tours and movement within individual IC entities. A young employee who decides to "move on" and has the option of moving to a different organization rather than just quit will be far more likely to stay and benefit the Community than one who doesn't.

Fourthly, the IC must **develop support services aimed at a younger workforce**. Today's support services – from health newsletters to financial seminars – are mostly aimed at the boomer generation who make up the majority of the workforce. While this is understandable, the culture of the Community relies, in part, on who is addressed by these support services. Clearly, different stages of life present different personal challenges, and the needs of youthful employees will need to be more seriously addressed in order to retain them.

Programs should be established or modified to assist new hires who come directly out of college. While college prepares students academically, it leaves them far short of knowing how to live in "the real world," ignoring such things as doing one's taxes, living alone and understanding insurance, to name a few. Current seminars on retirement planning and saving for children's college tuitions should be supplemented with seminars on learning how to draw up a budget and getting out of credit card debt. Emotional support services need to make an effort to reach out to young people who often

experience high degrees of isolation and depression following the highly social environment of college.

Conclusion

The IC is essential to the security of the United States. It is therefore vital that it adjust to today's unpredictable external security environment, in which continual change is the norm. The IC must adapt to technically savvy targets in a rapidly changing technological environment. It must strengthen communication within the IC and between the IC and outside elements in industry and academia. And it must take advantage of demographic transformation to a youthful workforce.

In the Intelligence Community of the Future, the researcher will find it straightforward to get the new technology noticed through use of an online inter-agency forum. She will work with a developer to create a doodad that will process the new technology and direct derived information into the existing intelligence system. Upon doing so, the analyst will suddenly start receiving data about his target that had disappeared, as the target had, after all, switched to new technology. Together, the three will write a paper about the technology, the doodad and the target and publish it in the IC library.

In the Intelligence Community of the Future, the employee will not waste six months on recreating an existing widget. She will be directed to an expert on widgets by a coworker she meets while doing an internship in his office one day a week. Instead of wasting six months, the employee will learn from a paper she finds in the IC's library about the doodad, which could benefit from being connected to a widget. Using instant messaging technologies, she will work across agencies with the developer and the expert to create a useful doodad-widget that interfaces with other systems. Her highly capable manager will write a glowing recommendation based on her work to help her secure the field assignment that she had been hoping for. She will then set off, bringing with her the recently gained knowledge and an eagerness to learn more.

In the Intelligence Community of the Future, the widget expert will happen to be a twenty-four year old who did his college thesis on widgets. In his two years in the IC, he will have already built several types of widgets with parts he downloaded from the Internet. All of these widgets will be put into a trial system with resources reserved for just such experimentation. And though only one widget will eventually be successful, the resulting intelligence will highlight the online conversation between the young man in the Middle Eastern village and his associate. They will be arrested before they can place the bomb, and hundreds of embassy employees will sleep soundly, unaware of the tragedy they narrowly escaped.

And this is all because the US Intelligence Community was willing to dare to revolutionize its practices to meet the modern challenge.

Let's Proceed to Plan C Because It Will Support Plan B (Basic Agency Reform)

By Michael Mears (CIA)

Plan A, the status-quo operation of the Agency, is now off the table. Rich discussions are underway of a transformational "Plan B" ranging from reorganization to cultural change.

But what do we do with all the erupting out-of-the-box thinking? Do we let the bureaucracy neutralize these ideas or do we nurture and protect them?

The answer is to simultaneously launch an organizational safe harbor for out-of-the-ordinary ideas, Plan C, which allows novel new management approaches, new methods of collection and fresh approaches to analysis to flourish.

Plan B

The currently evolving Plan B will contain in-the-box solutions on how we organize, manage and lead ourselves. While the current discussion focuses almost exclusively on DCI authorities and reorganization, Plan B will entail much of what has successfully worked in other public and private sector organizational transformations and engage the workforce, revitalize the management chain and start a serious effort to remove bureaucratic barriers.

The fact remains, however, that most transformation efforts in large organizations fail. Organizational failure is costly in the private sector but inconceivable in the Intelligence business. We have too much at stake and must develop a way to simultaneously launch out-of-the-box solutions safely away from the Plan B changes.

Plan C

But what do we do with all the "disruptive" reform ideas suddenly challenging current intelligence philosophy? (*A disruptive idea is one that calls for a significant change in the way the organization does its business – contrary values, processes, organizational form or even non-traditional "tradecraft"*). Most of the Galileo award submissions will be disruptive.. What do we do with the losing submissions? Worse yet, **what do we do with the winning Galileo entries?** An award winning idea not properly implemented simply generates additional organizational distrust and employee frustration.

Lone ideas, no matter how good, almost never survive their first anniversary in traditional organizations. Research by Clayton Christensen, author of the Innovator's Dilemma and the Innovator's Solution, shows that ideas radically different than the status quo have to be securely grafted at very high organizational levels for protection. However, the Community Management Staff in its present form is not equipped to be this high-level protector since it lacks the line authority needed to resource, monitor and grow disruptive ideas.

In the intelligence world, ideas falling under the control of directorate entities quickly take on the workplace values and practices of that directorate. Creative units like the Center for the Study of Intelligence and Global Futures have a very difficult time functioning effectively within a directorate structure. These units are ancillary to the directorate mission and spend a great deal of energy in self-preservation activities. The Agency's only serious anti-bureaucracy effort, the Improvement Team, quickly withered and died from lack of resources when housed in a directorate.

	Plan A	**Plan B**	**Plan C**
Strategy	Business as usual	Reorganization/ Transformation (In-the-box)	Safe harbor for disruptive ideas (Out-of-the-box)
Projected Results	Failure	Possibility of stalling	Multiple failures And successes

A Laboratory For Quantum Reform

The answer is to establish a permanent oversight board to analyze the flood of ideas springing from RIA groups, CMS, the Leadership Academy, CSI, Global Futures, Red Teams and employees and to bundle them for protection into a new structure attached at a high level. It is difficult to say specifically where the "Incubator Center" should be attached because of the different IC organizational structures currently being proposed. However, it should be higher than directorate level and overseen by a senior executive strong enough to defend against heresy charges from senior managers in traditional mainstream units.

Creativity requires that all aspects of the Incubation Center differ from the existing directorate structure. The Center should be established as a non-profit organization under the control and oversight of the IC or Agency much like In-Q-Tel.

Experienced officers suggesting novel ideas and approaches to solve chronic intelligence programs might be funded over a five-year period to safely carry out their experiments. These are ideas that would not normally gain traction inside busy directorates carrying out established missions but, once developed, could offer exciting future prospects for the Agency.

How are matured pilot projects brought back into the directorates? In most cases, to avoid organizational cannibalization, they won't be. Small creative units can remain inside the incubator or, in rare cases, be spun off as free-standing entities.

Actions For Success

How do you give the Galileo ideas the possibility of success? The rules for protecting these new structural forms and practices are similar to private sector lessons learned in fostering design and implementation of disruptive technologies:

- **Above all, provide a heavyweight shepherd for long-term protection**. Heavyweight is defined as a senior executive sufficiently high to work across IC boundaries and, because outcomes are difficult to predict, to manage expectations**. He or she must have the necessary power and mindset to override or reform existing culture, procedures and process to foster experimentation.**

- **De-couple from inefficient support systems by moving, in some cases, to non-government structures**. Inefficient processes cause employee time to be frittered away as identical problems are solved over and over. Look for goods and service support for the incubator elsewhere.

- **The new incubator organization must be autonomous and allowed to develop new culture and process**. New ideas are always disruptive and generate resistance. Be observant as the existing system, a mother hen of sorts, will view this as a refutation of the current business model and culture and attempt to peck the baby chick to death.

- **Furnish an impartial reform-minded expert senior support team to remove bureaucratic barriers**. This internal can defend against the "not-invented-here antibodies" found in every human organizational system. Also appoint a blue ribbon oversight panel largely composed of non-IC officials.

- **Allow failure and fail early**. Few organizations manage to learn from failure. It is important to fail early both to learn important lessons and to re-deploy human capital. Follow Pareto's lead and allow the 80 per cent solution. Rough and rapid solutions are OK.

- **Start with small Plan C pilot teams and enforce selflessness, humility and collaboration**. In addition to passion for improvement and open communications, pilot team leaders should trust others, be trustworthy and have a strong sense of direction. They should have an ability and hunger to learn.

- **Reward teamwork, speed and prudent risk taking.** Pilot project leaders should select team members for attitudes and traits. Use employees' ideas to encourage initiative and to build trust. Leaders can't know all the answers and must resist the tendency to defend their own ideas or views. Extensive training should include external internships and conferences to continuously capture proven external concepts.

Plan B, like any large-scale transformation, will take years to complete and might fail. Plan C offers a relatively low-cost hedge by potentially generating quantum breakthroughs in intelligence approaches and performance. Neither effort conflicts with the other. Can our national security afford to not buy this low-cost insurance? Whatever the outcome of the Plan B reforms, a little experimentation with Plan C can't hurt.