2006

Information Professionals and the Intelligence Community

Susanna Rogers Smith
THE FLORIDA STATE UNIVERSITY

COLLEGE OF INFORMATION

INFORMATION PROFESSIONALS AND THE INTELLIGENCE COMMUNITY

By

SUSANNA ROGERS SMITH

A Thesis submitted to the College of Information in partial fulfillment of the requirements for the degree of Master of Science

Degree Awarded: Fall Semester, 2006

Copyright © 2006 Susanna Rogers Smith All Rights Reserved
The members of the Committee approve the thesis of Susanna Rogers Smith defended on October 6, 2006.

______________________________
Michelle M. Kazmer
Professor Directing Thesis

______________________________
John C. Bertot
Committee Member

______________________________
John Gathegi
Committee Member

Approved:

______________________________
Larry C. Dennis, Dean, College of Information

The Office of Graduate Studies has verified and approved the above named committee members.
# TABLE OF CONTENTS

List of Abbreviations ................................................................. iv  
List of Figures ................................................................. v  
Abstract ................................................................. vi  

INTRODUCTION ................................................................. 1  

INFORMATION IN THE INTELLIGENCE COMMUNITY  
A Brief History ................................................................. 5  
A Look at Issues and Policy ................................................................. 8  
The Stove-Pipe: An Intelligence Community Information Sharing Model ................................................................. 14  

INFORMATION IN THE BUSINESS COMMUNITY  
A Brief History ................................................................. 16  
Some Corporate Examples ................................................................. 22  
The Ecosystem: An Information Sharing Model for the Corporate World ................................................................. 25  

APPLICATION OF THE ECOSYSTEM MODEL  
Comparing the Models ................................................................. 29  
Overcoming Policy Concerns ................................................................. 32  
Improving Information Sharing ................................................................. 36  

THE ROLE OF INFORMATION PROFESSIONALS  
Information Professionals in the Corporate World ................................................................. 41  
How the Intelligence Community and Information Professionals Can Work Together ................................................................. 44  
Analysts and Information Professionals ................................................................. 47  

CONCLUSION................................................................. 50  

BIBLIOGRAPHY................................................................. 53  

BIOGRAPHICAL SKETCH................................................................. 60
LIST OF ABBREVIATIONS

BP – British Petroleum
CIA – Central Intelligence Agency
CIO – Chief Information Officer
FBI – Federal Bureau of Investigation
GAO – Government Accountability Office
ILM – Information Lifecycle Management
IRM – Information Resources Management
NSA – National Security Agency
OMB – Office of Management and Budget
ORCON – Originator Control
OSS – Office of Strategic Services
SLA – Special Libraries Association
# LIST OF FIGURES

1. Stove-pipe model ................................................................. 14
2. Ecosystem model ................................................................. 26
ABSTRACT

This project proposes one possible solution to the information sharing and information processing problems within the intelligence community: include information professionals in each analytic division. By first creating a rough model of information and information sharing in the intelligence community and then comparing that model to one taken from information sharing practices in the corporate world, a new paradigm can be revealed which the intelligence community can use for further study. It is also of note that many of the successful corporations which utilize information effectively employ ideas first created by government policy, such as mandates within the Paperwork Reduction Act and various Executive Orders. These policies will also be reviewed for their impact on information in the corporate world and also for their reapplication in the world of intelligence.
INTRODUCTION

In their final report to Congress, the 9/11 Commission recommends: “The president should lead the government-wide effort to bring the major national security institutions into the information revolution. He should coordinate the resolution of the legal, policy, and technical issues across agencies to create a ‘trusted information network.’”¹ This recommendation stems from a lack of information sharing throughout the intelligence and law enforcement communities. This lack failed the United States in the terrorist attacks of 2001, and could fail the country again unless steps are taken to minimize that risk. The 9/11 Commission Report is not the most recent document calling for better information sharing capabilities across agency lines, but it is perhaps one of the most telling. Agencies designated to protect the United States need to improve information sharing, drawing on new technologies and expertise whenever possible. The 9/11 report highlights another critical problem all intelligence agencies face: not a lack of data, but the ability to analyze that data efficiently. Analyst pools in all agencies need to be larger and intelligence agencies need to collate and share their data better. Who better to help in accomplishing this than professionals trained in information storage and retrieval?

Information professionals are not analysts, but possess their own valuable expertise in cataloging, research and information retrieval. Information professionals would help already overwhelmed analytic divisions by cataloging data using current technology. With an advanced information organization and retrieval system in place, analysts could ask for and receive immediately all the data on a given topic from their agency files and they could receive data from

other agencies across the board, creating a more comprehensive picture of the topic they are reviewing.

The best way to explore this proposal is to briefly review the history of information in the intelligence community, especially those calls for better information sharing. This project will also review policy issues which hinder or deter this sharing in order to gain a clear picture of where information stands in relation to the rules, regulations and habits of the community. Once this rough model is created, it will be compared to an information sharing model that functions more smoothly – that of information and intelligence analysis in the arena of business, or competitive, intelligence.

Competitive intelligence has seen rapid growth in the past decade and as this project will show, much of that success lies in the corporate policies of the businesses who utilize this method of gathering data. Surprisingly, competitive intelligence has its roots in a series of government information initiatives dating back to the late 1970s. Though the business world and the government still utilize these policies, these concepts have not necessarily filtered down through the intelligence community as effectively as they should have. Once the information sharing model for competitive intelligence is completed, it can be set against the intelligence community model. Though the ideas of information resource management and the information life cycle had their origins within the government, the iterations of these concepts within the business world can now be reviewed. Through this lens of corporate information sharing, the intelligence community should find inspiration for possible re-application of its government’s own ideas.

The corporate world is similar to the intelligence community in one critical way: both collect information on competitors in order to improve themselves or their standing in the industry. In the intelligence community,
America’s agencies collect data about other countries while in the corporate world individual companies collect data on other companies within the same industry. These settings may seem incomparable, but they are not. Consider America as a company with many different divisions (intelligence agencies), collecting data on China, another company with similar capabilities. Think of IBM, a huge conglomerate with dozens of divisions each with a different focus, collecting information on Microsoft, a company of similar proportions. This broadly focused view makes it easier to understand the similarities between the corporate world and the intelligence community, and will help in the discussions which follow.

The final section concerns information professionals directly, and is the heart of this project. Once the broad picture is painted – policy issues considered, lessons learned from competitive intelligence – then a closer look at the role of information professionals in the intelligence community can begin. Many questions need to be answered: What are the advantages and disadvantages to adding more information professionals to the staff of intelligence agencies? How would this structure look and how would it function? Is there a precedent for a new cataloging and classification system for intelligence community data? Would the staff of the agencies accept such a change in their structure, and would there be enough support for the change to be effective? This project aims to answer these and other questions.

No research project is without complications, and the largest hurdle is gaining access to needed data in such a security-conscious environment. To overcome this, people involved in the intelligence community have enthusiastically supported this kind of research, and some have been willing to go on record with their thoughts and ideas. To maintain confidentiality, they will be referred to as “Subject A” (et cetera) and will only be identified by their role.
These interviews are important because not only do they provide insights from within the intelligence community, but they also cover a broad cross-section of agencies themselves. From the three interviewees who allowed their words to go on record, there is representation from the military, from law enforcement and from a traditional government intelligence agency. The subjects also have very different positions within their respective organizations: analyst, policymaker and agent. Thus these interviews provide a good generalization of what agency employees think about these ideas, which is necessary to provide positive support to the proposals presented in this project. In addition, this project is primarily hypothetical, so access to currently-classified documents is not necessary. Though it is possible that similar reports have been done in a classified environment, this project looks at the intelligence community through the eyes of an outsider and can offer valuable insights from a different perspective.
CHAPTER 1
INFORMATION AND THE INTELLIGENCE COMMUNITY

A Brief History

Dating back to the Truman administration, there has been a call for intelligence agencies to be better organized and to have better cross-channel data sharing, both within a single agency and among the many disparate agencies. These calls come from both within and outside agency walls, from the 9/11 Commission Report to the early Dulles Report in 1949. They hail from Congress, government oversight agencies like the Government Accountability Office, and even the Executive Office itself, as well as internal intelligence agency audits. The problem with these reports is that they rarely consider those who can most effectively deal with information – the librarians and information professionals who have been trained in such things as information processing and cataloging.

First, however, this chapter will look at the two main problems within the community: the need for better-organized information with data-sharing across agency lines and the impact of the policies that govern information sharing. It will also include a brief introduction to the role of information professionals, setting the stage for the later discussion.

There have been articles written as far back as the 1950s citing the need for a structured reference service for intelligence agencies similar to what an information professional can provide. In 1959 Paul Borel wrote:

[T]he present and future demands for reference service will lead to increased use of machines where these can be introduced without jeopardizing the performance of essential intellectual operations. This fact and the increasing volume of information which must be processed will bring about more centralization. The problem then becomes one of
insuring that central reference is at least as responsive to research needs as the reference facility which is an integral part of the research area. The solution is to be found in an approach which integrates the information-processing activities, wherever performed, into a single system within which collection, processing, and user components operate along well-defined lines.²

This cry echoes a need still unfulfilled in the intelligence community. There needs to be a means to integrate information processing without removing it from the intellectual (analytic) aspects. Information professionals are the key to this integration, and by including them in each discrete analytic division, huge inroads can be made towards Borel’s idea of a reference facility within each research area.

When Borel wrote this, the Central Intelligence Agency was barely ten years old. Unfortunately his call went unheeded, and the current agency structure still leaves much to be desired. A comment from a recent book by John Bodnar highlights this problem: “We must reconcile ourselves to the fact that the [Intelligence] Community is unlikely to pay human librarians and curators to support analysts in the way that other information-dependent organizations support their researchers.”³ Understandably, the information professional’s reaction to this would be tinged with alarm and concern. Why exclude those individuals trained in the very things needed to improve analysis? Later Bodnar describes a series of situations where having a librarian would resolve problems. He mentions two things in particular – the fact that the Intelligence Community’s classified datasets are impossible to use and the fact that there is no simple means for document retrieval because there has been no meta-tagging.⁴ Bodnar

---

³ John W. Bodnar, Warning Analysis for the Information Age: Rethinking the Intelligence Process, (Washington, DC: Joint Military Intelligence College, 2003), 45.
⁴ Bodnar, 49.
even admits that both problems have simple solutions: hire information professionals. Yet he discounts this as too expensive an outlay and prefers to seek computerized methods for accomplishing the same thing. Before continuing this line of thought, however, the broader picture of government information policy and history must be reviewed.

The United States Government Accountability Office (GAO) issued the results of a study on information sharing in March 2006. This report outlined the steps the government has taken since the events of 9/11, and concludes that while some small-scale information sharing initiatives are underway in a small number of agencies, ultimately “[n]o governmentwide policies or processes have been established by the executive branch to date to define how to integrate and manage the sharing of terrorism-related information across all levels of government…” \(^5\) This is a statement echoed throughout many commission reports and agency reviews since the creation of the intelligence community. From the Dulles Report of 1949, the Schlesinger Report of 1971, the Aspin-Brown Commission of 1996 and the House Permanent Select Committee on Intelligence’s IC21 Staff Study published the same year to post-9/11 writings like the 9/11 Commission Report and the GAO Report (both mentioned above), the cry for better information sharing, better and more timely information analysis and the need for better-organized information echoes throughout. In a 2005 article Bruce W. Dearstyne comments:

[The Clinton and Bush administrations made] quick and convenient sharing of information … a management priority. Neither administration ensured the FBI, CIA, and other security agencies actually put into place the policies, practices and systems needed to implement the vision of easy sharing of critical

---

information, timely analyses, meaningful summaries, and provision of actionable intelligence.\(^6\)

This telling comment reflects statements given by many authors of the past – the government knows it needs to share information, and needs to provide analysts with the best data so they can produce more accurate intelligence reports to policymakers. Of course, part of the problem with information sharing in an analytic context is that in many ways it competes with the political context of the intelligence community. Intelligence analysis does not happen in a vacuum, but rather within the larger framework of the intelligence community as a whole. This necessarily includes political parameters, as many top level administrators are political appointees. This can cause conflict when the analytic product (the intelligence) does not match what those with the political power want of believe. Though the political ramifications of intelligence analysis are beyond the scope of this paper, this conflict must be acknowledged as a significant policy issue. Unfortunately, even today, the agencies are still caught in the quagmire of policy – political or otherwise – institutional mindset and bureaucracy.

A Look at Issues and Policy

There are many problems to be overcome when considering the improvement of information sharing within the intelligence community. Some are products of their own making – cultural and bureaucratic – like internecine turf wars, the idea of “giving up control” of an agency’s “own” information, a lack of trust among agencies and the desire to “be the first” to give intelligence to a policymaker, and most importantly a resistance to change. Other issues are

more mundane: budgetary restraints, little interoperability among computer systems, and differences in classification of data (e.g.: one agency may call a report “Top Secret” while another agency calls the same report “Sensitive”.) Finally there are the policy issues at play: the Fourth Amendment, originator control, the federal Privacy Act, and the Homeland Security Act all affect different aspects of gathering and disseminating information. The following paragraphs provide a look at these issues and policies and point out their impact on information sharing.

The first policies to be discussed are two recent government publications which spell out needed changes to information sharing practices within the intelligence community. *The National Intelligence Strategy of the United States of America*, released by the Office of the Director of National Intelligence in 2005, sets forth a series of clear and concise objectives geared toward creating a vast reform within the intelligence community. As part of their “Strategic Objectives,” they call for policies to “ensure that Intelligence Community members can access the intelligence they need when they need it” and to “strengthen analytic expertise, methods and practices; tap expertise where it resides; and explore alternative analytical views.” 7 This point is quite interesting as it applies directly to the thesis of this project: add more information professionals to analytic divisions within the agencies. More about this idea will follow in the final section of this paper.

The second policy, the Homeland Security Act of 2002, calls for sweeping reforms as well, as it establishes the creation of the Chief Information Officer within government agencies, information-sharing among all agencies and

---

broader access to information across the board. In addition, the Office of Homeland Security calls directly for “a national environment that enables the sharing of essential homeland security information.” These policies have a positive impact on information sharing, as they clearly highlight the need for better information sharing and set in place directives designed to do just that.

On the other hand, policies such as originator control (ORCON), the Fourth Amendment and the Privacy Act limit how and what kinds of information the government may collect and disseminate. The post-9/11 world has seen dramatic changes in the way the United States must deal with threats within and beyond its borders. The key to preventing further attacks must focus on information, and that information necessarily includes data about individuals who may be plotting a terrorist act. Thus information about private individuals is a top issue today in terms of how much information can be collected, when it is appropriate to collect it, and what kinds of information can be collected.

Intelligence agencies use this collected data to disrupt terrorist cells while private citizens become worried that the government has too much power and too much control over their personal information. For example, the July 2006 terrorist plots in Toronto and New York were disrupted by the FBI which used personal data to track down the suspects. The FBI working with foreign officials followed money trails, monitored internet discussions online, and used other data to determine who the suspects were. This use of personal data allowed law

---

enforcement to track, move in, and detain the potential terrorists before their plans could be completed.\textsuperscript{10}

To better illustrate the problem surrounding the collection of personal data, consider the Terrorist Surveillance Program administered by the National Security Agency (NSA), a massive phone record database which includes data on millions of American citizens.\textsuperscript{11} The government argues that this allows them to track those individuals with alleged terrorist ties, and the opponents of this program argue against it on grounds of information privacy laws as well as the Fourth Amendment, which guards citizens against unlawful search and seizure. These issues, delving as they do into the vast arena of information privacy concerns, are beyond the scope of this project except to say that these policies do have a dramatic affect on information sharing – especially between agencies like the FBI and CIA. Because of these and similar conflicts, strict guidelines regarding information collection and information sharing remain in place which these two agencies must follow, both in America and overseas. In addition, there are also policies which dictate how and when the FBI and the CIA can not only collect information, but share it as well.

These particular conflicts go back to the creation of the CIA when William Donovan, head of the CIA’s predecessor, the Office of Strategic Services (OSS), made the proposal for the new agency to President Roosevelt in 1944. As part of this presentation, he emphasized that the CIA would have no police or law enforcement functions either in the U.S. or abroad.\textsuperscript{12} Primarily this was to head off any objections by J. Edgar Hoover and the FBI, but the results are seen


\textsuperscript{12} Nathan Miller, \textit{Spying for America} (New York: Marlowe and Co., 1997), 295.
clearly today as the two agencies continue to struggle over their respective roles in intelligence collection and to work through barriers still present in their information sharing capabilities. Barriers like this were created for a specific reason initially, and the same is true for barriers between other agencies. The original focus of these different organizations had different operation parameters and responsibilities at one time. These differences range from what types of information are gathered, like military or civilian data; what kind of data it is, like signals or imagery; or where the information is gathered, like domestic or foreign data. Over time these barriers have been breaking down as agencies are asked more often to collaborate on projects rather than work with a narrow focus. Unfortunately they are still struggling with the changing landscape, especially in terms of information sharing.

ORCON has a more direct impact on government information sharing. The substance of this rule allows originating governments (or agencies) the right to retain control over the declassification and release of information. ORCON became established in bureaucratic policy in early 1950s during the Cold War. More recently, it was clarified by Executive Order 12958, which states “classified information shall remain under the control of the originating agency.” Alasdair Roberts wrote an insightful piece about ORCON in 2004, where he takes a careful look at the policy of originator control and how it affects information sharing even as the nation’s leaders call for more. He writes:

Federal policymakers have taken steps to promote deeper flows of information among federal, state and local agencies engaged in work relating to homeland security... In every case, information sharing policies have incorporated the ORCON rule and strictly

---

limited the capacity of actors within these networks to publicly disclose shared information.14

While Roberts is specifically addressing publicly available information (available through the Freedom of Information Act) here, the same rules also apply to classified information within agencies. He goes on to say, “It has also been criticized as an impediment to effective information sharing among government agencies themselves. For example, it limits the capacity of a receiving agency to forward information to a third agency without consent of the originator.”15 Thus the CIA may not share the FBI’s information with the Defense Intelligence Agency without the express approval of the FBI.

These issues are slowly being resolved, as seen in the recent Bush administration amendment to Executive Order 12958, resulting in Executive Order 13292, which allows forwarding without permission “in an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland.”16 Unfortunately, this still does not resolve the problem satisfactorily. There is a great need to share information across the board in order to improve our strategic intelligence. Focusing on tactical intelligence – that which deals with any immediate threat or crisis – is important, but it is equally critical to develop long term, strategic intelligence in order to prevent the crises from occurring in the first place.

15 Ibid, 261.
The Stove-Pipe: An Intelligence Community Information Sharing Model

Upon reflection, the model currently in use by the intelligence community can be summed up in a few brief sentences. It is a closed model, with many individual loops of data which never quite connect. This separated loop structure makes it difficult to share information within an agency, and even more difficult to share information between agencies. The level of secrecy each agency places on its information creates impenetrable barriers, and makes the process of finding and retrieving information difficult as well. Current policies in place only add to the difficulties, despite government mandates calling for better information sharing. Thus “stove-pipe” is the perfect term for this model. A stove-pipe, in intelligence language, is a closed loop of information, not interacting in any way with other loops. The loop can be created and maintained by a division, a department, an agency or even a single analyst.

![Diagram](image)

Division A  Division B  Division C

Movement of information within the stove-pipe model.

Figure 1
Regardless of its makeup, a stove-pipe does not share information, and does not readily accept information from others. Lawrence P Farrell, Jr., the President of the National Defense Industrial Association and a writer for the National Defense Magazine, writes about the dangers of stove-piping, and says, 

The need for information sharing and coordination [is] huge. There is a danger that, if the government is not careful, the White House, the Defense Department and the new agencies for homeland defense will end up creating new stove-pipes. That would be bad news. The flow of information among agencies must be seamless. After all, our enemies have become quite astute at exploiting seams, when they see them.¹⁷

There is a fine balance which must be struck between keeping secrets and sharing information. Currently the intelligence community as a whole leans too far to the “secrets” side of that spectrum and is still dedicated to its stove-pipe model. This project will show that one solution to the stove-pipe problem is the addition of information professionals within analytic divisions. Their skills in information organization and technology management will greatly enhance sharing among divisions, ensuring that data is received by all those who need it. The next chapter will look at a different way of approaching information as intelligence, and offer a comparison to the stove-pipe.

CHAPTER 2
INFORMATION AND THE BUSINESS COMMUNITY

A Brief History

Many authors and commissions have made suggestions as to how to increase government information sharing, but few have put forth any sort of model to which these suggestions can be compared. Competitive intelligence is one such model, and with its beginnings rooted in government theory it should make an interesting lens through which to view the intelligence community stove-pipe model. From the works of Michael Porter to the government’s concepts of the information life cycle and information resources management to the idea of a Chief Information Officer, there are many parallels when comparing the government’s intelligence community to competitive intelligence in the business arena. Before a clear comparison can be drawn, however, these ideas must be addressed from the viewpoint of the business world, and that should begin with one of the top thinkers of the genre.

Michael Porter, a professor at Harvard Business School and author of many books and articles, is considered a leading contributor to strategic management theory. The rise of new information technology in the late 1970s and early 1980s vastly increased the flow and use of information within individual companies, among companies in their collective industry and among industries scattered throughout various nations. Porter looks at this vast increase in information technology, and sees it creating huge leaps forward in the way industries do business. His writings on competition have thus helped shape what has become competitive intelligence. One of his most important concepts, the
value chain, in his words: “divides a company’s activities into the technologically and economically distinct activities which it performs to do business.”\textsuperscript{18} These activities are connected by linkages, which occur when one activity affects in some way another activity.\textsuperscript{19} Each of these activities and linkages rely on information to keep them current and accurate, and the increase in information technology ultimately allows companies to use information in ways previously unheard-of in the corporate world, especially in the realm of creating competitive advantage.

His concepts of competitive strategy and competitive advantage eventually create a change in a company’s corporate strategy, or “what makes the corporate whole add up to more than the sum of its business unit parts.”\textsuperscript{20} This corporate strategy depends on comparisons to other companies’ activities in terms of financial viability, product diversity and manufacturing abilities and every other value chain within an individual company. These comparisons necessarily lead to what some call “corporate espionage” – gathering information on competing companies to create usable data – more politely known as competitive intelligence.

Before Michael Porter started his work on competition, competitive intelligence found its beginnings in government policy. The Commission on Federal Paperwork resulted in the Paperwork Reduction Act of 1980.\textsuperscript{21} With this Act Congress also took advantage of the rise in information technology to ensure that this technology was acquired and utilized in order to minimize the paperwork burden on citizens, companies and the government itself; to create

\textsuperscript{19} Ibid, 73.
uniform federal information resources management policies; to improve the quality, collection and dissemination of Federal information and to establish the Office of Information and Regulatory Affairs. The business world took notice of these new policies, and soon after F. Woody Horton Jr., the head of the Commission, published his book called *Information Resources Management* in 1979, executives started to include information resource managers as part of their staffs. Finally, in 1986, competitive intelligence gained international recognition as a professional organization with the creation of the Society of Competitive Intelligence Professionals.

Now, decades later, the Paperwork Reduction Act is still the primary law governing information resource management (IRM), and there remains interest in the concept, as seen by the revision and reauthorization of the Paperwork Reduction Act in 1995. But what exactly is information resource management? IRM in the federal government has two basic meanings: “the management of information resources, namely information, technology, and related resources; and the management of information as a resource.”

Proponents of IRM hold that information is a key resource, and in order for the organization to be effective it must be managed appropriately and efficiently. In the past 15 years, the focus of IRM has shifted from a primarily administrative role to a more strategic role, as seen in the Office of Management and Budget.

---

OMB Circular A-130: “The term ‘information resources management’ means the process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.” This shift in thinking emphasizes what Michael Porter claimed ten years previously:

Initially, companies used information technology mainly for accounting and record-keeping functions...Today information technology is spreading throughout the value chain and is performing optimizing and control functions as well as more judgmental executive functions.

Based in part on Porter’s ideas, now information and the use of information technology is the key to not only being an efficient business, but to creating the strategic plan for the organization as a whole.

The concept of the Chief Information Officer also evolved from a series of government mandates and reports, primarily the Clinger-Cohen Information Technology Management Reform Act of 1996. Only a few years after the Paperwork Reduction Act, the Clinger-Cohen Act responded to the government’s poor management of funds and resources by mandating that agencies create the oversight role of Chief Information Officer. This mismanagement of funds was uncovered by a 1994 GAO report on strategic information management and technology. Among other things, it found that the Veterans Administration spent $700 million to improve a claims processing system. After the system was installed, the wait time to receive compensation increased from 151 days to 228 days. Other problems involved unauthorized

---

student loans, mistaken Medicare payments, and the release of sensitive information about law enforcement informants.\textsuperscript{30}

After the GAO report was published, a direct response came in the form of Executive Order 13011 which states that agencies must “establish clear accountability for information resources management activities by creating agency Chief Information Officers (CIOs) with the visibility and management responsibilities necessary to advise the agency head on the design, development, and implementation of those information systems.”\textsuperscript{31} Thus the Clinger-Cohen Act was drafted in response to both the Executive Order and the GAO report. Unlike other government information policies, the Clinger-Cohen Act looked to private sector companies for guidance in the role and responsibility of CIOs. The government saw corporations with successful information policies in place, and responded by attempting to emulate them. This emulation may eventually be reciprocal, as now the corporate world has improved information sharing and processing strategies which can be utilized by the intelligence agencies.

Another key idea has arisen from the Paperwork Reduction Act and its attendant concepts: the information life cycle. As part of the U. S. National Commission on Libraries and Information Science, Woody Horton (who also headed the Commission on Federal Paperwork mentioned above) writes:

Information, whether government information or any information for that matter, having a \textit{life cycle} is not a new idea. A useful analogue often mentioned is the concept of the \textit{product life cycle}. That is, in the business world, as taught in business schools, a product is "born," "matures," "demand levels off," and then customer disinterest sets in and product


sales decline and finally the product is taken out of production and off the shelves ... Applied to the creation, handling, disposition, and archiving of information, the life cycle concept follows a similar circular path, which is both endless and continuous.\[emphasis original]\n
Again there is the merging of two seemingly disparate worlds – the government and the corporate. This life cycle shows up in a slightly different form as the traditional intelligence cycle in nearly every discussion of how information is obtained, analyzed and disseminated by the intelligence community. The information life cycle and the intelligence cycle are from the same mold. The origins of them are muddled, but the CIA has, in its Factbook on Intelligence, the “gold standard” of the intelligence life cycle. Most references to the intelligence life cycle lead back to the one defined by the CIA.\[emphasis original]\ The information life cycle has the government as its origins as well, as seen above, so it is difficult to know which came first. Regardless of its origin, the cycle of information through an organization is critical to collecting, analyzing and disseminating actionable intelligence.

The basic information life cycle, defined in the OMB Circular A-130 as “the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition”\[emphasis original]\ has grown into a staggering business, now called “information lifecycle management” or ILM. High-ranking officers from successful companies like Symantec, PriceWaterhouseCooper, IBM, and Sun Microsystems participated as


\[34\] OMB Circular A-130, ibid.
keynote speakers for the first stand-alone ILM Summit in February 2006. A quick search online will net hundreds of hits for ILM, most produced by internet technology companies selling software or hardware. Michael Porter’s ideas on competition and the government’s policies on resource management have merged to create an enormous and powerful industry dedicated to collecting, collating, and disseminating information in all its forms.

The concepts outlined above, information resource management, information technology, the information life cycle, and dedicated information manager positions like the CIO, begin to converge here as the government and the corporate world realize the necessity of utilizing information and its technology to its fullest degree. Today many government agencies are working diligently to make information more accessible not only to other agencies but to the public as well. This is seen most clearly in the federal website FirstGov.gov, where agencies from the IRS to the Census Bureau strive to place all the information a citizen might need in one convenient location. Unfortunately, within the intelligence community, change is slow in coming.

Some Corporate Examples

One example of these effective information practices is the Nippon Steel Corporation in Japan. They have a computerized information system that links their steelworks computers, plant terminals and research laboratories which allow any terminal operator to access data from all three divisions, creating a more complete picture of everything each department handles. This process has helped Nippon Steel increase its competitiveness among its rivals through

---

increased operational control and better information exchange. With this high-tech information sharing system in place, the company cannot do its job effectively and the margin of profit is reduced.

Ford Motor Company also sets an excellent example for information sharing in their Best Practices Replication. Every division in each plant receives several Best Practice emails a week, which detail some specific task or idea a single plant has discovered which makes part of the work they do easier. The emails have the same basic format which includes where the idea originated, a brief description of the practice, the savings and contact information. A single person, called the Focal Point, is responsible for retrieving the Best Practices and writing them when his own division has a new idea. These Practices are sent only to applicable divisions so the Focal Point does not have to sort through dozens of emails a day. Each Practice must be responded to by the Focal Point either by saying how they implemented the idea or why they did not, and the full reports with corresponding responses are reviewed at plant and vice-president level meetings. With this system in place, all Ford divisions hear about new innovations created by plants around the country. Information is shared and the reward for the originating plants is to see their ideas being implemented elsewhere.

One final example here is British Petroleum and their Knowledge Assets. Early on the company had a database reliant on a basic search engine which acted as the company’s knowledge repository. This evolved into the Knowledge Assets, which are BP’s accumulated knowledge about specific topics which are

---

37 Dixon, 56.
prepackaged for the identified end user. A team drilling offshore can pull the Knowledge Asset for offshore drilling and learn from all those teams that have gone before. These packages are compiled by knowledge specialists who have traveled to where the teams are working and synthesized the information based on multiple examples around the world.

It should be noted here that the information sharing practices reflected in these examples are based on secondary sources rather than collected data. As such, these accounts may be biased in favor of showing an idea information sharing environment. In the real world, it is possible that these policies and practices do not function as smoothly as they are described here. For the purposes of this project, however, they remain excellent examples of how information sharing can function smoothly and efficiently.

How do these companies manage this depth and breadth of information? They employ information professionals, both in the traditional role of company librarian and IT specialists, as well as newly developed roles such as “knowledge manager” or “information specialist.” This utilization of information professionals is growing. The Special Libraries Association (SLA) came out with a surprising statistic in 2005, stating that eighty-five percent of the companies ranked in the top 100 on the Fortune 500 list employed information professionals, compared to less than fifty percent of the companies ranked in the bottom 100. This is a hopeful statistic for information professionals and those who want to see their numbers increase in the corporate world and in the intelligence community and in the future, as more companies adopt their own information sharing practices, perhaps this model will be more evident.

38 Dixon, 103-4.
The Ecosystem: An Information Sharing Model for the Corporate World

James F. Moore coined the phrase “business ecosystem” in 1996, as it applies to business relationships and networks. The analogy between a network of businesses and an ecosystem in nature holds true because corporations continue to work together and share information, both within a single corporate structure and between companies as a whole. Competitive intelligence relies on this type of information sharing to be effective. A recent article in *Optimize*, the online journal for Chief Information Officers, states:

> In our increasingly interconnected world, standing alone is no longer a viable business model. Instead, smart companies rely heavily on networks of partners, suppliers, and customers to achieve market success and sustain performance. These networks look increasingly like a biological ecosystem, in which companies succeed and fail as a collective whole. They operate in a business environment of shared fates and business models, and see their ecosystems as helping them become more resilient to market changes and more responsive to customer needs.

Within a single corporation, the ecosystem relies on each division to perform its necessary functions, and trusts that there will be full sharing of relevant information in all directions. This means each division has the same information as all the others, so they can more efficiently work together for the broader success of the company. By learning from each other and sharing what they

---

know, divisions increase the effectiveness of their company’s competitive intelligence because no one is left out of the information loop.

As shown above, the intelligence community has a closed model for information sharing, preferring to share information as little as possible. Many companies in the corporate world stand in stark contrast to this with their call for shared learning, “intelligent organizations” and encouraging employees to know and learn as much as they can. Ethel Auster and Chun Wei Choo, editors of the book Managing Information for the Competitive Edge, are academics who have spent years researching the way information is utilized in corporations. They comment: “An information-savvy organization is an intelligent, learning organization that is skilled at creating, acquiring, organizing and sharing knowledge, and that is able to adapt its goals and behavior to reflect the new knowledge.”42 This succinct explanation exemplifies how different information sharing can be for the corporate world in comparison to the information sharing struggles of the

intelligence community. British Petroleum’s Peer Assist Program is a good example of this information-savvy culture described by Auster and Choo: it allows a team working on a project to contact another team with the requisite experience and ask for assistance. Ideally these two teams can then get together and discuss the problems and possible solutions, to the mutual benefit of both teams. There is no arguing over turf, or whose responsibility the assignment is – the goal is to accomplish the project and by working together the project often gets completed more quickly and more accurately.43

Granted, the same problems encountered in the intelligence world are often encountered in the corporate world, especially the reluctance to share data. The corporate world is not a perfect reflection of this ideal information sharing concept, but there are enough examples in the corporate world that do exemplify this focus on information to make them significant. Thus, this project will focus on those companies who have restructured their information sharing and information gathering capabilities and made it a top priority.

The corporate world often struggles with the same issues the intelligence community comes against: turf wars, bad management and bad corporate policies. In general, competitive intelligence in the private sector functions more smoothly than government intelligence as will be seen in the next chapter. The corporate struggles are dealt with in a more timely fashion, and certainly with fewer commissions, than the same struggles within government agencies, and that in itself makes it a worthy model to explore. As Helen Butcher notes in her book Meeting Managers’ Information Needs,

> It is clear, however, that many organisations now recognise the pivotal role which information and its processing plays in their organisation. Many such organizations are already

---

knowledge-based and recognise the value of their intellectual capital, and it is likely that many others will soon make the transition to fully-fledged learning organisations very soon. To fail to do so might seriously jeopardise their competitive position with serious consequences for both the organisation and its workers.\(^{44}\)

It is this which keeps corporations in a state of constant innovation when dealing with information: failure to do so would cause serious harm to the company in terms of competition and profit. If the “bottom line” is affected, the executives, managers, and regular staff take notice and look for ways to solve the problems at hand, and they are willing to share that information to bring a successful change. Intelligence agency employees have a similar motivation, but it is harder to see the commitment there. One possible reason for this is the difference in mindset – change the agency attitude so it freely accepts an open, sharing model like the business ecosystem and the employees’ mindset towards information sharing are changed as well. Granted this is easier said than done, but based on comments from intelligence agency employees shown in the next section of this project, it is an achievable goal.

Certainly the business ecosystem is not the only possible solution to the problems plaguing the intelligence community, but as a basic concept it has much to offer in terms of finding a new paradigm. The next chapter will discuss the pros and cons of the business ecosystem by comparing it to the government stove-pipe, and will investigate what lessons may be learned from companies operating in the private sector. The final chapter will bring to culmination this comparison by reviewing the critical role of the information professional.

CHAPTER 3
APPLICATION OF THE ECOSYSTEM MODEL

Comparing the Models

As seen above, the stove-pipe and the ecosystem models deal with the critical component of intelligence: information. Corporations and intelligence agencies must gather, analyze and disseminate critical information efficiently and expeditiously to give their policymakers the data they need to make their decisions. Whether the work is related to nuclear warheads in North Korea or in how automobiles get distributed throughout the world, the analyzed information – intelligence – is the key to the whole process. Information becomes intelligence as part of the information life cycle mentioned above – called the traditional intelligence cycle in most intelligence circles. First information is collected from a huge variety of sources, including human sources or technical sources like satellites or radio intercceptions. Then it is processed: human information is corroborated, satellite imagery is analyzed by specialists, and foreign language transmissions are translated. Finally, this data is collated with other relevant material and the created result is intelligence. Without information there can be no intelligence, no measured action can be taken, and the job cannot be done.

Each model has similar constraints it. Both have a need to protect their information from prying eyes. There are corporate policies in place on how the information can be shared within the organization and beyond. Both models require information about other organizations to make good decisions, and must

---

often prevent those organizations from discovering there is information-gathering taking place. However, the broad similarities end here. The ecosystem is designed to allow access to information by many levels and departments. The reasoning is that the more one person knows, the better for the company as a whole. In a paper presented at the 1995 Digital Libraries Conference, Choo asserts: “A wider distribution of information promotes more widespread and more frequent learning, making the retrieval of relevant information more likely, and allows new insights to be created by relating disparate items of information.”

What does this say in contrast to the intelligence community? Abram Schulsky states that in any intelligence agency, information should be spread around as little as possible to protect the data. Issues like this lie at the heart of the problem of intelligence sharing across agency lines. As seen above, information sharing is seen as a problematic task, fraught with complications involving the protection of information, policies and, more importantly, a cultural mindset. No longer can intelligence agencies sit idly by believing that a better computer system will solve all their ills. A technical solution will not solve a problem with sociopolitical roots, as the FBI proved by the issues it had in 2005 with its new analytic computer system.

The agency spent over 140 million dollars implementing Virtual Case File, a system designed to be a data warehouse for all the FBI case files, accessible by all agents and easily disseminated to other law enforcement agencies. According to Glenn A. Fine, Inspector General for the Department of Justice who

conducted an oversight audit on the FBI’s progress in counterterrorism and national security programs after 9/11, the FBI failed in three major areas during this review: an urgent need to upgrade their information technology systems, the need to share intelligence efficiently and a lack of human capital, especially noting that “more needs to be done to support the work of intelligence analysts, scientists, linguists, and other staff who are critical to meeting the FBI’s changing mission and duties.” This incident encapsulates the myriad problems within the intelligence community succinctly. The FBI personnel did not have adequate support to complete timely analysis of information: some of these missing staff roles could easily be filled with information professionals. Secondly, the organization relied too heavily on a “miracle” computer system to solve its information sharing and analytic problems. When that system was a failure, the FBI was forced to return to its archaic methods of paper-intensive case files. Thus the FBI continues to work in a stove-pipe environment until a change is wrought which encourages bringing information technology and qualified personnel together. This pattern can be seen in many intelligence agencies across the country, and they will continue to act as closed information environments until both the cultural mindset and the technology/personnel issues are solved.

This stove-pipe approach – keep information relegated to a limited number of people in order to protect the data and the sources – is where the intelligence community fails the policymakers. If the policymakers do not have up-to-date and accurate intelligence, they cannot make correct decisions for the country. Intelligence cannot be fully accurate and up-to-date if agencies do not

---

share different aspects of information relating to the same subject. Therein lies the crux of the problem.

The corporate versus intelligence agency mindset can be summed up quite succinctly: open versus closed. The closed vision of the stove-pipe model cries out for more information. Without some sharing how can the analysts gather the information needed to create actionable intelligence? The open sharing of the ecosystem model goes perhaps too far to the opposite extreme, because intelligence agencies have a duty to protect their sources and methods. This is not to say that the ecosystem concept does not have a useful place within the intelligence structure. The government, many times, has called for just such a structural change to make it easier to share data across divisional and even agency lines. The 9/11 Commission states: “Agencies uphold a ‘need-to-know’ culture of information protection rather than promoting a ‘need-to-share’ culture of integration…We propose that information be shared horizontally, across new networks that transcend individual agencies.”

**Overcoming Policy Concerns**

Many policy issues deter agencies from sharing information, from the top executives down to the low-level analysts and researchers. “Change at the top can be an aspect of structural change,” Orna notes in her review of business information policies. There must be executive level persuasion of lower level employees before any significant information sharing can take place on a regular basis. One analyst remarked, “Programs are started with great potential, but the

---

49 National Commission on Terrorist Attacks Upon the United States, 415.
folks in the trenches don’t use it so they are useless. Having more executive support for programs like this would encourage more people to use them.”

Another issue involving mindset is the need for managers to “persuade analysts to believe that irretrievable information is of no value. This will be the best way to convince them to build retrievable systems but especially to share.” This reflects earlier comments regarding mindset – if you can change the attitude of the individuals both at the top and at the bottom, true change within the organization becomes possible.

Another debilitating mindset caused by policy is the impression that in the world of government intelligence the agency which produces the most actionable position papers is the agency that gets the biggest budget. A policymaker at one of the intelligence agencies recently commented “You get the impression that if your agency turns in a report that is incorrect, or a report that another agency turned in before you, that your agency will be penalized financially.” Whether or not this policy actually exists, it is true that Congress sets the budget through two congressional oversight committees – the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Permanent Select Committee on Intelligence (SPSCI). Congress has a say in the intelligence budget as well. The HSPCI website says this about agency budgets: “it is also important to have an effective oversight process to ensure that intelligence resources are not misused … Because of the sensitivities of intelligence operations and resources, the intelligence budget is classified. These same sensitivities require that the budget receive an extra amount of congressional scrutiny, and there is a legal requirement that intelligence funding not only be

---

appropriated, but authorized as well.”54 Regardless of the actual facts, the mindset that Congress rewards the best intelligence reports must be changed in order to achieve any real information sharing across agency lines. Instead, perhaps, set policies which reward those agencies which produce intelligence and disseminate it broadly throughout the community as a whole. By removing the perceived money factor, it will be much easier to convince upper-level agency management that information sharing is of great benefit to everyone concerned.

Another long-held policy issue is the problem with information sharing between the FBI and the CIA. Until recently, as mentioned above, the two agencies had significant policies which prevented them from sharing information. According to FBI director Robert Mueller, however, many of those restrictions have been lifted as a result of the changes in the intelligence community after 9/11. In his congressional testimony to the 9/11 Commission, he states, “The legal walls between intelligence and law enforcement operations thankfully have been broken down… We are now able to fully coordinate operations within the bureau and within the intelligence community.”55

Other policies which trip up information sharing in the intelligence community have been mentioned previously: ORCON being one in particular. This issue of originator control, while necessary to protect sources and methods, is a great stumbling block. To compensate for this, a government-wide revision of the classification designations is called for. The GAO, in its March, 2006, report, notes

There are no governmentwide policies or procedures that describe the basis on which agencies should use most of [the

With mass confusion among the labeling of sensitive-but-unclassified information, one can imagine an equally confusing array in terms of classified designations. If the agencies were to come together and decide on how each of the designations will be used, then it would become easier to determine who has access to what data. This might also alleviate some of the problems with ORCON: if an analyst has a certain type of security clearance then he has access to this level of classified information, regardless of its origin. There are no unclassified studies regarding this suggestion, but it seems plausible if the security classification levels are the same across agency lines. Data classified at a high level of security would be accessible by those who have a top-level security clearance, and have thus been vetted more carefully by their respective agencies in conjunction with an FBI background investigation.

Other surmountable problems include the need for systems to be compliant with Freedom of Information Act and consistent with Archivists of the United States regulations. Unclassified information must be available in the required format to citizens who request it either through FirstGov.gov or through other FOIA means. In addition, the National Archivists of the United States have regulations relating to the preservation of physical materials and the documentation of materials of all kinds. Of course, information professionals are trained in these types organizing, classification and storage requirements, so this policy problem is easy overcome. These types of problems in general, however, fall outside the focus of this project. They are mentioned here merely to suggest

---

57 Subject B, ibid.
that some of these types of policy concerns agencies have may not be as problematic as previously believed.

**Improving Information Sharing**

After the policy issues are addressed, the first and most critical concern to be overcome is that of the institutional mindset surrounding information sharing. Intelligence analysts have commented more than once that it is this mindset that is the issue that prevents even the best information sharing ideas from coming to fruition. “People do not want to share sensitive information and that will always be the case.”\(^{58}\) Another analyst remarked, “There’s the ego of it – someone discovers a piece of information and doesn’t want someone else to get credit for it in a different division’s report.”\(^{59}\) Also noted by many analysts is the problem that there is no formal process for information sharing. “It is not stressed to folks that they should connect with other people. Sometimes something might come along which might be useful to someone else, but it’s not your turf so you didn’t know who to send it to. More should be done to improve data sharing. Some divisions would share with certain divisions, but not with any others.”\(^{60}\)

Of course, even corporations have to work through the idea of sharing information. “[T]he hoarding of information is inherent to management systems in both large and small companies because managers are rewarded for innovative ideas and original thinking.”\(^{61}\) Incentives for information-sharing in

---

58 Subject B, ibid.
59 Subject A, ibid.
60 Ibid.
the corporate world are easier to institute because the levels of bureaucracy are not as deep in many information-savvy businesses. Corporations are more likely to promote restructurings and bring new policies into play when the company’s success is at stake. There are many books, articles and studies that have been done on corporate restructurings, whether a hindrance or a help to the company in question. To note one comment from the results of a survey of chief financial officers in publicly traded companies: “Among the 100 respondents, researchers found that the companies whose stock outperformed the average for their industry sectors in their domestic stock markets (so-called "outperformers") placed their emphasis on the strategic, the external and change.”

As anyone involved in organizational change knows, bringing about the change can be a difficult and painful process. Information professionals and analysts would not be immune from this pain when their positions are directly affected. This proposal adds a new dimension to the structure of analytic divisions, and resistance by the staff may be encountered. Those information professionals who are not interested in pairing with divisions could remain in the agency’s main library, serving there in the traditional, but no less important, role.

One successful method of increasing information sharing is through negotiation which brings competing and uncooperative parties together in dialogue with the managers to bring about change together. This ability to foster change for the betterment of the organization, whether easy to accomplish or not, should be a good example to the bureaucracy of government intelligence.

---


Regardless of other incentives that may be offered to individuals (like pay bonuses or special perks), it is the corporate attitude as a whole that allows information to be broadly shared. “[T]he attitudes and orientations of people towards others are the ‘binding force’ of an organization. People don’t have to be motivated, they are motivated…people do things out of a sense of commitment, obligation, responsibility…”  

One organizational means by which information can be more easily shared is the method in which data is classified and cataloged, in the traditional library sense. There are two distinct meanings of the word “classified” or “classification.” One is the government designation used to denote the sensitivity of particular data, which is critical for the agency to know who has access to particular data at any given time. The other is the traditional library definition of categorizing, which includes descriptive cataloging, subject headings, vocabulary and authority control and classification. In the library definition, a document is first described per the Anglo American Cataloging Rules. Then it is assigned subject headings based on the appropriate vocabulary and schema, like the Library of Congress Subject Headings. Authority control is established for the author so he will not be confused with another author of the same name. Finally the item is assigned an appropriate classification number for easy storage and retrieval: the Dewey Decimal System would be one example of this.

Information that is cataloged much like the process explained above will be retrievable by a larger range of people. To some extent, that is being done now by the analysts themselves. Each department is responsible for cataloging its own data, which is then available to other divisions within the agency. It is difficult to

---

know, however, how often these resources are actually utilized.\textsuperscript{65} As one intelligence analyst put it; “as an analyst you are your own information specialist.”\textsuperscript{66} However, with the time constraints connected to an analyst’s primary responsibilities of creating strategic and tactical intelligence, there is little time left for in-depth data cataloging. There is also little guidance as to how to catalog a report or a study, which makes retrieval even more difficult.

Many organizations have specific categorization schemes in place. The United Nations is one such example, as they have a tailor-made classification scheme called the United Nations Standard Products and Services Code. According to the UNSPSC website, this code “provides an open, global multi-sector standard for efficient, accurate classification of products and services.”\textsuperscript{67} This global classification system is not just for documents, but for information on goods and services around the world. This system offers one model which could be reviewed for the creation of a classification schema like the Dewey Decimal system or a controlled vocabulary for the intelligence community so that all agencies would follow the same system and procedures. With something akin to the Library of Congress Subject Headings – call it the Intelligence Subject Headings, perhaps – it becomes easier to both catalog and retrieve needed data. At the same time, as the GAO report mentioned above suggests, also restructure the classification designations, including open source, sensitive and secret. Once that is done, then blend these two schemas together in order to create a more comprehensive database of information. Then each division could catalog its own material, but would also be cataloging that data for use by the larger agency as a whole. “[A]n agencywide categorization scheme would augment the system

\textsuperscript{65} Subject A, ibid.
\textsuperscript{66} Ibid.
that’s already there and increase the fluidity of the data. It would be a benefit, and maybe even do away with some of the stove-piping.”\textsuperscript{68}

Another interesting possibility is the idea of building crosswalks between varying standards in information and security classifications as a means to connect various agencies’ data without requiring those agencies to adopt a completely different classification schema, unlike the model mentioned above. Information professionals could maintain this bridge, which would be useful not only as mentioned above but also as a means to coordinate digital preservation, destruction or declassification of intelligence documents and data.

How do the intelligence agencies accomplish these vast changes in how they catalog and organize information? With the addition of information professionals to each agency division, the solution becomes clear. These professionals not only have the skill-sets to perform the cataloging, but by working within the same division they also attain specialization with their subject matter. Chapter Four reviews the key points of integrating information professionals more fully into the intelligence community.

\textsuperscript{68} Subject A, ibid.
CHAPTER 4
THE ROLE OF INFORMATION PROFESSIONALS

Information Professionals in the Corporate World

Much of what is discussed in the previous chapter deals with mindset and, more importantly, the structure and arrangement of information for ease of access. At this point the heart of this project is revealed: what can the intelligence community learn from the corporate world regarding the utilization of information professionals as key players in the battle for actionable intelligence? It has been shown that many corporate organizations engage in information gathering practices, whether it is discerning what the consumer will purchase next month, sharing information between divisions or plants, or discovering what the competitor’s next merchandising scheme will be. These organizations also employ information professionals, sometimes in the traditional role of the librarian, and sometimes in other ways. It is the latter that this project will investigate in the hope that these corporate entities may have something to teach the intelligence community about gathering, storing and retrieving information.

Corporations have their financial well-being at stake, and this is often the impetus needed to combine cutting edge technology and human experience to create a new paradigm. Even the title “librarian” is being dropped in favor of terms like “knowledge manager” or “information specialist.”69 Regardless of the title, however, it is clear that business practices of some companies warrant a review by the intelligence community. By looking at some of their policies, new

---

methods of information retrieval and management may come to light which may prove useful as the intelligence community struggles to adapt to the information age.

For example, the marketing research industry relies heavily on competitive intelligence to give their clients the data needed to make appropriate decisions. Nigel Culkin and David Smith, both business and marketing faculty at University of Hertfordshire and Jonathon Fletcher, Associate Director at DVL Smith Ltd, write the following:

[T]here is also going to be a competitive advantage to those market research and information professionals who, at the outset of studies, can help define the problem in a manageable way, whilst at the end of the study helping the decision maker through the decision-making process. This is done, in part, by listening carefully and factoring in the manager's own intuition and prior knowledge on the subject, and also by helping set the information in a wider analytical framework context, together with helping the marketing decision maker present and win the case in the arena in which the argument must be presented.70

By actively including information professionals in the entire process of the marketing study, they acknowledge the fact that the expertise information professionals bring is critical. An information framework is useless without the trained staff that can utilize the data effectively and turn it into useful intelligence.

Angela Cleaver, an information manager at Watson Wyatt LLP (a global consulting firm) has this to say about her position as an information professional: “At the end of the day we are able to contribute most to our organisations, whether we’re in pensions or pharmaceuticals, when we know our users and

---

meet (and anticipate) their needs in the most appropriate way.”

By relying on information professionals to do the jobs they were trained to do – research, information processing, cataloging and materials acquisition – this consulting firm continues to be successful even after 125 years of operation.

This organization has the information professionals compile a daily news brief containing any items of interest to the company. In many ways, this report mirrors the President’s Daily Brief, which until 2005 was created by the analysts at the CIA and is now prepared by the Office of the Director of National Intelligence. It would be interesting to see if by transferring this job to the information professionals two things would happen: the brief increases in usefulness and the analysts themselves have more time to devote to their area of specialty – creating intelligence. If this project’s recommendation were to be implemented, then information professionals imbedded in each analytic division could work together to create the Daily Brief. It is, at least, an interesting thought to consider.

A study by the Special Libraries Association determined that almost 60% of information professionals working in organizations other than libraries felt that they were being underutilized in the areas of research and almost half felt they could be useful in the areas of analysis and interpretation of information. Despite this, it is also clear from the SLA that the number of information professionals working in the area of “competitive intelligence” is growing, and the companies utilizing their services appear to be prospering, which is evident in the SLA statistics quoted earlier – 85% of the top Fortune 500 companies employ information professionals.

---


How the Intelligence Community and Information Professionals Can Work Together

Information science and the intelligence community can learn much from each other. David Batty, retired from the British Army Intelligence Corps and now president of a company specializing in information system and library design, has this to say:

Intelligence work could afford to incorporate some of the information science analysis/synthesis techniques into an explicit processing phase. A better organized assembly of associated data would ease the task of the intelligence analyst...not by usurping the role of analyst, but by allowing and even supporting a higher function of human analysis, synthesis, and even recommendation.\(^{73}\)

He also notes that “[intelligence work] has neglected the development of the intellectually more sophisticated processing techniques increasingly common in the world of information science. On the other hand, information science... has neglected the demands inherent in handling raw, undigested data...and is consequently at a loss in this electronic age.”\(^{74}\) Thus a collaboration of the two disciplines may be what is necessary, and is just what this project proposes.

Information professionals are educated in information storage and retrieval, trained in database management and data collection. An agency which tasks these professionals to organize collected data within each analytic division – reviewable and retrievable by any other division – would remove that burden

\(^{73}\) David Batty, “Intelligence Work and Information Science: Two Men in a Boat,” in Covert and Overt: Recollecting and Connecting Intelligence Service and Information Science (New Jersey: ASIST Monograph Series, 2005), 32.

\(^{74}\) Ibid, 31.
from the shoulders of the analysts, allowing them to do their jobs more effectively. As Angela Edmunds states: “It would seem an obvious solution to the problem of information overload in businesses to employ specialists in information handling to carry out the acquisition of relevant information-processing and packaging the information needed as appropriate.”75 This applies equally well to the intelligence agencies, as information overload is a critical problem to be overcome.

Even now, intelligence agencies like the Defense Intelligence Agency are working with options like XML as a means to code data for better retrieval.76 Rather than training analysts in this complex markup language, an alternative would be to hire information professionals who have the ability to do that already. With someone in each division trained to organize and store data, then it becomes a simple process for an analyst to query the database for information on whatever subject he is reviewing. In addition to using these types of advanced storage and retrieval tools, agencies should take advantage of the knowledge information professionals bring to the stage.

Finally, a recent article in Information Outlook states “Encourage specialization. It’s a given that the more research specialists work with certain individuals and business groups, the more adept they become at meeting their information requests.”77 This points to the concept of adding information professionals to analytic divisions rather than keeping librarians in the library – by encouraging specialization they can better assist the analysts and create a

77 Susan J. Leandri, “Focusing on the Competition: Librarians and Competitive Intelligence are a Natural Fit,” Information Outlook 9, no.4 (April 2005): 17.
more focused dataset of their particular specialty. Other organizations such as the Association of Independent Professionals\textsuperscript{78} and the IFLA Division of Special Libraries\textsuperscript{79} have indicated a need for specialists (analysts) and information professionals to work together, creating a more complete analytic product. By taking the corporate model of information collection and dissemination and applying it to the intelligence community, new areas of opportunity will be opened to the beleaguered analysts who process data necessary for our country’s protection.

The basic structure proposed here is simple. Adding an information professional to each analytic division reduces the number of tasks the analyst must do by transferring information management tasks to the information professionals. Information professionals can take primary responsibility for conducting basic research for needed material, processing and cataloging completed reports and collected reports, and most importantly creating, implementing, and maintaining a coherent classification schema – both in terms of cataloging and in terms of secrecy – used by agencies across the board. As mentioned above, the GAO found that every agency used a different security classification scheme, leading to extreme difficulty in cross-agency sharing. With input from the division analysts, an information professional could make quick work of this type of classification, and have uniformity across the board for the community. This would allow faster response when searching for data, because the same classification is applicable regardless of originating agency. If there were a single subject heading system in place, then the information professionals


familiar with that system could both assign and retrieve reports and other data quickly and easily, freeing analysts – again – to do their jobs more efficiently.

Analysts and Information Professionals

Now that the breadth of possibilities adding information professionals has been revealed, the simple question, “Should it be done?” must be considered. Should intelligence analysts and information professionals be integrated? Would it be possible to merge people from the two disciplines into one arena, creating groups of highly specialized, highly trained individuals who work together as a seamless team? Conversely, should a line still be drawn between these two groups, and if so, how do you identify that line without blurring it completely? In fact, can such a line be drawn without deteriorating the very collaboration this project is suggesting? The answer to these questions becomes more evident at this point in the project – it is possible to bring information professionals into a division; train them in a particular specialized division; and keep the roles of analyst and information professional separate, yet maintain a strong collaborative process.

First, as stated in the introduction, information professionals are not analysts, and analysts are not information professionals. Each has a discrete core of duties which should be kept separate in that sense. For example, a quick review of CIA job listings for analysts specify types of knowledge, like international affairs, area studies, economics, geography, physical sciences, and engineering. In contrast, the requirements for librarians at the CIA are very different, focusing on research, customer service and reference support, information systems development, archive and preservation duties.
From this one snapshot, it becomes clear that these are not similar positions with similar duties. However, they are mutually supportive. Analysts’ jobs require them to take the disparate bits of data that are collected and transform them into a product useful to policy and decision-makers.\textsuperscript{80} An information professional’s primary roles are broad, but they include the design and management of information content and systems in order to support the specific goals of the organization in addition to the roles of meeting a particular user’s information needs.\textsuperscript{81} With this in mind, an analyst can give an information professional many good ideas about what sources are most important to meet the needs of the policy maker. An information professional can collate that data and organize it in such a way for ease of access when the analyst needs it. By working together in the same division, they both become specialists in the same area, yet each with their own focus and purpose.

Librarians once dramatically influenced the intelligence community during the Cold War as the Library of Congress staff assisted military and intelligence agencies in their search for data on the Soviet Union. Colin Burke, a researcher and historian, writes, “The flow of librarians into the military and intelligence agencies seems natural. Their skills and experience fit with the job of accumulating and bringing order to thousands if not millions of individual facts and artifacts…Thus librarians helped to shape the organization of information, if not knowledge, in the various intelligence agencies during the Cold War.”\textsuperscript{82} He goes on to remark that in a recent meeting at the Defense Intelligence Agency a group spent several hours describing a new trend in training for analysts – send

\textsuperscript{80} Shulsky, 41.
\textsuperscript{81} College of Information, Florida State University, “Masters Concentrations,” http://ci.fsu.edu/go/graduate/masters_degrees/concentrations (accessed 10 February 2006).
\textsuperscript{82} Colin Burke, “Intelligence Agencies, Librarians, and Information Scientists” in \textit{Covert and Overt: Recollecting and Connecting Intelligence Service and Information Science} (New Jersey: ASIST Monograph Series, 2005), 107-9.
them to library schools. Instead of retraining the analysts, why not hire already-trained information professionals and let each specialist do the job they know how to do?

The job description for a librarian at the Central Intelligence Agency reads: “Librarians contribute an essential role within this function by researching the critical information needs of our various offices, sometimes on quite short notice, as well as through more traditional duties of the profession.”83 These duties are important, but an information professional has a broader array of skills than what are considered the traditional roles of a librarian: cataloging, archiving and research. Information professionals today are graduating with an education that includes these time-honored skills, but also with classes in database management, network maintenance and web design, all geared towards making information easier for a patron to retrieve. Rather than placing them in the library alone, does it not make sense to incorporate them throughout the agency, calling on their skills daily to assist analysts in their day-to-day work? In addition, by grouping librarians with specific divisions, the librarians become specialized in that area and can better serve the analysts with whom they are working.

---

CONCLUSION

Now, after looking through the theoretical lens of information gathering and processing in corporate organizations, a new paradigm has emerged for the national intelligence arena, and information professionals play a critical role. The corporate world took significant ideas from the governmental policies of information management, and now the business world can reciprocate by sharing its own information knowledge management strategies with the intelligence community. As librarians once influenced the way intelligence agencies organized data, information professionals can return to government work and share their collective knowledge again by providing needed assistance and support to analytic divisions. This collaboration between the two disciplines can greatly increase the intelligence community’s ability to not only store and retrieve information, but to create the critical strategic intelligence necessary to defend the nation.

There is little previous research on which to base this proposal, due in part to the classified nature of the subject. Robert Williams, Professor Emeritus at the University of South Carolina School of Library and Information Science, attempted a literature review on the use of information science theories, methods, processes and techniques by intelligence professionals in 2004. His conclusion: “I have maintained the contention that even though there is a clear connection between IS and intelligence practices, theories, processes, and techniques, these relationships have only minimally been documented in the available literature…What we have are hints, when what we need are more
examples, more exploration of relationships, and more stories.”84 Compare the literature available for information science and competitive intelligence, which could fill volumes, and the problem becomes more evident. Thus the proposed idea for more information professionals in the intelligence community can draw insight from competitive intelligence, and as this project has shown, there are many good examples to choose from.

In this project, key components are the comments from staff members who actually work for an intelligence agency. By gathering information directly from those who work in the intelligence community environment, a broad generalization can be drawn in terms of how agency staff would respond to these kinds of changes. Although only three people were willing to go on record with their comments, their assertions that the community needs better information sharing, better organization of information and their agreement that information professionals could help solve some of these problems are critical. Because they are from three very different agencies and play very different roles within those agencies, this cross section leads to a general consensus of opinion, backed up by other comments from those not willing to formally participate in this project. In such security-conscious environments as the intelligence agencies are, it is understandable that many do not want to offer comments for attribution to an unclassified project. That does not mean that because it is unclassified the project itself it without merit, however, and the preceding pages are proof of that as it points out problems and possible solutions to the intelligence community’s information sharing problems.

This project certainly is not a comprehensive analysis of all the benefits and problems which may be encountered in such a venture, but it may offer the impetus to research this proposal further. By planting a seed of interest, perhaps researchers in the classified world will take up the idea and create a new paradigm of information sharing and analysis community-wide. Their access to reports unavailable to this researcher may hold the key to instituting the changes needed to make the intelligence agencies more successful and more collaborative as a whole. If the examples here provide the motivation to continue exploring these possible paradigms, then this project will be considered a success.
BIBLIOGRAPHY


Leandri, Susan J. “Focusing on the Competition: Librarians and Competitive Intelligence are a Natural Fit.” Information Outlook 9, no.4 (April 2005): 15-17.


Williams, Robert V. “The Information Science and Intelligence Service Literature: An Overview.” In Covert and Overt: Recollecting and Connecting Intelligence
BIOGRAPHICAL SKETCH
SUSANNA ROGERS SMITH

Susanna was born in Gadsden, Alabama, in 1970. She received her BA in English from the University of the South in 1993. She has also taken classes in strategic intelligence at Patrick Henry College. Since then she has worked primarily in libraries and bookstores, notably at Florida State University’s Strozier Library and as the bookstore manager of a small college in Virginia. Susanna received her MS in Library and Information Studies from the College of Information at Florida State University in 2006.