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

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 Many of the official assessments on Intelink are outdated soon after publication.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

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

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

Intelink's Hierarchical Culture

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

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

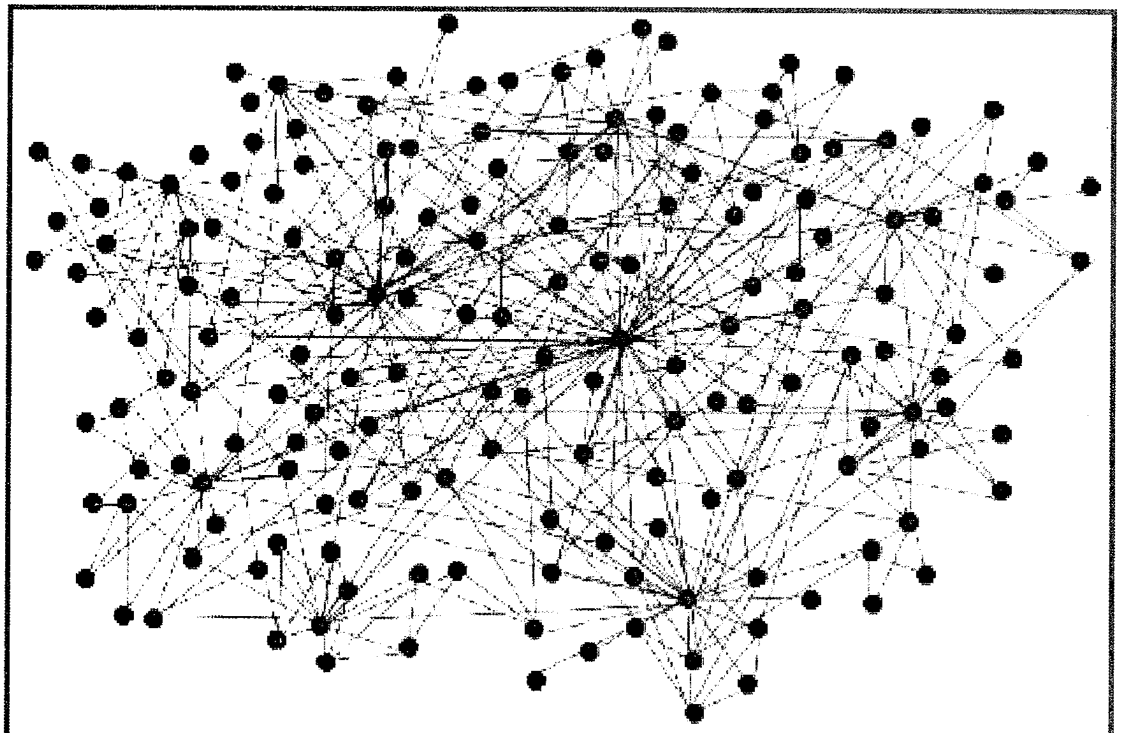


Figure 1: A figurative view of the World Wide Web. Users are allowed to link to any page they want but will naturally build communities of information with similar pages. The better sites receive votes of approval (in the form of links) from many pages.

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

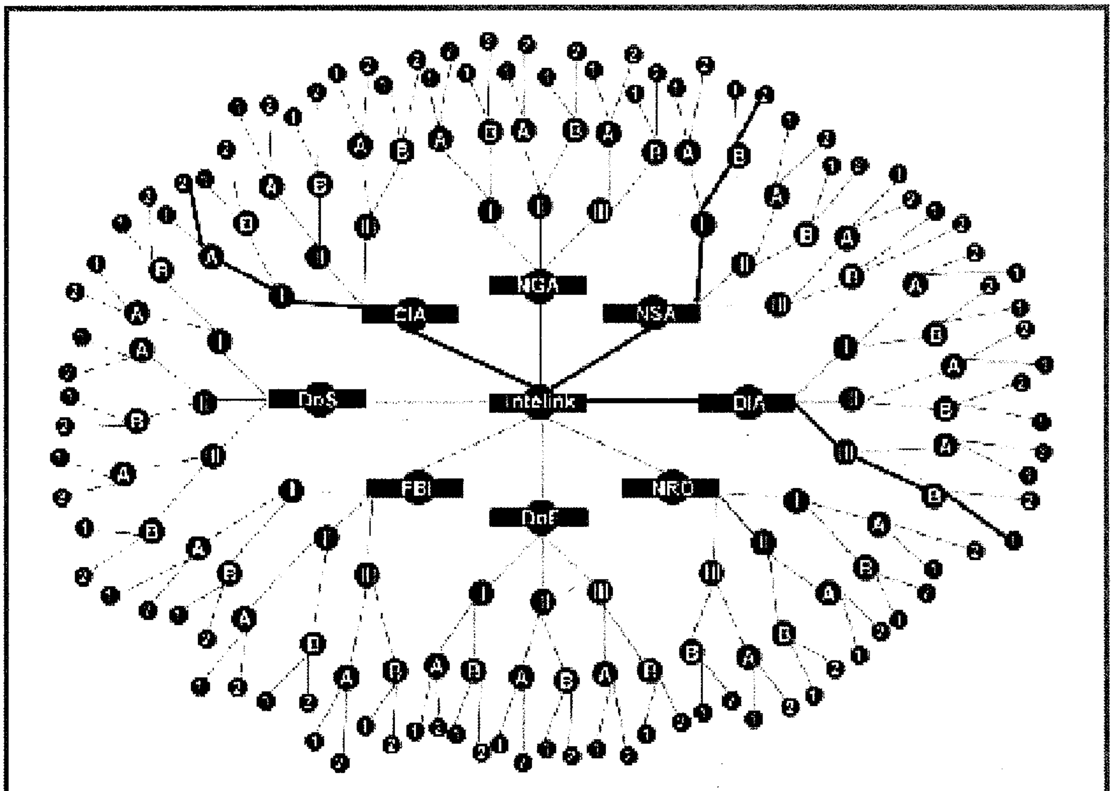


Figure 2: A figurative view of Intelink-SCI. Roman numerals, letters and numbers represent directorates, offices, etc. **Red Lines** show how distant like pages are on Intelink, making it harder for analysts trying to find a page buried deep within a site. It also keeps search engines from building logical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

Disconnected Data...

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

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

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

...And Disconnected Analysts

Intelink's structure has social implications as well. Before Google and the World Wide Web, the Internet was used solely as a way for people to directly communicate with each other and among large groups. It cultivated communities that became as close-knit as a suburban neighborhood. This camaraderie is nonexistent on Intelink. Its social culture is decades behind the one available through your home computer. While sociology and economics professors have projected the Web will mean the end of the nationstate, the borders between Intelligence Community agencies are still strong.

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

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

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

Your Counterparts, One (Virtual) Cube Over

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

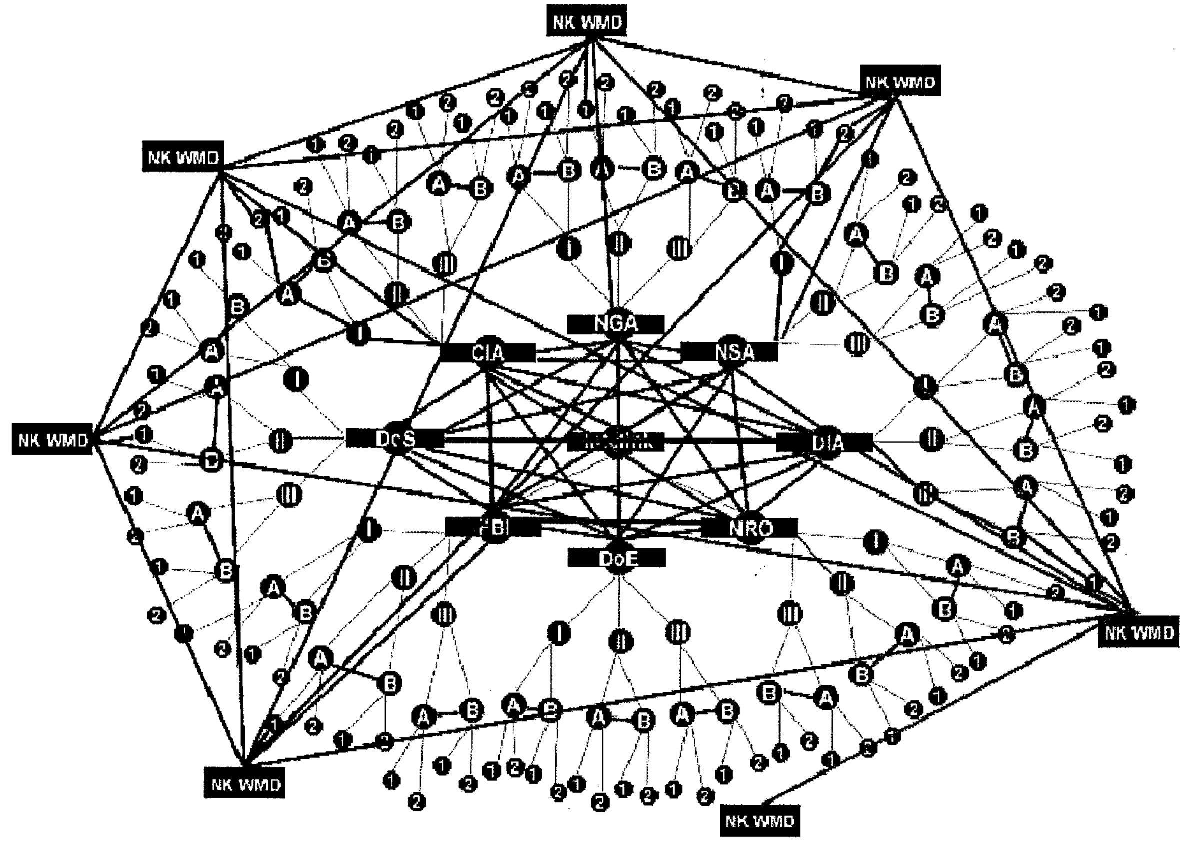


Figure 3: Intelink-SCI with the beginnings of a hypothetical online community. North Korean counterproliferation analysts have developed their own home pages and are now interlinking with counterparts' pages and analyses, making information on the subject easier to find for both humans and search engines.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

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

Endnotes

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

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

Executive Summary

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

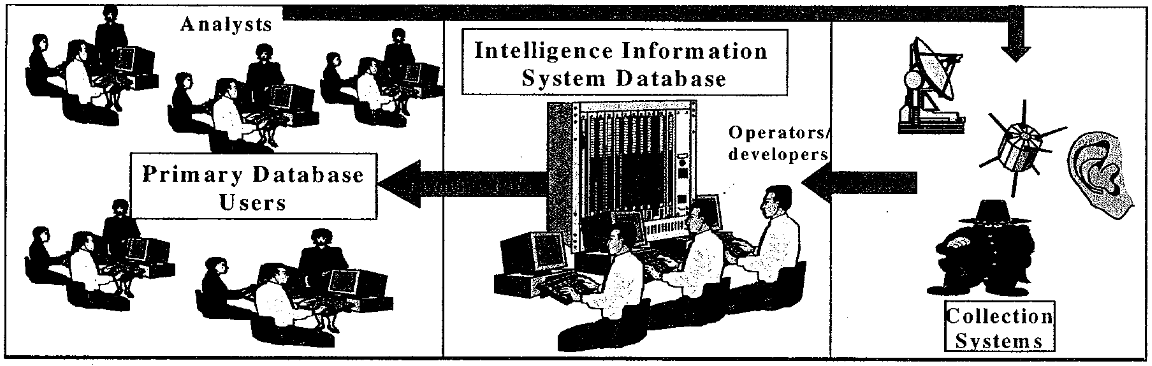
The Transformative Power Of Audit Log Data

Security auditing software can transform an IIS into an automated transaction processing system (ATPS). (See box below.) A product of the information technology revolution of the 1990s, ATPSs have been rapidly proliferating in the private sector and provide a model for the application of audit log analysis to IISs. Figure 1 shows a typical IIS, with the collection systems that provide the data, and the intelligence analysts who use it. The green line from the analysts to the collection systems indicates direct feedback from analysts to collectors about information needs and collection requirements. This figure illustrates the intelligence cycle in which analysts review IIS information, refine their information needs and provide feedback to the collectors who adjust their activities accordingly. The information flow focuses on substantive intelligence problems, including plans, intentions, actions and activities of key world political figures and their countries.

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

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

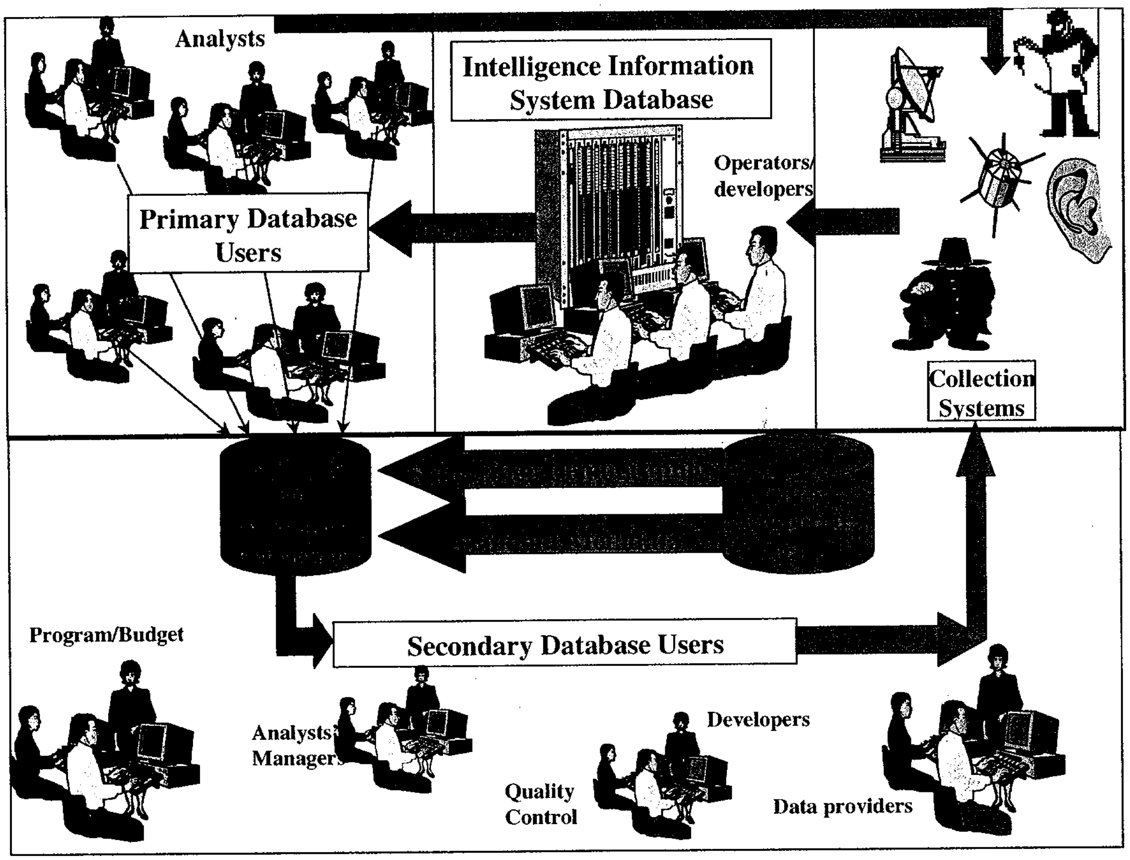
Figure 1: IIS Showing Collectors and Primary Database Users



ATPSs Create High Value Data For Entirely New Customers

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

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



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

[1] Audit log records contain the user name, document identifier, type of user-document transaction and the date/time of the analyst transaction on the document.

[2] Including user office/team, intelligence issue, analytic specialization, grade and years of experience.

[3] Including collection agency, collector type, document originator, publication date, date of receipt by the IIS; classification and document length.

Intelligence Value Metrics Available From ATPS Data

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

Why Audit Log Data Is So Valuable

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

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

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

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

[redacted]

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

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

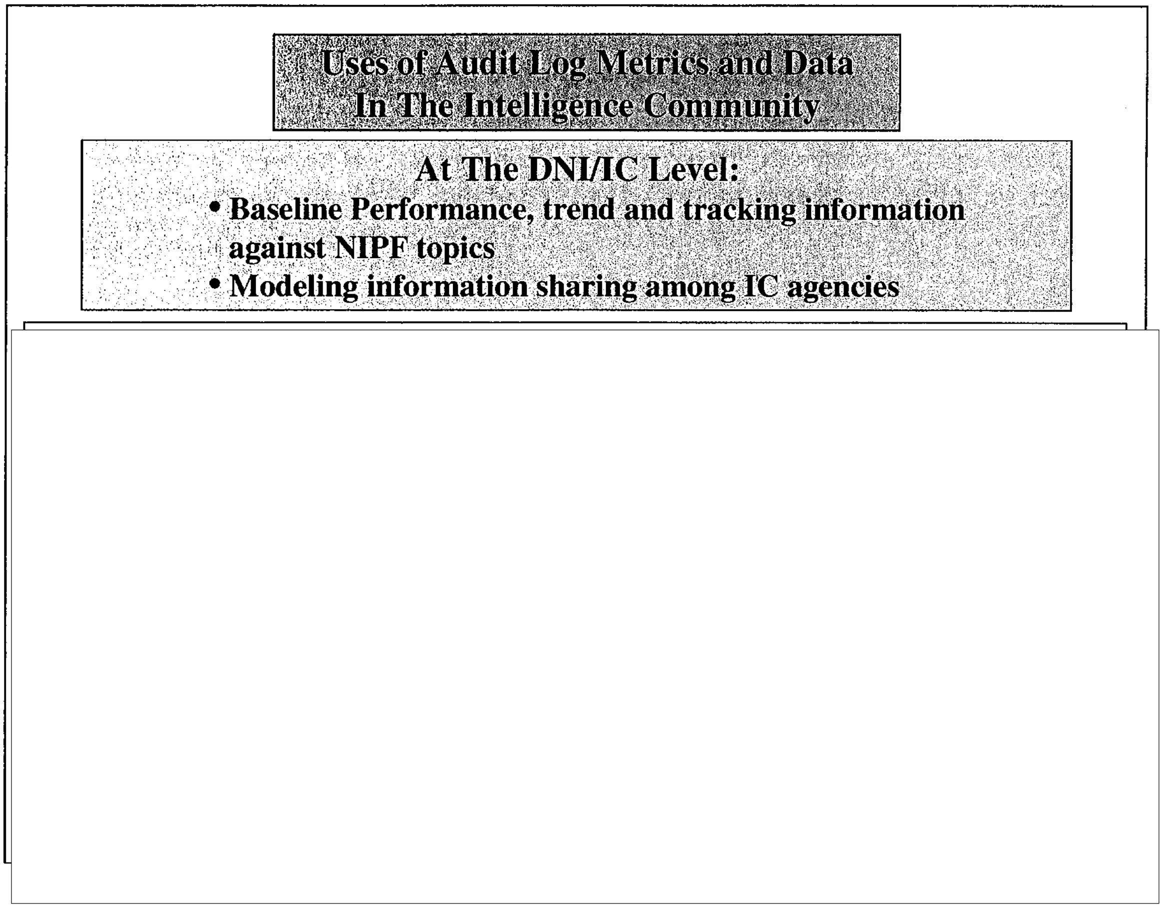
- Which groups of customers are using the IIS and data from specific providers?
- When and for how long are they are using the IIS and each of its intelligence reports?
- What they are using the intelligence reports for?
- Which intelligence reports are most valuable?
- Which intelligence reports have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

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

Uses Of Audit Log Metrics And Data

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

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



Uses of Audit Log Metrics and Data In The Intelligence Community

At The DNI/IC Level:

- Baseline Performance, trend and tracking information against NIPF topics
- Modeling information sharing among IC agencies

[redacted]

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

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

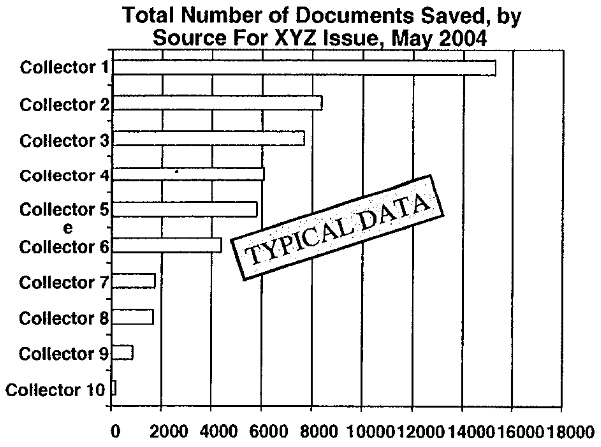


Figure 4: Baseline Example

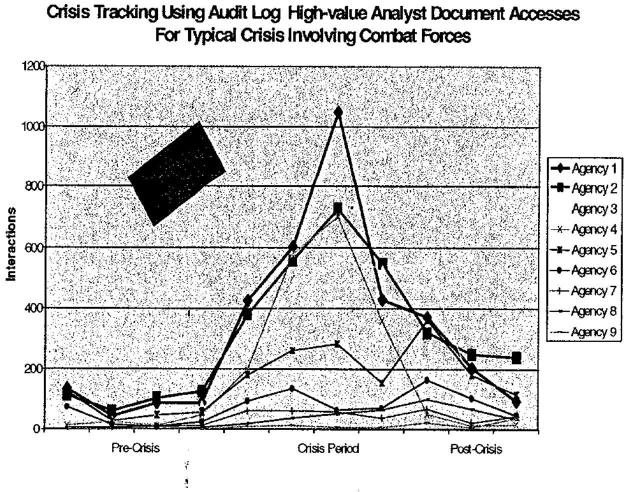


Figure 5: Trend/Tracking

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

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

- **Market research data** characterizing the customer base to database providers in terms of numbers of analysts, their intelligence specialization, issue affiliation and degree of interest in their reporting.

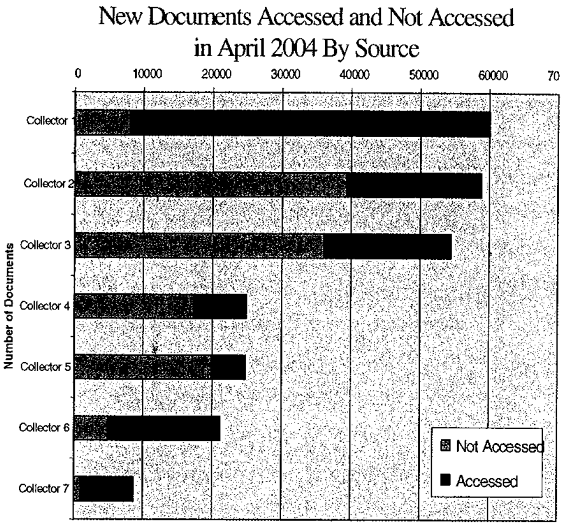


Figure 6 Documents Not Used Analysis

- **Determining which IIS reports are not used** by any analyst. Audit log data permits documents not accessed by any IIS user to be easily identified and called to the attention of the data provider. The percent not used is an important measure of collector performance. (See Figure 6.)
- **Estimating analyst workload** devoted to information search, retrieval and review functions on data in the IIS.
- **Hypothesis Testing:** Audit records can be seen as a vast new source of objective data with which to test hypotheses, myths, conventional wisdom and commonly asked questions about many aspects of the intelligence enterprise. Using appropriate aggregate statistical techniques[5], audit log records can be used for: assessing the relative value of different product lines, the relative importance of different sources, the productivity of different production processes and detecting changes and trends over time. Audit log analysis can provide valuable data to intelligence collectors seeking to assess the impact of their products. For example, are analysts reading their products and, if so, which ones? Does the reporting appear to be of value to the users? This information can be critical to intelligence-production organizations facing serious resource constraints in meeting their responsibilities.
- **Enabling benefit/cost methods:** Perhaps the most important application of audit log data is enabling greater use of benefit-cost methods in IC decision making and investment analysis regarding future collection and processing systems. For example, the value metrics available in audit log data can be combined with incremental cost data to generate a set of "willingness to pay" guidelines for use in evaluating alternative investments in future collection systems, collection architectures and system expansion/improvement alternatives. Audit log metrics can play an important role in anchoring subjective intelligence value judgments elicited in decision conferences for building integrated, cost effective intelligence, surveillance and reconnaissance programs. The abundance of objective intelligence value metrics from audit log data should also facilitate increased use of decision-analysis and operations research methods in the IC.

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

Audit Log Data Security

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

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

[redacted]

[redacted]

Future Applications Of CIA's Audit Log Project

[redacted]

[redacted]

- **Analyst Training**

[redacted]

[redacted]

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

ATPS Potential Applications In The Intelligence Community And Homeland Security

[redacted]

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

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

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

Audit Log Applications For Homeland Security

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

Conclusion

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

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu