RESEARCH PAPER
No. 104

(2006)

"TRADECRAFT VERSUS SCIENCE:"

INTELLIGENCE ANALYSIS AND OUTSOURCING

HAMILTON BEAN

(University of Colorado at Boulder)

RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES (RIEAS)
 # 1, Kalavryton Street, Ano-Kalamaki, Athens, 17456, Greece
RIEAS URL: http://www.rieas.gr

RIEAS MISSION STATEMENT

Objective

The objective of the Research Institute for European and American Studies (RIEAS) is to promote the understanding of international affairs. Special attention is devoted to transatlantic relations, intelligence studies and terrorism, European integration, international security, Balkan and Mediterranean studies, Russian foreign policy as well as policy making on national and international markets.

Activities

The Research Institute for European and American Studies seeks to achieve this objective through research, by publishing its research papers on international politics and intelligence studies, organizing seminars, as well as providing analyses via its web site. The Institute maintains a library and documentation center. RIEAS is an institute with an international focus. Young analysts, journalists, military personnel as well as academicians are frequently invited to give lectures and to take part in seminars. RIEAS maintains regular contact with other major research institutes throughout Europe and the United States and, together with similar institutes in Western Europe, Middle East, Russia and Southeast Asia.

Status

The Research Institute for European and American Studies is a non-profit research institute established under Greek law. RIEAS's budget is generated by membership subscriptions, donations from individuals and foundations, as well as from various research projects. The Institute is autonomous organization. Its activities and views are independent of any public or private bodies, and the Institute is not allied to any political party, denominational group or ideological movement.

John M. Nomikos
Director

RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES (RIEAS)

Postal Address:

1, Kalavryton Street
Ano-Kalamaki
Athens, 17456,
Greece.

Tel/Fax: + 30 210 9911214

E-mail: rieas@otenet.gr

Research Associates

Hamilton Bean, Intelligence Studies

Konstantopoulos Ioannis, Intelligence Studies

Paddy Mck Doherty, Central Asia Studies

Zacharias Michas, Independent Strategic Analyst

Nadim Hasbani, Lebanon-Syria and North Africa Studies

Florian Taux, East Asia Studies

Bjorn Fagersten, European Intelligence Studies

Christian Kaunert, European Union Politics

Aya Burweila, Middle East, Islamic Studies

Maria Alvanou, Terrorism Studies

RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES

(RIEAS)

RESEARCH PAPER
No. 104

(2006)

"TRADECRAFT VERSUS SCIENCE:"

INTELLIGENCE ANALYSIS AND OUTSOURCING

HAMILTON BEAN

(University of Colorado at Boulder)

Abstract

This paper explores contradictory analytical practices and processes within U.S. intelligence agencies and their private sector contractors. Using theories drawn from information processing, communication, and work and organizations, the author suggests that government officials and contractors conceive of intelligence analysis as either "tradecraft," i.e., a non-scientific enterprise, or conversely, an activity amenable to scientific rationalization. The metaphors of "intelligence as tradecraft" versus "intelligence as science" capture this tension and help explain patterns of technological development and organizational change within the U.S. Intelligence Community.

Keywords: Intelligence, Outsourcing, Technology, Tradecraft, Science

‘Tradecraft’ versus ‘Science’:

Intelligence Analysis and Outsourcing

Mistakes surrounding 9/11 and Iraq have led to major structural reforms within the U.S. Intelligence Community. The establishment of the Office of the Director of National Intelligence (DNI) is among the most significant of these reforms. The DNI oversees and coordinates the work of the fifteen agencies that comprise the Intelligence Community. It may come as a surprise to Americans that approximately half of the Intelligence Community’s $44 billion budget is spent on private sector contractors (Shorrock, 2005). This budget is spent on technology, information, surveillance, and management systems, analysts, and support staff among other goods, services, and personnel. It is more accurate to view the Intelligence Community as comprising both agencies and their private sector contractors.

This article provides a preliminary account of intelligence outsourcing in the case of open source intelligence (OSINT). Because it is unclassified, OSINT provides a window into the opaque world of intelligence outsourcing in ways the other intelligence disciplines, i.e., “imagery intelligence” (IMINT) or “human intelligence” (HUMINT), do not. I analyze the drivers of intelligence outsourcing and explain how outsourcing reflects and reinforces technological and organizational changes within the Intelligence Community. These changes can be explained, in part, by two juxtaposed metaphors: “intelligence as tradecraft” versus “intelligence as science.” These metaphors point to differing assumptions about the nature of intelligence and help explain often contradictory practices within intelligence agencies and their contractor organizations. These practices include inconsistent analytical methods across intelligence agencies and contractors, few analytical training programs within the Intelligence Community or private sector,

a focus on short-term issues rather than long-term strategic concerns, and a perpetual attempt to automate intelligence collection and analysis. I observed these practices firsthand while serving from 2001—2005 in management and business development positions for an OSINT contactor supporting the Intelligence Community. The metaphors of "intelligence as tradecraft" versus "intelligence as science" point to an underlying rationale for these conditions.

OSINT and Outsourcing

Intelligence Studies scholars and commentators maintain that OSINT is derived from, or is itself, publicly available information that responds to a stated intelligence requirement (Hulnick, 2002). Identifying the properties of materials used in the construction of buildings in a given country is an example of an intelligence requirement. When U.S. military officials create battle plans, they must know the specifications of facilities in order to determine how to destroy them. OSINT may be an effective source for meeting such an intelligence requirement. An intelligence analyst may be able to determine from public records, archived news reports, and subject matter experts the types of materials likely used during the construction process, when the facilities were built, the contractor that built them, and any number of other important details. OSINT is not only discrete bits of information, it is also the process of converting that information into useful knowledge for decision makers. The process of "doing" OSINT involves identifying relevant, reliable sources and analyzing information in a way that responds effectively to stated requirements. Beyond this simple description of OSINT as a product and process, the definition of the term is contested.[1]

[1] For example, questions circulate about: 1) whether OSINT is a "true" intelligence collection discipline or a foundation for other disciplines; 2) whether OSINT is collected from original sources or "acquired" secondhand information.

The literature concerning OSINT is limited and much of it tends to promote the field (see, e.g., Politi, 2003; Steele 2005). However, some Intelligence Studies scholars have offered a critical assessment. Hulnick (2002) states that OSINT is the "bread and butter" of analysis, but he also cites contingencies including information glut, unreliability, misinformation and disinformation, translation requirements, and the availability of the information to adversaries that limit the utility of OSINT. Similarly, Pringle (2003) states that OSINT represents a double-edge sword for the government analyst; its inherent ambiguity diminishes its usefulness. Lowenthal (1999) highlights how early Intelligence Community attempts to promote the increased use of OSINT failed due to analysts' preferences for classified sources. Mercado (2004, 2005), recognizing that challenge, offers proposals for how to better integrate OSINT into the Intelligence Community. Scholars have examined OSINT in contexts of federal policy initiatives including national competitiveness and the War on Drugs (Clift, 1993; Holden-Rhodes, 1997). Others have approached OSINT as a knowledge management or data mining problem and investigated the capability of new technologies to make sense of large data sets (Carroll, 2005). Sands (2005) states that the Intelligence Community must recognize that it competes for policymakers' attention with non-governmental sources of OSINT. Like most commentators, Sands argues that in order to take advantage of OSINT, the Intelligence Community must devote more human and technical resources to its exploitation.

Outsourcing OSINT

According to Lahneman (2003), outsourcing within the Intelligence Community "refers to the practice of…turning over entire business functions to an outside vendor that ostensibly can perform the specialized tasks in question better and less expensively than [the Intelligence Community] can" (p. 573). In the case of OSINT, a company takes over day-to-day

responsibility for collecting, analyzing (and perhaps disseminating) OSINT on behalf of a government agency. These services are often provided through a combination of specialized analysts and sophisticated technologies. The decision to outsource is based on the assumption that an agency does not possess equivalent resources. Officials may assume that an OSINT contractor can provide services more cost-effectively than were the agency to try to re-create the contractor's analytical or technological capabilities in-house. A typical contract for OSINT outsourcing lasts one year and is renewable based on performance. As Lahneman states: "[Outsourcing] agreements in business are usually long-term, with an average term of seven to ten years. Assessment of outsource firm performance is not through the measurement of individual tasks, as might be the case with [on-site] contractor personnel, but through compliance with some type of service level agreement (p. 576).

There are few statistics available regarding the level of outsourcing in the OSINT arena. Mercado (2005) and Steele (2005) suggest that less than one percent of the U.S. intelligence budget goes toward OSINT exploitation within the agencies. Nevertheless, there are dozens of North American and European private sector OSINT providers claiming to support U.S. government clients. Quarterback Consulting provides an overview of the larger private intelligence market in their *Private Intelligence Industry Report* (2003), and depending on how OSINT is defined, the multimillion-dollar industry employs thousands of analysts and marketers worldwide. Representative companies include, but are not limited to: Open Source Solutions; Open Source Publishing, Inc.; The Economist Intelligence Unit; Intelligence Online, Jane's Information Group; Eurasia Group; Stratfor; Oxford Analytica; East View Information Services; Booz Allen Hamilton; Kroll Inc.; Pinkerton Consulting; iJET Travel Intelligence, Inc.; Medley Global Advisors; and Toffler Associates Inc.

The U.S. government recognizes that it must promote a vision of OSINT's use in new ways if it is to succeed in integrating OSINT into intelligence practices and processes (Mercado, 2004; 2005). That is one reason why the DNI recently created the position of Assistant Deputy Director of National Intelligence for Open Source (ADDNI/OS). Eliot Jardines, who currently holds that position, is a former OSINT contractor. Jardines's task is to champion the benefits of OSINT and encourage its increased use throughout the Intelligence Community. One of the issues that Jardines confronts is that members of intelligence agencies and private sector contractors may implicitly conceive of intelligence analysis as either a non-scientific enterprise, or conversely, one amenable to scientific rationalization. The metaphors of "intelligence as tradecraft" versus "intelligence as science" capture that dynamic and help explain intelligence practices in the case of OSINT outsourcing.

Intelligence as Tradecraft versus Intelligence as Science

Intelligence as Tradecraft

The word "tradecraft" evokes images of a meticulous craftsman or a skilled, idiosyncratic artisan. Tradecraft also implies that "secret" techniques are handed down from one generation to the next – wise masters instruct new initiates in time-tested methods. Tradecraft is a term intelligence analysts themselves use to define their work and identity. In his ethnography of analytical culture within the Intelligence Community, Johnston (2005) notes the widespread use of the term among the hundreds of analysts he interviewed and observed. In using "tradecraft" to describe their work, analysts reproduce their beliefs about the exclusivity and non-scientific nature of their analysis. As one government analyst stated, "What we do is more art and experience than anything else" (Johnston, 2005, p. 20).

Some officials and policymakers assume that private sector analysts are even wiser and more skilled than their government counterparts. During a recent congressional hearing on the effective use of OSINT, Homeland Security Committee Chairman, Christopher Cox (R-CA), stated, "It would in fact be a real stretch to suggest that…[the] U.S. government could even compete with private sector expertise and outside sources in terms of either quality or currency" (*Using Open Source*, 2005). Multiple congressional and presidential commissions have called for the increased use of private sector expertise in meeting intelligence requirements (9/11 Commission, 2004; Commission on Intelligence, 2005), and "culturally sanctioned suspicions" about government's ability to compete with the private sector permeate the discourse surrounding intelligence reform (Conrad, 2004).

Although tradecraft is a term that applies equally to agency and contractor analysts, Johnston (2005) demonstrates that tradecraft corresponds more to analysts' self-perception and professional identity than to the reality of their work. He states, "The notion that intelligence operations involve tradecraft, which I define as practiced skill in a trade or art, may be appropriate, but the analytic community's adoption of the concept to describe analysis and analytic methods is not" (p. 17). Instead of exploring tradecraft as a useful metaphor for intelligence analysis, Johnston rejects the term:

> As long as intelligence analysis continues to be tradecraft, it will remain a mystery. The quality of any tradecraft depends on the innate cognitive capabilities of the individual and the good fortune one has in finding a mentor who has discovered, through many years of trial and error, unique methods that seem to be effective…. there [are], in fact, general methods that could be formalized and…this process would then lead to the development of intelligence analysis as a scientific discipline (p. 20).

Intelligence as Science

Johnston moves beyond a call for improved systemization and control; instead he proposes a scientific approach to intelligence analysis. A key consideration becomes to what extent intelligence analysis is amenable to scientific disciplining. Johnston states:

> [Scientific] steps include: observation and description of phenomena; formulation of hypotheses to explain phenomena; testing of hypotheses by independent experts; refutation or confirmation of hypotheses. These steps do not suggest that any specific scientific methodology results in what is ultimately the truth, rather that scientific methods are merely formal processes used to describe phenomena, make predictions, and determine which hypothesis best explains those phenomena. The principal value of any type of methodological formalism is that it allows other researchers to test the validity and reliability of the findings of any other researcher by making explicit, and therefore replicable, the means by which anyone reaches a specific conclusion (2005, p. 19).

Johnston's view of scientific method as "merely formal processes" risks minimizing two issues. First, a scientific approach risks asserting that human relations are a priori and objective. That assertion may reify taken-for-granted assumptions surrounding the constitution of knowledge. Some scholars question the premise that phenomena can be perceived independently from theory, values, or terminology (Lindlof & Taylor, 2002). Second, a question becomes whether an "infrastructure" based on scientific management is necessary to accommodate scientific approaches to intelligence analysis. I explore the latter issue below.

Does a Scientific Approach to OSINT Analysis Require Scientific Management?

"Scientific management" is associated with Frederick Winslow Taylor's management approach developed in the early 20th Century (Taylor, 2003). "Taylorism" was primarily

concerned with how to overcome the intentional restriction of worker output, i.e., “rate cutting.” Taylor sought to use scientific methods to enable management to control workers’ technique and pace in order to circumvent rate cutting. Taylorism relied on time and motion studies to discover the one best way to perform a given task.

The analytical ranks of OSINT contractors display some Taylorist principles. Analysts at one company are paid individual incentive wages as a way to promote output and avoid rate cutting. Management has established strict formats, timetables, and minimum word counts for deliverables. There is pressure among analysts to not exceed word count standards for fear that the standards will be raised. Production processes for OSINT deliverables are organized along factory lines; often analysts are given narrow, repetitive tasks to complete without understanding the wider context of their work. In other ways, OSINT contractors’ analytical processes do not resemble Taylorism. Taylorism is primarily concerned with laboring bodies; analytical tasks are more cognitive. Johnston’s call for a science of intelligence analysis as a replacement for tradecraft may not require an “infrastructure” based on Taylorist management principles. Johnston is not advocating that managers in the Intelligence Community determine the one best way for arriving at an analytical judgment. However, there may be an intuitive sense among analysts that overt attempts to “scientize” their work threatens their spontaneity and ability. They may object to the potential “de-skilling” or “re-skilling” that a scientific approach requires. As Johnston explains:

> The idea that intelligence analysis is a collection of scientific methods encounters some resistance in the Intelligence Community. The interview data analyzed in this study highlight many subtle-and not so subtle-prejudices that analysis is not a science. That is,

> it is an art or craft in which one can attain skill but not a formal discipline with tested and validated methodology (2005, pp. 19–20).

The future implications of attempting to create a science of intelligence analysis are unclear. However, it is certain that if the Intelligence Community moves toward scientific practices, their private sector contractors will necessarily follow suit in order to align processes and products. Johnston (2005) views his recommendations as ultimately empowering analysts. However, his conclusion that "intelligence analysis needs its own analytic heuristics that are designed, developed, and tested by professional analytic methodologists" (p. 73) is somewhat disconcerting. One has to wonder just how different Johnston's intelligence methodologists and Taylor's time and motion specialists really would be.

To be an intelligence "craftsman" implies that analysts themselves shape knowledge, execution, and control over the analytical process. While intelligence as tradecraft may, as Johnston suggests, be fraught with idiosyncrasies, it also promotes novelty – a quality necessary for innovative intelligence assessments (Slack & Wise, 2005). Johnston's assertion that analytical tradecraft is problematic while scientific analysis is ideal demonstrates the familiar pattern of attempting to control organizational processes through improved systematization in the face of ambiguity. In any large organization there is a risk that talented people will be difficult or impossible to hire. If there were an abundant supply of extremely talented analysts within the Intelligence Community, then perhaps Johnston's conclusion would be different. But in government, the problem of hiring and retaining "good people" is ever-present. Intelligence outsourcing only compounds the problem of hiring talented analysts because top performers tend to find better pay and work conditions in the private sector (Harris, 2005). Under conditions of uneven and uncertain analytical capabilities, minimal standards of efficiency and effectiveness

must be met within the agencies. Johnston's call for a scientific approach is a predictable step in an effort to achieve such standards.

From "Intelligence as Science" to "Intelligence as Technology"

"Scientizing" intelligence analysis is a step on the path to making it amenable to electronic processing. Transforming idiosyncratic tradecraft into a function performed by a computer has been underway across the Intelligence Community for many years (Lowenthal, 2006). Contractors are leading the way with new technologies "using open source information to experiment with software that has not yet been certified for classified environments" (Commission on Intelligence, 2005, Chapter 8).

> The Intelligence Community has only begun to explore and exploit the power of these emerging technologies. The Intelligence Community's current efforts should be coordinated, consolidated where appropriate, directed, and augmented. Therefore, we suggest that the DNI establish a program office that can lead the Community effort to obtain advanced information technology for purposes of machine translation, advanced search, knowledge extraction, and similar automated support to analysis (Commission on Intelligence, 2005, Chapter 8).

The metaphor "intelligence as technology" captures intelligence practices, processes, and initiatives that tilt toward automation. It is not my intent to assert the old opposition of "man versus machine," yet Zuboff (1988) sensitizes us to the fine distinctions between the phrase "automated support to" and the term "automation" that hold profound implications for the nature of intelligence work and identity. Zuboff defines "intellective skills" as abstraction, explicit inference, and procedural reasoning. She notes many examples of office and manufacturing technologies ostensibly created to *support* intellective skill but instead degrade those skills.

Technologies based on linguistic pattern recognition algorithms similarly hold the potential to enhance or degrade the intellective skills of intelligence analysts. Such technologies have been used in English-language environments to search for patterns within and between texts for many years, but a review of the United States Patent and Trademark Office database reveals that 9/11 spurred development of these technologies for foreign languages. These technologies search for linguistic patterns from electronic newspapers, magazines, websites, and other unstructured documents.

The development of these types of technologies raises two important questions in the context of this article. First, can these technologies provide accurate and consistent intelligence? Second, *should* analysts rely on these technologies? Serious issues remain in regards to the first question. For example, data reliability is a major concern. As Hulnick (2002) points out, the reliability of OSINT is notoriously problematic. A related problem is "herding." Garicano and Posner (2005, p. 155) note that intelligence analysts tend to focus on the same limited information when drawing conclusions:

> The stages by which a particular piece of information moves from its origin to the point at which it is combined with other information for purposes of analysis are often unknown to the analyst. Yet they are the key to the reliability of the information. [W]ithout knowledge of the structure of the network through which the intelligence has flowed, it is impossible to know how independent those confirmatory pieces of evidence really are.

Herding is no less a problem in the global media system than in the intelligence arena. Since it may be unclear whether a report in a local newspaper is original or is itself the product of

herding, the reliability of that data may be in doubt. Therefore, we should be wary of assertions about the precision of pattern-recognition technology.

Should analysts rely on these technologies? The answer depends on whether the technology enhances or degrades development of intellective skills such as abstraction, explicit inference, and procedural reasoning. The question is even more difficult to answer when considering that technologies alone cannot stimulate intellective skill development. The way in which technology is deployed and the organizational environment in which technology is embedded are critical to whether analysts will be able to use technology to add value (Zuboff, 1988). It is easy to imagine a case where analysts are given software without proper training and understanding of the assumptions upon which the software's algorithms are built. Organizations trying to control costs may find it economical to pay a junior analyst to monitor the software. Junior analysts may not possess the capability to "interrogate" the technology to check hunches or pursue alternative analytical paths. In that scenario, the analyst becomes more of a "functionary of the text" rather than its master (Zuboff, 1988, p. 182). Especially in a national security context where intellective skills are critical, automated processes that degrade analysts' know-how and abstraction, explicit inference, and procedural reasoning capabilities should be avoided.

Instead of using advanced search and knowledge extraction technologies to create connections, spur creativity, and add value to intelligence assessments, analysts may instead find themselves using these tools to simply keep pace with the unrelenting demands of their job. The pressure to meet strict deadlines for multiple clients required analysts to keep a close eye on the clock and avoid analytical detours and dead ends. It will never be known how many underdeveloped but potentially novel assessments are jettisoned at the expense of client

deadlines. It is simply too time-consuming to explore lines of reasoning that cannot be quickly edited and included in the day's production in order to make an explicit quota. These tensions suggest that extreme forms of systematization in order to meet deadlines may diminish analysts' commitment to excellence.

My observations correspond to Johnston (2005) finding that the vast majority of agency analysts have shifted their focus to "current production," i.e., short-term issues and problem solving. This has resulted in analysts re-conceptualizing the nature of their work. As one analyst in Johnston's study put it, "Everything I do is reactive. I don't have time to work my subject. We're not pro-active here" (2005, p. 13). Another analyst stated, "You know, somebody someday is bound to notice that velocity isn't a substitute for quality. We've gotten rid of the real analytic products we used to make, and now we just report on current events" (p. 16).

Analytical technologies hold the promise of easing the monotonous grind of current reporting. With technologies to do the grunt work of translation, web search, pattern recognition, and "knowledge extraction," analysts may be able to devote more time to strategic assessments, which few doubt are necessary for long-term foreign policy and national security planning. To date, new technologies have not fundamentally changed the culture of "tradecraft" within the Intelligence Community. In the future, the increasing number of technologies doing tasks now performed by analysts will necessitate changes in the culture of intelligence agencies as Johnston and others recognize. These technologies signal a challenge to traditional practices and processes. Zuboff's analysis provides clues for policy makers and officials for where to anticipate friction points as the Intelligence Community and its contractors move further toward automated processes.

Intelligence as Tradecraft versus Science in the Context of OSINT Outsourcing

The tension between intelligence analysis as tradecraft versus science takes on greater significance within the private sector than within intelligence agencies for two inter-related reasons. First, market pressures often require contractor organizations to adopt low-cost approaches to collection and analysis. These low-cost approaches mimic automation to the detriment of analysts and their deliverables. Second, since agencies are unable to monitor outsourced work processes, they exert control through contract requirements that compel organizations to adopt automation-like processes.

The economic realities of the private sector force a tradeoff between low-cost tradecraft and high-cost technology. This dichotomy seems counterintuitive – human labor is usually perceived as high cost. This is not necessarily the case in the OSINT domain. It is ironic that in manufacturing industries tradecraft generally signifies quality whereas "machine made" implies shoddiness. Johnston's (2005) findings suggest that in the Intelligence Community the connotations are reversed; tradecraft produces idiosyncratic errors and flawed reasoning whereas technology produces scientific accuracy and quality. Many of the technologies discussed herein are expensive. A site license for a "deep-web" exploitation tool may start at $100,000 per year. Especially in Washington, DC, where Masters and Ph.D.-level analysts are abundant, contractors may find it more economical to hire analysts to mimic automated processes rather than invest in technology that may soon be obsolete.

This tension explains why one organization—now defunct—routinely assessed new technological tools for its analysts as a way to improve quality but ultimately declined to purchase them. The potential benefits did not outweigh the cost savings of continuing to rely on "cheap" analytical labor and free or low-cost search technologies such as Google, Factiva, and

others. Management justified these decisions based on the premise that the company's value-added was not its technology, but rather the "analytical overlay" it provided to clients.

Agencies are unable to monitor contractor work processes; therefore they exert control through requirements that oblige contractors to adopt automation-like processes. It is difficult for the government to determine how a contractor rendered a particular analytical judgment. Whereas government analysts hold to a perceived tradecraft, private sector analysts are free to expand the boundaries of what constitutes intelligence. In the private sector it is often acceptable for an analyst to make analytical judgments without explicit references to source materials; a commercial client (such as an international bank) cares primarily whether judgments are accurate. When OSINT contractors offer government clients analytical judgments without explicit references to source materials it often creates considerable tension. This tension is due to the forced tradeoff between "information quality" versus "information efficiency" (DeLone & McLean, 2003; English, 2005). When an agency contracts with a private sector OSINT provider, the agency's primary goal is achieving a high level of information quality. Information quality for the government means assessments based on the contractor's unique, specialized knowledge and expertise. But quality also means source traceability and accountability because no government official wants to be put in the position of having to back assertions without sources and reasoning. Private sector OSINT providers are also concerned with information efficiency. The pressure to meet strict deadlines for multiple clients requires contractors to rely on their analysts' professional judgments; source traceability is often of less concern. It is simply too time-consuming within this product cycle to cite and organize the source material that influenced an analyst's particular judgment. Private sector OSINT providers are, of course, concerned with

information quality, but quality is often oriented to satisfying clients that do not require detailed sourcing.

Conclusion

Information processing speed and access to communication technology creates an environment where intelligence analysts have vastly more information more quickly than ever before. Such conditions should be a boon for analysts, but instead, those conditions create pressures to produce insights at a much faster rate to satisfy intelligence consumers. For Johnston (2005), this is the critical problem facing the Intelligence Community since it leaves little time for strategic assessments. Outsourcing intelligence does not solve the problem. The pace of production merely compels private sector organizations to mimic the agencies they support. Taken to extremes, time pressures force organizations to create assembly line processes to ensure minimum standards of quality and quantity. In a saturated global media environment, information glut rises to excessive levels where technologies are seen as the only viable way to achieve control over the initial steps of separating the “wheat from the chaff” in the analytical process.

In an organizational environment where intellective skill development is promoted, technologies help collect and analyze massive streams of information in order to “pre-process” it for analysts. In a poorly automated organizational environment, technology separates knowledge from analysts and degrades their intellective skills. Some OSINT contractors may be tempted to created work processes to mimic automation and control provided by technology where it is absent. These automating strategies can create numbing work conditions and generally diminished the ability of analysts to conduct useful intelligence collection or analysis for their clients. Paradoxically, when management introduces new technologies that hold the potential to

enhance intellective skill development, it may create anxiety among analysts who resist viewing their work in “scientific” terms.

Some of what I have recounted here should trouble stakeholders who promote intelligence outsourcing as an answer to many of our intelligence problems. Intelligence practitioners may conceive of intelligence as either tradecraft or science, and as either amenable to outsourcing or not. What matters most is whether any position results in intelligence that meets national security objectives and protects lives. The Intelligence Community is a complex system, and it may be impossible to predict how outsourcing OSINT will ultimately impact the larger whole. However, one thing is certain: the Intelligence Community will require ever new technologies, communication strategies, and managerial approaches in efforts to mitigate a perpetual “crisis of control” (Beniger, 1986) inherent in a complex intelligence system.

References

9-11 Commission. (2004). *Final report of the national commission on terrorist attacks upon the United States*. Available from http://www.9-11commission.gov/.

Beniger, J. R. (1986). *The control revolution: Technological and economic origins of the information society*. Cambridge: Harvard University Press.

Braverman, H. (2003). The degradation of work in the twentieth century. In H. J. Handel (Ed.), *The sociology of organizations: Classic, contemporary, and critical readings* (pp. 32-38). Thousand Oaks, CA: Sage Publications. (Original work published 1974)

Carroll, J. M. (2005). OSINT analysis using adaptive resonance theory for counterterrorism warnings. *Artificial Intelligence and Applications 2005*, 756-760.

Chesebro, J. W. & Bertelsen, D. (1999). *Analyzing media: Computer technologies as symbolic and cognitive systems*. New York: Guilford Publications, Inc.

Clift, D. A. (1993). National security and national competitiveness: Open source solutions. *American Intelligence Journal, 14*(2), 25-28.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. (2005). Available from http://www.wmd.gov/report.

Conrad, C. (2004). The illusion of reform: Corporate discourse and agenda denial in the 2002 'corporate meltdown.' *Rhetoric & Public Affairs, 7*(3), 311-338.

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems, 19*(4), 9-30.

English, L. P. (2005). Information quality: Critical ingredient for national security. *Journal of*

Database Management, 16(1), 18-33.

Garicano, L., & Posner, R. (2005). Intelligence reform since 9/11: An organizational economics perspective. *Journal of Economic Perspectives, 19*(4), 151-170.

Harris, S. (2005, May 15). Intelligence incorporated. *Government Executive Magazine 37(8),* 40-47.

Holden-Rhodes, J. F. (1997). *Sharing the secrets: open source intelligence and the war on drugs.* Westport, CT: Praeger.

Hulnick, A. S. (2002). The downside of open source intelligence. *International Journal of Intelligence and CounterIntelligence, 15,* 565-579.

Johnson, L. K. (2006). A shock theory of congressional accountability over America's intelligence agencies. Paper presented as part of the panel "Intelligence Community Reform, One Year After" at the annual meeting of the International Studies Association, San Diego, CA, 22-25 March 2006.

Johnston, R. (2005). *Analytical culture in the U.S. intelligence community: An ethnographic study.* Washington, DC: Center for the Study of Intelligence.

Lahneman, W. J. (2003). Outsourcing the IC's stovepipes. *International Journal of Intelligence and CounterIntelligence, 16,* 573-593.

Lindlof, T., & Taylor, B.C. (2002). *Qualitative research methods* (2nd ed.). Thousand Oaks, CA: Sage.

Lowenthal, M. (1999). Open source intelligence: New myths, new realities. *Intelligencer, 10*(1), 7-9.

McGill, G. M. (1994). OSCINT and the private information sector. *International Journal of Intelligence and CounterIntelligence, 7,* 435-443.

Mercado, S. C. (2004). Sailing the sea of OSINT in the information age. *Studies in Intelligence, 48*(3). Available from http://www.cia.gov/csi/studies/.

Mercado, S. C. (2005). Reexamining the distinction between open information and secrets. *Studies in Intelligence*, *49*(2). Available from http://www.cia.gov/csi/studies/.

OSINT History 1988-1995, 2006 Update. (2006). Retrieved April 28, 2006 from www.oss.net.

Pincus, W. (2006, May 7). Lawmakers want more data on contracting out intelligence. *Washington Post*, A07.

Politi, A. (2003). The citizen as 'intelligence minuteman.' *International Journal of Intelligence and CounterIntelligence*, *16*, 34-38.

Pringle, R. W. (2003). The limits of OSINT: Diagnosing the Soviet media, 1985-1989. *International Journal of Intelligence and CounterIntelligence*, *16*, 280-289.

Quarterback Consulting. (2003, January). *The private intelligence industry report*. Cheshire, CT.

Sands, A. (2005). Integrating open sources into transnational threat assessments. In *Transforming U.S. intelligence*, J. E. Sims & G. Burton Gerber, Eds. Washington, DC: Georgetown University Press, 2005, 63-78.

Shorrock, T. (2005). The spy who billed me. *Mother Jones*, January/February [online edition].

Slack, J. D., & Wise, J. M. (2005). *Culture + technology: A primer*. New York, NY: Peter Lang Publishing, Inc.

Steele, R. D. (2005). Portal: open source agency. Retrieved Nov. 09, 2005, from the World Wide Web http://www.oss.net/extra/news/?module_instance=1&id=2573.

Taylor, F. W. (2003). The principles of scientific management. In H. J. Handel (Ed.), *The sociology of organizations: Classic, contemporary, and critical readings* (pp. 24-31). Thousand Oaks, CA: Sage Publications, pp. 17-23. (Original work published 1911)

Using open-source information effectively: Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security, House of Representatives, 109th Cong. (2005).

Webster, F. (1995). *Theories of the information society*. New York: Routledge.

Yates, J. (1989). *Control through communication: The rise of system in American management*. Baltimore, MD: The Johns Hopkins University Press.

Zuboff, S. (1988). *In the age of the smart machine: The future of work and power*. New York, NY: Basic Books.