Watchin' the Analysts

Ross Stapleton-Gray, Ph.D., CISSP
Stapleton-Gray & Associates, Inc.
P.O. Box 7615
Berkeley, CA, 94707, USA
ross@stapleton-gray.com

Keywords: Information Sharing and Collaboration, Knowledge Discovery and Dissemination, Social Analysis

Abstract

The intelligence analyst communities ought to be themselves more thoroughly analyzed, through tools for surveillance. A variety of tools and technologies might be applied to examine analysts, individually, in collaboration, and in their transactions with the "outside world," to better understand capabilities, to identify issues spanning numerous individuals (who may be individually unaware of them), and to more coherently interact with outside parties. Such surveillance clearly raises privacy issues; policies and practices that achieve the benefit of more closely examining the analytic life while avoiding undue invasion of privacy ought to be pursued.

1. Introduction

"Gentlemen do not read each other's mail."

- Secretary of State Henry Stimson; rationale for dismantling U.S. government cryptographic capability, 1929

"You can observe a lot just by watchin'."

- Yogi Berra

Intelligence analysts bear more watchin'. Stimson's famous quote referred to eavesdropping on one's adversaries; the rejection of that premise is the spirit of modern intelligence. But there are valid reasons to look over one's friends' shoulders, too. Intelligence agencies have a responsibility, interest and need in doing so. Analysts, like any other employees, like any other humans, will resent some aspects of such monitoring. But some balance of respecting human needs and nature, while gaining the benefits of a better view of both the "forest" and the "trees," should be sought.

Some basic monitoring could unquestionably be justified as precautionary: another Aldrich Ames, Robert Hanssen, or Ana Montes could be just as crippling as they were, betraying valuable sources, and tainting untold man-years of intelligence collection and analysis (Maybury *et al.* 2004). But better, smarter oversight could also provide valuable insights to management, giving a much better, overarching view of the nature of our intelligence, and its implications. And such monitoring could assist the analysts themselves in doing their work, more efficiently and effectively.

By monitoring I do not necessarily mean capturing every keystroke, mapping out detailed graphs of analysts' contacts and communications, or parsing through all inbound and outbound traffic for clues to malicious action or intent. (But that's not to say any of those couldn't have value.) By monitoring I mean becoming more aware of macro-level organizational behavior, of the interaction between analysts, and of the assets possessed by each analyst, and their own networks of contacts and colleagues.

I served six years at the Central Intelligence Agency and Intelligence Community Management Staff (1988-94); my comments below are most informed by my experience in the CIA Directorate of Intelligence and a decade since in commercial ventures, an industry trade association and academia, but ought to be relevant throughout the Intelligence Community, in its analytic communities. The discussion below cites a variety "real world" tools for collection and analysis of transactional information, some of which may already have found applications within the IC, but all of which might prove useful in the roles described.

When such monitoring is done, it ought to be done right. The challenge would be to implement what is effectively surveillance, in a manner to promote some necessary degree of trust.

2. The Analyst as Asset

Analysts are known formally by their organizations through two primary means: by their production (published and planned), and by their organizational billet. Analysts are the authors of finished intelligence ("FININTEL"); some (but not all) analyses will be attributed to their authors. And analysts can be found by tracing down hierarchies, e.g., inferring that the China military analyst might most likely be found in the China branch in the East Asian division of the office that covers Asia.

But analysts aren't confined to narrow disciplines, and will be authorities on a great many things worth knowing, outside of their defined roles. In addition to formal expressions of knowledge, one might gain a better understanding of what analysts themselves care about—to know them by their interests, skills and expertise. This oughtn't to be through the "fill in the questionnaire annually" sort of survey; all manner of agency information systems ought to be integrated to share and correlate information about employees, as strategic assets.

As noted in a recent *Studies in Intelligence* article (Medina 2002), it's hardly a new idea to imagine stepping outside the rigid FININTEL box: "In 1996, for example, in a submission to an in-house electronic discussion database, [Carol Dumaine] noted that the future intelligence officer would 'produce unfinished intelligence—all of it on line, interactive, iterative, multidimensional, an interdisciplinary fabric of specialist contributions, and available 24 hours a day to trusted consumers.'" (All of which sounds an awful lot like what we now know as blogging. I suspect that Dumaine's vision, if it's realized within the IC, will arrive as commercial blogging software is blessed as acceptable COTS, and the agencies adopt it so as not to lag even further behind the outside world.)

Beyond knowing analysts' work in progress, one could also back it up further, and analyze their queries as well. Google's "zeitgeist" feature displays its millions of users' aggregate interests (http://www.google.com/press/zeitgeist.html)… one could imagine deriving intelligence from "forest-level views" of the analyst "trees" through the questions they think to ask, anticipating some major issues even as they only slowly emerge in bits and pieces among individual analysts.

3. The Analyst in Collaboration

Analysts interact among themselves, as a complex community web of knowledge. Analysis of those sorts of networks would be worthwhile, and is being done in the commercial sector, through a variety of tools.

In the fall of 2000, the CIA shut down a so-called "chat room" operating unofficially over Agency networks; four employees lost their jobs, with other employees and contractors given reprimands (Loeb 2000, Loeb 2000a). I had left the Agency in 1994, but numerous of those involved were friends and former colleagues. My impression was that what occurred was more embarrassing than threatening, and that agency management ought to understand how and why such virtual communities form—whether they're facilitated or frustrated by the "official" infrastructure—and appreciate their value. Various network visualization tools would have readily revealed anomalous (at least as far as official business was concerned) traffic, but analysts will want and need an environment that fosters creativity and community, and ought to be given one.

On a more positive aspect of monitoring, the Netscan project being pursued at Microsoft Research constructs "detailed reports on the activity of Usenet newsgroups, the authors who participate in them, and the conversation threads that emerge from their activity." All of the inferences made on conversational activity are derived solely from "envelope" information, e.g., posting header data, and not message content. One application of the project is to enhance Microsoft's management of customer service: observation of posting patterns, even absent looking at the content, reveals those individuals whose contributions to online discussions tend to pull things to useful conclusions, or who elicit participation by others.

One could look to other areas of analysis, e.g., legal discovery, for clues as well. I am an advisor to Cataphora, whose C-Evidence tool is used to plow through a company's file systems, and knit together a narrative about who corresponded on what, with whom, and when, highlighting patterns of corporate communication. Its current market is litigation support, but its tools might be as applicable to better visualizing the interactions within an analytic community.

Some degree of "monitoring" might also come from merely affording new means to express and share interests and perceptions. A variety of Web-based tools allow collaborative sharing across the Internet; any might prove valuable within the closed, classified environments of the IC. As one example, Del.icio.us (http://www.del.icio.us) is a "social bookmarks manager," which allows for a shared structuring of metadata—information about how the Web is perceived by a community.

Again, the "blog" approach to a more ready, collaborative, and networked sharing bears examination. It not only forces more semi-finished thoughts out into a more interactive forum, but facilitates citations and cross-linking. There is something of a validation in the marketplace of ideas.

The DARPA "futures market," a public relations disaster when news of it broke in the popular press, and it was summarily terminated, might also have been a valuable strategy for greater elicitation. Encouraging analysts to test their theories within a common framework would promote greater interaction, an interaction that can then be more readily monitored and assessed.

4. The Analyst as a Node in Many Networks

As much as intelligence analysts work within a "secure bubble," they also communicate electronically with outsiders, e.g., in unclassified conversations with academic or business colleagues. The *modus operandi*, in the absence of effective and widely-deployed multi-level secure systems, is that these logically separate worlds are often structured as air-gapped, physically separated ones. In a gesture to efficiency, there may be a means to pipe information from outside systems, and in particular the Internet, into agency-internal networks.

Here is perhaps the most obvious place for monitoring, with a critical concern that sensitive information not pass out from the IC, to inappropriate parties. A similar concern is shared by an increasing number of organizations in the private sector, certainly for competitive reasons, but also because of recent regulatory impositions, e.g., in the financial sector (Gramm-Leach-Bliley), health care (HIPAA) and corporate governance more generally (Sarbanes-Oxley). As a result, a range of commercial tools (Vontu Protect, Tablus Content Alarm) is available to target the organizational perimeter as a security concern.

More intriguing, on the "positive" side of monitoring, might be tools aimed at *facilitating* better communication with external parties, e.g., tools for what commerce terms customer relations management (CRM). Twingle, an e-mail monitoring and analysis tool, was pitched by its developer as a means to pull together collaboration regarding outside parties of common concern. In any organization some number of people who may or may not know each other will have contact with members of other organizations; those contactees similarly may or may not work with or be otherwise aware of each other. Learning of their common interests, one could bring together parties to collaborate on exploiting external contacts.

If the analyst is an asset, one should also consider them as "assets ever after." University development offices invest considerable effort in tracking and exploiting alumni—they're continued sources of endowment-building revenue. (If my personal experience is any guide, the only reliable authority on ex-CIA employees' whereabouts is the Thrift Savings Plan!) Agencies might direct more attention to being aware of their "alums," for potential mutual future benefit.

5. Balancing Competing Concerns: "Need to Know," Security and Privacy

The challenge of management of sensitive information is often dodged, through an over-reliance on an "us/them" partitioning of the world, granting no access to outsiders, but far too much to insiders. That "M&M" model for security—a hard outer shell, but an all too soft inside—makes any sort of nuance in access management difficult, e.g., in opening up one agency's classified systems to another's employees. (It also heightens the need to surveil one's friends, for the more unfortunate reasons.)

And likewise, while I've advocated broadening interaction between analysts, there are some necessary steps to take to enforce some "need to know" constraints, and sufficiently protect sources and methods. Use of techniques for semi-blinded communications might be appropriate, e.g., to introduce analysts to one another through a process of gradual revealing expertise and interests. Some guidance might also be taken by social networking sites like LinkedIn: while they do not need to ensure protection of classified knowledge, they're entrusted with other quite valuable resources, their members' time and privacy, and have established protocols for trusted introductions.

Overall, though, we ought to keep in mind that "need to know" is actually a two-sided coin: while it is most commonly encountered in the negative—"You have no need to know"—it is equally an admonition to inform: "You have need to know this." A primary premise of this piece is that the IC has a need to know more than it does about the state, interests and potential of its analytic community.

6. Recommendations… "Anything You Can Do, I Can Do Meta…"

The IC's Advanced Research and Development Activity's call for 2005 Challenge Workshop proposals (ARDA 2005) suggested a topic of interest whose solution demands more self-awareness from the analytic community:

> *"Present information in future contexts: Intelligence analysts share a recurring nightmare that begins with some investigative commission asking 'What did you know, and when did you know it?' All too often, the conclusions drawn from the analysis of present information are irrelevant at best or incorrect at worst in the context of future events or discoveries (including analytic discoveries). Is there a way to revisit 'old' data and conclusions (particularly when those 'conclusions' result in bypassing data) to alert analysts that their previous impressions now require revision?"*

A useful question to ask, and presumably prompted by the continuing controversy over assessing "weapons of mass destruction" in Iraq. But prior states are not merely the documents available at the time, and analyses produced from them; they are complex meshes of interactions. And a still better question would be, "What did you believe, and why did you believe that?"

There is a measurable market for FININTEL—it is the expected output of the analytic arm of an intelligence agency, and of the IC, and the final justification of its budget. Analysis of *how* the work is actually done may be harder to justify, but no less important.

In her "The Age of the Smart Machine," the Harvard Business School's Shoshana Zuboff documented the case of "Global Bank Brazil," a bank that had invested in automation to facilitate its primary activities, of borrowing and loaning money (Zuboff 1988). In doing so, it developed a whole new business line: the sale of derivative analysis, information *about* the borrowing and loaning of money. A similar attention to the transactions between and among analysts, their expressions of interest, and other attributes and skills, would provide valuable insights to intelligence agencies as well.

The final report of a recently-completed ARDA-sponsored workshop, on addressing the threat of malicious insiders, concludes with a call for an annual "spy catcher" exercise, where participants would deploy analytic tools to detect indicators in traffic and transactions representative of agencies' actual activities (Maybury *et al.* 2004). I think the IC would similarly benefit from an annual (if not continuous) exercise in demonstrating what can be gained by conducting meta-analysis, aggressively seeking to understand what might emerge from treating itself more as an object of study.

The intelligence agencies also have a formal invitation to think much more creatively about privacy, as a consequence of the 2004 Omnibus appropriations bill. Enacted as Public Law 108-447, it mandates that each agency will appoint a Chief Privacy Officer, with responsibilities to include ensuring protection of both employees and the public. A chief privacy officer in an intelligence agency ought not to be regarded as an oxymoron; there ought to be myriad opportunities to take a hand in ensuring that agencies are both effective *and* responsible.

A challenge I'd put before the agencies' new CPOs would be to assess both where limits in intruding on privacy ought to be, and how to be imaginative, within those limits, to maximize self-awareness.

While information technologists may be responsible for the architecture to support a more self-aware analytic community, customers, first and foremost the analytic community itself, ought to take the lead in examining the opportunities. Other stakeholders would include those responsible for security, and management more generally, but the analysts ought to take the opportunity to preemptively establish an environment that both accrues the benefits of more "watchin'," without unduly inconveniencing those watched.

Acknowledgments

I would like to thank the Central Intelligence Agency for their permission to publish, and for the education I gained there; I would like to dedicate this paper to all those friends and colleagues still there, a fascinating place in most interesting times.

References

ARDA 2005 Challenge Workshop solicitation. http://nrrc.mitre.org/arda_explorprog2005_cfp.pdf

Loeb, Vernon, 2000. "Chat Room Penetrates CIA Net; 160 People Probed For Offensive E-Mail," The Washington Post, Nov. 12, 2000, p. A10.

Loeb, Vernon, 2000a. "CIA Shuts Chat Room, Fires 4, Suspends 10; 9 Firms Dropped in Covert E-Mail Operation," The Washington Post, Dec. 1, 2000, p. A2.

Maybury, Mark, *et al.* 2004. Insider Threat Challenge Workshop: Final Report. The Mitre Corporation, May 2004.

Medina, Carmen, 2002. What to Do When Traditional Models Fail. *Studies in Intelligence*, vol. 46, no.3, 2002, unclassified edition. http://www.cia.gov/csi/studies/vol46no3/article03.html#fn1

Zuboff, Shoshana, 1988. *In the Age of the Smart Machine: the Future of Work and Power*, Basic Books, Inc., New York, New York, 1988.