

An Ethnographic Study of Culture and Collaborative Technology in the Intelligence Community

SAND 2007-2593-J

Jessica G. Turnley,
Galisteo Consulting Group, Inc.
Albuquerque, NM
jgturnley@aol.com

Laura A. McNamara
Sandia National Laboratories
Albuquerque, NM
lamcnam@sandia.gov

Introduction

Since 9/11, significant public and political attention has been focused on the (lack of) collaboration that exists between and among the various organizations that comprise the U.S. Intelligence Community (IC). To proactively address this question, the IC supported and funded a program called Knowledge Discovery and Dissemination (KDD). Its published statement of purpose is to “improve the quality and timeliness of intelligence analysis by creating effective methods to merge multiple sources of information and cooperatively analyze the information through multi-agency analytic teams” (KDD Program Staff 2005). Most of its sponsored projects involve the development and deployment of various software-based tools to enhance data-sharing and communication among analysts.

Research question

As anthropologists who study how technologies and organizational values interact to generate behavior, we suggested that the determination of the type of tools developed and the success of their deployment might depend upon socio-cultural (organizational) factors not normally considered in the development of such tools. We hypothesized that organizational values attached to the production of work products and the associated definition of analysts' identity in the workplace would drive analysts' decisions to (not) engage in collaborative behavior. Tools would facilitate behavior deemed desirable by other criteria, but would not generate the desire.

To test this hypothesis, we conducted ethnographic fieldwork in two intelligence agencies, one of which houses a large number of all-source analysts, and another that

develops and deploys technologies for tactical intelligence problems.¹ The question we initially used to frame our study – “Why do analysts (not) collaborate?” – was informed by a great deal of reading about analytic tradecraft in the intelligence community, much of which emphasizes the need for greater collaboration. However, once we got into our field sites, we discovered that regular collaboration already takes place among intelligence analysts, within and across organizations in the intelligence community. Moreover, a great deal of analysts’ work – especially collaborative work – is conducted via computers, most of which are already equipped with a wide range of tools designed to enhance analysis and enable information sharing. As a result, our research questions changed slightly, so that we found ourselves asking, “What does collaboration mean in the analytic environment, and what is the role of technology in supporting collaboration?”

Approach

We explored these questions using field observation and interview data collected at three sites that conduct intelligence analysis under the Department of Defense. Data was collected in the summer of 2006, and analyzed in the context of previously written theories and critiques of the intelligence community and of tradecraft itself.

Our ethnographic approach is based on the tenets of grounded theory (Glaser and Strauss 1999 [1967], Strauss and Corbin 1998). Grounded theory recognizes that human social behavior in the day-to-day world is sufficiently complex, mutable, and variable to render impossible an objective, transcendent view of any social reality (Haraway 1991: 189-191; Strauss and Corbin 1998: 4). As the researcher conducts interviews, observations, and gathers site-specific ephemera (e.g., reports, briefings, photographs, drawings, and other artifacts), she revisits her initial themes, refining them to generate hypotheses that may explain what she is observing. She then uses these emerging hypotheses to develop questions, select and prioritize opportunities for field observation and interviews, and to search out materials that can be used to confirm or deny her hypotheses. Following this model, our research consisted of three basic activities, conducted iteratively: study of narrative and graphical material (reports, white papers, internal publications, and the like) that describes or relates to the analytic work pursued in each of the field sites; interviews with field personnel in each of the teams; and observation of group activities as well as routine work activities performed by team members in the course of their daily jobs

Any work with human subjects must be sensitive to the rights and safety of both the subjects and the researchers. Accordingly, we submitted our research design to the Sandia National Laboratories’ Institutional Review Board, whose members are charged with review of projects involving human subjects. The Board approved our final research design, which included a statement of informed consent each participant in the study

¹ KDD funded Sandia National Laboratories to conduct the research. Laura McNamara is a technical staff member at Sandia, and Jessica Turnley is a contractor with a long-standing relationship with the labs, DOE, and the intelligence community.

reviewed and signed. To protect privacy, each interviewee was assigned a unique number, which was used throughout all interview transcripts and field notes to identify the person being interviewed or observed. The key linking the identification number with the identity of the interviewee is maintained in a controlled access file.

The first challenge in our research was gaining access to field sites where we could gather data to explore the problem of collaboration. Conducting ethnographic research is tricky in classified environments. Ethnographers are “professional strangers” (Agar 1996). As outsiders, ethnographers can make great use of their ignorance to ask questions and raise issues that a community’s established members may have come to take for granted. Secondly, ethnographers rely on field notes and interview transcripts, both of which require that the researcher record as much as she can of the activities going on around her. As a result, ethnographic research is an uneasy fit with intelligence activities, where strangers are viewed with caution and recorded information is carefully categorized, managed, and stored.

As originally designed, our study would take place at four sites, preferably in four different agencies in the intelligence community. We had planned to begin by piloting our methodology in a Department of Energy (DOE) Field Intelligence Element (FIE) at Sandia National Laboratories, an environment familiar to us because of our relationship with Sandia. We would pursue the body of the work at core sites of the IC. Ideally, we would compare sites across agencies. We were also encouraged by our KDD sponsors to consider a cross-agency institution, such as the National Counterterrorism Center (NCTC), that was established after the 9/11 attacks to bring together different intelligence and law enforcement agencies. We planned to conduct two weeks of team observation at each site, followed by a week or so of interviews with the individuals that we had observed.

Results

The context

The United States Intelligence Community (IC) consists of 16 major government agencies, military and civilian. Broadly speaking, the IC engages in three major activities: collection of information, analysis, and operations. Our efforts were focused on intelligence analysis, rather than operations or collection. This is largely because the KDD program itself is focused on developing technology to improve analysis, but also because intelligence analysis is more accessible to outsiders than collections or operations, which are highly sensitive activities.

A great deal of post-9/11 analysis of the IC focused on reasons why the community could not ‘connect the dots’ prior to 9/11 and piece together patterns of suspicious behavior from data provided by different organizations. From this literature, we have identified three models that experts have offered for explaining why intelligence analysts periodically fail to forecast major emerging events that, in retrospect, should have been

'forecast-able.' Note that while these models are not mutually exclusive, differences in diagnosis lead to quite divergent remedies, with the result that 'fixes' tend to be introduced at a particular level (i.e., structural) without careful consideration of their consequences for the other levels (i.e., small analytic groups or individual intelligence analysts).

- **PSYCHOLOGICAL.** This mode of critique locates the problem at the level of *individual analysts*, emphasizing cognitive capabilities and psychological biases. Tradecraft is conceived as a form of cognition. This school of critique is epitomized in the work of Richard Heuer, a psychologist (Heuer 1999). "Fixes" in this model emphasize improving technique by training analysts to recognize, then take steps to counter, cognitive bias.
- **TRADECRAFT AS PRACTICE.** This second frame for critiquing intelligence analysis focuses on analysis as craft knowledge. In this view, the practices, skills, and understandings comprising "analysis" are transmitted across generations of analysts through formal training programs, on-the-job experience, and expert-novice mentor relationships. The learned-skill model complements the psychological model, insofar as it identifies organizational elements that influence how individuals approach problems, gather and process information, and develop opinions, keeping the focus on the individual. "Fixes" in this model emphasize changing the methods that analysts employ in their work.
- **STRUCTURAL.** A third stream of critique emphasizes structural problems in the institutional organization of intelligence. In this paradigm, processes within institutions, as well as the interactions among institutions, can either enhance or degrade the community's collective ability to assemble information into a coherent, accurate, timely, and effective product. "Fixes" in this model emphasize changes in organizational structures and processes.

We suggest that the prevailing U.S. model of intelligence production is a structural one, specifically one that defines the IC as a rule-based bureaucracy (Weber 1947 [1924]). This is deduced from the criticisms of the IC in which what it means to fail is very clear (violation of a rule or process such as inappropriate release of information), while what it means to succeed is less so (the unprovable 'attack that didn't happen'). Therefore, as in any bureaucracy, management tends to be driven by the constraints on behavior (negative incentives) rather than by focus on organizational purpose or task (positive incentives) (Wilson 1989). In the case of the intelligence community, these constraints range from the explicit (e.g. security procedures, classification protocols) to the more implicit ones of budget and resource allocations which direct analytic efforts and determine collection and analytic capabilities. This also tends to shift the definition of high-valued behavior from accomplishment of ends (providing timely, accurate support for national security decision-making at strategic and tactical levels [Sims 2005]) to adherence to rules and procedures and control over assets (e.g. the maintenance of

compartmentalization of information). Structure and process also have been used to diffuse authority and responsibility to act as a 'check and balance' against the potential abuses of civil liberties that could arise from a stronger, more centralized function (Turner 2004).

That the prevailing U.S. model of intelligence is the bureaucratic (structural) is further supported by the nature of the post-9/11 reforms of the IC which all focus on changes in organization and process. The new function of Director of National Intelligence (DNI) with its associated staff and support functions was created by the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). The dissolution of the procedural walls between domestic and foreign intelligence and national and local approaches to terrorism was and still is a focus of interest, activity, and concern. A number of new topically focused 'centers' (such as the NCTC) reporting to the DNI also were established by P.L. 108-458 to bureaucratically or structurally help with this realignment. And finally, and perhaps most importantly for this study, P.L. 108-458 speaks not of enhancing collaboration in the intelligence community but of improving 'information sharing' (P.L. 108-458 § 1016). The language used and the mechanisms set up to effect such sharing treats information as an artifact, almost like a tangible good. The focus is on the vehicles for passing information artifacts from one individual to another or from one organization to another, mechanisms to allow access to these artifacts by a broader range of individuals, rather than on individual biases that might affect either the desire to use additional or different data (the psychological model) or the actual way in which that data is used (the tradecraft as practice model).

Recognizing the intelligence community as comprised of bureaucratic institutions leads to two lines of questioning. The first concerns how the bureaucracy coordinates collectors', analysts', and operators' work through rule-based structures to ensure maximum coverage across the community's area of responsibility. The second line of questioning concerns how bureaucratic interests influence the behavior of individuals. Bureaucracies have their own interests as institutions: stability, survivability, and control over resources. Insofar as bureaucracies are composed of people, however, their institutional interests are inevitably linked to the personal interests of the people who work inside these institutions. As a result, concern for one's career and livelihood is not so far removed from the bureaucracy's interest in maintaining its collective existence. Lastly, bureaucracies have reward structures that motivate behaviors at the individual level that can be counterproductive vis-à-vis institutional goals. As Sims put it, "the most important measure of success for any intelligence service is not the number of secrets it collects or the truth of the analysis it generates, but rather the timeliness, efficiency, and accuracy with which it supports national security decision-making" (Sims 2005:15). Today, however, analysts are still measured by quantity not quality, and joint or contributing authorships are not valued as highly as single or primary authorships.²

² Several conversations between Turnley and analysts and management in defense intelligence over the course of 2005.

Compounding the bureaucratic complexity of the intelligence community is the unique nature of intelligence information as *consequential knowledge*. Because intelligence information is produced for the consumption of decision makers, every action an analyst takes is potentially loaded with outcomes beyond her control. Intelligence analysts (and probably operators and collectors as well) pursue their work with the explicit recognition that information they produce will be used to support high-consequence decision makers in tactical and strategic action (see also Turner 2004).

Field work

To establish access to research sites, we leveraged our personal contacts with individuals at key places in organizations within the IC to gain entrée to gatekeepers. However, although the people to whom we described our project (generally in high-level positions in these organizations) were universally enthusiastic about it, they themselves did not advocate at the operations level for our extended presence in sensitive information environments. Furthermore, upper managers often rotate in and out these organizations on a regular basis, making continuity of contact a challenge. In any event, we were unable to establish our pilot at Sandia's FIE, and ended up with two of our three field sites within the same organization, and all three of our sites within the DoD intelligence family. Two of our sites (in Intelligence Agency One, or IA-1)³ were analytic groups focusing on the production of strategic intelligence. There also was some engagement with in-house tool developers in this environment. The analysts at these sites were representative of the types of users KDD envisioned for its collaborative software tools. The third site in Intelligence Agency Two (IA-2) was chosen to give us insight into the interface between developers of these tools and the environment into which they would be inserted. The organization observed developed software tools for tactical intelligence environments. Table 1 lists the field sites.

Table 1: Field site locations

Location	Team	Researcher	Dates	Team Purpose
IA-1 (DoD in Washington, DC area)	Rapid Knowledge Team	McNamara	June 19- July 7, 2006	System of Systems Model Development and Analysis – strategic intelligence
IA-1 (DoD in Washington, DC Area)	Nonproliferation Assessments Team	McNamara	July 10- July 26, 2006	Analysis of WMD Proliferation Networks – strategic intelligence
IA-2 (DoD in California)	Military service-focused: private contractors, military, civilian federal, state, local government personnel	Turnley	August 2006	Field test of tool for use in tactical intelligence activities

³To ensure privacy and confidentiality, these agencies are aliased as 'Intelligence Agency One' (IA-1) and 'Intelligence Agency Two' (IA-2) in this report. Unless otherwise noted, all names of organizations, individuals, teams, and projects are aliased.

We are pleased to report that we had no issues with managers in either IA-1 or IA-2 regarding access to interview or observation data. The managers in IA-1 made significant effort to reassure analysts that participation in the study would have no bearing on any kind of performance review. Managers in IA-2 gave the same assurances, emphasizing that the data collected would be on social interaction not substantive contribution.⁴

Intelligence Agency One

IA-1's main offices are located in the vicinity of Washington, DC. Between June 19th and July 26th, 2006, McNamara spent five and one-half weeks observing and interviewing analysts at two sites in this agency. The first field site was the Rapid Knowledge (RK) team, a recently formed multidisciplinary group charged with developing new analytic capabilities for defense analysts. The second group was the Nonproliferation Assessments Division, another recently formed analytic team that is responsible for analyzing the networks that enable weapons proliferation. Both of the groups studied are relatively new within the IA-1's analytic directorate, but both have their roots in well-established analytic divisions.

Data was collected through thirty formal interviews and forty hours of direct workplace observation, including sitting with analysts as they performed tasks and attending team meetings. This was supplemented by perusal of unclassified and classified documents describing each group's efforts and activities.

IA-1 is an all-source intelligence agency, meaning that its analysts have access to and utilize the full range of intelligence information sources (human intelligence, signals intelligence, communications intelligence, et cetera) in their work. Its core workforce consists of full-time staff as well as a large number of contract personnel.

Like most bureaucracies, IA-1 has a complicated hierarchical structure. The agency is headed by a director and her/his supporting staff. Below the director are several directorates that have responsibility for executing the IA-1 mission. Directorates are divided into units, each of which is led by a manager. Each unit is further organized into divisions, which are the main workplace or "nuclear family" for analysts. Divisions consist of between ten and twenty analysts who work under a single line manager, and who are responsible for a specific thematic focus.

Within a division, individual analysts tend to have specific areas of responsibility, known as "accounts," often comprising a combination of a geographic and a subject area focus. In addition, among the analytic line staff, there are further formal gradations of rank and responsibility. For example, the title "Analytic Senior Expert" represents a quasi-

⁴ It is interesting to note that, although acting from the best of intentions vis-à-vis the research, the managers in IA-2 implied that the social interactions and contextual environment was peripheral to the 'real work.'

management position reserved for analysts with several years of experience doing intelligence work. These individuals are often subject matter and methodological experts who play an intellectual leadership role in developing products, prioritizing research efforts, and coordinating analytic activities within the division and with counterpart divisions. Finally, ad hoc functional teams may form around a particular problem, and disband when the exercise is over.

The IA-1 workplace is a physically open and somewhat noisy environment that affords little privacy. Fabric-covered dividers provide office space, or cubicles, for the vast majority of the workforce. Analysts working in the same division and unit tend to be physically collocated in the same area of cubicles. Signs hanging from the ceiling indicate the name of the division that occupies a particular area of office space, although there are secure spaces in the building that are designated for handling of particularly sensitive material. Although the entire building is a Secure Compartmented Information Facility, or SCIF (a space where classified information can be safely stored and used), the security boundary is at the front door of the building. The interior physical environment – open cubicles, conversations that take place in everyone's earshot, few locking offices – does not physically restrict the flow of information.

The formal hierarchy described above is important for several reasons. It provides a mechanism through which IA-1 can identify and map areas of responsibility onto a very large and diverse workforce, thereby coordinating their actions towards a common set of goals. As formal requests for information come into IA-1, they are fed into an automatic tasking system that matches queries to analysts. Secondly, it is through this formal hierarchy that resources and decisions flow through IA-1. Thirdly, the structure offers an important and visible path for career advancement for those individuals interested in management. And finally, the division (the lowest level of the hierarchy) provides the primary locus of organizational identity for analysts, evidenced by the fact that analysts identify themselves first and foremost by the division that employs them (e.g., "I'm an analyst in the such-and-such division."). Interview data indicates that IA-1's center of gravity is decidedly located in the mission-focused directorates, where intelligence data gathering, analysis, and operations reside.

As is also true in most bureaucracies, there is also a powerful *informal* hierarchy, which we refer to as a "prestige hierarchy." Prestige hierarchies represent the distribution of social, political, and intellectual capital in an organization. They often act as center of gravity in an organization, and can easily come into conflict with the goals and aspirations of formal managers. For younger staff members who are not interested in management, senior members of the prestige hierarchy can be important role models who demonstrate a successful career in the IA-1 work environment. Their work and actions of senior members of the prestige hierarchy help define what it means to be a "respected expert" in the organization, one engaged in what is perceived to be the most important, difficult, high-profile, risky, or significant work. They also tend to have social, political and intellectual capital both within and outside the IA-1 environment, which they activate

through social networks. These social networks are vital channels through which information flows throughout the IC. As several mid-career and novice analysts pointed out, being taken under the wing of an experienced and respected analyst is the fastest ticket to membership in these information networks that stretch across (and through) the formal organizational boundaries that separate the institutions comprising the IC.

Although McNamara's time was spent almost exclusively among analysts, she did have some contact with the IA-1's 'technical developers,' the software developers who work with analysts to develop databases, analytical tools, and the like. Technical developers often – but not always – reside in the Computing, Software and Tool Development (CST) Directorate. Even though both directorates sit at the same level on the organizational chart, the directorate where the analysts work occupies a higher place in the prestige hierarchy: members of the latter are doing mission centered work – namely, producing intelligence data – and do so on tight timelines, with very sensitive information, and often for the consumption of high level decision makers that sit outside IA-1's boundaries. In contrast, CST Directorate is seen as a support organization with its customers largely internal to IA-1.

Since 9/11, IA-1 has invested considerable resources in experimenting with new organizational initiatives to improve intelligence analysis. These have included changes in workspace configuration, in analytic approaches, and in the ways in which work is organized. Workspace reconfigurations include a major remodeling of part of the IA-1 building into the Collaboratory, a workspace with an open, airy, circular layout. In consultation with intelligence analysts, the Collaboratory core staff members identify timely, relevant analytic problems that cut across multiple areas of expertise and responsibility. They use these problems as an opportunity to assemble temporary, interdisciplinary teams of analysts whose members come from both within and outside IA-1. In addition, analysts use its facilities for meetings and projects, and can be involved in longer-term organizational "experiments" that the Collaboratory developed to identify ways to enhance collaboration, innovation, and analytic products.

New approaches to work are exemplified by both the Rapid Knowledge team and the Nonproliferation Assessments division. The goal of the Rapid Knowledge team is to develop computational modeling environments to simulate the interactions among physical systems in specific geographic regions. The systems that the RK team is integrating have traditionally comprised separate areas of analysis, even separate accounts within IA-1. The Rapid Knowledge team also is organizationally located in an unexpected place. Most software development activities occur in the Computing, Software and Tool Development Directorate. The Rapid Knowledge team, in contrast, resides in the same directorate where analysts work, giving its project more *gravitas* due to its location high in the prestige hierarchy. The Nonproliferation Assessments Division also is working to establish a new focus area for analysis: in this case, the focus would be on the different networks that support proliferation throughout the world and across technological capabilities.

The perception that collaboration is a problem worth consideration is a widespread one in IA-1. When asked to explain why collaboration is so problematic, even in an environment as physically open as the IA-1 work environment, analysts had several responses, most of which fell into one of five general categories.⁵

- *Innate psychology.* Interviewees frequently characterized themselves and their fellows as introverts. Interviewees who spoke of innate personality traits seemed to believe that introversion mitigates against collaborative behavior – although the same interviewees also described the importance of professional networks in furthering their own careers.
- *A sense of ownership over subject matter.* Over time, an analyst who has worked closely on a particular account can develop a reputation throughout the intelligence community as an expert in a subject and/or a region. Moreover, the analysts in IA-1 take their responsibility to produce high-quality, reliable intelligence products very seriously. Expertise, coupled with a sense of personal responsibility for accuracy and reliability, can translate into a strong sense of ownership over a research area.
- *The formal reward system.* Other analysts emphasized the role of the IA-1 reward system as a factor that influences collaborative initiatives. Analysts believe that the formal career ladder at IA-1 privileges individual achievement over group efforts. McNamara's interviewees reported that in many areas of the analytic community, collaborative activities tend to 'count' less in one's career than individual efforts.
- *Organizational knowledge.* Before collaboration can occur, an analyst must be able to identify likely candidates who can bring valuable insights and information to a subject. An analyst must thus know not only who does what. This is challenging, given that she might be one of several thousand IC professionals, each of whom is working on specific subject and geographical problems across the entire world. Moreover, she must develop a sense for how work done elsewhere is relevant to questions she is asking about her own accounts.
- *Turf wars.* New institutions and new rules can be difficult to interpret and define, raising the level of uncertainty around what information is releasable and what is not. When this is coupled with the fact that analysts are rarely rewarded for releasing information (but can easily face reprimands, even punishment for inappropriate release), "The tendency across the community is to overclassify, compartmentalize, make things harder to release."

⁵ Interestingly, many of the explanations offered by 'native' analysts echoed Susan Fussell's research, in which she points to social networks, organizational knowledge, and reward policies as factors that influence collaborative behaviors.

Intelligence Agency Two

This section describes Turnley's fieldwork in Intelligence Agency 2 (IA-2). IA-2 was not an intelligence agency *per se*, but a research and development organization focused on information management technology to support the warfighter. The technology of interest for this research supported the production of tactical intelligence. The site Turnley visited was located on a military base in California, where she spent about 20 hours familiarizing herself with the site and the organizational context for the development team and process, 40 hours of observation, and conducted five interviews with key members of the team. This was supplemented by perusal of documents and visual material related both to the technology and to the development process.

The technology development period was about three years which took the technology through to prototype. This observation was conducted at the end of that three-year period, when the prototype was about to go through a simulated field test.

There were several different types of players involved in the development process. These were the businesses directly engaged in the development of the technology; the civilians who worked for the research and development organization; the Washington, D.C. Pentagon-based military service component that issued the Small Business Innovation Research grant (SBIR) which funded the development and so was the actual purchase decision maker; and the warfighters who were the end users of the technology, and functioned as purchase decision influencers, but not purchase decision makers.

The development team itself was a consortium of up to 12 small businesses located throughout the country. Over the three-year period, some portion of the roster of participating businesses remained constant, while others moved in and out of the development process as they developed and integrated their portion of the technology. The nature of the technology was such that one company served as a system integrator throughout the process, ensuring interoperability of all the component pieces. We call that company INTEGRATE.

The SBIRs were administered by the research and development organization in California, itself a part of the military service component but staffed by civilians. These civilians had dual roles. They acted as intermediaries and facilitators between the business consortium and the SBIR office in the Pentagon, and between the technology development team (aka the business consortium) and the end user community (the warfighter – the uniformed service component). The SBIR office in the Pentagon answered to oversight structures regarding funds disbursement and use. The warfighters provided the definition of the use environment.

The end user was a shadow presence in the development process. The declared end users were uniformed personnel engaged in certain types of counterterrorism activities. However, the military procurement process is such that formal, direct communication between the technology developer and the end user is precluded and in fact, there is

significant institutional and temporal separation between the user, the purchase decision maker, and the developer. The technology developer receives a set of requirements, not a statement of user needs. This is contrary to the ideal development process which sees the developer in in-depth, iterative conversations with the user, focusing on needs not technology specifications. This process is illustrated in Figure 1. Note the weak link between the Commanders in Chiefs (CINCs), who represent the end user community although they themselves are not the end user, and the developer as represented by the dotted line

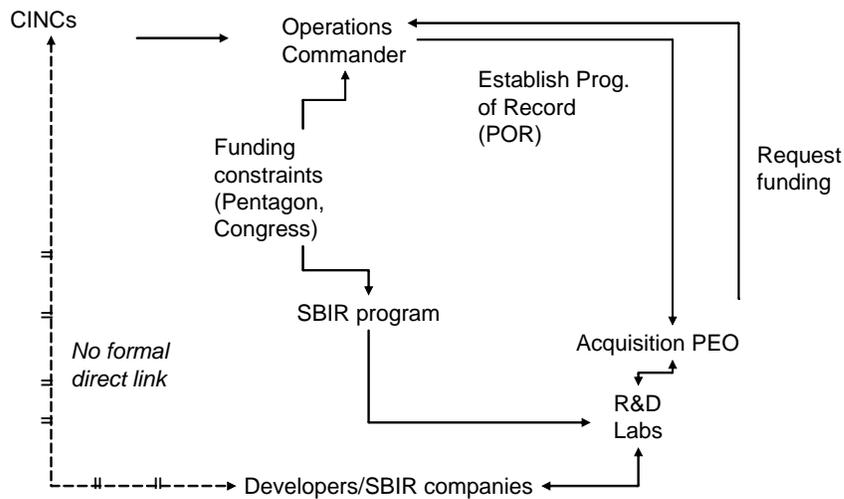


Figure 1: Requirements to development

The players in the observed exercise did work hard to overcome this separation between the technology developer and the end user. INTEGRATE had on staff an individual who had recently come out of the uniformed use environment and was now working in a civilian capacity. He provided advice and input on technology design and functionality. The sponsor at the research and development organization also worked hard to get the developers access to uniformed personnel who would be using the new technology, with variable success. His success rate depended upon the particular individual who occupied a key position that served as a formal liaison between the civilian-staffed research and development organization and the uniformed service component. At one point, that individual was fairly sympathetic to the developers' access needs. That person rotated out partway through the project, however, and the individual who replaced him was not similarly sympathetic and access by the developers declined significantly.

A simple sketch of these relationships and the communications link is given in Figure 2. Those directly observed for this project are those within the dotted line. The tenuous

relationship between the companies (as represented by INTEGRATE) and the warfighter is represented by the dotted line.

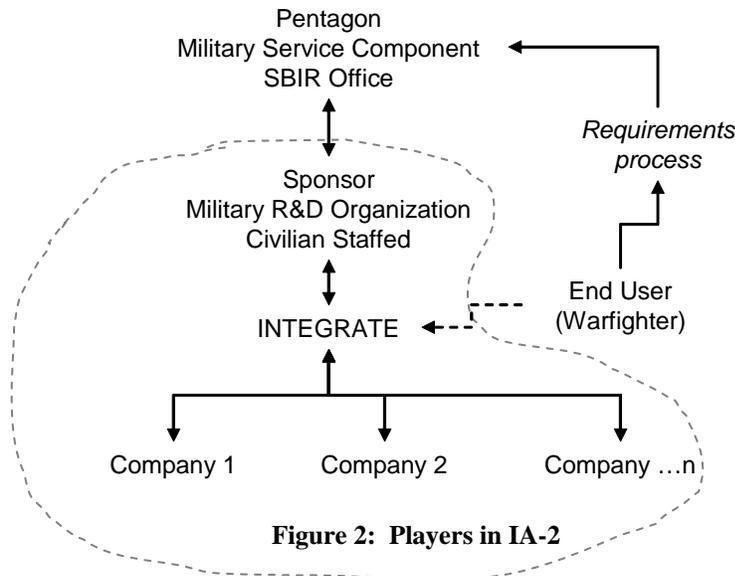


Figure 2: Players in IA-2

The actual technology demonstration was to take place a day or two into the second week of a two-week exercise. The first week and a half were devoted to working out the glitches and bugs that showed when the various components of this information management technology (developed separately) were integrated into a single, working system. This work was conducted partially in a SCIF (the data set to be used for the demonstration was classified) and mostly in an unclassified environment.

There were four companies present at the technology demonstration (including INTEGRATE), along with the direct sponsor, for a total of about 10 people. For the exercise, the sponsor played a dual role. One was a traditional sponsor role, managing the demonstration activities. The second was as an active part of the development team as the sponsor provided some of the equipment and data collection vehicles necessary for the exercise itself.

The information management technology under development was configured such that INTEGRATE had a key role in ensuring system interoperability. INTEGRATE had developed this role early in the process, and it was never challenged by other member companies. Conversations with members of the team revealed that this technology integrator role had evolved naturally into a role where INTEGRATE also became the consortium representative with the sponsor. INTEGRATE developed and managed the implicit, informal project plan that guided activity over the observation period, and clearly were the focal point for many conversations among team members, and the primary interface to the sponsor. It is important to note that relationships among the members of the development team clearly were very collegial.

Each participating company had a different agenda or purpose for its participation in the consortium as revealed through conversations with Turnley, conversations among themselves, and through the formal interviews. INTEGRATE had a vested interest in ensuring that the whole system worked – the effectiveness of its piece clearly depended upon the effectiveness of all others. The other companies needed to be sure their component functioned as promised...but clearly also were using the consortium for visibility with the sponsor (many of them had either other existing products for sale or products under development for which they hoped to get research funding).

The consortium SBIR model was a new model for the military service component; the civilian sponsors had worked hard to sell the concept to Washington as they believed this was the most effective way to achieve their technology development goals. They thus had strong vested interests in the success of the technology itself, as well as in the success of the process by which the technology was developed. It was to their significant advantage that the participating companies worked well together.

There were two areas in which collaboration could be of concern in IA-2. The first involved collaboration among the companies involved in the development process itself. As we discussed earlier, collaboration among those involved in the development process was not an issue. Although agendas of individual players varied, there was enough overlap to allow smooth functionality. The second area of interest to a study of collaboration was the way in which the tool fostered collaboration among the different components of the use environment after the tool was inserted. It is the second area that proved to be most interesting in the context of this study.

The technology was an information fusion technology that allowed an analyst to cross-verify data received from multiple types of collectors fielded on a single platform. Historically, each type of collector or sensor was 'owned' by a different organization (a collection agency or a military service) and fielded on a separate platform. The platform was owned by the same agency or service component that owned the sensor. As field conditions during an operation changed, tactical requirements drove the targeting of these separate collectors. The ultimate targeting decision was made by the owning organization which allowed it to make trade-offs in asset allocation among its several concurrent demands. Data from each sensor was downloaded, separately processed and analyzed, and 'fused' at the end of the initial analytic process.

The new technology allows different types of sensors to sit on a single platform so they can be simultaneously tasked by the analyst, and the data is cross-verified before it gets to the analyst, reducing uncertainty.⁶ This will require changes in practice, or, in military terms, a change in concept of operations (CONOPS), in two areas. First, it will change

⁶ This is a very simple description of a very complex technology and does not accurately represent capabilities. Details have been omitted for classification and security reasons. However, as the key question here is not about the technology per se, enough information has been given to make the points necessary for this research.

the organizational control over the tasking of the sensors and hence over deployment of the platforms. Secondly, the reduction in uncertainty of the data will have implications throughout the decision-making chain.

The shift in organizational control over the tasking of the sensors turns out to be very problematic. Interviews with the former end user now on the development team, reinforced by knowledge drawn from Turnley's historic interaction with the intelligence community, established that sensors are considered an organizational resource by the 'owning' organization. First, as the sensors and platforms are hard assets, control over them represents control over tangible resources – an important marker in the determination of organizational status in a bureaucratic environment. Secondly, control over the sensors and their associated platforms gives the owner (a feeling of) control over the information they generate. In the intelligence world, control over knowledge is power. Under the current regime (prior to introduction of this new technology), knowledge of sensor availability is held by the 'owning' organization and that organization reserves the right to assign a particular sensor to a task. If someone other than the owning organization wishes to task the sensor, there is a formal process for going up the chain of command of the owning organization with the request to the actual decision maker. Permission or denial then flows back down the chain. While in practice this chain may be short-circuited in the interest of a tactical operation, the fact of its existence signals the location of the ownership of the resource and allows the actual owner to declare his right over the resource if and when he so chooses. This question of the locus of ownership is further complicated by the new system because it requires that sensors historically owned by different organizations and deployed on individual platforms will be physically grouped onto a single platform. Finally, there is the perception that once resources are relinquished, it is (perceived to be) very difficult to get them back.

Analysis

In the IA-1 context, collaboration is a kind of *cooperative communicative event* that typically occurs in the context of developing an intelligence product. Cooperative communicative events can entail everything from a brief, willing exchange of information about a topic of interest, to the long-term development of a major report or briefing. Whether or not a communicative event counts as collaboration in the mind of analysts seems to depend on the length of time over which the communication occurs and the level of commitment on the part of the analysts involved. More specifically, analysts identified three kinds of cooperative communicative events that occur in the IA-1 workplace: information exchange, the coordination of activities and products, and "collaboration." Each of these involves a progressively higher degree of commitment and a longer period of time, as described below.

Analysts agreed that a willingness to *exchange information* (from 'raw' data to finished products) is a necessary, if not sufficient, condition for collaboration, both within and

across institutional boundaries. Any barriers to the flow of information represent potential roadblocks to the emergence of collaborative relationships.

Coordination is a routine communicative activity that involves checking one's analysis against the expertise of others who might claim a stake in the analytical product. When analysts were asked to comment on the impact that coordination has on the quality of a product, most described coordination as a helpful form of peer review. Coordination plays an important social role as well, as analysts demonstrate respect for each others' areas of responsibility and experience by requesting opinion and input to a product.

Analysts distinguish between coordination and collaboration by emphasizing *collaboration* as a type of relationship among individual analysts, which often –but not always – results in the production of a formal product in which each perceives a sense of ownership and responsibility. True collaborative relationships can involve coworkers within the IA-1 environment, or even across the IA-1 institutional boundary into other intelligence agencies. Given that the IA-1 reward system strongly emphasizes individual accomplishment, the key factor in these partnerships seemed to be the emergence of a strong trust relationship.

Observation at IA-2 raised some interesting questions related to the deployment of tools to support collaboration. Some of these questions are particular to tactical intelligence and a military environment; others are more generic and apply to a general intelligence or information analytic space.

Deployment of the technology under development at IA-2 required changes in CONOPS, or practice.⁷ These changes whereby the analyst directly tasks a collection resource and several different types of resources are deployed on a single platform can have significant implications for collaboration. Who owns the platform itself? How are competing demands on the sensors on that platform resolved (competing in that they may be simultaneously required for multiple tactical operations or for tactical and strategic collections that have different targets)? Who 'owns' the data that comes from those sensors? (This can be important from a classification standpoint, as well as for the power that comes from controlling and managing data.) It is conceivable, then, that an owning organization will refuse to relinquish control over a sensor for a variety of reasons.

The second important implication – and related to the first – is that these types of tools have the potential to change the character of the information with which the analyst works—in this case, by reducing its uncertainty and by speeding up its flow. It was unclear from observations, interviews, or conversations how that changed nature of the information and the increase in the rate of transmission would be communicated through the analytic chain, and how the impact of these changes on the nature and tempo of

⁷ There is an important difference between general business practices and CONOPS. CONOPS are formal and explicit and in written form; general business practices are informal and implicit, and would need to be elicited through observation and interviews.

operations and decision-making would be managed. What was clear was that this was not considered part of the technology development or deployment area of responsibility.

The sensors and associated platforms thus are not just data collectors. They are representations of organizational 'wealth' and of the organization's control over a resource that is critical to its own success and which also operates as a coin of the realm – information. However, these potential barriers to effective deployment and use were not considered at all by either the software development team or by the civilian sponsors. Interviews, conversations and observations suggested that the perceived area of responsibility for the development team was bounded by an incoming data set on one end and the outgoing taskings to assets and intelligence products to operators on the other. The production of the data sets, the reconfiguration of the assets, and the behavior of the decision makers who received the intelligence products was outside the perceived purview of the development team. A lack of change of practice in these areas could compromise the effectiveness of the tool even though from a technology standpoint the tool could be said to 'work.' However, organizationally and institutionally, management of this change 'fell through the cracks.'

Conclusion

This research did support the assumption that stimulated it. We had assumed that there are factors beyond technology itself that determine the effectiveness of a given technology in a use environment. We discovered that, indeed, tools that support collaborative activities are fully embedded in the social environment of the intelligence organizations, and that failure to consider the consequences of their impact on the full analytic process and the self-definition and social location of the analysts who use them will significantly impact their effectiveness.

The word "collaboration" is a surrogate term for a tangle of issues around trust, information, and power in the highly politicized environment that is the intelligence community. Efforts to develop collaborative technologies that facilitate information sharing among analysts might well be aiming at the wrong target: the analysts. This is because failure to 'collaborate' (that is, to make a demonstrated effort to share information and build knowledge across institutional boundaries) has its roots in the very nature of the intelligence community. This community is a set of institutions that are, in turn, composed of smaller units – such as directorates, units, divisions – each of which has its own mandates, focus areas, and interests. The analyst thus operates with a set of 'nested identities,' *all of which are operative at any given point in time*, but which may vary in influence and impact on the analyst's behavior over time and situation. Since any decision to release information has the potential to boomerang in disruptive ways on the institution and the individual that released it – and since analysts operate with multiple, nested identities – they must negotiate their institutional allegiances with themselves as well as with others in every encounter.



Figure 3: Nested identities in IA-1

Furthermore, ‘collaboration’ is not an event narrowly bounded by space and time. As observations in IA-2 showed, it requires a notion of intelligence-as-process. The analyst is only one node in a very complex operation that involves institutional power, resources, personnel, assets, and processes. Any type of analysis consumes organizational resources. Every intelligence organization must balance its interest in acquiring and processing all information with limited resources which require it to focus in some way. Technology-based tools that change that organizational focus also impact resource allocation and ownership and the associated power structures. This has a large impact on the potential for tool utilization.

The highly consequential nature of intelligence products, both strategic and tactical, imbues all parts of their development with political and operational dimensions that have significant implications for analyst activity. The intelligence community both produces information for the consumption of decision makers who have political impact, and is itself a highly politicized world. Analysts who release information are not just responsible for their areas of responsibility narrowly defined: they have to consider

possible ramifications for their coworkers, for the institution, and even for the 'national security' community. Thus the collaboration activity simultaneously is formed by and informs the analyst's identity and her impact on others in the intelligence process.

If the changed nature of the information is to be accepted, the analyst and those in the decision chain must have trust in the technology – must believe that the technology actually does what it says it does. It would be an interesting follow-on study to develop how this kind of trust is developed, established, and communicated in these types of environments. The researcher could look at questions such as the impact the level of operator familiarity with technology in general has on his ability to trust new technologies, and the relative importance of the trust in the individual passing on the data vice trust in the technology which produced it.

It also would be fruitful to observe some environment where a technology had been deployed that required use practices significantly out of synch with existing practices or with CONOPS. How do analysts operate in that kind of environment? Where does an impetus to change practices arise? For purposes of this study, however, this forces the recognition that a clear understanding of existing general business practices or CONOPS, of changes required for utilization of the proposed tool, and of a plan to effect those changes are an integral part of the technology development process. Without them, we assert that the chances for the fielded technology to be fully utilized are significantly reduced.

The lessons for the KDD program are important ones. Our research clearly showed that tools that support collaborative activities do not operate in isolation from the social environment within which they are deployed. As the analytic environment varies tremendously from within and across organizations, so too do the needs of analysts. A narrow focus on technology *qua* technology, without due consideration of the social environment within which the tool will be embedded, will significantly reduce its likelihood of use. These factors in combination suggest that the definition of 'collaborative technologies' must be broadened beyond the narrow definition of software-hardware combinations to include full consideration of the use environment. This 'use environment' needs to go far beyond the traditional assessment of the relationship of a single individual to the tool to considerations of the user-in-organization. Without recognition of the rich socio-cultural dimensions of the use environment, the KDD program (and other tool developers) runs the risk of developing elegant but unused technologies.

List of References and Suggested Readings

- Agar, Michael. 1996. *The Professional Stranger*. San Diego, CA: Academic Press (Elsevier Science).
- Betts, Richard. 1978. "Analysis, War and Decision: Why Intelligence Failures are Inevitable." *World Politics* April: 61-89.
- Davis, Jack. 1999. "Improving Intelligence Analysis at CIA: Dick Heuer's Contribution to Intelligence Analysis." Introduction to Heuer, Richard, *The Psychology of Intelligence Analysis*. Washington, DC: CIA Center for the Study of Intelligence. Available on the World Wide Web at <https://www.cia.gov/csi/books/19104/index.html>.
- Glaser, Barney G and Anselm L. Strauss. 1999 (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. New York: Aldine de Gruyter.
- Haraway, Donna. 1991. *Simians, Cyborgs and Women: the Reinvention of Nature*. New York: Routledge.
- Heuer, Richards. 1999. *The Psychology of Intelligence Analysis*. Washington, DC: CIA Center for the Study of Intelligence. Available on the World Wide Web at <https://www.cia.gov/csi/books/19104/index.html>.
- Johnston, Robert. 2005. *Analytic Culture in the US Intelligence Community: An Ethnographic Study*. Washington, DC: CIA Center for the Study of Intelligence.
- "Knowledge Discovery and Dissemination Program Staff. November 2005. "Knowledge Discovery and Dissemination Program (KDD) Focus, Process, and Instructions for 2006" Washington, DC http://mentoring.isi.edu/YoungScientists/Download/2006/2006-03-29_KDD-BAA.pdf
- Merton, Robert. "Bureaucratic Structure and Personality." *Reader in Bureaucracy*. Editors Robert K. Merton, Alisa P.Gray, Barbara Hockey, Hanan C. Selvin. New York: The Free Press, 1952.
- National Commission on Terrorist Attacks upon the United States. 2004. *The 9/11 Commission Report*. New York: WW Norton and Company.
- Parsons, Talcott, *The Structure of Social Action: A Study in Social Theory With Special Reference to a Group of Recent European Writers*. 1937. Glencoe, Illinois: The Free Press, 1949.

UNCLASSIFIED

DRAFT

DRAFT

Do not cite or quote without authors' permission

- Pechan, Bruce L. 1961 [1995]. The Collector's Role in Evaluation. 99-107 in Westerfeld, H/B., ed. *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992*. New Haven, CT: Yale University Press.
- Richelson, Jeffrey T. 1999. *The US Intelligence Community*. Boulder, CO: Westview Press.
- Rittel, H., and M. Webber. 1973. "Dilemmas in a General Theory of Planning." 155-169 in *Policy Sciences*, Vol. 4. Amsterdam, NL: Elsevier Scientific Publishing Company.
- Strauss, Anselm and Juliet Corbin. 1998. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA: Sage Publications.
- Sims, Jennifer. "Understanding Friends and Enemies: The Context for American Intelligence Reform." *Transforming U.S. Intelligence*. Editors Jennifer Sims and Burton Gerber. Washington, DC: Georgetown University Press, 2005. 14-31.
- Treverton, Gregory. 2003. *Reshaping National Intelligence for an Age of Information*. New York: Cambridge University/RAND Corporation.
- Turner, Michael A. "A Distinctive U.S. Intelligence Identity." *International Journal of Intelligence and CounterIntelligence* 17 (2004): 42-61.
- Turnley, Jessica Glick. *Implications for Network-Centric Warfare*. Hurlburt Field, FL: The JSOU Press, 2006. JSOU Report 06-3
- United States Government, 108th Congress. *Intelligence Reform and Terrorism Prevention Act of 2004*. Public Law 108-458. 2004.
- United States Government, Department of Defense. "DoD Dictionary of Military and Associated Terms. Joint Publication 1-02. 2006. <http://www.dtic.mil/doctrine/jel/doddict/> accessed January 2007
- Weber, Max. 1947. *The Theory of Social and Economic Organization*. New York, NY: The Free Press.
- Westerfeld, H. Bradford. 1995. *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992*. New Haven, CT: Yale University Press.
- Wilson, James Q. *Bureaucracy: What Government Agencies Do and Why They Do It*. New Edition Basic Books, 2000.