Studies in Intelligence Vol. 47 No. 1 (2003)

Failing to Keep Up With the Information Revolution

The DI and "IT"

Bruce Berkowitz

During 2001-2002, I was a Scholar-in-Residence at the Sherman Kent Center for Intelligence Analysis, the "think tank" attached to the CIA's training center for analysts. The CIA has long used such scholars as expert analysts, but the Kent Center wanted to try something new: using an outside scholar to study the process of analysis itself. In particular, I was charged with looking at how the Directorate of Intelligence (DI) uses information technology (IT), and how it might use this technology more effectively.

My approach was to watch as many DI analysts as practical and ask them how they performed their work. We discussed what kinds of tasks were hard to do and what technologies or procedures seemed to work smoothly. We also talked about their own ideas about how they might use IT more effectively.

I met with three dozen analysts over six months. The sessions ran from about an hour to more than three hours. The analysts ranged from new employees to DI veterans with ten or fifteen years of experience. My sample included a mix of analysts from geographically focused offices in the DI and cross-directorate "centers" that address transnational issues. In addition, I met with several CIA and Intelligence Community (IC) managers, DI technical security staffs, and program managers at In-Q-Tel, the CIA's experiment in venture capital and commercial information

xp pit
technology.

For the sake of comparison, I also met with analysts at other IC agencies and researchers at organizations that perform functions similar to those of the DI (e.g., the Congressional Research Service; *The Washington Post*; and business risk assessment services). Finally, I drew on my own experience in business and non-government research institutions.

In sum, I was able to observe at close quarters and in great detail nearly 100 analysts, technicians, and managers in the business of producing national security analysis. Moreover, from my vantage point, I was able to watch the DI respond to the terrorist attacks of 11 September 2001 and ramp-up for the war on terrorism.

I came away from this experience impressed by the quality of DI analysts, but also concerned about their lack of awareness of and access to new information technology and services that could be of critical value to their work.

The DI Work Area

At first glance, the equipment at a DI analyst's desk does not look much different from what one finds in the offices and cubicles at most research organizations. But there are some significant differences, and even the small ones can have a huge effect on how an analyst works.

The basic DI work area consists of at least two computers linked to a single monitor, a secure telephone, and a commercial telephone. One of the two computers is connected to the CIA's classified network and is approved for most levels of classified work. The second computer is usually for Internet access from the Agency service provider and is not approved for any classified work. A switchbox allows an analyst to shift from one computer to the other, and eliminates the need for duplicate keyboards, mice, and monitors.

Almost all CIA activities are conducted on the classified network. The unclassified computer is used mainly to browse the Internet and send unclassified e-mail. It is possible to move data from a lower classified network to a higher classified network, and to move data from the

a high
classified network to portable media, using one of the authorized processes or systems. Sending data to comparably cleared individuals outside the Agency network via classified e-mail is possible, via an interface with an IC e-mail network that has become markedly easier to access in recent years. Despite improvements, however, this Intelligence Community e-mail connection requires unfamiliar addressing protocols and offers no searchable directory. This, of course, undermines the speed and convenience of electronic communication.

Until a recent one-way transfer capability was introduced, DI analysts lacked any direct connectivity to the secret-level SIPRNET system used throughout the DoD community as the standard means of electronic communication. For the past year, DI analysts who obtain SIPRNET accounts have been able to receive incoming SIPRNET e-mails in their Agency e-mail inboxes, but not send outgoing SIPRNET e-mails. That is, data can "move up" to the higher classified Agency network but not "down" to SIPRNET. To send SIPRNET e-mails, analysts must go to separate SIPRNET terminals. Until recently, few such terminals were available in CIA workspaces. The number of these terminals has risen sharply since mid-2002, but they are not yet a standard part of the analyst work area, let alone integrated into a single terminal.

Security processes and regulations also dictate how the DI disseminates its products. For example, although Intelink—similar to a classified World Wide Web—receives much attention in the press, many highly classified CIA products are not posted there because, once a document is posted, the Agency cannot control further dissemination. The CIA does post almost all of its products on CIASource, a website maintained on the Agency's network that is linked to Intelink. However, only approved outside users—who must be individually authorized and have access to specifically designated computers—can retrieve documents from CIA-Source. So, a person can have a non-CIA Top Secret/SCI clearance, and even be cleared to read the material on CIASource, but not have either the CIA network access certification or the equipment able to access the website.

The result is that DI analysts work in an IT environment that is largely isolated from the outside world. If they need to do work that is classified in *any* way, there is virtually no alternative other than to use the CIA's own, restricted system. DI analysts can use their unclassified computer connected to the Internet, but this is suitable only for material that is *completely* unclassified.

There is no middle ground. Moving from one environment to another is, for the most part—and despite recent improvements—still anything but a natural process. All of this has the effect of making it hard for DI analysts to interact even with the classified outside world. The CIA view is that there are risks to connecting CIA systems even to classified systems elsewhere. But current arrangements to mitigate those risks send implicit messages to analysts: that technology is a threat, not a benefit; that the CIA does not put a high priority on analysts using IT easily or creatively; and, worst of all, that data outside the CIA's own network are secondary to the intelligence mission.

Databases and Search Tools

The DI has used automated databases since the 1970s and has gradually improved its capabilities. For the typical DI analyst, the most-used database is CIRAS (Corporate Information Retrieval and Storage). With CIRAS, analysts can perform most searches for source documents from CIA archives at their desks and retrieve the documents electronically.

The CIRAS database contains source documents from a variety of CIA entities and IC agencies. An analyst can search CIRAS by using a key word search profile. Most analysts have profiles that they have tuned through experience, so that by entering their profile each day, they can keep up with the "take"— that is, new documents that have been added to the collection.

CIRAS is an improvement over earlier systems, but compared to systems available in the outside world, the search and networking capabilities of CIRAS are primitive. One indicator of CIRAS's shortcomings is simply the fact that an important part of a DI analyst's tradecraft is building an informal source network. A good analyst either knows someone, or "knows someone who knows someone," at another office or organization who can get the information they need. A good analyst will use these contacts to develop more leads in the process.

This, of course, is exactly what the World Wide Web does in an automated fashion when it is combined with a search engine like Google or Alta Vista. Unfortunately, DI analysts lack this capability for most classified

information, and their own information environment is so segmented that it would be cumbersome to perform such searches in any case.

The DI has planned for several years to deploy an IT architecture that would enable the directorate to communicate and exchange data more easily and allow analysts to move quickly from one data source to another. But these plans have not been implemented because the money has not been available.

Despite what one sees on TV, there is not much "gee wiz" software at the typical DI analyst's desk. A few analysts use some specialized tools for sorting and displaying data (e.g., terrorist networks), and analysts who cover the more technical accounts use computerized models (e.g., analyzing the performance of foreign weapons). But these are the exceptions.

One reason is that DI offices cannot easily get funding for new software packages. The funding required for the development and testing of such tools—typically, tens of thousands of dollars per year—is small in comparison to the CIA's total budget. But it is enormous in the context of the discretionary funds that an individual office has—let alone an individual analyst.

Even if more money were available, however, the DI would not be able to use information technology effectively unless it changed its mode of operation and culture. CIA and DI policies and practices create five kinds of constraints that prevent the DI from acquiring new IT and using it effectively.

Security and IT

Security is probably the single most important factor that prevents the DI from applying information technology more effectively. Security is absolutely essential for intelligence, of course. The problem is that, when it comes to IT, the CIA's approach is not "risk management," but "risk exclusion." It is rare for anyone to do a formal cost-benefit analysis for a security rule affecting the use of IT, and hardly anyone asks whether a proposed rule will affect the ability of analysts to do their work.

Until recently, for example, Palm Pilots (along with handguns and explosives) were forbidden in CIA facilities. The CIA only slowly brought the Internet into Headquarters, and took even longer to put it at the desk of each analyst. Analysts cannot develop skills in using these technologies unless they can use them in their day-to-day work. By delaying or excluding the technologies, the Agency is allowing DI analysts to fall behind their outside counterparts in knowing how to use IT in their work, and is preventing DI analysts from integrating these technologies into DI tradecraft.

Such exclusionary rules also send an implicit message to DI analysts that information technology is dangerous and not essential for DI analysis. DI analysts are, by the nature of their work, especially aware of security threats. So when they are told that a technology is potentially dangerous, their instinct is to avoid it unless absolutely necessary. Over time, these security policies, prohibitions, and warnings have had a cumulative effect, so that many, if not most, DI analysts have become wary of IT in general. At best, they think that it is too risky to be worth the bother.

It is interesting to compare the CIA's approach to IT security with the private sector's approach. A few months ago, I attended a meeting in which I happened to sit next to the CEO of one of the leading manufacturers of portable computing systems. He was using a laptop to take notes. I was shopping for a new computer myself, so I asked him about it during a break. The CEO told me that his laptop was his *only* computer. He did all of his personal and business work on the machine.

When I asked him whether he thought it was prudent to keep internal information about a $1.8 billion company on a laptop, the CEO explained that he was well aware of the risks. That was why he kept his most sensitive data on separate media and encrypted his files (including temporary files used by programs). He also used strong passwords, firewalls, and virus protection, and his computer contained some additional tricks that would make his data useless if the machine were stolen. The CEO understood the risks, but realized that the cost of doing without the technology was too great. So he became more knowledgeable about the threat and took precautions.

If the DI expects to develop a more agile organization, it will need a similar approach—not only with laptops, but also with technical security in general. Instead of blanket rules, security must become integrated into DI tradecraft so that analysts can secure a personal information space.

Security staffs must develop a better understanding of how analysts work. Rather than simply excluding technologies, their goal should be to develop methods of applying IT that are so user-friendly that DI analysts can operate securely with as few hindrances as possible.

By making technology a bogeyman rather than an ally, the CIA is reinforcing the well-known tendency toward introversion among most DI analysts. IT would not only help to avoid this; it would subtly encourage analysts to expand their horizons.

Challenges of Compartmentation

Despite decades of trying to reduce the barriers between the Directorate of Intelligence and the Directorate of Operations (DO), sharp divides still exist. The DI and the DO, for example, have separate databases and separate IT architectures. Several DI analysts even told me that they had a better working relationship with their counterparts at NSA than with their own CIA colleagues in the DO.

The CIA already has experience that proves the gulf between the directorates is not inevitable. DI and DO personnel, for example, work well together in the Counterterrorist Center (CTC), which falls organizationally under the Director of Central Intelligence (DCI). In CTC, DI and DO personnel work side by side. As a result, DO officers treat DI counterparts like full members of "the team." DI analysts in CTC have access to DO databases and tools that few analysts elsewhere in the DI can tap into. By working closely together, DO staff members come to know their DI counterparts better, understand how essential they are to the process of intelligence, and are more willing to provide them with information.

Procurement Protocols

Even if CIA managers agreed today to put a new computer, integrated software suite, and data links on the desk of every DI analyst, one would not see many changes for two to three years. This is partly because CIA

y chang e y his is p tly b
acquisition is paced by the annual federal budget cycle, and partly because of the CIA's own procedures.

Thanks to the budget cycle, it takes one year to develop a new IT plan for inclusion in the CIA's budget request; one year to pass the required legislation; and one year to buy and install the system. But this is only if the process moves without a hitch, which, of course, is rarely the case. It usually takes more than a year for the CIA to develop a plan for an IT upgrade. Requests for equipment often fall under the "cut line" the first time they are proposed, or they are funded in the always-elusive "out years." And the legislative process is a complex phenomenon that has been the subject for countless texts, dissertations, documentaries, and abject wonder.

Clearly, CIA procurement is not a process that is running at "Internet speed." Once DI managers manage to put *something* on their analysts' desks, only a masochist would soon dive into the process again. Other matters need attention—like producing intelligence.

Many DI analysts and managers say that IT acquisition has actually become worse in recent years as the CIA has centralized the IT procurement process. The goal was to streamline procedures and produce an integrated IT architecture. The DI, however, is a small player compared to the DO and the Directorate of Science and Technology. As a result, centralization has made the IT acquisition process less responsive to DI needs, not more.

Coordination and Review Bottlenecks

One of the DI's core beliefs is that coordination improves the analytic product. This idea goes back to Sherman Kent, William Langer, and other founding fathers of the analytic side of the CIA. Most were college professors who viewed coordination as the counterpart of the peer review process in academia.

The problem is that coordination can defeat the direct interaction that modern IT makes possible. Networks allow officials to skip several echelons of bureaucracy and permit analysts to respond directly to users—but not if requirements for coordination prevent them from doing so.

I heard widely divergent views on whether traditional DI coordination is having a good or bad effect today. Some DI managers strongly favor the traditional approach because collective responsibility makes the DI different from other information sources. Others believe just as strongly that the traditional DI approach is slow and out of step with how information consumers have changed. They argue that consumers often want the direct response of a trusted expert rather than the corporate voice of an organization.

The bottom line is that before the DI can determine how to use IT effectively, it must decide on its policies for coordination and review. Currently, the DI is ambivalent about whether it will use the new technology to its full potential, and in a manner that other analytic services are adopting.

One underlying issue is quality control. The traditional DI process ensures quality by employing multiple layers of managerial review of each product. But this is only one approach to quality control. Other organizations ensure quality by focusing on the people in the organization, rather than on each product. In other words, instead of doing quality control in the production process, they do their quality control in the promotion process.

It would seem that a 35-year-old DI analyst with ten years of experience ought to be able—routinely— to take calls directly from, say, an NSC staff member and give an assessment of whatever topic he or she specializes in. The experienced analyst ought to be expected to reflect the prevailing DI view, noting where there is important uncertainty or disagreement.

Inefficient Resource Management

The DI does not use technology for managing people effectively. One reason is that the DI has no process for assigning the time of a particular analyst to a particular task requested by a particular consumer. This may seem like a mundane issue, but it has large implications for the ability of the DI to use IT, and for the agility of the DI.

In the business world, managers routinely use software tools to move people quickly from one task to another. These tools tell them how their

staffs are allocated, and thus they can assign and reassign people more efficiently and effectively. Some government organizations also use such tools. For example, the Congressional Research Service (CRS) logs requests into a central accounting system, and assigns analysts to tasks in a manner analogous to how businesses assign analysts to charge numbers. CRS managers can always download an up-to-date record that analyzes its workflow, allocation of personnel, and the status of requests.

Some people I spoke with were concerned that such a "billing system" would focus DI analysts too much on current events. To avoid this problem, the DI could have an "overhead account" that analysts would bill their time to so that they could cover long-term issues—that is, questions beyond what consumers were currently asking.

The information generated by this kind of system would provide the DI a better estimate of how much effort is used (and is needed) for specific kinds of products. Also, such information would justify DI budgets to the DCI, OMB, and Congress. It would show, for example, when the DI has unused capacity— or, more likely, when the DI is being asked to perform more work than is reasonable or even humanly possible.

Long-Term Implications

By not encouraging analysts to use information technology more creatively, the DI is hurting its future. Most "killer apps"—unusually powerful and effective applications software developments—originate from users, not programmers. The first step in developing software is recognizing that a need exists, and users are the ones at the scene who know what they need. That is why the best source of new ideas for relevant IT will most likely be the DI itself, not Silicon Valley.

Consider for a moment one of the most famous user application software systems, the spreadsheet program. Dan Bricklin, a business administration student at Harvard, originally came up with the idea for an automated spreadsheet in the mid-1970s. Bricklin then contacted Bob Frankston, a computer science engineer from MIT. Together, they designed VisiCalc, which they later sold to Lotus, which developed it further into Lotus 1-2-3. Microsoft eventually adapted the idea into an application for the Macintosh—the program we now know as Excel, which

pplic e pr g
was adopted for virtually all personal computers.

If Bricklin had been in today's DI, he would have been told first that the tools he saw on his computer were all that he would need for his job. Then, he would be told that new technology is generally risky and that he did not have any time for talking about his tradecraft with a programmer. Finally, he would be told that no money was available to pay the programmer to develop a prototype.

This is essentially the situation we have in the DI. To be sure, In-Q-Tel is developing some very advanced IT, but In-Q-Tel is—by design—outside the DI mainstream. There is a gap between the people who understand the analytic problem intimately and the opportunity and resources to address the problem with technology.

Technologies That Could Help

During the course of my project, I saw several opportunities where IT could facilitate DI analysis or make the DI a more agile organization. Many others probably exist, but these examples illustrate how the DI is missing the boat. All of the ideas use off-the-shelf technology. All aim at supporting the tradecraft that DI analysts currently use, rather than forcing analysts to change their methodologies to accommodate new gizmos or software. All aim to maximize the payoff from the current DI analyst workforce.

Analyst Websites. One of the obstacles to moving DI analysts to new assignments is the challenge of bringing them up to speed on new substantive accounts. Currently, only two options exist: the analysts currently covering the accounts can take time off and brief the new team members; or the new analysts can try to find their way around by performing CIRAS and CIASource searches or plodding through folder after folder of hardcopy.

If analysts had personal websites on the CIA classified network, they could post links to all of their products as they are written. New analysts assigned to the account could then simply go to the website to get "read in."

NSA analysts use similar technology to grapple with a problem like the one

that the DI faces. One of the hard parts of cryptanalysis is developing an "attack" on a particular communications network. But, once an analyst figures out the step-by-step process to crack a system, he or she can post the attack plan on the NSA network. That way, others can try it themselves without bothering the analyst.

A DI analyst's publications are analogous to the NSA analyst's attack plan —they contain the knowledge that the analyst has developed by covering an account. A personal website would be an efficient way to capture this knowledge and make it available to others without taking the original analyst off his or her assignment.

Integrated Workstation Assistants. Every day, DI analysts sit at their workstations and read through the daily take. They look at a variety of data from a variety of channels: CIRAS, domestic and foreign media reports, e-mail from other analysts, and so on. This labor—expert analysts working in specialized fields, retrieving data, filing them, and making mental links between items of strategic interest to US officials—is valuable intellectual property. In fact, it may be the most unique "value-added" product the DI generates.

Simple IT could make it possible for analysts to develop this knowledge more easily, capture it, and make it available for other analysts and intelligence consumers. A tool like a Google Search Appliance at their workstation would permit them to perform Boolean searches through their personal files. Several analysts could pool their personal files together and conduct combined searches, cross-correlations, etc. Again, this kind of tool would exploit the DI's existing investment in analysts more effectively, and increase the power of their current tradecraft. For example, suppose missile proliferation in a particular country unexpectedly became an issue of concern. It would be possible to network the personal files—including notations—of several analysts from different backgrounds related to the issue: trade, technology, personalities, and so on. Each analyst could search for information throughout the pooled database and identify any links among all of the documents in the datatbase.

HTML Post-It Notes. One DI product that has become popular in recent years is the "annotated cable," in which an analyst reviews a raw intelligence report, adds commentary or new information, and passes the cable on to a consumer. The annotated cable combines the "hands on" feel of raw intelligence with the context and depth of analysis.

If the DI had an integrated web-based environment, "HTML Post-It Notes" could be used to annotate cables. The Post-It would show the analyst's comments and could include links to other relevant DI products and DO cables; the analyst's website and e-mail address; and additional information that the analyst thought important. This would increase the power of an analytic cable and promote networking among analysts and consumers.

This technology would raise issues concerning security and chain of command. Another way of looking at the problem, though, is that this is exactly why the CIA and the DI need to re-examine policies and practices for security, compartmentation, and coordination and review.

Recommendations

The CIA currently is developing a comprehensive plan to improve the information technology available to DI analysts. For this program to be effective, the effort must be combined with a re-examination of policies, practices, and culture.

One step that DI managers could take that would be fast, cheap, and useful, is simply to make it clear to analysts that the DI expects them to be aggressive and innovative in using IT. Currently, analysts are getting a mixed message.

In addition, leaders should make sure that the DI has a "go it alone" option for its most important IT upgrades. The directorate needs to be confident that the really important upgrades will survive the setbacks and budget cuts that will inevitably slow improvements in the CIA's IT architecture as a whole.

The most critical upgrade for the DI is deploying a fully integrated workstation that allows DI analysts to move easily among programs, databases, and security levels. In addition, the DI should put a high priority on introducing SIPRNET— DoD's SECRET-level network—into each workstation. SIPRNET may become the nucleus of a secure communications system for homeland security (that will include law enforcement and emergency response personnel, in addition to a broad set of military users). Use of SIPRNET would also give DI analysts an IT