

1 May 2000

NOTES FOR 15 MAY 2000 INFORMAL PRESENTATION AT OSS CONFERENCE

**INTELLIGENCE ANALYSIS IN A NEW CENTURY:
A CUMUDGEON'S VIEW**

Jack Davis

1. Our OSS host, Bob Steele—who is definitely a pathfinder for intelligence for the 21st century—has been kind enough to give me the opportunity to say a few words about what made intelligence work effectively in the 20th century.

2. I started work as a CIA analyst in 1956. The Agency is still paying me for what I know, and what I put up with, in the year 2000. But in my view the "New Century" does not start until 2001. At least until then, I remain a student of analysis in the "Old Century."

3. I assume that most members of my audience are New Century leaders engaged in reinventing intelligence analysis to take account of the Information Revolution. I admit that, because of this Revolution, much of the old ways of doing the intelligence business are best archived to personal story telling and institutional history. But leaders of the New Century ignore some Old Century wisdom at their peril. New Century leaders should balance their understandable enthusiasm for new processes with respect for constants in the game, so to speak, *of men of the word serving men of the sword.*

4. I have a short list of thoughts to mull over in the New Century, some of which represent a restatement of points from my *DI Analytic Tradecraft Notes* which have been made available to you.

5. But first a word on my authority to speak doctrinally about intelligence analysis. The views I present here are mine, based on my experiences and my biases. They should not be taken as the official views of the Agency or its leaders.

6. You will have to decide on the basis of your experiences and biases how seriously to take the following list of recommendations.

1. On most issues, unbridled pursuit of "being first to know" is a losing game.

Effective analysis in support of decisionmaking takes three main ingredients: information, expertise, and tradecraft. Information will always be by far the most expensive component.

But take care not to exhaust your budgets here—whether for secrets or for OSL—at the expense of expertise and especially tradecraft.

Even someone as technically challenged as I, can reach the conclusion that in the New Century only the biggest and richest vendors of news and views can prevail regularly in the game of being the first to know. Even if Congress continues funding at today's levels, the IC will have to decide on which issues it is worth competing to be the first to know—with the media, the chattering classes, the Internet, and OS companies with state of the art search tools.

Of course there are issues heavy in strategic national security importance and laden with secrets on which, say, CIA has to be the first to know. Private intelligence firms working with Open Sources will likely have their own proprietary accounts—those on which they will sweat to be first to know.

But most subjects on which policy decisionmakers and other clients of analysis insist on being kept informed will be open more or less equally to all collectors and commentators. Regarding speed, big guys like the media and specialized correspondents with E-mail access are going to win the competition to be first to know much of the time.

In the end, every effort to be the first to know entails costs as well as benefits. Especially opportunity costs. If you look at US intelligence analysis in the 20th Century, you will see it started out staffed mostly with easily-trained Cipher Clerks as the information managers of the military commander and other decisionmakers. Only in the last half of the century did the highly-educated analyst become what Sherman Kent referred to as the *intelligence device supreme*.

I do not know at what point, but at a certain point of pursuit of being the first to know across the board, I fear the intelligence analyst will again become a Cipher Clerk. With increasingly heavy investment in obsolescing technology, that's all that intelligence may be able to afford. For some private sector information-management firms that is good news. For most, I believe, it is fair warning.

2. Being the first to understand is a necessary but not sufficient component of competition for the respect and patronage of decisionmakers and other clients.

Substantive expertise, understanding the context and implications of available information, is essential for analysts to compete to be the "intelligence device supreme," but the OS revolution is going both to increase the number of and to reduce distinctions among experts.

The Directorate of Intelligence and other IC and OS components are on track in increasing investments in the substantive expertise of their cadres. The increased

volume of available information requires more and more expert boxes—or nuanced contexts—to ensure effective support of clients.

But I believe the OS revolution among other driving forces is going to continue to expand greatly the numbers of reasonably well-informed authorities on subjects related to national security. Take a look at the issue of Castro's Cuba, which has been continuously important to the USG for over 40 years.

When I started in this business in the late 1950s, I think you could fit around a large conference table all of the Cuban specialists worth listening to in and out of government, and you could fit in a small bookcase all the pertinent OS literature helpful for understanding the so-called "intelligence traffic."

Today, you would need the conference facilities of a large hotel, a sizable library, and a multi-layered set of electronic folders. Decisionmakers, to put a point on it, are less dependent on IC analysts or any single set of OS analysts for the expertise for evaluating and structuring information on issue after issue affecting the national interest.

I fear that for IC units and OS units alike, with the exception of maybe a handful of issues, the effort to excel—to gain the authority to speak to decisionmakers—through command of unique substantive expertise will be an investment in an increasingly-expensive game of catch-up.

IC and OS cadres will be good enough to do the job, and impressive to some clients. Most of the time, though, they will have to compete for the attention of clients not only with each other, but with the clients' immediate staffs, and with authorities from the university, the think tanks, the media, the business world, USG and foreign officials on the spot. All of the latter essentially accessible to the decisionmaker through E-Mail and its technological successors.

Again, substantive expertise in terms of being the first to understand will be a worthy quest, but, in itself, as unreliable as quest to be first to know for commanding a comparative advantage with the discriminating client.

3. Being first to make a difference to the decisionmaker is the only thing sure to pay the bills for increasingly costly all-source information and substantive expertise.

To the extent that most clients of intelligence analysis are action officers—whether strategic planners, warfighters, diplomats, law enforcers, or businessmen—purveyors of evaluated and organized information can only make a difference by increasing the clients' ability to take actions that maximize policymaking opportunities and minimize risks.

If my cloudy view of the New Century is to be credited, technological changes will increase the volume of venders of information much faster than the hard-cash consumers. In this context, whether the commodity is spiced with secrets, OSL, or all-source analysis, it will increasingly be competing in a buyers' market.

Indepth intelligence studies, the equivalent of conceptual R&D, will always be needed. And newsletters and other forms of story-telling analysis will have a market if only from habit. But it will increasingly be actionable analysis—difference-making intelligence—that pays the bills for substantive expertise and information hunting- and-gathering.

I am not talking only about current intelligence—vetted information for fighting fires. Analysts can also make a difference by helping clients with contingency planning, strategic directions, and long-term investment choices. The key is analysis that reduces risk and enhances opportunity in these actions.

At least as I read the past and gaze through the fog of the future, *nice-to-know analysis*, often what analysts and their managers are proudest of because it pushes back the experts' frontier of ignorance—will have to compete with more alluring forms of clients' R&R. It will be *need-to-know analysis*—that distinguishes winners from losers.

4. The key to making a difference is knowing your clients' secrets.

Nothing increases the value-added of intelligence analysis more than knowing where the client is on her learning curve and decision cycle. That is, to make a difference with the answer, analysts first must make sure they know the client's precise question.

One can argue endlessly about the relative importance of secrets and OSL regarding the subject matter of intelligence inquiry—whether foreign country or nonstate organization or global issue. But knowing the customer's secrets—her real action agenda—has no OSL competitors. You can learn first or second hand about what the client says, but that will not necessarily tell you what she means. Regarding secrets and OSL here, I am reminded about tradecraft learned half a century ago for playing contract bridge—*one peek is worth two finesses*.

My experience—admittedly limited to national security affairs—is that clients, whether policy decisionmakers or action takers, share their secrets only with intelligence providers who regularly deliver distinctive value-added.

What happens when clients' reputations, not to mention national or corporate interests, are on the line? Consumers of intelligence care less about where analysis comes from in terms of which intelligence institutions and corporate venders, and

more about the tradeoff between the risks and benefits of exposing game plans to "outsiders," who after all, will not take direct hits from policy failures.

That brings my informal discourse to the issue of what gets policymakers to provide feedback and other forms of secret-sharing guidance to intelligence makers—those insights that help in providing need-to-know assessments

5. Evaluation of information for authenticity and diagnosticity is the first key.

The accelerating increase in the availability of information on the broad agenda of issues relating to national security puts an enhanced premium on distinguishing between signal—information that helps get the job done—and noise—information that misleads, confuses, and distracts both providers and consumers of analysis.

I suppose there is someone at this Conference who has done the homework on signal and noise—terms borrowed from communication theory by Roberta Wohlstetter to explain the intelligence and policy failures in her epochal study of the surprise Japanese attack on Pearl Harbor. My own intuitive view is that year by year, important issue by important issue, signals increase arithmetically while noise expands geometrically.

When human behavior is at the heart of the subject—for example, US relations with Russia, China, Iran—and human reporters are the main providers of information—on what a foreign leader said, what he meant, what he will do next—unevaluated information runs a close second in uselessness to no information.

Again, I am speculating on what some at this Conference can address with the benefit of research. I believe the information revolution is providing a field day, not only for sophisticated purveyors of Denial and Deception, but also for enterprising seekers of collectors' dollars and attention, and, not least, that large and wordy gang of self-defined experts who are 90 percent right 10 percent of the time.

I wish I had my notes from Graduate School. But in the late 1930s, the publishers of the first Edition of the Dictionary of American Biography paid academics by the word for submitting short biographies of distinguished dead Americans in their fields of specialty. A study a decade or so after publication revealed that some 13percent of 15,000 distinguished Americans listed in the DAB, for which the scholars already had gotten agreed payment, never existed.

What percentage of information out there *today*—however collected—is about men and events that never existed?

I do not want to get into the specifics of tradecraft for combatting D&D and other means of evaluating information for authenticity. But resolving the tension between

speed and volume of analysis, on the one hand, and reliability of analysis on the other rests with the managers of analysis.

In my view, each production unit should set rigorous standards for testing information for authenticity, raising the bar as the subject becomes more important to the client. The responsible manager should know, through periodic intervention, that her analysts are doing their homework here. In turn, the client should know that what she is asked to rely upon from the supplier of analysis has taken careful account of the credentials, shall we say, of the information.

I will, with your permission, be similarly brief on the issue of diagnosticity. Relevancy—that is the standard of reporting to the consumer information that is relevant to his or her issue—was never a useful standard. Now that all issues are increasingly inter-related, it becomes a more questionable standard. For someone worried about WMD in Iran, for example, what information about Iran, about potential supplier countries and organizations, about regional rivals is not relevant.

Think of diagnosticity in terms of reporting a sick child's symptoms to a doctor over the telephone. That the child is running a fever may narrow identification to some 50 illnesses. If you are to provide actionable analysis you have to report to the doctor those symptoms that narrow the issue to one or no more than a few diseases.

So here too the manager of analysts has to insist on corporate standards for reducing judgment error by deciding which information is most distinctive in distinguishing among, say, competing hypotheses.

6. Corporate standards for challenging assumptions is a second key.

Two lessons from reflecting on my analytic career: (1) most analytic issues were both more complex and their outcome more uncertain than I thought when I worked on them. (2) The human mind, even a fine and experienced human mind, faces many more hard-wired cognitive obstacles to avoiding error in assessing complex and uncertain issues than I thought.

Most of my analytic experience required battles against indeterminacy as well as inadequate information. For example, *when, why, and with what consequences will the dictators of rogue countries X, Y, and Z lose power?* Of course, even the dictators could not know.

Now, available secrets and OS helped address such issues wisely, but not with certainty. Not only was the number of inter-related variables larger than the best minds could handle, but often an overlooked or under-appreciated factor turned out to be the key or driver to the outcome.

My studied estimative judgments about these situations pleased me, impressed bosses, and perhaps helped clients. But when I read some of the assessments I wrote 20 years ago, I cringe about how simplistic my mental model of the issue was.

What is more, the very mental model or mindset that enabled me to meet time deadlines and space limits profoundly affected the way I perceived and weighed information. In the end, I was smart, quick, and, thankfully, lucky to have been mostly right as often as I was.

To cut to the quick here, every information-processing organization needs transparent standards for vetting and challenging assumptions on complex and uncertain issues. Especially under two circumstances. First, when everything falls neatly and quickly into place. Usually, a complex issue does not have a simple answer. Second, when you have worked the same or a similar issue several times—and haven't proved wrong, yet.

Now, determining through experience the precise tradecraft tools and formats that are most effective for vetting and challenging assumptions on a particular issue is important. In some notable ways, every intelligence analysis challenge is distinctive. But even more important, in my view, is having, as with evaluation of information, some common corporate standards by which colleagues can provide constructive criticism and bosses and clients can know that standards for sound argumentation were heeded.

Two sample techniques:

- *Make the key assumptions of the judgment transparent.* Analysts estimate when, after vetting of available information, they do not or cannot know in unqualified terms the answer to an intelligence question. They interpret what Fidel Castro said yesterday about Elian Gonzalez, for example. They predict what he will do if and when Elian returns. Such judgments are based, for example, on inferences about how Castro calculates gain and risk. These assumptions should be put on the table for criticism and refinement. Nothing is more deadly for sound estimating than hidden assumptions.
- *Express clearly levels of confidence in judgments.* Whether the expert (the man of the word) is lawyer, investment advisor, or intelligence analyst, the client (the man of the sword or action-taker) has a right to know his advisor's level of confidence in estimative judgments. Here too I believe analytic organizations should set corporate standards to avoid confusion internally as well as externally. Terms such as *real possibility* and *good chance* should be shunned. Often use of a simple but clear term accompanied by a depiction of general numerical odds help avoid confusion. We judge that "X" is unlikely (less than one chance in five).

7. Lastly, pay more attention to the seemingly unlikely.

What the IC or OS provider calls intelligence analysis, the client calls risk and opportunity analysis. Often a well-structured assessment of a danger or an opportunity that is judged to be only, say, 20 percent likely is more actionable than an assessment that focuses on the much more probable trend or outcome.

To focus on the issue from the point of view of the action officer, clients need to know which unlikely dangers to pay attention to—say through contingency planning—and which longshot initiatives are worth staking a reputation on.

But here, as elsewhere in the relationship between producer and consumer of organized and evaluated information, knowledge of the client's secrets is one key to a favorable reception. Too often, attempts at what is often called "Alternative Analysis"—including Devil's Advocacy, What-If Analysis, and High Impact-Low Probability Analysis—are met with a confused response. The clients' laments include such comments as "What am I supposed to do with this," or "Is this CYA or have you changed your mind."

At the same time, clients complain when analysts feed them a steady diet of assessments that repeat the conventional wisdom on what is probable, especially when this trivializes the dangers they fear most and the policy goals, difficult as they are, that they have come to Washington or corporate headquarters to achieve.

Some tradecraft rules for dealing with seemingly unlikely developments.

- Search for the client's pain or ambitions. That is where alternative analysis is most likely to be welcome.
- State the analytic unit's bottom line judgment and the key assumptions that underlie it.
- State whether the alternative view is held by some analysts or is deliberately developed for the illumination of substantive uncertainty.
- Tie the alternative judgments to alternative assumptions—either about what drives the issue (its not the economy, its ethnic strife) or the assumption about the key variable (it is the economy, but we are talking about dimmer prospects than usually assumed).
- Make it actionable. Remember, most clients are action officers not philosophers. How will US actions or a corporation's actions likely affect the odds and the outcome. The client is the decisionmaker, but the intelligence analyst can point to how his bundle of carrots and sticks could influence events.

01-OSS 21 PRIMER Essential Elements of Information Joint Planning, Operations Other Than War and Open Source Intelligence - Link Page

[Previous](#) [OSS '00 PRIMER 008 Analytic Tradecraft Contents Page \(No Idea Where 007 Went....\),](#)

[Next](#) [OSS '00 PRIMER 008 A Compendium of Analytic Tradecraft Notes by Jack Davis,](#)

[Return to Electronic Index Page](#)