Scientific and Technical Intelligence Analysis

~~SECRET~~

The birth and development of scientific intelligence

Robert M. Clark

In 1939, the British decided to assign a scientist to the Intelligence Branch of the Air Staff. Inasmuch as no scientist had previously worked for an intelligence service, this was a new and revolutionary idea. A tall, solemn physicist named R. V. Jones, then working at the Royal Aircraft Establishment, Farnborough, was picked for the job. Jones's first job was to study "new German weapons" which were believed to be under development. The first of these was a blind bombing system which the Germans called Knickebein. Knickebein, as Jones soon determined, used a pair of radio beams which were about one mile wide at their point of intersection over the city of London. German bombers flew along one beam, and when their radio receivers indicated that they were at the intersection with the second beam, they released their bombs.

At Jones's urging, Winston Churchill ordered up an RAF search aircraft on the night of 21 June 1940, and the aircraft found the Knickebein radio signals in the frequency range which Jones had predicted. With this knowledge, the British were able to build jammers whose effect was to bend the Knickebein beams so that German bombers for months to come scattered their bomb loads over the British countryside. Thus began the famous "battle of the beams" which lasted throughout much of World War II, with the Germans developing new radio navigation

systems and the British developing equally effective countermeasures to them.

Jones went on to solve a number of tough Scientific and Technical Intelligence problems during World War II and is generally known today as the "father of S&T Intelligence." The basic principles of S&T Intelligence analysis which Jones worked out during World War II and which have been previously discussed in *Studies in Intelligence*[*] are just as useful today as they were in the beginning.

Purpose of S&T Intelligence

The primary purpose of S&T Intelligence since Jones's day has been *to identify new enemy weapons and to describe their characteristics.*

Once you know the characteristics of an enemy weapon system, then his tactics and strategy for using the weapon system follow naturally. If, as a result of a heavy research, development, and testing effort, the Soviets manage to squeeze the accuracy of a particular ICBM down below .25 nautical miles CEP, then the primary target of all such ICBMs is almost surely going to be U.S. Minuteman missile silos. If the ICBM has no better than one-half nautical mile accuracy, then it probably will be used against cities, industrial complexes, and other soft targets. As another example, the range of the Soviet BACKFIRE bomber is a critical factor in determining whether BACKFIRE is intended for use against ground targets in Western Europe and for naval use, or whether it is intended for. strike missions against the Continental United States.

Also, once you know the characteristics of an enemy weapon system, countermeasures against that system become much easier. For instance, we knew a great deal about the SA-2 surface-to-air missile system which was deployed extensively to defend North Vietnam. When the decision was made to launch mass raids against North Vietnam with B-52 aircraft, we were able to tailor our countermeasures against the SA-2 so well that on some raids the North Vietnamese SAM system was almost completely ineffective. On the other hand, we knew very little about the SA-6 SAM system which was deployed in Egypt prior to the Yom Kippur War. Largely as a result of this lack of knowledge, countermeasures against the SA-6 were not effective and the Israelis

lost large numbers of their strike aircraft to Egyptian SAM systems.

Cases of S&T Intelligence

Jones found that all the S&T Intelligence problems which he encountered fell into three general cases. Unfortunately, since Jones's time, S&T analysts have had to contend with a fourth case.

S&T CASE #1:

WE DEVELOP WEAPON —

THEY DEVELOP WEAPON

This is the most common problem encountered by S&T intelligence officers. We develop an ICBM — the Soviets develop an ICBM. We put MIRVs on our ICBMs — they are putting MIRVs on their ICBMs. The Soviets developed an ABM system — we developed an ABM system. Both sides are now developing a laser kill weapon. And so forth. In this case the S&T Intelligence officer's job is not so difficult, because he can turn to his own country's experts on that particular weapon system. Use of your own experts has its own pitfalls, however, as we note later on. A classic example of some of the pitfalls is "The Case of the SS-6."* U.S. ICBM experts, insisting on applying U.S. design approaches to Soviet missile designs, managed to hold up an accurate intelligence assessment of the SS-6 for a number of years.

S&T CASE #2:

WE DEVELOP WEAPONS —

THEY DON'T DEVELOP WEAPONS

In this case the intelligence officer runs into a real problem: it is almost impossible to disprove anything in S&T intelligence. The fact that no intelligence information exists about a particular foreign development cannot be used to show that the development itself doesn't exist. As an Air Force intelligence officer in the early 1960s, I read year after year the USAF estimates that said, "the USSR is probably developing a pulse doppler radar for its interceptor aircraft," and "the USSR is expected to deploy a computerized air defense system similar to the U.S. SAGE system." Years later, the Soviets have still done neither — so far as we can tell. But both estimates are just as difficult to disprove in 1974 as they were in 1964. And the BACKFIRE we mentioned earlier ... how can anyone conclude that the Soviets do not intend to use it as a strategic bomber against the U.S., no matter how unsuited it may be for such a mission?

S&T CASE #3:

WE DON'T DEVELOP WEAPONS —

THEY DEVELOP WEAPONS

This is the most dangerous case. Here the S&T Intelligence officer has to overcome opposition from skeptics from his own country. Very often these skeptics are scientists who themselves tried a similar approach, failed, and then felt themselves obligated to discourage everyone else from trying the same thing.

One of the most dramatic examples of Case #3 was the Soviet development of the antiship cruise missile. Segments of the U.S. intelligence community sounded a warning in the early 1960s that the Soviet antiship missiles represented a real threat to the U.S. surface fleet. The threat was not taken seriously, however, until the sinking of the Israeli destroyer Eilat by an early model Soviet cruise missile in the Six Day War of 1967. Unfortunately, many Defense Department officials then overreacted, and have since repeatedly labeled the U.S. surface

navy "a bunch of sitting ducks."

Analysts in the bacteriological warfare and chemical warfare business will become more and more familiar with Case #3 now that the U.S. has stopped all BW/CW weapons research.

S&T CASE #4:

WE DON'T DEVELOP WEAPONS —

THEY DON'T DEVELOP WEAPONS

R. V. Jones never had to contend with this case, since the British were involved in a war and had no resources to waste on academic problems. Case #4 is the most frustrating; it resembles Case #2, but since we haven't developed the weapons system in question, physical restraints can be ignored and any of the players can change any of the rules of the game at any time. Our first real encounter with Case #4 was the SAM upgrade problem, described by Sayre Stevens in "SAM Upgrade Blues."*

SAM upgrade — the possibility that the USSR could develop a limited ABM defense using the SA-2 (and later SA-5) SAM systems — made life exciting (and frustrating) for many CIA analysts and senior officials. Any time an analyst working on SAM upgrade seemed to be making progress toward a solution, someone would find a new wrinkle in the problem which forced a fresh start. One lesson of SAM upgrade is that we can no longer produce only conventional intelligence assessments. Intelligence analysts will continue to answer questions which read, "What is the capability of weapon system 'X'?"; but more and more analysts will encounter questions which begin "What if ... ?" These are usually the Case #4 questions.

Last summer, DDS&T intelligence analysts had to address the idea that the Soviets might be developing a space-based laser ABM system. This concept was proposed by a senior official of another government agency (interestingly, most Case #4 problems are proposed by people who are outside the intelligence community but have contact with it; seldom if ever are such cases proposed by intelligence officers). The idea was that

the Soviets might be working on a program to put large high-powered ultraviolet lasers into synchronous altitude (25,000-mile-high) orbits. By focusing the laser energy on U.S. ICBM reentry vehicles during their midcourse phase of flight, the Soviets would then be able to destroy any number of the reentry vehicles. The fact that such a program would cost the Soviets more resources than the U.S. put into the Apollo Program seemed to daunt no one — least of all the advocates who insisted that we look for evidence of a Soviet program. After considerable expenditure of analyst time and effort, we concluded that the Soviets were *not* developing a space-based laser ABM system. Unfortunately, this was probably only the initial effort on this particular problem. It seems characteristic of Case #4 problems that they never go away; they simply go through cycles.

Sources of S&T Intelligence

Jones used the analogy of the human head to describe how S&T cases were handled. In his analogy the eyes represented photo intelligence and the ears represented signal intelligence. Both of these intelligence inputs were fed to the brain, which handled the job of collating the intelligence, analyzing what it meant, and making decisions. To complete the analogy, one might consider the mouth to represent the dissemination process.

Despite Jones' comment about the eyes and ears, an S&T analyst normally uses six sources of information in his work. They are:

Photo Intelligence
Signal Intelligence
Human Sources
Foreign Literature
Results of U.S. Work
Basic Physical Laws

Many intelligence analysts refer to the first two of these as "hard" intelligence and the second two as "soft" intelligence. This unfortunate

terminology reflects a common bias that photo and signal intelligence information is more reliable than the other kinds. Actually, human and foreign literature sources have provided some of our most valuable insights into foreign scientific and technical developments. Their evaluation, however, requires more judgment and analytical skill than do the photo and signal intelligence sources.

The last two sources — U.S. work and basic physical laws — are not generally considered as sources of intelligence at all. But these sources tell you what has been done and what *can* be done. And they take as much analytical time as any of the other sources. In some cases, they may take *more* time; some analysts claim that it is easier to get information on Soviet than on U.S. R&D work.

Intelligence analysis — the brain function in the Jones analogy — is the process of pulling together all the sources of information and drawing conclusions. It is a difficult process, probably no better understood than the functioning of the brain itself. There are a few guidelines, however, the most important of which Jones described as "the cardinal principle of scientific intelligence."

The Cardinal Principle of Scientific Intelligence

Back in the fourteenth century, a philosopher named William of Occam did a great deal of thinking about the best way to draw conclusions from the results of scientific experiments. His conclusion has been used as a guiding principle for scientific researchers in all the centuries since. It also serves as the single most important guiding principle for intelligence analysts. It goes under the name of *Occam's Razor: Use the least number of hypotheses to explain your observations.*

Occam's Razor works this way: Suppose that we discover that the Soviet embassy in Washington has received a copy of a classified briefing which was presented recently in the Headquarters Auditorium. I might then announce to you: "The Soviets must have a bug in the igloo — go find it." After you have finished tearing the igloo apart, you come back and report that no bug is to be found there. My reply is: "Do you *really* expect the Soviets to put the bugs out where you can find them so easily? Call in the sweepers!" So after a very thorough electronic sweep

of the wrecked igloo, you come back with a negative report. But I'm ready. "Ah-ha," I say. "It's just as I suspected — the Soviets have developed an unsweepable bug!" As you see, we could carry this game on for quite some time — unless you use Occam's Razor and say, "No! There must be a simpler explanation for our observations."

Now this story may sound a bit farfetched, but it describes the sort of thing that goes on in the intelligence community every day. We recently went through an exercise of this sort with an acquaintance of mine on the Intelligence Community (IC) Staff which ended up with his conclusion that every Soviet satellite had some sort of a clandestine mission. And the only reason we hadn't found out about all these clandestine missions was that we hadn't looked hard enough!

Some S& T Intelligence Maxims

In addition to the cardinal principle, there are a number of rules of thumb which most intelligence analysts learn sooner or later through hard knocks or experience. The first of these is: *Suspect all crusaders.*

An intelligence officer should never have an ax to grind. The day an analyst says to himself, "I'm going to prove ...," he's left the path of reason. Of course you have to present proof for any conclusions you draw from analysis. This is quite a different thing than setting out to prove something before you know the facts. The objective of any intelligence analysis effort is the *truth* — not the proof of some preconceived notion. There probably exists no better illustration of this point than the story of the "SS-8 controversy" which David Brandwein described in the Summer 1969 issue of *Studies in Intelligence* (XIII/3).

In 1961, the Soviets began testing a new missile system, the SS-8. Air Force intelligence analysts concluded very quickly that since the Soviets had a large ICBM (the SS-6) and a small ICBM (the SS-7), the SS-8 would be an even larger ICBM than the SS-6. CIA analysts disagreed. By the beginning of 1962, the intelligence community analysts were divided into two camps — a "large SS-8" group and a "small SS-8" group — and the struggle had all the marks of a full-blown crusade. Neither side would concede that its analysis was less than flawless. Each side searched for evidence to "prove" its case. By the middle of 1962, an objective analysis

of the SS-8 was no longer possible within the intelligence community. The impasse was not broken until an independent and reasonably impartial committee was formed to assess the problem. The controversy did not end completely until 1964, when the SS-8 was photographed in the Moscow parade and turned out to be a small missile. Unfortunately, much time and money had already been wasted because a few people were more concerned with "proving" their case than in finding the truth.

The mark of a true crusader generally is an inability to admit that he might be wrong. The intelligence community seems to have more of its share of crusaders than most government or industrial groups; unfortunately, many of the crusaders are in the S&T Intelligence field — the last place a professional scientist would expect them to be. Professional scientists instinctively distrust crusaders. Crusading is incompatible with the scientific method, which tries only to establish the facts — never to prove something. One of the great scientists of all time, Louis, Pasteur, put it concisely:

> "The greatest derangement of the mind is to believe in something because one wishes it to be so ..."

A second rule of thumb in S&T Intelligence is: *Experts can be wrong.*

Of necessity, the intelligence community has to use experts as consultants. It is often argued that the experts are the best people to do the analysis, but an expert can develop a closed mind in his own field of expertise more readily than the non-expert. Experts are particularly dangerious in S&T Case #3. When Jones concluded his successful analysis of the Knickebein signal, his proposal to send a search aircraft up after the signal was strongly opposed by Britain's leading expert in radio wave propagation — who contended that the Germans couldn't be using such a signal because it would have to bend around the earth's surface to be received over London. Fortunately, Churchill didn't learn of the expert's opinion until after the search aircraft had obtained the Knickebein signal.

A big problem with experts is that they impress people unnecessarily because they are labeled "expert." The expert's opinion may be given more weight than it deserves. Perhaps the mentality of official Washington — which spurns pearls offered by a research assistant for

the dross from a research director — has something to do with the problem. Any intelligence analyst foolish enough to propose a major analysis effort on "Possible Soviet Development of a Space-based ABM Laser Weapons System" would have been laughed at. Unfortunately, the idea was proposed by an expert who happened to be influential, and no one laughed (out loud, at least). We did the project.

Experts tend to be most obstinate when they are in the wrong. A few years ago, CIA analysts were trying to assess a particular Soviet ABM radar, Some experts who were consulted came to the conclusion, based on incomplete information, that it was actually two radars — that a large flat structure located next to the main radar antenna was the antenna for the secondary radar. After we had done some additional analysis and had taken a close look at Soviet antenna technology, it became apparent to most intelligence community analysts that the flat structure was an antenna feed structure, not a radar. The experts dismissed this interpretation, and CIA analysts were obliged to search for a signal from the secondary radar. Finally, the Soviets built an operational version of the radar, the flat structure was replaced by a strange-looking flat apparition which on one in his right mind could call a radar antenna. While conceding that the new flat structure was clearly a feed system for the ABM radar antenna, the experts never did admit that their original estimate of the secondary radar had been wrong. They merely avoided all discussions on the subject. Even today, I occasionally ask one of the analysts who were involved int he project if he has found the secondary radar signal yet. Fortunately, our ABM analysts all have a good sense of humor.

When the expert's opinion differs from all other available sources of intelligence, you have to question the expert's opinion just as you would question any other intelligence source, for reasons which the expert can seldom appreciate. Treat the expert just as you would any other intelligence source; don't worship him. The same could be said for the contractors, who are just another form of expert. Which brings us to our next maxim: *Never trust a contractor.*

This is a bit strong; perhaps I should say "Don't rely unreservedly on a contractor." There are good contractors and bad ones. Note that I didn't say never use a contractor — I said don't trust him. We do and should use contractors in S&T Intelligence analysis to perform jobs which would take too much analyst time, but we tend to depend too much on the contractors. I once asked a good friend of mine, an ABM analyst, about

the technical capabilities of a particular ABM radar he was studying. His reply was "I'll have to check with my contractor first." Giving him the benefit of the doubt, I assume that his remark was tongue-in-cheek. But it points to a dangerous trend in CIA as well as much of the rest of the intelligence community.

Remember, a contractor is in the business for the money, much as a professional spy is in the business for the money. Any case officer can tell you how to treat a professional spy. You use them when you have to, but you never trust them. The same is true for contractors.

We once awarded an electronics analysis contract to Company "Z" on the West Coast. Shortly thereafter, the company "Z" project officer visited Headquarters to receive his instructions on how to proceed. After a few formalities and a cup of coffee, we sat down to discuss the contract details. His first question was unforgettable — and typical of many contractors. He said: "OK — What is it that you want us to prove?" We should have canceled the contract on the spot.

Because the contractor wants to earn the money you're paying him, he feels obligated to come up with *something* — whether there's something there or not. A contractor also knows what every good newspaper man knows: *Bad news sells.* So the contractor is particularly vulnerable to the Anak syndrome (a vulnerability which contractors share with new intelligence analysts who are trying to make a name for themselves).

The Anak syndrome goes back to the tithe when the Israelites found it necessary to spy out the land of Caanan. The spies came back with a completed intelligence analysis which they reported in Numbers 13:32-33:

> "... And they brought up an evil report of the land which they had searched unto the children of Israel, saying, The land, through which we have gone to search it, is a land which eateth up the inhabitants thereof; and all the people that we saw in it are the men of a great stature.
>
> And there we saw the giants, the sons of Anak, which come of the giants: and we were in our own sight as grasshoppers, and so were

we in their sight."

The results of this report were disastrous for the Israelites: 40 more years of wandering in the wilderness.*

Based on previous experience with contractors, I will always be convinced that the next day Moses received a letter something like this one:

Israelite Research Projects Agency
Kadesh 3
Wilderness of Paran

Commanding General
Palestine Liberation Army
Kadesh 7
Wilderness of Paran

Unto Moses, Shalom:

1. Recent intelligence reports indicate that Canaanite Army field units have deployed GIANTS. This unprecedented advance in human engineering on the part of a potential enemy puts our forces at a severe tactical disadvantage. IRPA war gaming analyses indicates that PLA units encountering GIANT — equipped Canaanite units one-on-one would incur 76.8% casualties while inflicting only 16.4% casualties on opposing forces.

2. IRPA believes that the magnitude of this challenge to Israelite survival requires a full-scale R&D effort to counter the Canaanite threat. Accordingly, we are pleased to submit our proposal entitled, "The Feasibility of Developing GIANTS from Israelite Racial Stock."

3. IRPA is well qualified to conduct this R&D effort. Our related experience includes two prior assessments: "The Biological Impact of Locust Swarms on Egyptian Wheat" (Secret/ Israelite Use Only) and "A Tactical Mobility Problem: New Approaches to Crossing the Red Sea" (TS/IUO).

4. We propose to undertake this effort on a cost-plus-fixed-fee basis for a fee of 2,000,000 shekels. The contract effort is expected to be completed in 40 years.

Signed,
Ammiel the Son of Gemalli of the Tribe of Dan
Director of Research

Attachments: Proposal

Our final maxim is an obvious one: *Look at the whole picture.*

Or, to put it another way, never ignore sources of intelligence. This rule may be obvious, but it's one of the most difficult things for an S&T analyst to do. The chief problem is one of available intelligence information. NSA, CIA, and Naval Intelligence Command, to name three groups, have many information compartments. An S&T Intelligence analyst on almost any topic will find that the information he needs is scattered across several of these compartments. And sooner or later, in trying to get the information which he needs out of these compartments, he has to face up to the paradox of *S&T Intelligence: The more important the subject, the more difficult it is to obtain access to the available intelligence.*

This paradox results not from security regulations, but from human nature. Very few intelligence collectors or analysts are willing to reveal (to other analysts, at least) the most interesting and exciting bits of information which they possess. This is due to a fear — often justified — that the analyst to whom you reveal the information will take it, use it for his own purposes, and get the credit for your work.

Almost all intelligence services over the years have paid a heavy price for this over-compartmentation and professional jealousy. Soon after the British began jamming the Knickebein system, Goering became aware that the British knew in advance when his bomber raids were coming. He put together a team of counterintelligence officers to locate the source of the leak. Goering gave them access to all available information *except* the Knickebein project, which he considered too sensitive to release to them. Of course, Knickebein was the tipoff of the German air raids, so Goering's counterintelligence effort was a failure before it started. As another example, Pearl Harbor resulted in part from too much compartmentation; the people at the top didn't have the whole picture.

Even when the information is available to analysts, we don't always use it intelligently. The bias on "soft" vs. "hard" intelligence mentioned

previously is one example. We seem to be training many telemetry analysts, ELINT analysts, photo analysts ... people who rely primarily on one source of information, and use the others as background. Such people are S&T Intelligence specialists. They are not S&T Intelligence analysts.

An S&T Intelligence analyst has to have a sense of perspective. He must have an instinctive feel for what the foreign R&D groups are like their biases, preferred approaches, weaknesses and strengths — and the resources that act as constraints on their developments. You can't get perspective from a single intelligence source. You can't get perspective in three months, or even six months, of intensive work in one S&T subject. It takes years of work, with all the available intelligence information, to gain the perspective and the insights that a first-line S&T Intelligence analyst must possess.

Postscript

This article has addressed some aspects of S&T Intelligence analysis as it has developed since Jones's day. Its stress has been on weapons intelligence, or the application of science and technology for military purposes. In recent years, as the focus of international competition has shifted somewhat from the military to the economic instrument of national power, a new purpose or objective for S&T Intelligence has begun to evolve: to assess the technical capability of our economic competitors (France, Japan, etc.) in the high technology areas of international trade. The S&T Intelligence community is still groping for a role in this rapidly expanding area of civil technology assessment. It is a job which is foreign to much of our past experience. It would be a very familiar role, however, to the industrial espionage group at General Motors which must keep tabs on the latest developments at Ford and Chrysler. Many of the rules discussed above will apply; some will not. The development of ground rules will be an interesting and exciting task in this new field of S&T Intelligence.

Footnotes

*Jones, Reginald V. "Scientific Intelligence," Studies VI/3; and "The Scientific Intelligencer," *ibid*, VI/4.

*Wonus, M. C., *Studies in Intelligence*, XIII/1.

**Studies in Intelligence*, XVIII/2.

*For another View of Moses as policy maker and intelligence officer, see "Decision Trees," *Studies in Intelligence*, XVIII/4.

Posted: May 08, 2007 08:43 AM