(b)(3)-P.L. 86-36

Operations Security Techniques: An Analysis of GIANT SCALE (U)

~~(S)~~ Occasionally, quantitative methods – or operations research techniques, if you will – can be used effectively in attacking complex threat analysis problems which confront the operations security (OPSEC) community from time to time. This is the story of one such case involving a threat posed by North Korean (DPRK) [redacted] to SR-71 reconnaissance operations in the Far East; these operations are known by the unclassified nickname, GIANT SCALE.

Background (U)

~~(SC)~~ In early 1976, [redacted] of GIANT SCALE sorties staging [redacted] the Pacific Command, SAC, [redacted] agreed to collaborate on an OPSEC field survey of the operation. Accordingly, a joint survey team was assembled and tasked to evaluate the planning, coordination, and execution procedures for the missions and to examine such diverse support activities as transportation, refueling, maintenance, and communications. Conclusions and recommendations of that survey have been fully documented in CINCPAC's GIANT SCALE OPSEC Survey Report (1976) and need not be reiterated here. It will suffice to say that several problems were uncovered and that, in February 1977, remedies were implemented which curtailed even the hint of prior awareness for the next fourteen months.

The Problem (U)

~~(SC)~~ But then, beginning in April 1978, [redacted] some concern about the continued effectiveness of OPSEC measures which had been introduced some fourteen months before. When the situation continued into May, CINCPAC decided to take a closer look at [redacted] GIANT SCALE. At issue was whether the North Koreans had regained actual foreknowledge of SR-71 sorties, as some suspected, or whether they were simply guessing.

The Analysis (U)

~~(SC)~~ This posed an interesting challenge to the analysts involved. By special arrangement with [redacted] Through similar arrangements with SAC, it was possible to assemble all relevant operational data for the same period.

~~(S)~~ Formally, the hypothesis to be tested was that DPRK [redacted] had foreknowledge of SR-71 operations [redacted] This turned out to be a relatively complex issue because of various unknowns which had to be reckoned with. For example, what assumptions were to be made about the North Koreans' perceptions and motivations? Which data were relevant and which irrelevant? And, ultimately, how could the issue be decided? Therefore, the analysts decided to examine the hypothesis of foreknowledge from two perspectives:

1. That the North Koreans had prior awareness of all SR-71 sorties [redacted] including both operational missions and training flights, and
2. That the North Koreans had prior awareness of operational missions only.

~~(SC)~~ A third alternative concerning training sorties only was rejected as insignificant from a probability as well as an OPSEC standpoint; training sorties never approached the sensitive area around

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Korea and never entered North Korean radar range. It was also necessary to allow for the possibility that observed [redacted] to the SR-71 could have reflected either all sorties scheduled or only sorties actually flown, alternatives which would have indicated significantly different levels of insight.

~~(S~~ [redacted]

Sorties scheduled	111 days
Sorties flown	85 days
Operational missions scheduled	61 days
Operational missions flown	52 days

[redacted]

~~(S~~ [redacted]

~~(S~~ Obviously, if the DPRK [redacted] was gaining foreknowledge, it was not perfect. On the other hand, if North Koreans had true foreknowledge even 25% of the time, it would be a serious OPSEC concern. Looking at percentages alone gave no clue to the mystery, and some other approach clearly had to be taken. This is where some simple operations research techniques came in.

~~(S~~ The approach taken was to test a complementary hypothesis that the observed pattern of DPRK [redacted] did not reflect foreknowledge but rather was random – which is to say, the North Koreans were guessing. The analysts reasoned that if the number of correct alerts proved to be consistent with a pattern of random guessing, it could be concluded there was no problem. On the other hand, if the number of correct alerts was too high, then the original hypothesis of prior awareness could be supported, even though the North Koreans' record was less than perfect.

The Tools (U)

(U) As it turned out, a distribution known as the binomial was perfect for the problem at hand. It is not important to understand the mathematics of this distribution, but only to know that it can enable an analyst to determine his expectations about any event which has only two possible outcomes – the event can either occur or not occur.

(U) From the data available, the probability of an event in any of the four above-mentioned domains of interest can be estimated simply by dividing the number which occurred by 180 days. The analysts found the probability of a sortie being flown on any given day to be 85/180 = .47; the probability of a sortie being scheduled was 111/180 = .62, and so on. Using probabilities derived in this way, the analysts were able to use the binomial distribution to determine an average number of right guesses to be expected in a random guessing scheme, as well as the chances of getting any specific number correct.[1]

~~(S~~ For the sake of brevity, the ensuing discussion focuses only on sorties and operational missions actually flown, but scheduled events were analyzed in a similar way. Consider the following:

SORTIES FLOWN	Pr (sortie):	85/180=.47
	Expected average # correct guesses (.47x8)	3.76
	Observed average correct	3
	Observed maximum correct	4
MISSIONS FLOWN	Pr (mission):	52/180=.29
	Expected average # correct guesses (.29x8)	2.32
	Observed average correct	2
	Observed maximum correct	3

[1](U) It may be argued that the binomial model is not precisely correct in this circumstance because GIANT SCALE had a quota of missions to be completed each month. Consequently, the events were not truly independent, resulting in a situation where the probability of missions later in the month could vary depending on how many had been completed earlier. However, the actual distribution of events was such that any errors incurred were not large and could be safely ignored.

(S) Using these data and a standard table of the binomial distribution, which can be found in any probability or statistics reference, it was determined that the probability of 4 or fewer correct guesses occurring in 8 tries was about .43 (this is for all sorties flown). Furthermore, the chances of never getting more than 4 correct guesses during any of the six months were calculated as $(.43)^6$, or only about 6 in a thousand. This is a rather small number and suggests that the North Koreans not only did not have foreknowledge, but their performance was considerably worse than could have been expected from a purely random guessing scheme. What a surprising result!

(S) One explanation for this result, and the one finally settled on by the analysts, was that the North Korean [redacted] To illustrate this point, we may contrast the first result with probabilities calculated for operational missions only. In this case, the probability of 3 or fewer correct guesses in 8 tries was found to be .95, and the probability of getting a maximum of 3 right in any six consecutive months to be $(.95)^6$ or .73. These numbers are significantly different and quite consistent with a pattern of guessing, as the analysts had postulated. So while both measures tended to refute the prior-awareness theory, only the second one made much sense in context of the presumed domains of interest.

(S) Just to be sure, the analysts applied one additional technique to confirm their judgment about the pattern [redacted] This technique involved use of another well-known probability distribution — the normal distribution. Although binomial analysis had suggested the North Koreans were anticipating operational missions exclusively, the aggregate time profiles of sorties flown and missions flown looked fairly similar when charted by day of month, week, and time of day. Consequently, it was difficult to discriminate between them when making comparisons with the [redacted] Some other measure was needed, so the analysts decided to examine not the date/times of discrete events but rather the intervals between them. It was reasoned that if the average time between missions was similar to the time [redacted] yet significantly different from the interval between sorties as a whole, then the binomial analysis would be confirmed.

The Solution (U)

(S) This turned out to be true. The manipulation of data in this case required a mean and standard deviation to be calculated for each of the three sample distributions. Without going into computational detail, it will be sufficient to note that the mean times between missions [redacted] were 3.49 days and 3.89 days, respectively, but that the interval for all sorties was only 2.20 days. This was found to be a statistically significant difference.

(S) And so the mystery was solved. Using new primary data and a variety of analytical techniques, the analysts were able to conclude that the North Koreans had *not* regained prior awareness of SR-71 operations [redacted] Furthermore, the analysts were able to infer that the pattern [redacted] was attributable to educated guessing or anticipation on the DPRK's part, and that this anticipation was probably based on the pattern of operational GIANT SCALE missions the North Koreans were able to perceive by radar tracking, [redacted]

Conclusion (U)

(U) The important point of this story is simply that quantitative techniques can be very useful in the analysis of complex OPSEC questions. Sometimes, as in this case, they might even be crucial to the successful resolution of a problem. Every OPSEC analyst should at least be aware of these techniques and their value in solving problems under conditions of uncertainty. This does not mean every analyst needs to be a statistician to succeed in the OPSEC business; as with lawyers and engineers, you don't have to be one to use one. But it does mean keeping an open mind and having the good sense to ask for help when needed.

(U) [redacted] has been employed by the National Security Agency since 1964. Most of that time he has served in the Communications Security Organization. He participated in the original joint OPSEC survey of GIANT SCALE conducted in 1976, and at the time of this writing was NSA's representative to the CINCPAC Operations Security Staff.