Something May Rub Off!

F. W. LEWIS

~~*Confidential*~~

As an itinerant journeyman cryptanalyst, I have spent a fair portion of my Agency life visiting operating sections for varying periods of time—days, weeks, or months. These house-guest tours have usually been occasioned by the appearance of a new and possibly challenging (but hopefully yielding) problem or an unexplained twist to an old problem. They were made with my host's approval—occasionally even on invitation—so it would scarcely display good manners to impute to them any lack of awareness of the need for improved technical procedures and higher standards of scientific approach. But increasingly I have become conscious of a possible blind spot in our cryptanalytic vision which may seriously hamper the continuing growth of within-section cryptanalytic competence.

The problem, simply stated, is "How does the working cryppie, in sections where most technical challenges are of the same kind and where there is little opportunity for original analysis of widely varying systems, acquire the knowledge, experience, and skill necessary for the expeditious handling of a cryptographic innovation?"

An equally serious (though possibly less frightening) poser might be "Have we any assurance that middle-level analysts are not muddling through, laboriously bludgeoning answers out of a problem with outmoded techniques?"

The answer to these questions may well lie in a more judicious application of an old educative stand-by—the tutorial method of learning.

In the leaner years of our intelligence effort (from a standpoint of resources—personnel and tools) it was taken for granted that the best training for the novice was as an apprentice to a more experienced analyst who was willing and eager to share his crypt knowledge, and even the fairly well-trained analyst could benefit from working at the elbow of a proven master of the science. This implies a certain amount of rapport between the various levels of skills and experience, and a willingness to spend a few moments in explanation, theoretical analysis, and technical shop-talk.

However, with the gradual—and quite logical and proper—change in the character of the Agency from a small, more personalized, and highly motivated fraternity to a large organization embracing many

different specialized skills and semi-autonomous full-scale activities, it is quite natural that attendant problems associated with communication, training, and technical breadth should crop up.

Among the many understandable reasons for the appearance of well-appreciated but difficult-to-solve dilemmas, one might include:

(1) The requirement for large numbers of less professionally-trained workers in jobs calling for specific rather than broad skills.

(2) The magnitude of problems involving so many different technical and management aspects that few people are in position to appreciate more than selected portions.

(3) The security constraints which necessitate much tighter controls, compartmentation and established need-to-know.

(4) The fantastically powerful tools available, the complexity of which demands a team approach rather than single-handed effort. (Combined with item 2 above and the changing character of so many problems, this relegates the "Black Chamber" romantic concept of individual victory to a historical period somewhere between the Black Knight and Sgt. York.)

Among the less understandable reasons for this present alarum and excursion, I would list several evils which I sincerely trust are only indicative rather than wide-spread:

(1) The lack of technical understanding and appreciation on the part of certain middle-level supervisors. Perhaps this is an attendant evil of the healthy desire to give all established personnel equal opportunity to grab the next rung on the ladder, but too narrow a field of personal technical achievement may place a very competent technician in one restricted field in the awkward position of making decisions affecting problems completely beyond his understanding.

(2) An overly insistent attitude on the part of some section heads that they must appear to be self-sufficient, even when help is obviously needed. The striving for an intra-mural technical competence is laudable; the pettiness that sweeps incompetence under the rug rather than admit a need for assistance is not. This has reached nadir when section analysts are called on the carpet for seeking the advice of staff specialists, thereby making the section "look bad."

(3) A total lack of appreciation on the part of a few analysts of the new and powerful tools at our disposal. When RYE suggests only a beverage to technicians who have been pushing a pencil for ten or more years and when STETHOSCOPE is only something that needs warming before application, our methods salemen have obviously not been making the correct rounds.

(4) The tendency on the part of some consulting analysts, detailed temporarily to a section, to bury themselves in a corner, and independently and individualistically work out the answer to a knotty problem before emulating the Arab tent-folders. Bailing out a section is not enough; the visiting analyst has failed in a major part of his mission if the problem had been alleviated, but the human factors have been ignored.

It is with regard to the last of these complaints that I make my strongest plea. While we as individuals perhaps cannot always fully appreciate the more subtle problems of administration within the Agency's unique confines of mission and security, we as technicians can make the most of our technical consciences to do the best job possible according to the highest professional standards. This implies a dedication to the principles of professional integrity and scientific achievement, with full regard for the continual growth of the technical competence of the Agency to handle its collective problems, as well as concern for the growth of individual technicans.

The mechanics of fostering a wider technical understanding and competency in an informal way can be kept rather simple if certain assumptions are made. These assumptions involve:

(1) A climate of professionalism that can make the science of cryptology a stimulating challenge to the majority of analysts;

(2) A recognition of the fact that a broad spectrum exsits, which embraces varying degree of skills within levels of technical proficiency. As in many other professions, there are apprentices, journeyman technicians, and master craftsmen, with a logical progression through the various levels contingent on talent, training, and technical application—plus time and opportunity.

The precepts I would recommend to be followed as personal guidelines (within the natural boundaries of administrative and security procedures prescribed) are:

(1) *Learn the trade.*—The inquiring mind—hopefully never quite satisfied in the search for new ideas, new techniques, new knowledge—can take advantage of the experience of other professionals by a receptive attitude towards formal training courses, lectures, literature and personal contacts with more experienced technicians. Admittedly, an important factor in this is opportunity, but few of us take advantage of a fraction of the chances that do present themselves.

(2) *Learn the tools.*—Many cryptanalytic techniques have been revolutionized within the last decade, due to the impact of large-scale, high-speed computers. Theoretical attacks of yesterday are routine procedures now, and both diagnostic procedures and exploitation methods have vastly different potential applications. However, the gulf between raw data and finished product may yawn even wider if the human *interpretive* element is neglected in a blind devotion to the principle of mechanization. We must first know what to do and how to do it—which diagnostic technique, which machine approach promises the best opportunity. Then, in many cases where a machine can only go so far in presenting facts for consideration, the real problem of analysis begins. The more conservative voices who insist that no machine has ever "solved" a problem may be quite right—a silver-platterful of important raw ingredients does not constitute the dainty dish our customers might be expecting. Whether it be cryptanalytic phenomena, the potentials of a traffic analysis exploitation, or tid-bits of semi-processed intelligence, someone

must decide what the stuff means and what it implies as our next step. Finally, the use of optimum procedures for continued exploitation demands knowledge of perhaps entirely different techniques and machines.

Oftentimes tools are left unhoned merely because certain experts feel they don't need them. For example, experienced linguists have the tendency to consider language frequency counts, pattern lists, and stereotypes as implements too primitive for their professional status. The result is that a willing experienced non-linguist may be frustrated in a basic attack, since relative weights are presumably applied intuitively. ("I'll recognize it when I see it!") We know of established sections where a valid frequency count has never been made on individual letters of plaintext, let alone the more sophisticated statistical tabulations of digraphs, word endings, and the like.

(3) *Read—and write.*—The amount of available written information concerning historical crypt systems, the cryptography and cryptanalysis of the major enciphering machines, and the theoretical approach to almost any potential problem is admittedly overwhelming. But judicious use of background material, historical documents, library information and text-book approaches may save months of trial and error. A bright and determined eager-beaver can usually figure out for himself an approach that has long been recognized as applicable. But wheels do not have to be continually reinvented.

As a corollary, one should feel compelled to economize on another person's time and effort by recording progress (or lack thereof) on any non-trivial project. How often we see the same problem tackled over and over by succeeding waves of analysts, each time starting from scratch, with the same elementary statistics forthcoming and the same preliminary deductions independently worked out. Building on a predecessor's groundwork is entirely valid, provided that proper sampling and spot-checking justify confidence in the accuracy of the work and logic of first reasoning. Properly labeled work sheets, intelligible notes, technical devices, and interim reports—each has its value when you (or another analyst) may venture to pick up the thread at a later date.

It is unfortunately true that need-to-know and other security restrictions inhibit the rather wide inter-section exchange of progress reports and technical notes that made for vicarious experience in the older days; but within authorized limits there is still opportunity to learn typical problem approaches and typical procedures in the not unrealistic hope that one may be able to use the same trick tomorrow on a problem within his own bailiwick. Even comparatively trivial desk aids may be worth mentioning to others; for example, a clever little plastic "make-your-own-grille" device I saw the other day for the first time.

[redacted]

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

(4) *Give out as well as take in.*—This could be paraphrased as "Strive to be a good teacher as well as an apt pupil." Almost every technician, regardless of his rank within the hierarchy of talent and experience, has at some time acquired a special knowledge, some useful technique or a helpful suggestion that would make life simpler for the poor soul at the

next desk. At the risk of seeming to put into the script a stage set for one loud continuous scene of conflicting dialogue, I say "talk it up a little." With all due respect to the conservative supervisor who likes to survey a nice quiet roomful of deeply concentrating, strong-but-silent types, I feel that there is room for the desk-level give-and-take technical discussion, the informal technical "bull-session" (or what the British refer to as tea-parties), and the occasional spontaneous black-board talk on an immediate problem, a noteworthy phenomenon, or an exciting development Naturally, such activities should be kept within reasonable bounds, both as to time and place. (Perhaps certain areas should be reserved for more rough-and-tumble competitive mental gymnastics, while other spots are off-limits to anyone other than the "Quiet-Man At Work" type.)

The need for the closely-buttoned lip one sees in the Security posters (and I hasten to agree with the intent and spirit of such) does not extend to technical exchange of ideas relating to a specific problem within the confines of the section having proper jurisdiction over it.

In summary, let's not degrade the professional approach. We must be prepared to be sponges in the matter of absorbing ideas and techniques, and well-controlled faucets when the next-door neighbor's well is in danger of running dry. Above all, we must not be too proud to listen or too hesitant to speak up if something of apparent value is gettable or giveable. For cryptanalytic experience can be shared, and the time, effort, and patience of the more experienced analyst could not be better spent than on insuring our Agency's future cryptanalytic know-how through sharing knowledge with a competent and willing but less experienced apprentice. More positively stated than in the title of this essay—something is *bound* to rub off.