William F. Friedman

The Need for Continuity in Cryptanalytic Studies

(An excerpt from A Brief History of the Signal Intelligence Service, *soon to be published in U.S. Cryptologic History, Special Series.)*

There are four basic reasons why continuity in cryptanalysic studies is so important:

1. It must be realized that cryptanalytic activities have no counterpart in civil life. Therefore, on the outbreak of war there is no important source from which trained, experienced personnel can be drawn for immediate usefulness. Since skill in cryptanalysis can hardly be developed in a short time and cryptanalytic units capable of producing quick results can not be improvised in a hurry, unless there is a good-sized nucleus of such trained and experienced personnel, no good cryptanalytic operations can be conducted in the early phases of a war; that is, just at the time when results can usually be obtained most easily and when such results are extremely important. Moreover, it is in the upper strata of cryptanalytic brains that continuity in studies is most important. It is possible, under pressure, to obtain large numbers of recruits of high intelligence from colleges and universities, but until they have had at least five years actual experience and training they are wholly unprepared to attack the more difficult problems encountered in modern, up-to-date secret communications. Consider the present "Purple" system, for example. It required almost two years of concentrated effort to break down this system, and it was indeed fortunate that this had been accomplished by September 1940. If we had only been able to start this study in December 1941, it would not have been possible to read these messages short of two years' study, if at all, because the problem is so difficult to begin with, and moreover, if we did not have the two years' experience with the ordinary "Purple," the task of reading the special "Purples" now occasionally employed would be extremely more difficult, if it could be done at all, before it was too late to be useful. Again, our present difficulties with Japanese military systems are in large part occasioned by our failure to devote sufficient study to these systems over the past few years; but it must be realized that limitations on funds and personnel made such studies impossible, because with the small SIS staff from 1930 to 1940 it was all that they could do to keep abreast of the Japanese diplomatic systems for which G–2 was clamoring.

2. Continuity in cryptanalytic studies also requires continuity in intercept work, for without the basic raw material, no studies at all can be conducted on actual traffic, and purely theoretical studies may be far off the real target altogether, no matter how successful. Continuity in intercept work means, of course, that the equipment and personnel of the intercept service have to be maintained, so that these are available at the outbreak of war for immediate, useful work. Unless cryptanalytic studies are pursued, the need for the maintenance of adequate intercept stations soon disappears, for it presently begins to look as though the work done by the intercept personnel is useless and funds for this activity are withdrawn.

3. Continuity in cryptanalytic studies is necessary because *cryptanalysis is not a static science or art*—it must progress as cryptographic science progresses. In the past few years great strides have been made in the latter, especially as regards the development of complex electrical and mechanical cryptographic devices and

machinery. Moreover, the cryptanalytic work done during the last war has been publicized. *The American Black Chamber*, in particular, has exercised a wide influence in putting certain nations which had been quite backward in their cryptography on their guard, causing them to engage in studies and developments for the improvement of their codes and ciphers. The result is that the cryptographic systems of these nations have become more and more difficult to analyze. *It is important to note that improvement in cryptography usually comes in successive small steps, and if the opposing cryptanalyst can keep in step with these progressive increases in complexity he can, as a rule, be in a position to read the new systems almost as fast as they are put into usage.* If there is much of a lag in the cryptanalysis, the cryptographer gets too far ahead for the cryptanalyst to catch up quickly; in some cases, catching up becomes impracticable or impossible.

4. Finally, it may be noted that continuity in cryptanalytic studies brings improvements in our own cryptographic systems and methods, without which we may be lulled into a false sense of security and remain blissfully ignorant of what some foreign cryptanalytic bureau may be doing with our supposedly secret communications. It can be said that the greatest blow that can be dealt to signal security work is *loss of continuity in cryptanalytic studies*, for it means that a disastrous blow has been delivered to *technical efficiency of both the cryptographic and cryptanalytic services for war-time functioning.*

Mr. Friedman (1891–1969) was the dean of modern American cryptologists and a pioneer in developing the science of cryptology. In the course of his career (1918–1955), his inventions and exceptional contributions won him a Congressional award (of $100,000) and two Presidential awards. (For further details see article by Lambros D. Callimahos in Winter 1974 issue of *Cryptologic Spectrum*).