REPORT OF THE JOINT COMMITTEE ON THE INVESTIGATION OF THE PEARL HARBOR ATTACK

Page 232:

"The success achieved in reading the Japanese diplomatic codes merits the highest commendation and all witnessess familiar with Magic material throughout the war have testified that it contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."

~~SECRET~~ Budget

The spectacular successes of the signal intelligence services of the Army and the Navy throughout World War II have been sufficiently publicized during the various investigations of the causes of the military disaster we suffered in the surprise Japanese attack on Pearl Harbor to require no detailed elaboration on my part before this committee. It is certainly more than possible that the final result of the war might have been very different but for the information furnished our high command by Army and Navy ~~signal~~ Communications Intelligence (COMINT) services. By that statement I don't mean to indicate that we might have lost the war, but that it might have been so long drawn out as to have become in effect a stalemate. This much, however, I do know: Major General Chamberlin, who was ~~as~~ the officer in charge of operations on General MacArthur's Staff throughout the war in the Pacific, ~~I am in a position to~~ [illegible] on becoming Director of Intelligence for the Army in 1947 stated that the information ~~I~~ he received from ~~the intelligence people~~ U.S. COMINT organizations in that theater ~~alone~~ saved ~~me~~ many thousands of lives and shortened the war by no less than two years. Let us leave aside the matter of what this saving of lives and preventing the maiming of several hundred thousand of our young men means to the United States in terms of manpower, for such savings can hardly be evaluated in terms of money. Let us consider only what the financial savings amounted to, by shortening the war by two years.

In 1945 and 1946 we spent for the Army's ~~signal intelligence~~ COMINT activities alone a total of a little over 48 million dollars; the Navy's ~~signal intelligence~~ effort was approximately the same as the Army's in extent ~~and~~ cost, so that both services cost

Prepared for Gen Chamberlin + submitted 24 Feb 47 F.

~~SECRET~~

say 100 million dollars for the two years. Now for those same two years' operations of the Army and the Navy the Congress appropriated a little less than 37 billion dollars. Simple arithmetic tells us that by spending 100 million and shortening the war by two years, we saved 37 billion. In other words, spending only a relatively small amount of money for ~~signal intelligence~~ COMINT activities results in a very much greater saving than anybody could ever anticipate--the ratio is around 500 to 1.

But I do not wish and haven't time to talk about what signal intelligence meant to us or can do for us in actual war-time. The point I must try to make clear to you now is why we need to conduct those activities on a fairly large scale in peace-time, for the reasons may not be obvious.

If ~~signal intelligence~~ COMINT is an acknowledged essential to victory in war-time, it is even more essential in peace-time. With the tremendous reduction in our armed strength since the end of hostilities there has, of course, also been a very important reduction in our signal intelligence activities, but below a certain point we can cut only at great hazard to our national security. In fact, as the size of our armed forces decreases, our signal intelligence potential must increase.

~~Late last~~ December 1946 the House Military Affairs Committee[1] released "A report on the system currently employed in the collection, evaluation, and dissemination of intelligence affecting the war potential of the United States." It opens with the following paragraph:

1 House Report No. 2734, 79th Congress, 2d Session. Union Calendar No. 860.

> "In time of war, intelligence--that is, in non-technical terms, reliable information on the strength and weaknesses, the capabilities, plans and actions of foreign powers--is an acknowledged essential to victory. In time of peace, intelligence is equally essential for the preservation of that peace, and for the prevention of still another war."

The report then goes on to give reasons for its insistence on the necessity for intelligence work in peace-time. The first part of the report ends with the following significant summarization:

> "The point is important: we cannot continue to live and breathe the air of freemen without adequate intelligence; and intelligence of itself, no matter how good it is, is not enough; the cold facts have to be understood and used."

The Majority Report of the Joint Congressional Committee on the Investigation of the Pearl Harbor Attack has many references to the importance of intelligence in peace-time. For example:

> "Efficient intelligence services are just as essential in time of peace as in war, and this branch of our armed services must always be accorded the important role which it deserves."

Again quoting from the same report:

> "Nevertheless, there is substantial basis, from a review of the Pearl Harbor investigation in its entirety, to conclude that ... the security of the Nation can be insured only through continuity of service and centralization of responsibility in those charged with handling intelligence."

And the Senate War Investigation Committee in its report of 31 August 1946 stated:

> "Under present world conditions the national defense will suffer unless the United States has a more efficient intelligence agency, in both military and nonmilitary fields, than we had before World War II. Knowledge of international economic, political, and social conditions is necessary if sound diplomatic decisions are to be made. Furthermore, data obtained by an intelligence service can assist in determining the size and character of the armed force to be maintained for the defense of our Nation. The establishment of a superior intelligence organization is good economy."

Now none of these reports say so, but I am in a position to affirm that while intercepting and solving secret messages is only one of many sources of and ways to acquire information about foreign nations, that method is by far the most important and valuable. And it is superior to all the others in at least two very important respects:

(1) In the case of a foreign nation having rigid censorship and strong internal security it can well be the major or even the only applicable method of acquiring information.

(2) While the other methods produce information about a target nation's actions, and seldom (except indirectly) about its intentions and plans, signal intelligence, when most effective, is capable of providing direct and categorical evidence of what the target nation's leaders are thinking almost while they are thinking it.

But it is not only because signal intelligence operations yield valuable and current information about other countries in peace-time that these operations must be provided with support. There are other vital reasons and I must go into them, if only in bare outlines.

First comes those which can be summarized under the heading of technical continuity. The progress and increasing complexities in weapons and operational techniques during the recent war years had their counterparts in the apparatus and methods of signal intelligence and communication security. We entered the war with a very small group of people experienced in solving, by what are today rather simple methods and machinery, certain foreign communications. We ended the war with a well-trained force of over 10,000 men and women, who with highly specialized and intricate machines were successful in breaking down practically all the communications of our enemies and, moreover, these communications had been subjected to constant improvements over the years. One of the most vital factors in our success was the fact that as our enemies progressed in making things more complicated our solution experts made parallel progress and thus were able to keep up with them. We maintained technical continuity, in other words. It is a well-established and very important fact that if the opposing cryptanalysts can keep in step with the successive and progressive increases in complexity in the codes and ciphers they are studying they can, as a rule, read the new systems almost as fast as they are put into usage; if, on the other hand, there is much of a lag, the enemy cryptographers get too far ahead for the cryptanalysts to catch up quickly and in some cases catching up becomes impracticable or impossible. The analogy of getting lost in a pitch-dark cavern is applicable: if you ever lose the thread which connects you with those you're following, you may end up a corpse. In

SECRET

this connection I may tell you that the serious consequences of lack of technical continuity and unpreparedness for effective operation immediately upon the outbreak of hostilities are nowhere more clearly demonstrated than in the case of the Japanese Army high-echelon secret communications. It is a fact that during the entire period from 7 December 1941 to the summer of 1943, we couldn't read any of these communications. Had this been otherwise, the military situation might have been quite different. To judge purely by the disastrous effect that the solutions obtained by us after the autumn of 1943 had upon Japanese operations, it is legitimate to think that the important early Japanese penetrations to the south might have met with greater obstacles and that as a result the war in the Pacific might have been terminated many months earlier. If an adequate staff of cryptanalysts had been engaged in studying Japanese Army traffic continuously from 1939, when the systems were solvable with comparative ease, complete continuity could have been maintained from the very outset of the war. But practically all the cryptanalysts we had at that time--and we had only about 20--were assigned to work on the solution of diplomatic traffic. After 1939 the systems became more difficult but never more difficult than they were in 1945 when, because of the possession of a background of knowledge and experience built from successful reading of earlier periods, they were solved.

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, that the intercept equipment and techniques must be kept abreast of new radio transmission techniques and that these are available at the outbreak of war, for immediate, useful work.

There is another angle to the matter of continuity that must be mentioned, and that is the necessity for continuity in training. The necessity for maintaining a highly specialized staff possessing very rare skills and of providing for continuity in training of personnel in peace-time so as to be effective in war-time also is a need peculiar to signal intelligence. For it must be realized that you can't find cryptanalysts in commerce, manufacture, or industry, since cryptanalytic activities have no counterpart in civil life. There are no civil cryptanalysts who, like doctors or dentists, can be inducted into service and put to work practicing their profession immediately. Therefore, on the outbreak of war there is no important source from which trained, experienced personnel can be drawn for immediate usefulness. And 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 sufficient 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 several years actual experience and training they are wholly unprepared to attack the more difficult problems encountered in modern, up-to-date secret communications.

Moreover, the very difficult cryptanalytic problems of these days require large numbers of skilled personnel. It is not sufficient to maintain only a small nucleus of such personnel. We did that in the years immediately prior to 7 December 1941, and I've already told you what that policy cost us in respect to the war in the Pacific, and those unfortunate consequences will be repeated if we follow the same policy again. It will mean that the output of signal intelligence during the early stages of a new war will again be very small in quantity and not too important in quality, since it would be unlikely that difficult cryptographic systems could be read by relatively unskilled personnel. It takes a good deal of time to build up from scratch a new signal intelligence organization to the point where the output is of vital importance in both quality and quantity.

In addition to the problem of cryptanalytic training, there is the one of training in intercept work, for intercept operations and intercept personnel are by no means the same as radio receiving operations and radio receiving operators. Efficient interception is highly specialized work and requires highly-skilled operators.

It takes months of training to make an ordinary radio operator an effective intercept operator; and it takes much time to establish an effective intercept station. Improvisation immediately before hostilities will result in great inefficiency and, what is most important, the loss of intercept material which usually affords excellent clues to the solution of the enemy's early cryptographic systems and communications. Technical continuity in cryptanalysis and in interception are indissolubly connected to each other and both are essential for success in war. Both require continuity of training in peace-time.

So far I've talked only about the necessity and importance of technical continuity and training in signal intelligence operations during peace-time, but I must not omit at least a reference to its similar necessity and importance in communication security operations, which are those connected with the protection of our own communications--our cryptography, in other words. These two fields of cryptography and cryptanalysis are really one and the same. Only by knowledge and experience in breaking down enemy codes and ciphers do we learn how to protect our own messages; and as we bring improvements into our own codes and ciphers we learn things of great benefit in solving the enemy's. Thus, continuity in cryptanalytic and cryptographic studies form one problem. 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 handicap that can be dealt to communication security work is loss of continuity in cryptanalytic studies, for it means that a serious blow has been delivered to technical efficiency of both the cryptographic and cryptanalytic services for war-time functioning. And while I'm on this phase I can tell you that it was no accident that our President and his entourage of important officials and officers could make journeys half-way around the earth not once but several times and meet with no "accidents" such as Admiral Yamamoto met with. For our communications security was adequate to the immense burden placed on it during the war; our cipher machines were and are the best in the world and we must keep them so.

In a thoughtful little study entitled The Future of American Secret Intelligence by Professor Pettee of Amherst College, published last October by the Infantry Journal Press, there is an analysis of our faults and errors in intelligence before Pearl Harbor. Pettee lists several weaknesses. "The first", he says, "was the lack of any idea that intelligence should give warning of a surprise attack before a declaration of war." As to this, I can only point to what the Majority Report of the Joint Congressional Committee said:

> "With the exercise of the greatest ingenuity and utmost resourcefulness, regarded by the committee as meriting the highest commendation, the War and Navy Departments collaborated in breaking the Japanese

diplomatic codes. Through the exploitation of intercepted and decoded messages between Japan and her diplomatic establishments, the so-called Magic, a wealth of intelligence concerning the purposes of the Japanese was available in Washington."

As a matter of fact, it was not lack of signal intelligence but a weakness in the use which was made of it that stands out as the principal fault. Pettee says that "the second glaring weakness was the lack of realization that modern intelligence is a big job." This applies to signal intelligence especially, because there are only a few people who are in a position to understand and to realize that the days when codes and ciphers could be solved by individual experts working only with pencil, paper, and intuition have disappeared. Cryptanalysis and cryptography have become big businesses and highly mechanized ones--and they take lots of people, lots of machines, and lots of money. In the budget which I am here to talk about today, the amount asked for personal services reflects this point. We need for these activities a total of 2,324 people, and funds amounting to $7,089,215 to pay their salaries. That's the largest item in our budget, and I'd like to impress on you the fact that the people we have to hire for this type of work can't all be minor clerks. Some of them rank in brains and ability with the greatest scientists of modern times and we've got to pay them accordingly, if we are to keep them.

Now the next largest item in our budget is for research. I don't think I have to emphasize the importance of research today--

everybody realizes it and I'll pass over the matter with the simple statement that the cryptographic and cryptanalytic fields present special problems in this connection. That's because they really don't have their counterparts in civil affairs, and as a result ordinary commercial or industrial organizations don't go in for them. Moreover, such concerns as are best equipped to conduct research are most reluctant to accept contracts from us unless the end product will have commercial applicability--which very few of our things really have. As a consequence, the military can't get the direct benefit of basic commercial research in these fields, and if there is going to be any research in them, we've got to do most of it ourselves. Only occasionally are there special research problems that can be farmed out by contract, and when we find them, we do so. Our cryptographic and cryptanalytic experts feel that while the progress made in the past half dozen or so years has been very significant, in reality they are currently operating only in the opening phases of what they foresee as revolutionary changes and developments in these fields. And please remember that the amount of money desired, $1,276,700, is to cover research and development not only of signal intelligence mechanisms but also of security equipment. In fact, the larger share is to be devoted to the latter, for we must provide our armed forces with cipher machines better than those of any other army in the world. As to the share to be devoted to research in signal intelligence, we realize that while funds spent on research cannot produce intelligence, only by continuous research can we assure technical continuity in

mechanical equipment for solution purposes, to assist the many people who actually produce the intelligence. Without such mechanical aids they would be powerless today.

As for the other items in the budget, I want to mention briefly only two: Project 120, for $312,910, is to cover the production of communication security equipment for combat organizations. A large share of that is for the conversion of one of our cipher machines for peace-time distribution so as to reduce the hazards of compromising the real machine reserved for war-time use. Project 221 includes $817,275 for equipment and this is to cover our special needs in the way of machinery for intercepting radio messages. I must tell you that radio transmission mechanisms have entered a new era, too, for the days of hand-sent, dot and dash messages are over. Various forms of extremely rapid and complicated non-Morse transmissions, with or without scrambling or encipherment, are coming to be used more and more; if we are to study such transmissions, we've got to be able to copy them. Also, we must be able to locate such transmitters by direction finding techniques, for in war-time this is highly necessary. Combined success in interception and direction finding demands that we provide ourselves with new equipment to meet new methods.

In closing, I want once again to impress upon you the fact that signal intelligence and communication security constitute some of our best weapons and that to use them successfully we must keep them up-to-date and sharp. Finally, I want to say

that in all these matters the Army and the Navy cooperate and are coordinated to a maximum degree within the limits imposed by the present separate organization of the two services. There is no overlapping and no unnecessary or undesirable duplication of work, and there is a complete sharing of results between them.