NATIONAL SECURITY AGENCY

TICOM NOTE 36

11/54/~~SECRET~~/NSA-18

Copy No. 27

From: NSA 18

To C-T

This document contains information affecting the National Defense of the United States within the meaning of the Espionage Laws, Title 18, U.S.C., Sections 793 and 794. See also Public Law 513, 81st Congress, Second Session. Its transmission or the revelation of its contents in any manner to an unauthorized person is prohibited by law.

TICOM NOTE 36

11/54/~~SECRET~~/NSA-18

Russian Sources of Information.

When Part III of Flicke's "War Secrets in the Ether" was reviewed by higher authority, four pages were removed from the section entitled "Where did the Russians get their information?" since the material was thought to require classification. The content of these pages, 77-80, is reproduced here for the benefit of a suitably limited circle of readers.

The author's surmise that German enciphered traffic was read by opponents is interesting, even though he admits that he has no absolute proof. The fact that a man of his experience and with his background entertains this idea suggests the necessity for constant vigilance lest one's own systems suffer compromise due to complacency.

Translated: R.W.P. 4 pages
August 1954
Distribution: normal 30 copies

I do know when they [the Russians] succeeded in breaking into the German cryptographic systems. In my estimation, they were able by early March 1942 to read currently at least one or two of the cryptographic systems used by the German High Command. That put them in a position to recognize all details of the German initial assembly in the Kharkov area and the underlying operational ideas. For there is no doubt that they knew all this long before the beginning of the fighting. And it testifies to their confidence in the strength and striking power of the Red Army - this army which Hitler was supposed to have broken long before - that as soon as they knew of German intentions and preparations, they decided to undertake a strong concentration of troops in the opposite area and to strike the German assemblies with great force.

The "Kharkov case", which will be clarified later in another way, was not an isolated one. There were numerous indications that the Russians on all sectors of the front were well informed regarding the situation on the German side. I have already said that my view of this matter rests on the symptoms observed and deductions therefrom. I might illustrate this general statement by an example.

The cipher machine had been introduced by the German army for radio traffic about 1927. After years of work the so-called "Enigma" was developed, a cipher machine which was operated like a typewriter and automatically transformed plain text into cipher text by a system of wheels, ring settings, and pluggings. By changing the wheel order, the ring setting, and the plugging, a vast number of variations could be introduced into the cipher text and the key could be changed daily. In the view of the cryptanalytic experts, messages enciphered with the [Enigma] could not be deciphered by unauthorized parties and were therefore secure against foreign intercept services.

Some experts of the German intercept service had warned from the very beginning against attributing excessive significance to this machine, since it would suffice if the enemy reconstructed a considerable number of the machines - which was possible at any time - and then typed off in a purely mechanical manner the various possibilities - which could be done very rapidly. With one machine it would be possible to test four variations in a minute; i.e., 5,500 to 6,000 possibilities in 24 hours. By using a greater number of machines this total could be increased correspondingly.

When Czechoslovakia was occupied by German troops, evidence was found in Prague that the Czechs had deciphered messages enciphered with the "Enigma". How this was done remained unknown. But this proved that unauthorized decipherment of Enigma messages was possible. One of the German cryptanalytic experts then undertook to check the machine and found that solution was possible given a minimum of 25 messages enciphered with the same setting of the machine. Now it is quite easy to find 25 messages in 24 hours, consequently foreign cryptanalytic services had a good chance of reading enciphered German army traffic. The "Enigma" was then altered somewhat by increasing the number of wheels from three to five, whereupon the cryptanalytic experts in Berlin declared that henceforth messages enciphered with this machine would be secure.

Years passed. The Second World War brought Germany three years of great victories and two years of equally great defeats and reverses. During all this time the German military staffs had worked to their heart's content with the Enigma. And hundreds of thousands of radiograms had been shot out into space. Then in the spring of 1944 the following happened.

A German office in France inquired via Paris of the cryptanalytic unit of OKW in Berlin whether messages on a Polish agent network with a certain characteristic were being deciphered and read. Due to some disturbance of the teletype network, the answer was sent by radio; it was affirmative and was enciphered by the daily key of the "Enigma". Before 24 hours had elapsed the Polish cipher ceased to be used.

Someone may object that there might have been intentional or careless betrayal on the part of the German military office in France and that the content of the Berlin answer was revealed to the enemy <u>after</u> it had been deciphered at the office to which it was addressed. Of course this is a possibility. However, I consider it unlikely. I am convinced that the messages enciphered by this "Enigma" were currently deciphered and read by both the English and Russian cryptanalytic services.

In spite of this obvious warning, nothing changed in Germany. Any idea of doing away with the "Enigma" met immediately with resolute opposition. In the competent offices there was no longer the vigor or the possibility of carrying out the long chain of measures and changes which would result from

abolishing the "Enigma." Total mobilization resulted not in the total utilization of our material and spiritual forces but in their exhaustion. Hence even in this field its results were negative. Here, too, people did what they had learned and practiced for years; they strewed sand in their own and in each others eyes so as not to see things as they really were.

I said earlier that I was not in a position to offer proofs; this applies simply to the question whether the Russians could or could not decipher German cryptographic systems. I can readily offer proof that they were well informed in other ways regarding events on the German side. This has already been done in the brief description of the work of the "Rote Drei".

The Otwock case affords further evidence.