From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
VOLUME 26 • NUMBER 1 • Fall 2020
$15 SINGLE COPY PRICE

ASSOCIATION OF FORMER INTELLIGENCE OFFICERS
7700 LEESBURG PIKE, SUITE 324
FALLS CHURCH, VIRGINIA 22043
WEB: WWW.AFIO.COM * E-MAIL: AFIO@AFIO.COM

When Intelligence Made a Difference

— COLD WAR —

William Weisband

by Naiomi Gonzalez

During the Cold War, the United States and the Soviet Union engaged in a frantic cat-and-mouse game: both struggled to gather the intelligence to parse the other nation's political and military weaknesses, strengths, and intentions, while working to insure their own information remained secure. Gathering intelligence from the enemy, while also protecting one's own, were matters of life and death, and both nations achieved major breakthroughs and suffered stunning losses. During 1948, the Soviet Union scored a significant intelligence coup and the United States suffered an intelligence loss that would have major implications in Korea.

Breaking the Soviet Code – The Venona Project

During World War II, the Soviets used a system of codes and encryption to communicate with one another that Americans were initially unable to break: random sets of numbers replaced the text in the messages being transmitted. Both the recipient and the sender had identical copies of a pad comprised of additive keys that aided in the encryption/decryption of the message.[1] At the heart of Soviet encryption was the use of this one-use pad system. In theory, because the pads were to be used only once, each message had a unique cipher not repeated in any other message. Even if an adversary were to intercept thousands of messages, each message would have a unique, non-repeating key, making it impossible to decipher the message without access to the specific one-time pads.

In practice, maintaining such secrecy proved impossible. The use of the one-time pad necessitated the creation of hundreds of thousands of unique, non-repeating key pages during World War II when the Soviets were sending out thousands upon thousands of messages. Moreover, digital computers that could quickly create one-time pads in large quantities did not exist yet. As a result, Soviet cryptographers resorted to replicating the pads, turning them from one-time use pads to two-time pads or more. In order to mitigate the increased risks, the Soviets did not reproduce whole pads. Rather, they copied individual pages, which were inserted into different pads.[2] While not as secure as the one-time use pad system, the Soviets assumed that the resources needed to decode the message would be too time-consuming. An enemy power would need to have the resources to gather enough of the duplicate keys and hire a large number of cryptanalysts, who would then need to spend years trying to break Soviet encryptions.[3]

However, members of the Army's Signal Intelligence Service (SIS) Venona Project, a highly classified program, focused on deciphering Soviet diplomatic, military and intelligence messages, discovered in 1943 that the Soviets were using duplicate key pages. Army cryptanalysts were able to decipher portions of Soviet messages.[4] While still a struggle, SIS cryptanalysts made substantial headway. By 1946, they were aware of the scope and depth of Soviet intelligence activities against the US.[5] For example, that year, Meredith Gardner decrypted a 1944 NKVD[6] message that included the names of scientists working on the atomic bomb, demonstrating that the Soviet Union's intelligence apparatus had received information on one of America's most closely guarded projects.[7] By the late 1940s, Army cryptanalysts were able to keep track

1. For a more detailed description of the Soviet encryption system see John Earl Haynes and Harvey Klehr, "Breaking the Code," in *Venona: Decoding Soviet Espionage in America* (New Haven, CT: Yale University Press, 1999), pp. 25-28.

2. Haynes and Klehr, "Breaking the Code," p. 29.

3. Haynes and Klehr, "Breaking the Code," p. 29.

4. Michael J Sulick, "America's Counterespionage Weapon: Venona," in *Spying in America: Espionage from the Revolutionary War to the Dawn of the Cold War*. Washington, D.C.: Georgetown University Press, 2012, p 175.

5. The FBI was brought into the Venona project in 1945. Through defections, such as Whittaker Chambers in 1939, Elizabeth Bentley and Igor Gouzenko in Canada in 1945, the FBI was already investigating the penetration by Soviet agents of the government. David Major and Peter C. Oleson, "Espionage Against America," *The Intelligencer*, Vol. 23, No. 1, Summer 2007, pp. 62-4.

6. The NKVD, established in 1934, became the NKGB from 1943 to 1946, when it was superseded by the MGB. The KGB was established in March 1954 and dissolved in 1991, when it was divided into the FSB and SVR. The name changes reflected internal Soviet political decisions; the fundamental missions remained the same. For clarity in this article NKVD is used despite the changes in nomenclature.

7. Sulick, "America's Counterespionage Weapon," pp. 174.

of Soviet military logistics, gaining valuable insights on Soviet capabilities, dispositions, and intentions.

Over a period of several months in 1948, the progress American cryptanalysts had made came to a halt as the Soviet Union implemented countermeasures making it much more difficult to decipher their messages. It became increasingly clear to Army cryptanalysts that somehow the Soviet Union had been made aware of America's ability to at least partially decrypt their messages. Americans at Arlington Hall[8] began to worry that they had a spy in their midst. They were correct.

William Weisband

William Weisband served both the American army and worked for the NKVD. Born in 1908, either in Odessa, Russia or Egypt,[9] he moved to the United States in 1925. He traveled to the Soviet Union in the 1930s, most likely attending the Comintern's Lenin School.[10] During his time in Moscow, he was recruited by the NKVD.[11] By 1936, he was back in the United States, working for the NKVD's New York rezidentura as a courier. In 1941, he was transferred to California where he served as liaison between Jones York, who worked for Douglas Aircraft, and the NKVD,[12] passing on military technical aviation information. York developed a relatively friendly relationship with Weisband, meeting with him over ten times.

When he entered military service, the Army quickly recognized Weisband's aptitude for languages, sending him to study Italian to supplement his English, Russian, and Arabic skills. After Officer Candidate School, he was assigned to the U.S. Army Signal Security Agency and served in Great Britain, Africa, and Italy. After the war, he received a position as a civilian linguist in Arlington Hall where he became lead Russian language translator responsible for translating decrypted messages from the Soviet Union.[13] While not part of the Venona Project, his position placed him in proximity to those who were. Additionally, he had access to key information regarding the U.S.'s decryption process. Cecil Philips, a cryptanalyst working on the Venona Project, claimed, "He managed to roam around with great ease. He cultivated people who had access to sensitive information. He used to sit near the boss's secretary, who typed everything we did of any importance."[14]

The Soviet Union regarded Weisband as one of their most important assets. In a 1949 report, the NKVD stated that the materials provided by Weisband informed them that Americans had gained information "about the disposition of Soviet armed forces, the production capacity of various branches of industry, and the work being done in the USSR in the field of atomic energy."[15] The NKVD also admitted that the information provided enabled them to take defensive measures that drastically impeded the American's ability to decipher their messages. In the 1949 report the NKVD stated:

> *On the basis of materials received from "Zhora," our state security agencies implemented a set of defensive measures, which resulted in a significant decrease in the effectiveness of the efforts of the Amer. decryption service.*[16]

In the 1950s, Weisband's role was discovered, and he was fired from the newly established Armed Forces Security Agency (AFSA). He was not tried for espionage out of fear that the trial would require revealing even more information that would further damage U.S. national security. However, he served one year in prison for contempt of court. [17]

Ramifications of Weisband's Spying

The intelligence provided by Weisband to the Soviet Union proved devastating for America. Up until the cryptanalytic blackout in 1948, Americans were able to decipher enough messages to gain a broad understanding of Soviet military movements. They were able to track Soviet military equipment, providing American intelligence officials and policymakers with some indication of Soviet intentions and capabilities. However, access to that information, which included

8. Headquarters of the U.S. Army Security Agency, (ASA), later known as the Armed Forces Security Agency (AFSA) in May 1949, precursor to the NSA in 1952.

9. William Weisband claimed to be born in Egypt, but was probably born in Odessa, Russia. See John Earl Haynes and Harvey Klehr, "Alexander Vassiliev's Notebooks and the Documentation of Soviet Intelligence Activities in the United States during the Stalin Era," *Journal of Cold War Studies* 11, no. 3, 2009, p.17.

10. The Lenin School was a training ground for international communists, teaching ideology as well as underground techniques. Wikipedia citing Julia Köstenberger, "Die Internationale Lenin-Schule (1926-1938)," in Michael Buckmiller and Klaus Meschkat (eds.), *Biographisches Handbuch zur Geschichte der Kommunistischen Internationale: Ein deutsch-russisches Forschungsprojekt*. Berlin: Akademie Verlag, 2007; pp. 287.

11. John Earl Haynes, Harvey Klehr, and Alexander Vassiliev, "American Couriers and Support Personnel," in *Spies: The Rise and Fall of the KGB in America*. New Haven, CT: Yale University Press, 2009. p. 398.

12. Haynes and Klehr, "Breaking the Code," p. 50.

13. Haynes, Klehr, and Vassiliev, "American Couriers and Support Personnel," p. 18.

14. Haynes and Klehr, "Breaking the Code," p. 49.

15. Haynes and Klehr, "Breaking the Code," p. 403.

16. Haynes and Klehr, "Breaking the Code," p. 403 and English translation of Alexander Vassiliev's notebook: *https://www.wilsoncenter.org/sites/default/files/Black%20Notebook%20Translated1.pdf*, p. 75.

17. Haynes, Klehr, and Vassiliev, "American Couriers and Support Personnel, p 24.

Soviet communications in the Far East and related to the divided peninsula of Korea, ceased when the Soviet Union implemented defensive measures to improve their communications security. As a result, the United States was caught by surprise when the North Koreans invaded the South on June 25, 1950. The North Koreans depended on the Soviet Union for the majority of their military supplies and equipment.[18] Had American cryptanalysts been able to continue to decipher and decrypt Soviet messages, they most likely would have been alerted to the massive amounts of supplies the Soviet Union was transferring to the North Koreans. This, in turn, would have provided American policy makers and military leaders with the time to develop options that may have avoided the Korean War.

Weisband was a spy who provided the Soviet Union a significant strategic advantage and prevented indications and warning of the outbreak of the Korean War.

Naiomi Gonzalez is a PhD student at Texas Christian University. She has an MA in Middle East and Islamic Studies from George Mason University and an MDiv from Brite Divinity School.

18. David A. Hatch and Robert Louis Benson. *The Korean War: the SIGINT Background*, Fort George G. Meade, MD: Center for Cryptologic History, National Security Agency, 2000, p. 5.