Doc ID: 6660648

UNCLASSIFIED

DAILY ENTERPRISE

(U) HISTORY TODAY - 27 August 2015 - Soviet Cryptologic Work during WWII

FROM: CCH, CCH
Run Date(s): 08/27/2015

(U) The film, *Enemy at the Gates*, 2001, showed the battle of Stalingrad from the Soviet perspective. A grim opening sequence depicted the slaughter of reinforcements crossing the Volga River and sniper teams in action in the ruins of the city.

(U) One scene in the film is of interest to cryptologists. A former Moscow University German language major named Tanya monitors Nazi voice and Morse code communications. She asks for an assignment to a sniper group. The political officer berates her request, and says that each time she hears and decodes German messages hundreds of lives are saved.

(U) The Center for Cryptologic History is frequently asked about Soviet cryptologic work during World War II. Did the Soviets, independent of their British and American allies, break into the German ENIGMA machine or the Japanese diplomatic cipher known as PURPLE?

(U) The Soviets in the 1990s, before the fall of the Communist Bloc, made claims of some success in these endeavors, but they released no documents to substantiate their statements. Most of the documentary evidence comes from German sources, material captured during the war. Here is a summary of what we do know.

(U) First, the U.S. and UK shared very little SIGINT with the Soviets, but there were a few important occasions when information derived from cryptanalysis was sanitized and passed to the Soviet leadership. In mid-1943, the British even provided the Soviets with a captured ENIGMA and its operating manuals. However, London insisted there be no high-level sharing of cryptanalytic information with Moscow. It didn't matter, though -- the Soviets knew what Bletchley Park was exploiting thanks to spies, particularly members of the Soviet spy ring popularly referred to as the "Cambridge Five."

(U) Earlier this year, *History Today* published a series of articles on the Cambridge Five. Here is the link to the last article, from which you can take further links to earlier articles.

(U) After the Bolshevik Revolution in 1917, the new Red Army developed an intercept and code-breaking effort during the war with Poland (1919-1920). In the interwar period, the Red Army organized a radio intelligence service that performed intercept, direction finding, and traffic analysis at the tactical level. Each Red Army division had a small section attached to it that performed all of these activities. At each level of the command structure there was a correspondingly larger SIGINT element. Usually, at the Army or Front (multi-army) level there was an entire regiment of such "special-purpose troops."

(U) The Soviet General Staff also had its own fixed stations at cities like Smolensk, Kiev, Leningrad, Minsk, and Riga. Each of these stations, in turn, controlled smaller fixed stations close to the western border of the USSR.

(U) Cryptanalysis, however, was seldom performed at the tactical level.

Doc ID: 6660648

(U) Cryptanalysis was done at "special centers," either the Front Headquarters or General Staff HQs in Moscow. According to some sources, intercept and cryptanalytic functions were controlled by the General Staff's Eighth Department, which also included communications security.

(U) Shortly after the German invasion of the USSR, the SIGINT structure was decentralized and Front commands got greater resources. Fronts also got cryptanalytic centers: each Front HQ had an operations company that performed tactical functions of intercept, direction finding, and traffic analysis, but an operations section was added that could do low-level cryptanalysis. Intelligence was reported up the chain of command to the Front commander, and probably back to the General Staff in Moscow.

(U) Evaluations of this system vary greatly, and may reflect experiences at different times in the war. Russian General Andrei Vlasov, who later collaborated with the Nazis, claimed that Russian COMINT support was negligible and usually wrong.

(U) Other Russian prisoners of the Germans, captured later in the war, claimed that they had detailed information on the German order-of-battle and tactical intentions on several occasions.

(U) A German observer, Wilhelm Flicke, who after the war wrote about German COMINT and codebreaking, suggested that many Soviet operations were based on information from COMINT. In several cases, such as the Kharkov offensive in August 1942, and the German offensive into the Caucasus to seize Soviet oil facilities in the fall, the Red Army seemed to know a good deal about German movements and intentions, and managed to stay ahead of their tactical actions.

(U) Soviet POWs told German interrogators that much German tactical air and ground force traffic was readable--virtually all low-level manual cryptographic systems were exploited by the Soviet cryptanalysts.

(U) In the 1990s, a former KGB colonel who participated in some conferences at U.S. universities claimed that the Soviets had solved both the German ENIGMA machine and Japan's machine-generated PURPLE cipher. She said, however, that exploitation was inconsistent, since the Soviets did not have the capabilities of constructing machines such as the *bombe* that enabled regular and rapid exploitation of ENIGMA messages.

(U) It is probable that the Soviets had a limited ability to read ENIGMA by exploiting captured machines and key, and from the interrogation of captured German code clerks and radio operators.

(U) It is unclear if the Soviets could read PURPLE, the Japanese diplomatic cipher machine, during the war. As with the ENIGMA, Russian and former Soviet sources have made claims of success, but they have produced no documents to back up their assertions.

(U) The Soviets had an active and effective tactical COMINT capability during World War II. However, the answer to the question about Moscow's ability to cryptanalytically exploit high-level cipher devices such as ENIGMA and PURPLE must remain mostly conjecture based on tantalizing hints and snippets of information.

(U) The article is based on an earlier article by now retired historian Robert J. Hanyok.

(U) The illustration shows Soviet forces laying commo wire at Stalingrad. (Commo wire = a common way of saying in the military and NSA/CSS community.)

(U) To discuss historical topics with interesting folks, visit the Center for Cryptologic History's blog, *History Rocks* ("go history rocks").
(U) Have a question or comment on *History Today*? Contact us at DL cch or [redacted]

(b)(3)-P.L. 86-36

[redacted]

Doc ID: 6660648

Information Owner [redacted]
Page Publisher [redacted]
Last Modified: August 27, 2015
Last Reviewed: August 27, 2015

(b)(3)-P.L. 86-36