Link: https://chris-intel-corner.blogspot.com/2013/07/soviet-codebreakers-of-wwii.html

Soviet codebreakers of WWII

WWII histories of signals intelligence and codebreaking are currently focused on the theatres where German and Japanese troops fought against the Anglo-Americans. The influence of ULTRA intelligence on the Battle of the Atlantic, the North Africa campaign, the Normandy invasion, the battle of Midway etc is mentioned not only in specialized books but also in the popular histories of the war.

On the other hand the Eastern Front is completely neglected in this aspect, despite the fact that millions of troops fought in countless battles and endured horrendous losses for several years in the largest land campaign in history.

Codebreaking and signals intelligence played a major role in the German war effort. We know that the Army had 3 signal intelligence regiments (KONA units) assigned to the three Army groups in the East (Army Group North, South and Centre). In addition from 1942 another one was added to monitor Partisan traffic. The Luftwaffe had similar units assigned to the 3 Air Fleets (Luftflotten) providing aerial support to the Army Groups.

Both the Army and the Luftwaffe also established central cryptanalytic departments (Horchleitstelle Ost and LN Regt 353) for the Eastern front in East Prussia. So as we can see the Germans certainly invested significant resources on sigint.

During the war this effort paid off. We know that the German codebreakers could solve Soviet low, mid and (for a time) high level cryptosystems. We also know that they intercepted the internal radio teletype network carrying economic and military traffic. Traffic analysis and direction finding also played a big role in identifying the Soviet order of battle.

Having looked at the German side we need to turn our attention to the Soviets. What were the successes of the Soviet side in this shadow war?

Unfortunately there is no clear answer to this question. The Soviet archives relating to signals intelligence are closed and information on codebreaking is hard to find and verify. This means that there limited sources that a researcher can use and in some cases it will be necessary to resort to deductive reasoning.

Prewar developments

The Tsarist empire invested considerable resources in the field of secret intelligence and codebreaking. The agents of the feared Okhrana monitored revolutionaries and other enemies of the regime and its 'Black Chamber' (Cherniy Kabinet) could decode the telegrams of foreign ambassadors.

The new Soviet state took over some of these codebreakers and put them back to work. In 1921 the Spetsial'niy Otdel (Special Department) was created and it was housed in a building of the People's Commissariat of Foreign Affairs on Kuznetskiy Most Street, Moscow. In 1935 it was moved to the NKVD's Lubyanka office complex. Security measures were draconian with the personnel being told not to reveal even the location of their offices to their relatives.

Head of the department from 1921-37 was Gleb Ivanovich Bokii, a loyal Bolshevik who had ruthlessly suppressed enemies of the Soviet state during the Russian civil war. His deputy was Major Pavel Khrisanfovich Kharkevich.

The Spetsodel initially employed many former Tsarist codebreakers who were assisted in their work by compromised cipher material provided by foreign spies. The Soviet foreign intelligence service was able to recruit personnel with access to cipher material in many countries during the 1920's and 30's.

During this period the Soviet codebreakers were able to exploit the codes of several foreign nations including Britain, France, Germany, Italy, Japan, USA, Poland and many others. The main target was Japan due to the military incidents in the Far East between the Soviet forces and the Kwantung Army.

The Soviet codebreakers also took part in the Spanish Civil War, the Sino-Japanese war and the battle of Khalkhyn Gol.

Special operational groups of the Spetsodel were sent on these operations. A small group went to Spain in 1936 were it succeeded in reading the messages of Franco's military forces and also of their spy network.

In early 1938 a group was sent to China to assist the Government forces of Chiang Kai-shek in their fight against Japan. In the course of the following months 10 Japanese tactical cryptosystems were solved.

In 1939 the codebreakers were able to assist General Zhukov in the battle of Khalkhyn Gol by reading the code used by the Kwantung Army.

The purges of the 1930's

The many successes of the Special Department did not shield it from the purges of the 1930's. During that period people from all aspects of Soviet society suffered from accusations of spying and sabotage and there were show trials and executions.

The purges crippled the cryptologic service since many of its workers were executed along with the top administrators. Bokii was executed in 1937 with most of the section heads and the Tsarist era personnel suffering the same fate.

These self inflicted wounds came at the worst possible time since in September 1939 Germany invaded Poland and thus started World War II.

The Great Patriotic war

In 1941 the crypto service was redesignated as the 5th Department of the NKVD under the efficient administrator Major Ivan Grigoryevich Shevelev.

The German invasion led to the rapid expansion of the department and Shenelev recruited some of the best mathematicians and technicians in the Soviet Union. According to Matt Aid '*By the end of World War II, the 5th Directorate controlled the single largest concentration of mathematicians and linguists in the Soviet Union.*'

The Red Army also had its own signal intelligence and codebreaking department under the Chief Intelligence Directorate - GRU. In 1930 the GRU decryption department became part of the Spetsodel but was split off again in 1938.

In 1941 the radio intelligence service was the 8th department of the Intelligence Directorate of the Army General Staff. Head of the unit was Engineer 1st Rank I.N. Artem'ev. The GRU controlled special radio battalions called OSNAZ. At the start of the war there were 16 of these battalions.

How did the Soviet radio intelligence organizations perform during the war?

Period 1941-42

We know that in 1941 they were suffering from the loss of experienced personnel. It also seems that the numerous GRU radio battalions were primarily tasked with monitoring their own military forces for breaches of security and thus neglected to keep foreign units under close observation.

The German surprise attack caught the entire Soviet military in the process of mobilization and movement of units. The great defeats of 1941 led to the loss of equipment, cipher material and personnel. However it seems the Soviets were also able to win some important victories in the radio war.

In the autumn of 1941 a group led by NKVD cryptanalyst Sergei Tolstoy was able to solve the PURPLE cipher machine used by the Japanese Foreign Ministry. The decrypts showed that Japan would not attack the Soviet Union in support of the Germans. This information allowed the Soviet leadership to concentrate all available resources against Germany. Japanese diplomatic traffic continued to be read throughout the war and provided important insights into the political and military developments in Axis countries.

In the military front there is no indication that German cipher machines were solved cryptanalytically but in late 1941 the Soviets were able to capture Enigma machines and documentation of the German Second Army. The information obtained might have played a role in the Battle of Moscow.

Germany's Allies were easier targets. According to a recent book on Russian cryptology the Army codebreakers were able to read messages exchanged between the Romanian high command and General Manstein in the Ukraine during the period 1941-42.

The Soviet Stalingrad offensive took advantage of the fact that the sides of the German front were held by Romanian and Hungarian troops. It is not unreasonable to assume that some of this information was acquired through signals intelligence.

A report from the GRU to Stalin dated November 29, 1942 says that: '*Direction finding of German army radio stations provided valuable information about enemy groupings, their activities and intentions….The cryptanalytic service of the Chief Intelligence Directorate of the Red Army identified the main German and Japanese general military, police and diplomatic ciphers, including 75 systems of German intelligence. More than 220 keys to them, and more than 50,000 German messages were read…The research group of our office has revealed the possibility of solving German messages enciphered on the ''Enigma'' machine, and started to construct equipment, speeding up the solution.*'

The crypto systems mentioned must have been the hand ciphers used at low and mid level by the German military, police and Abwehr.

In 1942 there was a major reorganization of the NKVD and GRU radio intelligence services. The 5th department took control of the evaluation and distribution of Soviet crypto systems and also absorbed the GRU cryptanalysts.

The 8th department concentrated on traffic analysis and direction finding in order to reveal the order of battle of the German units.

Period 1943-45

In the second half of the war the German forces were in retreat and the Soviets liberated the occupied territories and ended the war by capturing Berlin. During this period the Soviet military had a significant numerical advantage in troops and equipment against the Germans. This makes it difficult to assess the importance of signals intelligence in the Soviet victories since many different factors were at play.

Still we do know that through direction finding and traffic analysis the Soviets were able to identify German formations and follow their movements. For example the article 'Spies, Ciphers and 'Zitadelle': Intelligence and the Battle of Kursk, 1943' says : '*a captured intelligence report of the Soviet 1st Tank Army dated 5 July 1943 revealed that radio intelligence had identified the positions of the headquarters and units of II SS Panzer Corps, 6th Panzer and 11th Panzer Divisions before the offensive began. Other captured documents disclosed that 7th Panzer Division, XIII Corps and Second Army headquarters had all been similarly 'fixed' by Soviet radio intelligence*.'

The Soviet codebreakers were definitely able to solve German hand ciphers and they must have captured Enigma machines and their keylists when they encircled German units (especially in the summer of '44).

Help from abroad

The Soviets received assistance from two foreign sources. On the one hand the British occasionally shared some of the intelligence that they acquired by breaking German codes. The source was always camouflaged since the Brits did not want to reveal their cryptologic successes to the Soviet government.

Apart from general warnings about impending German actions the Brits also sent more detailed reports. In April '43 they transmitted a report sent by General von Weichs to Foreign Armies East that revealed the main points of the German plan for the battle of Kursk. In October of the same year they informed the Soviet authorities about the Abwehr's Klatt network.

Although the British authorities were careful to hide the source of their reports the Soviets already knew about Bletchley Park and the Enigma codebreaking through their spy network. During WWII Kim Philby and Anthony Blunt passed along information on Abwehr ciphers while John Cairncross was able to infiltrate Bletchley Park.

According to 'The Crown Jewels: The British Secrets at the Heart of the KGB Archives', p218-9 in 1942 apart from decrypted messages Cairncross was able to get '*two volumes of the secret training manual on deciphering, a guide for the reading of the German Enigma key codenamed TUNNY and a description of a machine constructed by the British to read the Luftwaffe's cipher traffic*'. Tunny must refer to the SZ42 teleprinter and not Enigma. The part about the machine used on the Luftwaffe cipher traffic could refer to the bombes but it is not clarified in the book.

The information provided by Cairncross could have allowed the Soviet codebreakers to overcome cipher research problems.

Working backwards

Since we do not have details on what systems the Soviets could exploit it might be best to work backwards. By looking at the cryptosystems used by the Germans we can check if their security was such that they would have resisted a well organized attack by a group of mathematicians and linguists.

Overview of Axis cryptosystems

Germany

Military

The German military used cipher teleprinters of the SZ42, T52 and T43 types for top level communications, the Enigma machine from regiment upwards and various hand ciphers for frontline use.

Lorenz SZ42

The main radio-teletype machine used in the East was the Lorenz SZ42. This was quite a complex machine and regular solution required the use of very advanced cryptanalytic equipment. The Brits built the Colossus computer in order to decode this traffic. The Soviets were probably unable to build similar equipment but they could have decoded messages 'in depth' using hand methods. This was the standard practice at Bletchley Park prior to the introduction of high speed cryptanalytic equipment.

At this time there is no information on Soviet analysis of German teleprinters.

Enigma

The plugboard Enigma was used by the German Army, Navy and Airforce as their main cipher system. Throughout the war its security was upgraded with new procedures and modifications. Could the Soviets have decoded Enigma traffic like Bletchley Park?

The GRU 1942 report says '*The research group of our office has revealed the **possibility** of solving German messages enciphered on the ''Enigma'' machine, and started to construct equipment, speeding up the solution*'. However there is no mention of actually decoding traffic.

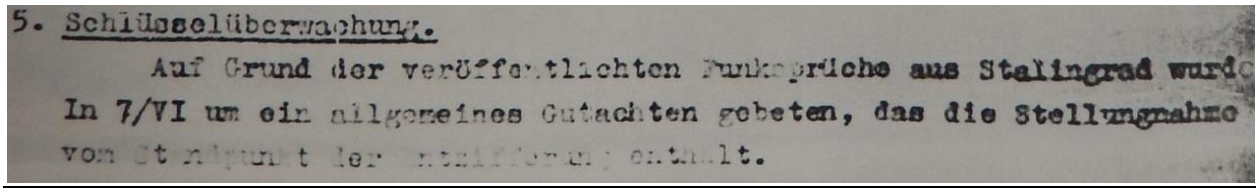
This possibility was examined by Geoff Jukes in a series of articles in the 1980's. However both his articles were based on inferential evidence and the responses by Milner-Barry and Ralph Erskine effectively countered Juke's arguments.

David Kahn who interviewed KGB General Nicolai Andreev (head of the KGB's sigint department in the 1970-80's) in 1996 was told that the Soviets knew how to solve the Enigma and although they didn't have bombes '*it might have been possible to organize people to replicate the mechanisms work*'. From Andreev's statement it is not clear if this was actually done with real traffic.

The Soviets definitely captured intact Enigma machines and valid keylists during the war. Using them they would have been able to decode older traffic. However there is no indication so far that they were able to recover the settings cryptanalytically.

On the contrary the recent article '*О ВКЛАДЕ СОВЕТСКИХ КРИПТОГРАФОВ В ПОБЕДУ ПОД МОСКВОЙ*', says that in late 1942 the Soviet codebreakers analyzed the Enigma cipher machine and developed ways of solving it. However their efforts failed in January 1943 due to German security measures.

This information seems to be confirmed by the war diary of the German Army's Inspectorate 7/VI. The March 1943 report of Referat 13 (security of German cipher machines) says that based on the published radio dispatches from Stalingrad Inspectorate 7/VI was asked to give an opinion from the point of view of decipherment.


5. Schlüsselüberwachung.

Auf Grund der veröffentlichten Funksprüche aus Stalingrad wurde In 7/VI um ein allgemeines Gutachten gebeten, das die Stellungnahme vom Standpunkt der Entzifferung enthält.

Schlüsselüberwachung

Auf grund der veröffentlichten Funksprüche asus Stalingrad wurde In 7/VI um ein allgemeines Gutachten gebeten, das die Stellungnahme vom Standpunkt der Entzifferung enthält.

Thus it seems that the Soviet effort to decrypt Enigma messages was identified early and countered by the Germans.

Such a failure could be attributed to several factors:

1). They started their analysis of the Enigma late in the war and thus could not exploit the insecure signaling procedures of the period up to May 1940. In the period 1942-45 the Germans introduced many new security measures that would have made a solution much more difficult than in 1939-40 when Bletchley Park made its start.

2). Most of the Enigma traffic in the East would be from Army units that traditionally had a higher level of security than their Airforce counterparts. Army traffic routinely caused problems for Bletchley Park, despite their large number of 'bombes'.

Hand ciphers

The German army used hand ciphers at division level and below. For most of the war the main systems were double Playfair and 3-letter field codes.

The double Playfair- Doppelkastenverfahren was a modification of the well known Playfair cipher but instead of one square it used two. The text was broken up into digraphs and they were enciphered using the two alphabet squares. According to Dr Fricke, a German cryptologist who evaluated the security of Army systems, up to 1942 the digraphs were enciphered only once but from that point on they were enciphered twice. A report by Allied personnel who worked on this system says that '*Each German division had its own set of cipher boxes. It was assigned six different boxes for each day. These were paired in different combinations for each day's eight three hour periods. In effect, there were eight keys per day.*'

The army also used 3-letter codes. Initially these were used unreciphered but from 1942 they were enciphered with daily changing trigraphic substitution tables.

Both these systems had limited security. It is probably safe to assume that this traffic was regularly solved by the Soviets and gave them tactical intelligence and OOB data. However their success with military hand ciphers could not have lasted for the entire war.

In 1944 the double Playfair was replaced with the Rasterschlüssel 44, a transposition system using a stencil. The RS 44 had impressive security for a hand cipher and confounded the analysts of Bletchley Park. The Soviet codebreakers must have been similarly annoyed that the double Playfair was replaced by such a secure cipher.

Radio procedures

According to German personnel the radio procedures of their units (callsigns, indicator groups) were insecure and thus simply through traffic analysis and direction finding the Soviets were able to identify enemy units and concentrate their attacks at their flanks.

Intelligence services

The military intelligence service Abwehr infiltrated spies in the Soviet rear areas through WALLI I, a unit controlled by Major Hermann Baun**.** The ciphers used by the Abwehr in the field were mostly transposition systems. The codebreaker of Bletchley Park were able to solve Abwehr ciphers throughout the war. There is no reason why these simple systems would resist solution by the Soviets. The GRU report specifically mentions the Abwehr traffic: '*….including 75 systems of German intelligence.'*

Additional information on Abwehr ciphers was provided by the Cambridge spy ring.

Central Abwehr stations also used a small number of Enigma G machines. The G (Counter) version did not have a plugboard since its security laid in the irregular stepping system of the wheels. Bletchley Park was able to solve this machine in late 1941 and the traffic was regularly read. There is no indication that

the Enigma G was solved by the Soviets, although it would be theoretically possible (for example by using reencodements from hand ciphers).

In one case we definitely know that the Soviets exploited the communications of the Abwehr. In Sofia, Bulgaria the Klatt bureau gathered intelligence from sources that were supposedly working inside the Soviet Union. The traffic of the Sofia station was intercepted by the Brits who found the information valuable. Through their spies inside British intelligence the Soviets learned of the Klatt bureau and started intercepting the Vienna-Sofia traffic from autumn 1941. According to 'The Crown Jewels: The British Secrets at the Heart of the KGB Archives', p197 the Soviet codebreakers were able to solve the cipher in July 1942 and found it to be '*a letter cipher of a comparatively simple system*'. The same source says that the traffic on the Sofia-Budapest link was also decoded.

The intelligence service of the SS – Sicherheitsdienst recruited POW's and after a brief period of training and indoctrination sent them to the Soviet rear on espionage and sabotage missions. This operation was called 'Zeppelin' and it was clearly a numbers game. The Germans did not expect their agents to survive for long. The SD probably used several different cryptosystems, however just like the Abwehr it seems that the most widely used one was double transposition. Considering the limited training afforded to the 'Zeppelin' agents it is probably safe to assume that they would not be taught complex cryptosystems. Just like the Abwehr there is no reason to assume that these messages were secure from Soviet eavesdroppers.

Organisations in the rear areas

Could the Soviet radio intelligence services have gotten information on events in the occupied areas of the Soviet Union? Although the Germans were well supplied with radios they only used them when landlines were not available. In the East they quickly built up a ground network using telephone cable and drehkreuz lines. This means that most traffic in the rear areas would go by landline.

However some organizations had to use the radio more often and their traffic could potentially be exploited.

Police

The German police - Ordnungspolizei was a militarized organization and during the war several of their units served as occupation troops in the East. Their radio communications were enciphered with the simple and double Playfair system and from 1944 the RS44 stencil. According to Major Schlake, head of communications in the Main office of the Ordnungspolizei only a small number of Enigma machines (about 20) were used by the police. According to 'The history of Hut 6' the Enigma was introduced in February 1944 for use by higher police officials in occupied Europe. The Brits called this key 'Roulette' and were able to solve it mainly thanks to reencodements from double Playfair.

There is no reason why the simple and double Playfair would resist an attack by the Soviet codebreakers. The GRU 1942 report says that police ciphers were identified and '*valuable reports were*

obtained about the fighting ability of partisans on territory occupied by the Germans.' This information must have come from police reports.

German railways

The German railways - Deutsche Reichsbahn used a small number of rewired commercial Enigma machines for radio traffic. The key used in Eastern Europe was named 'Rocket' by Bletchley Park and was first solved in early 1941.

The commercial Enigma was not as secure as the military version because it lacked a plugboard. On the other hand the wheels were wired separately for the Reichsbahn, so a cryptanalytic attack would need to recover the wirings first.

So far there is no indication that the Soviet codebreakers were successful with that task but it would be theoretically possible since no special cryptanalytic equipment was needed.

German Allies

Apart from German troops there were also Finnish, Romanian, Italian, Slovakian and Hungarian units fighting in the Eastern front. Their contribution was important especially in the period 1941-42, with numbers peaking in summer '42 at roughly 850.000 troops.

These countries used mainly hand ciphers so in theory their traffic should be vulnerable to cryptanalysis. As has been mentioned previously the traffic of the Romanian command was read in 1941-2 by the Soviet codebreakers.

The Germans were aware of the insecurity of some of their Allies cryptosystems and in 1942 they gave them a number of plugboard Enigmas but still most of the traffic would go through insecure systems. For example the cipher used by the Romanian police was found to be very simple and it was a security risk since the police routinely reported the movement of German units passing through their country.

Additional research is needed to identify the cryptosystems used by the minor Axis nations in the East and their exploitation by the Soviets.

Conclusion

The use of signals intelligence and codebreaking by the Germans and Soviets in the Eastern front is a subject that has received very little attention by historians so far. The main reason was probably the lack of adequate sources. That excuse might have been valid a few years ago but today the newly released TICOM material allows the researcher to discover many details about the performance of German sigint in the East.

When it comes to the Soviet side we know that they performed well prewar but there is limited information on the codesystems they solved during the war. The Soviet state invested significant resources in its signal intelligence agencies and the NKVD crypto department apparently gathered the

top mathematicians and linguists in the country. The collaboration of such a gifted group of individuals must have led to the solution of numerous foreign cryptosystems.

Unfortunately the information we have so far is limited and fragmentary. Perhaps more information will be released in the future.

Sources: 'The Mitrokhin archive', 'The codebreakers', 'The Crown Jewels: The British Secrets at the Heart of the KGB Archives', 'Russian cryptology', 'The History of Information Security: A Comprehensive Handbook' chapter 17-'Eavesdroppers of the Kremlin: KGB sigint during the Cold war', 'British intelligence in the Second World War vol2 and vol4', 'Decrypted Secrets: Methods and Maxims of Cryptology', 'The history of Hut 6' vol2, 'Kursk 1943: A statistical analysis', FMS P-038 'German Radio intelligence' , FMS P-132 'Signals Communications in the East - German experiences in Russia', 'The Soviet cryptologic service', NSA report: 'A World War II German Army Field Cipher and How We Broke It', Cipher Machines and Cryptology, CryptoCellar Tales, Inspectorate 7/VI Kriegstagebuch, '*О ВКЛАДЕ СОВЕТСКИХ КРИПТОГРАФОВ В ПОБЕДУ ПОД МОСКВОЙ*'

Various TICOM reports including DF-112, DF-292, I-20, I-91, I-121, I-129.

'Cryptologia' articles: 'Summary Report of the State of the Soviet Military Sigint in November 1942 Noticing "ENIGMA"',' Russian and Soviet cryptology iv – some incidents in the 1930's', 'Soviet comint in the Cold war'

'Journal of Contemporary History' articles: 'Foreign Armies East and German Military Intelligence in Russia 1941-45', 'Spies, Ciphers and 'Zitadelle': Intelligence and the Battle of Kursk, 1943'

'Intelligence and National Security' articles: 'The Soviets and Ultra', 'The Soviets and Ultra: A comment on Jukes' hypothesis', 'More on the Soviets and Ultra', 'The Soviets and naval enigma: Some comments', 'Kōzō Izumi and the Soviet Breach of Imperial Japanese Diplomatic Codes'.

Acknowledgements: I have to thank Ralph Erskine for sharing the 'Intelligence and National Security' Enigma articles, Frode Weierud for information on the German cryptosystems, Grebennkov Vadim Viktorovich for sharing information from his book on Soviet cryptologic history and Anatoly Klepov for general information on the history and achievements of the Soviet codebreakers.

Pics: Soviet flag from wikipedia

Copyright © Christos Triantafyllopoulos 2011-2024