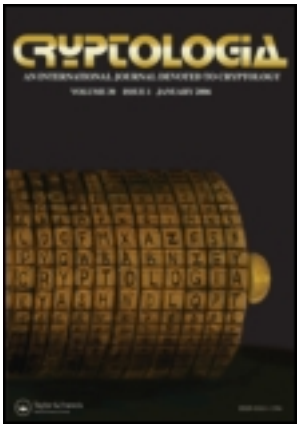


Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

# The Russian Fish with Caviar

Randy Rezabek

Published online: 21 Jan 2014.

To cite this article: Randy Rezabek (2014) The Russian Fish with Caviar, Cryptologia, 38:1, 61-76

To link to this article: http://dx.doi.org/10.1080/01611194.2013.797046

*Cryptologia*, 38:61–76, 2014

ISSN: 0161-1194 print
DOI: 10.1080/01611194.2013.797046



# The Russian Fish with Caviar

RANDY REZABEK

**Abstract** Historians have noted that the capture of the "Russian Fish" from the Germans was probably the most important outcome of the 1945 TICOM operation. Recently declassified documents have now provided a wealth of information pertaining to this vital break into Soviet communications at the dawn of the Cold War.

**Keywords** Caviar, GdNA Groupe VI, Karrenberg, Russian Fish, Steeple Clayton, TICOM



## Introduction

The first account in the open literature of the top-secret 1945 TICOM (Target Intelligence Committee) mission to capture German cryptologic materials, personnel, and equipment was by Thomas Parrish in his 1986 book, *The Ultra Americans*. In a chapter entitled, "The Russian Fish," he provided a general description of the operation and featured its most important outcome, the capture in Bavaria of a German intercept unit that specialized in the collection of Soviet multichannel teletype signals. The capture of this equipment and its operating personnel came at a moment, now that Germany was defeated, when Anglo-American intelligence officials began to focus their attention on the "Russian Problem." Parrish revealed that this unit was "flown to England, where the equipment was set up at an installation about twenty miles from Bletchley. It appears to have been put to work by the Allies immediately" [10, p. 284].

A year after Parrish's book was published, an amazing article appeared; a photo essay of the mission from the personal collection of Lt. Paul Whitaker, one of the TICOM officers who was a member of the team that recovered the "Russian Fish" at Rosenheim [15]. The photographs of the then still top-secret operation showed the progress of the TICOM team from Bletchley Park through various scenes in Germany to the digging up of the equipment by the PWs.

Little further information was published about the operation until James Bamford recounted the story in his second book on the NSA, *Body of Secrets*. He added a few additional details from other aspects of the mission, but concluded that the capture of the "Russian Fish" was "one of the most important, and most secret, discoveries in the history of Cold War codebreaking. . . . The discovery of the Russian code breaking machine was a principal reason why both the U.S. and British governments still have an absolute ban [as of 2002] on all details surrounding the TICOM operation" [4, p. 15, 17].

Address correspondence to Randy Rezabek, 213 Colonial Drive, Webster, NY 14580, USA. E-mail: rrezabek@rochester.rr.com

The following year, in his account of the TICOM mission, Michael Smith added the fact that "the top secret equipment was taken together with its operators, to Wavendon Manor where it was set up and tested against real Soviet transmitters." Richard Aldrich, in his history of the GCHQ, revealed that once the "Russian Fish" operation was set up in England it was given the codename "Caviar."[1]

These authors provided the gist of the story, but as these things go, the full story is much more nuanced and complex. Recent declassified TICOM documents from the NSA are beginning to fill in the details, including the identities of the German PWs, the number and types of the teletype receivers, the location of initial operations in England, and the type of Soviet traffic intercepted.

## The Discovery

On 21 May 1945, TICOM Team 1 (Figure 1) officers Lt. Cdr. Howard Campaigne, Maj. Edward Rushworth, and Capt. Thomas Carter went to the POW camp at Bad Aibling to follow up on a tip that a German prisoner, an Unteroffizier Dietrich Suschowk, had knowledge of certain signals intelligence equipment and documentation pertaining to the interception and decoding of Russian traffic. Suschowk explained to the TICOM team that he worked for General der Nachrichten Aufklärung (GdNA) Gruppe VI, a platoon size unit lately responsible for intercepting high level Soviet radio teleprinter traffic. The last location of this unit was at the Pionier-Kaserne, a barracks at Rosenheim, Bavaria. Suschowk, described as "the natural leader" of this group of 20 or so prisoners, was eager to cooperate with the Allies [7, Appendix 14].

The next day, the TICOM officers returned to Bad Aibling and escorted the Gruppe VI prisoners back to their quarters at Rosenheim (Figure 2), now occupied by a U.S. Army ration dump, and were put to work digging up the equipment buried under the cobblestones (Figure 3). The prisoners recovered a dozen large chests, 53 smaller chests, and another 53 boxes totaling about 7.5 tons [4, p. 16]. Suschowk and his team then volunteered to put one of the machines together and demonstrated that it was in good working order. TICOM officer 1st Lt. Paul Whitaker, who had joined the party at Rosenheim, later reported, "They were intercepting Russian traffic right while we were there. And pretty soon they had shown us all we needed to see" [10, p. 283].

The equipment was a special receiver that the Germans called the "HMFS" (Hartmehrfachfernschreiber; i.e., multichannel intercept teletype).[2] Designed to intercept the Soviet equivalent of the "Fish" traffic, these encrypted radio teletype signals had a twist (Figure 4). The Russians had devised a method to break the message into pieces and to transmit these segments multiplexed on up to nine separate channels. Without knowledge of the signal characteristics and the proper equipment, interception was very difficult.

The German prisoners and their gear were then taken to Seventh Army H.Q. in Augsburg and held awaiting transportation to the U.K. This provided both TICOM and Seventh Army G-2 an opportunity to initially interrogate the prisoners, who consisted of a senior NCO, three mechanics, 11 operators, two decoders, and four evaluators. Three in particular were found to be most helpful. The aforementioned Suschowk was described as an intelligent man with a firm grasp of the specialized

[1]See [13, p. 293] and [3, p. 49].

[2]*IF-162, Evaluation of Multichannel Teletype (HMFS).* NSA FOIA case #64093, 29 March 2011.

**Figure 1.** TICOM Team 1 in Germany: (left to right) PFC William E. Hoin (US), driver; LAC L.H. Howells (BR), radio communicator, F/Lt. Geroge H. Sayers (BR); Lt./CDR Howard H. Campaigne (US); Sgt. H.G. Anderson (BR) radio communicator; Capt. Louis T. Stone (US); 1st Lt. Selmer S. Norland (US); Maj. Angus McIntosh (BR); Major Ralph P. Tester (BR); Capt. Edward Rushworth (BR); W/Cmd. Oscar A. Oester (BR); Sgt. Clarence L. Ray (US), driver. (Photo by Paul K. Whitaker, originally published in Whitaker and Kruh [15].)



apparatus and its operating procedures. Unteroffizier Werner Hempel, an engineer by profession, was not only responsible for maintaining the equipment but also helped the Lorenz Company build it. TICOM commented, "He is not a leader like Suschowk, preferring as he does to get on with his job in a quiet and apparently efficient way." However, the most useful prisoner for TICOM eventually proved to be Unteroffizier Erich Karrenberg, a cryptanalyst. He was born in Poltava, Russia in 1911, the son of a German manufacturer. After being educated in Russia, he returned to Germany in 1930 to study music and was later employed as a lecturer in the History of Art and Music at Berlin University. He either joined the Army in 1939 or was called up in 1941 (sources vary), but nevertheless he ended up utilizing his Russian language skills in a wire-tapping detachment at the front. After a stint

**Figure 2.** The courtyard at Pionier-Kaserne barracks at Rosenheim, Bavaria, 23 May 1945. (Photo by Paul K. Whitaker, originally published in Whitaker and Kruh [15].)

**Figure 3.** German PWs from Gruppe VI, GdNA, at Rosenheim digging up the equipment buried in the courtyard, 22 May 1945. (Photo by Paul K. Whitaker, originally published in Whitaker and Kruh [15].)

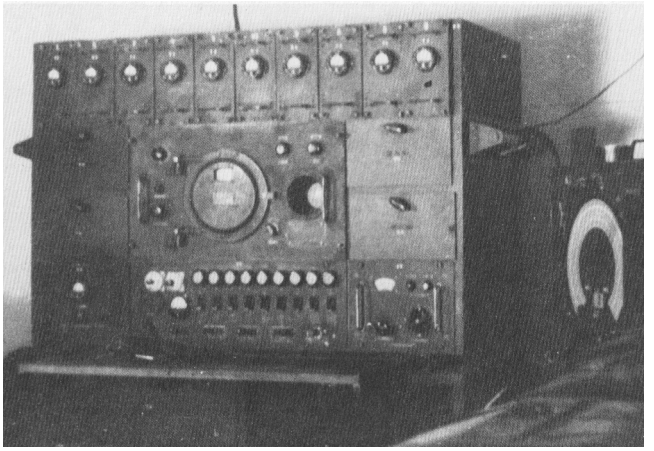

**Figure 4.** The Russian FISH itself, probably the Gerät 1309, or ''HMFS'' universal set. (Photo by Paul K. Whitaker, originally published in Whitaker and Kruh [15].)

teaching Russian to trainees at an Army school, he took a cryptologic course in August 1944 at Jüterbog and was later assigned to GdNA Gruppe VI, Referat 1b, where he specialized in working out the daily letter-scramble of the teletype text that the Russians transmitted.[3] TICOM's German specialist, Dr. Frederick Pickering, started chatting with Karrenberg during the packing of the equipment. Karrenberg's use of certain technical terms such as ''wheel-lengths,'' ''turnovers,'' and ''depths'' alerted Pickering that this was a specialized unit on par with Government Code

[3]CSDIC SIR 1717, *Consolidated Report of Six German Prisoners of the General der Nachrichten Aufklärung (Army Intercept Service)*. British National Archives, Kew, Surrey (PRO), HW 40/166. Available from *Christos Military and Intelligence Corner*, http://www.scribd.com/doc/85584902/CSDIC-SIR-1717 (accessed 7 July 2012).

and Cipher School's (GC&CS) units assigned to break the German "Fish." "We have not, in our TICOM field experience, met a more intelligent batch of Germans," Pickering later wrote. He immediately recommended that Karrenberg and his fellow NCOs be transported to England for detailed interrogations.[4]

Initial processing and transportation difficulties delayed the party at Augsburg. The equipment, all 7.5 tons, was boxed up and flown to the U.K. on 5 June accompanied by Maj. Rushworth and Capt. Carter. Six of the GdNA prisoners, selected for further interrogations, went by road to the jail in Wiesbaden, accompanied by Lt. Whitaker. In addition to Suschowk, Hempel, and Karrenberg, this group also included Unteroffiziers Erdmann, a specialist in NKVD traffic, Grubler, an electrician and radio mechanic, and Schmitz, an intercept operator.

## Tests at Steeple Clayton

The men were delayed in travel and did not arrive in England until 29 June, when they were sent to a site at Steeple Clayton, a village some 15 miles southwest of Bletchley Park. The captured gear sent down to the site by TICOM in the previous two days awaited their arrival, and the party was immediately put to work reconstructing the intercept equipment. Despite a few technical delays such as fitting the proper type heads to the printers and a lack of some test meters and tools, the nine-channel universal set was set up by the next evening. In addition to the intercept receiver, a wide band Fu. H.E.c., with two antennas, one 30 meters tall in a tree and the other an 18 meter on a mast were erected.[5] As a test, the German operator picked up some loud and clear Russian signals.[6]

The next day, 1 July, the printers were connected to the intercept unit and operations began. By midday, some traffic on a two-channel circuit around 8 MHz was intercepted, and by evening, the nine-channel Baku station (at 12.6 MHz) was picked up. Karrenberg kept busy preparing charts and index headings to begin the documentation of the intercepts. The Baku traffic was unencrypted and provided data such as locations of factories, the names of their managers, imports, shortages, and various types of commercial information.

At this point, the TICOM officials debated the question of priority. The engineer, Mr. Harold Kenworthy,[7] wanted to limit operations in order to do an in-depth examination of the machinery, but the traffic analysts, Capt. Jack Magilavy and D.R. Uzielli, wanted copious traffic. Since TICOM had shown a deep interest in the nature of the Soviet traffic, a decision was made to let the Germans practice their craft since "example was better than theory."

"On subsequent days therefore, the operators worked under the general direction of the evaluator (Karrenberg); they picked out the circuits which would give

[4]*TICOM IF-5 Notes on Field Interrogations of Various German Army and Air Force SIGINT Personnel.* NARA-CP, RG 457, Entry P-4, Box 1, Item #7419, 9.

[5]Fu. H.E.c, Funkhorch Empfänger-c (Monitoring receiver), 3.5 to 25 MHz. For illustrations of this set, see http://www.laud.no/ww2/fuhec/index.htm (accessed 30 May 2011).

[6]Details about the operations at Steeple Clayton are all from *TICOM M-8, Diary kept by Capt. T. Cartes, I.C. of Tests on Baudot Equipment conducted in the U.K. June 29 to July 8, 1945.* NARA-CP, RG 457 Entry 9037, Box 44, Item #6862.

[7]Kenworthy, former Marconi engineer and pre-war signals expert for the Metropolitan Police intercept station that collected diplomatic traffic for GC&CS, was by this time the chief of the Foreign Office Research and Development Establishment (FORDE) responsible for the interception of German "Tunny" traffic at the Y station at Knockholt, Kent.

him the T.A. data he required, held them for as long as he wanted and then left them."[8]

Over the next few days, traffic from two-channel and nine-channel circuits was printing solidly. The German PWs had attempted to set up the six-channel machine to monitor traffic on a Rostov-Moscow circuit but had experienced trouble due to jamming from an American commercial transmitter. The efficiency of the six-channel set was questioned, but the prisoners insisted that it was their best set; having been built in 1939, it served them in Russia.

Controversy among the TICOM evaluators continued with the engineers eager to get into the equipment, pointing out that there were many reception problems at the current site, there was a lack of directional aerials and facilities for diversity reception, and the few sets operating could not provide adequate coverage anyway. The operation's commander, Capt. Carter, felt that that they had a unique opportunity to observe German interception and traffic analysis technique firsthand, rather than learning about it through interrogations. A compromise was reached in the usual manner, and it was agreed to continue to collect traffic but put an increasing importance to the technical considerations.[9]

Finding that the propagation conditions were much better in the evening, an evening shift was added to the workload. By this time, some 10 to 12 two-channel links were discovered, but most of them were sending only synchronization signals. The Baku circuit continued to transmit unencrypted traffic of no great value. Work continued in setting up a second two-channel set, and the Germans were assisting in translating technical instructions.

However, the activity at Steeple Clayton was beginning to attract attention. The post office delivered a complaint that there was interference with local reception of the B.B.C. In addition, the amount of equipment the group was powering was exceeding the local 15 amps limit. Capt. Carter bought time by requesting the local authorities to investigate the trouble from their end and to let them know the results.

Over the next few days, work continued with both the engineers and the evaluators gaining confidence over their mastery of the system. A second two-channel machine was up and running in a separate hut by British personnel without German help. The T.A. effort was yielding results. However, the post office authorities were still concerned, reported that the trouble was in the electrical mains, and asked if the group had any unusual electrical machinery. A noncommittal reply was given.

The next day, 6 July, Capt. Carter along with the engineers, Kenworthy and Mason, reported to Bletchley Park to brief TICOM officials. The technical challenges of the site along with the unwanted attention from the post office resulted in the decision to cease operations in the next 24 hours. The Carter party was asked to write recommendations for both the short-term disposal and the longer-term future of the equipment and POWs.

The following day, final tests of components of the last nine-channel set were completed in the frame of the original machine while the rest of the equipment was packed up. The six-channel set was finally made to work satisfactorily. An interrogation team from TICOM also came down that morning to conduct the first formal interview of Karrenberg. It was also learned that Unffz. Erdmann, the NKVD specialist, was married with a wife and five children in the Soviet zone and would

[8]*TICOM M-8*, 3.
[9]Ibid., 4.

be unable to go home. Carter and the rest of the TICOM officers, always sensitive about the morale and motivations of their prisoners, were concerned.

The collection effort of Karrenberg's unit, GdNA Gruppe VI section 1b, was specifically responsible for the interception and evaluation of Russian Baudot traffic.[10] Its work could be broken down into three phases; interception, decryption via key recovery, and supporting traffic analysis, all of which were demonstrated during its week at Steeple Clayton. However, Karrenberg and his fellows could not explain everything; the output of Gruppe VI had been sent to GdNA Gruppe IV, the cryptanalytic division, whose section 3, under Lt. Alex Dettmann, did the actual analysis and evaluation of the Russian materials. Gaps in this knowledge were filled in piece by piece by TICOM over the next few months by careful examination of captured documents and further interrogations of other German personnel [1].



## The Technology

The technology behind the interception of "Russian Fish" can be traced back to 1874 and the efforts of the French telegraph engineer Jean-Maurice-Émile Baudot. In a desire to increase the speed, amount, and accuracy of transmitted text, Baudot adapted principles of the Hughes telegraphic printer and a five-unit code devised by Gauss and Weber to invent what would now be described as a synchronous time division multiplex system. The heart of his system was a distributor, which rotated brushes over a set of contacts, which connected a series of transmitter and receiver circuits into a single line. This allowed up to four channels to operate simultaneously [8]. The transmitted characters were interleaved so that the signal occurred in different time slots. Further development of multiplexing by Western Union allowed for the simultaneous transmission of eight channels by 1913. By 1936, further Western Union development of the Varioplex increased capacity to 72 channels of transmission [11].

The code Baudot devised for this system represented letters of the alphabet with five electrical impulses, the unit representing either a pulse (mark) or its absence (space). This resulted in 32 combinations, 26 representing the letters of the alphabet and six that could be assigned as control characters, such as a shift or a number. In contemporary terms, it can be described as a five-bit code.

The transmission was generated by a skilled operator manipulating a series of five piano-like keys in the proper pattern to generate the character signal, which could be printed out at the receiving end. In 1902, Charles Krum, a cold storage engineer, devised a "start-stop" code sequence to add to the Bardot code that allowed automation of the transmission. Both the transmitter and the receiver were now cued as to the start of the next 5-bit sequence, allowing a standard typewriter device to become the keyer. In 1908, the Morkrum Company developed the first commercial printing machine, and by the First World War this technology was being adopted by cable companies, railroads, and other corporations that had a need to communicate large amounts of textual data [9]. By this time, paper tape readers had been devised which allowed the message to be punched out ahead of transmission and then run through a reader. The communication demands of the war led to military interest in teletype, but

[10]This unit was part of the signal intelligence service of the army High Command, the *Oberkommando des Heeres/General der Nachrlchten Aufklärung* (OKH/GdNA), not as Parrish stated, the Armed Forces High Command signal agency, OKW/*Chi*. For a description of the organizational structure of GdNA, see [6, vol. 4, p. 12–16].

they also had to contend with the additional difficulty of security. Gilbert Vernam, an AT&T engineer, developed an automatic means to encrypt the Bardot code punched onto the paper tapes. By creating another tape of randomly generated letters (a key) and running it in step with the plain text, the two message streams could be added together with Boolean "exclusive or" (XOR) function to create a cipher of the original message. Thus, a space + space = mark; a mark + space = mark; a space + mark = mark; and a mark + mark = space. By reversing the logic at the receiving end with an identical key, it would automatically recover the original plain text message.

However, this system had a weakness, as identified by U.S. Army Signal Corps officer Major Joseph Mauborgne in 1918. The key tape had been formed into a loop and run continuously through the reader. If the message was long enough, this key sequence was repeated, creating a critical clue that would be exploited by a cryptanalyst. Mauborgne's solution to this problem was to utilize a key sequence that was as long as the message, thus never repeating. This created an unbreakable one-time tape system [17, p. 270–275]. However, this system was logistically difficult to manage, it required that two copies be produced of the key tape for each message, and could only be used once.

Teletype systems continued to develop throughout the 1920s and came into common use by both commercial and military users. By the beginning of World War II, German military communications services were replacing the paper key tape with encryption machines to produce the key sequence used in encrypted teletype messages. The Siemens T-52 Geheimschreiber and the Lorenz SZ-40/42 devices were based upon this design. The United States was rather late in getting into this game, not producing a similar crypto device until 1944 when it came out with the SIGTOT.[11] Multiplexing also continued to develop among the belligerents with the British developing a pulse-modulated microwave (UHF) radio relay known as the No. X10A early in the war. The U.S. Army Signal Corps also developed the AN/TRC series of VHF/UHF multiplexed transceivers utilizing up to seven channels, primarily for radio relay [14, p. 499].

Thereafter, Vernam encryption and multiplexing of teletype signals became a common practice among the major powers. The ability of RTTY to cover long distances without the need for landlines and the capability to transmit vast amounts of detailed texts without the need for highly trained Morse code operators were ideal for the Soviet Union. By the mid-thirties, the use of Baudot communications was extending across the USSR, and the Germans realized that they needed a means to intercept it.

## German Developments

In 1936, the OKW contracted with the Berlin firm of Lorenz to design and build a receiver that could convert the transmitted Baudot impulses into printed text. The Germans first intercepted Russian traffic of this nature in 1940 in Warsaw, however other priorities, including a reorganization of the intelligence effort giving the Army responsibilities for the military and diplomatic intelligence on Russia, followed by the increased workload of the invasion, put a low priority on the monitoring of Soviet internal communications [12]. In 1942, a Baudot interception unit was created as part of the Intercept Control Station, East (HLS Ost) at Lötzen, East Prussia. It was

[11]"T-52 Geheimschreiber." Crypto Museum. http://www.cryptomuseum.com/crypto/siemens/index.htm (accessed 19 April 2011); [5, p. 386].

equipped with the Lorenz technology, two nine-channel, two six-channel, and five two-channel sets. According to Section Chief Alex Dettmann, there were numerous problems with reception at Lötzen, and half the intercepted material was unreadable because of distortion, 35% of the material was of some value, and 15% was private messages dealing with family matters. Much of the evaluated material was of industrial and administrative matters, such as manufacturing requirements, plant completions, personnel training, and routine reports. Nevertheless, the material also included military matters such as special announcements from high military command and coded messages between the General Staff and various front staffs. Most of the Baudot circuits regularly covered included those links between Moscow and major regional centers such as Baku, Leningrad, Sverdlovsk, and others, along with inter regional circuits, including coverage of shipping, airline, and rail traffic [12, p. 2–3].

On 18 September 1943, a very rare meeting between "Goering's Research Bureau," the Forschungsamt (FA), and the Army cryptanalytic service was held at the FA headquarters in Berlin. The purpose of the meeting was to pass on technical information from Dr. Martin Pützel, the head of mathematical research at the FA, to his counterpart in the Army, Dr. Pietsch.[12] Pützel reported that for some time the FA had been intercepting Russian Baudot traffic and had made some progress on its decipherment. Traffic analysis indicated that these circuits were between Moscow and the high staffs at their Army fronts, communicated on one or two channels. FA cryptanalysis determined that it was machine-generated cipher with a particular anomaly; at every pause, it transmitted a compromise of seven characters of apparently pure key before shutting off. This of course produced a major crib for the cryptanalyst. The deciphered text yielded a plain (non-enciphered) five-digit code.[13]

Later, Dr. Otto Buggisch, who worked for both GdNA and OKW/*Chi* during the war, related to TICOM what he knew of the matter: "(I)... heard in 1943 that the FA had claimed some success on a Russian teletype machine and had reconstructed the machine. It was a machine with a very long cycle being not prime but the product of several smaller cycles like the SZ 42." He heard this from Doering,[14] "who was then doing his research on the T 52 but liaison with the FA was bad anyway...," and the next Buggisch heard was that the traffic found by the FA had stopped. Buggisch was again questioned about this teletype machine success of the FA and answered in written homework that

> The FA had analyzed a Russian cipher teleprinter system in 1943, and recognized that it must have been based on a machine having certain similarities with the German SZ-40. After a short time, the Russians altered the system. The FA then communicated its results to my unit... This was one of the very rare cases where the FA and In 7/VI exchanged results.[15] I did not study the FA results at that time, as I was not responsible for work on cipher teleprinters, and hence can give

[12]The Forschungsamt was the Nazi party's signal intelligence bureau, which reported directly to Herman Goering. They concentrated on internal monitoring and on foreign diplomatic and commercial communications.

[13]*TICOM DF-98, Russian Baudot Teletype Scrambler*. NARA-CP, RG 457, HCC, Box 1394, Item #4459.

[14]Mathematical researcher in GdNA, a specialist in machine ciphers.

[15]In 7/VI was the Army predecessor to GdNA.

> no details. At all events the Russian machine (just as in the German types SZ-40, SZ-42 but in contrast to the T-52 a, b, c, and d) gave only 32 different substitution alphabets, the succession of which became periodic only after an astronomically large number of steps. This succession was given by a system of pin wheels the peripheries of which were prime to each other at an estimate lay between 30 and 90. In any case there was no complicated mutual influence of the pin wheels on each other (as for example in the T-52 d). [6, vol. 7, p. 84–85]

Buggisch also added that "the Mathematics section of In 7/VI . . . worked on it and at the end of 1943, there was a 'Kompromiss,' (compromise) and a depth of 8 messages with the same setting was created. The section was able to recover 1400 letters of pure key, and to determine that the traffic was derived from a 5-figure code. The Germans postulated a machine like the German T-43, but was [*sic*] not able to prove any theories they had." [6, vol. 4, p. 111]

Sometime after September 1943, the Army took the project over from the FA and assigned their Baudot station to the interception of this Russian traffic.

The haul of gear later captured at Rosenheim included three different types of intercept receivers: the WA PRUF 7/IV, a six-channel machine built by Siemens-Halske, distinctive in its use of a cam mounted on a rotating shaft functioning as the distributor; the Gerät 1313 or the "HZFS," a two channel receiver; and the Gerät 1309, or "HMFS," a larger, "universal" set that could be configured to operate with two, three, four, six, or nine channels. Both the HZFS and the HMFS functioned similarly:

1. A standard radio receiver fed the intercepted RF signal into the machine. The signal was similar to a standard carrier shift teletype circuit, except that the shift was of 5000 Hz rather than the standard 850 Hz, indicating that it was probably generated by two separate crystal oscillators. The standard teletype start/stop pulse had been deleted from the signal and each individual pulse compressed to 10 milliseconds, most likely to increase traffic carrying capacity.
2. An automatic Volume Control and a rectifier unit changed the frequency into direct current.
3. A double mechanical distributor on a single shaft, utilizing brush contacts, synchronized to regenerate each channel. Synchronization, accomplished via the use of an oscilloscope, could be locked in with automatic circuits. With the HMFS, different distributors could be inserted into the machine to configure it for the different number of channels.
4. The output was sent into a pulse regenerator as a final stage that inserted a start-stop signal into the data flow and then stored it in a band of five relays that acted as short-term memory buffer (a "Speicher") before being transmitted to a corresponding teletype printer. This was necessary to expand the compressed Russian signal back to the standard 20-millisecond length.[16]

After the Russians went on the offensive and HLS Ost was forced to retreat out of East Prussia in fall 1944, the Army's signal intelligence service reorganized into

[16]*TICOM IF-162, Multichannel Intercept Teletype (HMFS)*. RG 457, Entry 9037, Box 44, Item #6860; and *TICOM M-9, Report on German Multiplex Intercept Equipment*. NARA-CP, RG 457, Entry 9037, Box 44, Item #6862.

the *General der Nachrichten Aufklarung*. The Baudot intercept section moved from Lötzen to Zossen and a few months later to Jüterbog in an attempt to improve reception, and was redesigned as Gruppe VI, Section 1b, under the command of Captain Rowder [6, vol. 4, 11–12, 15, 50, 83–84]. Unteroffizier Karrenberg was the technician primarily responsible for this traffic. The two-channel enciphered military traffic (codenamed "Bandwurm" by the Germans), was determined to be high-level circuits from Moscow to the Front Armies. There were also one or two links to the Air Force and one possible link to the Far East. Moscow acted as the net control station, and traffic from one Front Army to the other routed through this central point.[17]

Information derived from operator chat, message externals, and the study of frequent depths in the traffic led to some German assumptions about the system. Karrenberg stated to TICOM that the system contained two elements: a Baudot teleprinter producing 32 characters made up of the Russian alphabet along with a figure and a letter shift, and a cipher attachment consisting of five small wheels driven by one large wheel, creating a cipher with a period of 43. Despite this knowledge, the Germans made no effort to reconstruct the wheel patterns.[18] The cipher attachment had two settings, a "large" setting that gave a simple one-letter substitution for the key (i.e., the wheels of the cipher device did not move) and a "small" setting that engaged the gears of the cipher device, producing a seemingly endless stream of non-repeating key. The Russian teleprinter operators used the large setting to establish contact and test the mechanism.[19] This was probably done to simplify the process of setting up the circuit; the operators only had to refer to a table of the "letter of the day" to establish contact. This letter, sent in the clear, was repeated three times to ensure that the receiver had his machine set up correctly.[20]

Experience with the traffic, specifically close study of preambles, initial contacts, and operator chat, provided many clues into the cipher. Preambles of messages were always enciphered, but their stereotypical format and content provided cryptanalysts a clear insight into the beginnings of the cipher text. Contact traffic of the operators, in the "large" setting, often gave the setting away. When the key was not revealed in the set up chat, the Germans could often rely on depths (i.e., repeated messages) where the same plaintext is transmitted more than once at different positions in the key stream, giving cryptanalysts a means of comparison. Depths were due to bad reception, sometimes requiring repeating the message three or four times. Depths were also caused when the reciprocal station got out of phase with the sending station and the key sequences did not synchronize. Karrenberg commented, "When traffic is running smoothly, and on a day when a lot of material is transmitted, one can count on key-identity being given away by repeats."[21]

As to the nine-channel traffic, Karrenberg stated that the Russians had introduced two modifications during the war. First, the impulses of channels

[17] *TICOM I-153, Second Interrogation of Uffz Karrenberg of OKH, on the Baudot-Scrambler Machine (Bandwurm)*. NSA FOIA request, case #63702. 19 January 2011.

[18] *TICOM I-30 Report on Interrogation of Uffz Karrenberg at Steeple Clayton on 7th July, 1945 at 1100 a.m.* NARA-CP, Entry P 4 "Historians' Source Files Relating to Target Intelligence Committee Interrogation Reports," Box 1, Item #6889.

[19] *TICOM I-169 Report by Uffz. Karrenberg on the Bandwurm.* NSA FOIA request, case #64093. 29 March 2011.

[20] *TICOM I-30*, 2.

[21] *TICOM I-169*, 3–5.

1–2, 3–4, and so on were interchanged, thus leaving the ninth channel clear. Later channels 1–4 and 4–8 were scrambled, again leaving channel 9 in the clear. Karrenberg felt that the Russians assumed that this was enough to secure the system, but that a depth of 2,000 letters was enough to enable him to reconstruct it [7, p. 41].

## Traffic Analysis

The traffic analysis study by Magilavy and Uzielli at Steeple Clayton showed that the bulk of the traffic was two-channel military, with commercial traffic passed in the clear on six and nine channels. The message preambles and endings, such as originating station, serial numbers, group count, dates, address, routing, priority, and indicator were mapped out. In addition, some internal police (SMERSH) traffic was identified in the two-channel system. The frequencies used varied between 8 and 11 MHz and were changed at irregular intervals, which were easily tracked from the simple code used in the operator chat.[22] The Russians had a lack of security discipline when tuning, and operator chat often revealed the identity of the net. The call signs of all Soviet ground stations were made up of three letter characters, or a combination of three letters and figures [6, vol. 9, p. 5, 17].

Once the key was recovered and traffic deciphered, there were further challenges. Although commercial traffic was in plaintext Russian, military traffic was encoded in a variety of systems, including two, three, four, and five figure and five letter codes. A postwar TICOM chart lists 35 three-figure, over 40 four-figure, and at least 15 five-figure Russian codes attacked by the Germans [6, vol. 1, chart 1–2, 101–104]. How many of these codes were successfully read is not certain, but at least a few were. At the highest level, most secret communications were five-figure codes enciphered by one-time pads, a common practice of the Soviets, which the Germans did not even bother to attack.[23] The rest of the enciphered traffic was judged medium grade, which "the German cryptanalysts state . . . readily yields a solution while the One Time Pad messages are used only for traffic analysis. In general the Russian cryptographic and communications security is very poor, in fact, incredibly poor."[24]

However, this German effort against Russian Baudot communications was not without its problems and limitations. The war effort took many of the most experienced and talented operators and evaluators into other assignments, leaving less qualified and less motivated personnel in the unit. A post war U.S. Army intelligence report concluded

> It can be conclusively stated that the possibilities of the intercepting and evaluating branch were not fully utilized. The ease with which important results could have been obtained in unlimited quantities and in the shortest length of time was not recognized, or it was not properly valued. If the Russians now maintain operations in the same fashion, in less than half a year there could be important results in evaluating, if a sufficient number of baudot receivers are used" [12, p. 3].

[22] *TICOM I-33, Report on Traffic Analysis of BAUDOT Traffic by Capt. Jack Magilavy, A.U.S. and D.R. Uzielli, SIXTA*. NARA-CP, RG 457, Entry 9037, Box 121, Item #11284.

[23] The famous "Venona" intercepted Soviet cables were of this type. See [2, p. 6].

[24] *TICOM IF-162*, 3.

Gruppe VI remained at Jüterbog until the deteriorating situation forced them to again retreat, first to Stuttgart and finally to Rosenheim in Southern Germany, where they set up shop in the Poinier Kaserne and awaited their fate.

After the week of demonstrations at Steeple Clayton, the Karrenberg party was transferred to the Combined Services Detailed Interrogation Centre (U.K.) for further interrogations, which continued through October, November, and into December. They were questioned about the German effort against Soviet communications, NKVD signals, and German knowledge of Allied cipher machines, while Karrenberg was questioned about the specifics of the Baudot intercept effort and his knowledge of "Bandwurm."[25]

After the conclusion of the testing week at Steeple Clayton, the British moved the operation to its intercept station at Knockholt. Established in May 1942 at Ivy Farm, Knockholt, Kent, it was an outstation of GC&CS designed specifically to intercept German teleprinter traffic. It housed the Foreign Office Research and Development Establishment (FORDE), created to intercept German teleprinter Tunny traffic and transmit it to the cryptanalysts at Bletchley Park.[26] By May 1945, it had a staff of 815 civilian and military personnel. With the drying up of this traffic on VE day, Knockholt, with its specialized rhombic aerials, receiving huts and trained operators, was looking for a new mission. As station director, H. C. Kenworthy boasted in a November 1945 report "The Research Station, Laboratory and Workshops authorized by the Director especially for Non-Morse is able to tackle any problem put to it, and is able to arrive at solutions in a very short time."[27]

Armed with their newfound knowledge and technology, the British went into production of Russian teleprinter intelligence under the codename CAVIAR. Hoping for quick success, the British built up the program throughout the summer and fall. An example of their work can still be found in the archives, a collection of some two score intercepts from the Berlin-Moscow Baudot circuit reporting Soviet "Y" service data. These reports of wavelengths, bearings, station call signs and identities, and content (probably plain language), show that the Soviets maintained an active intercept and D/F program after the surrender and were now targeting the Western allies. This data was sent in a code the Russian called "SANATORIJ," a three-digit code written in five digit groups that was being read in part by the British.[28]



---

[25]See for instance, *TICOM I-30; TICOM I-149 Report by Uffz. Karrenberg and Colleagues on Allied Cipher Machines.* Available from *Christos Military and Intelligence Corner* (http://tinyurl.com/TICOM-I-149; accessed 16 October 2012); *TICOM I-153; TICOM I-168 Report by the Karrenberg Party on Miscellaneous Russian W/T.* NSA FOIA Case# 63702; *TICOM I-169; TICOM I-173 Report by the Karrenberg party on Russian W/T.* NSA FOIA Case# 63702; and *TICOM IF-123 Consolidated Report on Information obtained from the following: Erdmann, Grubler, Hempel, Karrenberg, Schmitz, Suschowk. CSDIC SIR 1717,* NSA FOIA Case# 63702.

[26]For more information on this topic, see PRO *History of interception of German teleprinter communications (FISH) by Foreign Office station, Knockholt, by HC Kenworthy, GCCS.* HW 3/163.

[27]*G.C.W.S. Ivy Farm, Knockholt Pound.* Kent & Sussex History Forum (http://sussexhistoryforum.co.uk/index.php?topic=1471.msg4887#msg4887; accessed 1 November 2012); [2, p. 14]; PRO. "Peace-Time Interception of Non-Morse Transmissions." HW 14/137.

[28]"Russian Y-Service Reports." NARA-CP, RG 457, Entry 9032 HCC, Box 202, Item #978; "Appendix D: Notes on Baudot Traffic" from folder "Baudot Charts Labeled Appendix A, B, C, and D" RG 457, Entry 9032 HCC, Box 1473, Item # 4903.

Shortly after VE day, negotiations began between GC&CS and the U.S. Army-Navy Communications Intelligence Board to extend their wartime cooperation to the Russian problem. From the American perspective, as laid out by OP-20-G Director Captain J. N. Wenger, cooperation with the British would provide a greater volume of raw traffic, increase the overall effort, and increase the collection of collateral information and physical possession of code books, translations of messages, and other related materials due to the worldwide presence of the British intelligence network. However, Wenger also expressed concerns about lack of American security control over these British assets and the possibility of high policy complications due to deviations between American and British foreign policy, such as on colonial policy.

## Caviar

Internal discussions and negotiations with the British continued through the summer. Details of the exact nature of the material to be shared and the liaison channels to be set up were completed by the end of July. The code name BOURBON was adopted for this program, and exchange of this material began on 15 August.[29] Undoubtedly, the CAVIAR material was a large part of the exchange.

The booty was divvied up by the end of July. The British sent one nine-channel unit and two two-channel units to the United States for use by the Army and Navy. Receivers, teleprinters, and associated spare parts were also sent along. By September, OP-20-G, under the leadership of former TICOM officer Lt. Joseph Eachus, was attacking the CAVIAR machine. However, by the following year, CAVIAR began to run into difficulties in both the British and American intelligence services, mainly due to personnel shortages caused by demobilization. The war diary of OP-20-G4-A noted that in April 1946, ''the big problem now coming up is CAVIAR. The British and the Army have both dropped it temporarily, leaving us with the whole responsibility. The greatest need is more long key, which is only available by reading depth.'' The following month, in relation to CAVIAR, ''some progress has been made on this, just how much will not be clear until the smoke blows away.'' Yet by early August, Cmdr. Howard Campaigne noted, ''CAVIAR is being put to bed by Blankinship as comfortably as possible. This is because lack of personnel forces us to temporarily abandon this project.''[30]

## Conclusion

The legacy of the Russian Fish and CAVIAR lived on into the Cold War. ASA collection and exploitation of Russian plain text teleprinter traffic began on a part-time basis in 1946, probably utilizing the ability of the Russian Fish to intercept nine-channel traffic. This program was expanded in May 1947 and placed under the direction of Jacob ''Jack'' Gurin, an ASA Russian linguist, who had the insight that this traffic, although individually not of much value, could in the aggregate track strategic trends in the Soviet economy. This program, a sideshow at first,

[29]''RATTAN Liaison.'' NARA-CP, RG 457, Entry 9032 HCC, Box 1471, Item #4870.

[30]OP-20G4-A War Diaries, September 1945, April, May, and July 1946, and Campaigne, handwritten note dated 7 August 1946. I thank Ralph Erskine for bringing these documents to my attention.

became crucial after "Black Friday," 25 August 1948, when code and cipher changes by the Russians dried up the traffic that had been exploited since the end of the war. For many years, this traffic provided the only SIGINT insight into the Soviet Union [16].[31]

Despite the wealth of information about the "Russian Fish" from recently released TICOM documents, many details are still obscured in the mist of classification. Much of the cryptanalytic data provided by Karrenberg in 1945 are still redacted.[32] Many questions are still unanswered in the archives: Did the Anglo-American SIGINT agencies produce their own (perhaps improved) version of the "Russian Fish"? Did the allies ever reconstruct the Soviet cipher machine? How much of the Soviet two-channel military traffic was read in the immediate postwar era? Did the CAVIAR program contribute to the breaking of the Longfellow and Coleridge machine systems? Hopefully, historians must not wait another 70 years for the mist to clear.



## About the Author

Randy Rezabek, PhD, is a retired instructional technologist and former US Navy combat photographer now embarking on his third career as an intelligence historian. He has been interested in cryptology and signals intelligence since serving a tour with the Naval Security Group in the 1980s. He became fascinated with James Bamford's description of the top secret TICOM mission in the book *Body of Secrets* and has spent the past four years studying it. He has published articles on the subject in *Intelligence and National Security*, *Cryptologia*, and the *Encyclopedia of U.S. Intelligence*. He is currently working on a book about TICOM.

## References

1. Aid, M. M. June 2003. The Russian Target: The U.K.-U.S. Cryptologic Effort against the Soviet Union: 1945–1950. Unpublished paper presented to the Annual Conference of the Society for Historians of American Foreign Relations.
2. Aid, M. M. 2009. *The Secret Sentry*. New York: Bloomsbury Press.
3. Aldrich, R. J. 2010. *GCHQ*. London: Harper Press.
4. Bamford, J. 2001. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. New York: Anchor Books.
5. Bauer, F. B. 2007. *Decrypted Secrets: Methods and Maxims of Cryptology*. Heidelberg New York: Springer.
6. *European Axis Signal Intelligence in World War II as Revealed by 'TICOM' Investigations and by Other Prisoner of War Interrogations and Captured Material, Principally German*. 1 May 1946. WDGAS-14, Chief Army Security Agency, Top Secret/Cream report: Vol. 1 Synopsis; Vol. 4 Signal Intelligence Service of the Army High Command; Vol. 7 Goering's "Research" Bureau; Vol. 9 German Traffic Analysis of Russian Communications. All nine volumes are available at the National Security Agency website, http://www.nsa.gov/public_info/declass/european_axis_sigint.shtml (accessed 5 January 2013).

[31]For British examples of this type of intelligence, see PRO HW 75/101–75/341, which includes a considerable amount of postwar Soviet economic, civil, and military reports including information on MGB personalities. The author thanks the reviewer for this reference.

[32]See for instance *TICOM I-169 Report by Uffz. Karrenberg on the Bandwurm.* NSA FOIA Case# 13586.

7. *Final Report of TICOM Team 1*. 16 June 1945. National Archives and Record Administration-College Park, MD (NARA-CP), RG 457, Entry P-11 "Archival and Historian's Source Files," Box 114, Item #10248. This and all other TICOM documents referenced in this article can be found on the author's website, "The TICOM Archive," at http://www.ticomarchive.com.
8. Hobbs, A. G. and S. Hallas. A Short History of Telegraphy, Part 2: Making a Record. http://www.samhallas.co.uk/telhist1/telehist2.htm (accessed 19 April 2011).
9. House, D. R. A Synopsis of Teletype Corporation History. http://www.baudot.net/docs/house–teletype-corp-synopsis.pdf (accessed 19 April 2011).
10. Parrish, T. 1986. *The Ultra Americans*. New York: Stein and Day.
11. Pollard, B. Muliplexing History. https://sites.google.com/site/mdprcp/multiplexinghistory (accessed 19 April 2011).
12. "SI-32 German Signal Intelligence Branch for Intercepting and Evaluating Internal Communications (Baudot and W/T) of Russia, Particularly Communications Concerning Economic and Industrial Development." *Christos Military and Intelligence Corner*. http://www.scribd.com/doc/90475797/SI-32-Special-Intelligence-Report (accessed 7 July 2012).
13. Smith, M. 2003. *The Spying Game*. London: Politico's.
14. Thompson, G. R. and D. R. Harris. 1991. *The Signal Corps: The Outcome*. Washington DC: Center for Military History, U.S. Army. http://www.history.army.mil/ html/books/010/10–18/index.html (accessed 8 January 2013).
15. Whitaker, P. and L. Kruh. July 1987. "From Bletchley Park to Berchtesgaden." *Cryptologia*, 11(3):129–141.
16. Williams, J. with Y. Dickerson, Researcher. 2001. *The Invisible Cryptologists: African-Americans, WWII to 1965*. NSA, Center for Cryptologic History. http://www.nsa.gov/about/_files/cryptologic_heritage/publications/wwii/invisible_cryptologists.pdf (accessed 17 October 2012).
17. Wrixon, F. B. 1998. *Codes, Ciphers & Other Cryptic & Clandestine Communications*. New York: Black Dog & Leventhal Publishers.