Before BOURBON:
American and British COMINT Efforts against Russia and the Soviet Union before 1945

MICHAEL L. PETERSON

INTRODUCTION

~~(S-CCO)~~ BOURBON was the formally assigned covername for a joint American-British COMINT project to target the Soviet Union after World War II. But it quickly came to be used as a covername for the target country itself. This was because, from the beginning of the project in August 1945 until June 1946, the project was compartmented.

~~(S-CCO)~~ Why, looking back from the 1990s, would the Soviet problem be compartmented? The simple answer is that Russia was an ally of the United States and Great Britain, and allies were not supposed to be listening in on each other's communications. Nevertheless, what started out as policy quickly became habit. Correspondence produced several years after the project title was formally cancelled continued to refer to the "BOURBON problem." It wasn't the Soviet Navy, it was the "BOURBON Navy." Those weren't Soviet or even Russian callsigns, those were "BOURBON callsigns," and so on.

~~(S-CCO)~~ BOURBON is believed to be the first organized, collaborative, cryptologic attack on the Soviet Union, although, as we will see, the Army's Signal Intelligence Service (forerunner to the Army Security Agency) actually assigned two cryptanalysts full time to the Soviet diplomatic problem in 1943.[1]

~~(S-CCO)~~ But this story, "Before BOURBON," is about the earliest documented American and British ventures against Imperial Russia and the Soviet Union. It should come as no surprise to anyone that the British, who were experts in this business for a couple of hundred years, had been reading Imperial Russian diplomatic correspondence since the eighteenth century. As might also be expected, the junior partner's interest went back only to the World War I era, when Russia was but one on a long list of the United States' "potential" threats.

(U) It is well known, of course, that following World War II, the Soviet Union grew into an aggressive military superpower with intentions of world domination. For almost fifty years, this cold war colossus heavily influenced America's international politics, distorted its economics, monopolized its national security seminars, and absorbed most of its defense dollars.

~~(S-CCO)~~ At the height of the cold war in the 1980s, the Soviet problem was the focus of an enormous SIGINT enterprise, with a [redacted] budget, employing [redacted] of highly skilled people, many for their working lifetimes. These included civilian and military collectors, signals processors and analysts, linguists, traffic analysts,

(b)(1)
(b)(3)-P.L. 86-36

cryptanalysts, supported by engineers and computer analysts. They all operated sophisticated computer-controlled or computer-assisted intercept, processing and analysis equipment to extract the intelligence from a wide range of communications and electromagnetic emissions, signals that could be found across almost the entire radio spectrum.

(b)(1)
(b)(3)-P.L. 86-36

~~(S-CCO)~~ During those years, the United States SIGINT System [redacted] used fixed stations, airborne platforms, ground-based communications satellite dishes, geosynchronous and orbiting satellites, and [redacted] facilities around the world. They poked every size and shape of antenna into the different electromagnetic environments to record a vast variety of Soviet military Morse networks, clear [redacted] links, single-channel [redacted] clear [redacted] voice communications, [redacted] But where did the cycle begin? Let's find its origin.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(U) Unfortunately, searching for the origin of a cryptologic event such as the beginning of the Soviet problem is a bit like looking for the headwaters of a great river: There are many tributaries, all of which are sources of a sort. But which tributary is the "original" source, the fountainhead?

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(U) Organized cryptology itself, like both general history and rivers, seems to have no absolutely clear-cut beginnings. It is more like a continuum, its origins lost in the misty past, its turning points arbitrarily dated and ill-defined, its outline revealed mainly by example (from which generalizations are drawn at great risk), marked by high points, low points, and occasional no-points, all affected by the uneven application of usually insufficient resources, and often hindered more than helped by the inevitable governmental reorganizations, restructurings, upgradings, and downsizings. Nonetheless, there are several places we can begin to look.

(U) If we define cryptologic history to include any form of secret communications, Mr. William Friedman, America's foremost cryptologist, will hark us back to the Spartan "scytale" (pronounced 'sid-ah-lee') of 900 B.C. as the origin of military cryptography.[2] If we narrow the definition to comprise only secret electrical communications, he will cite the invention and development of Morse wire telegraphy in the 1830s and its fairly extensive use in the Civil War, with all the expected cryptographic and cryptanalytic consequences.[3]

William F. Friedman

(U) If we want to get serious about the origins of U.S. cryptology in the era of wireless or radio communications, a practical starting point is World War I (1914–1918). And in a world where there is very little one can be certain about, it's a sure bet that in the United States there was no Russian problem before 1914. In fact, there was no significant U.S. government-sponsored COMINT effort until then, a situation that prevailed essentially from the end of the American Civil War.[4]

Herbert O. Yardley

(U) So, it's here in World War I where one can begin to detect traces, vaguely drawn, of the origins of U.S. interest in what was to become the Soviet problem. It was at about this time, 1914-1916, that both the British, who had been reading virtually everyone's diplomatic and commercial correspondence, in some cases for centuries, and the U.S. (in the person of Herbert O. Yardley at the State Department, who had had some success in diplomatic cryptanalysis), began to include Imperial Russia in their focus. When the Tsarist government was replaced in 1917 by the revolutionary Bolshevik regime, Russia became an increasingly important entry on the "potential enemies" list, which included just about everybody who counted: each other as well as the larger, more advanced countries of the world like Austria, China, France, Germany, Italy, Japan, Spain, Sweden, and Turkey.

(U) But before we proceed further, let's go back the beginning of Russia's cryptologic efforts and the two Allies' early attacks. This is essentially the story of three countries – Russia, Great Britain and the United States. First, let's look at what the fuss was all about in Britain and America. The target: Imperial Russia and the Soviet Union.

RUSSIAN AND SOVIET CRYPTOLOGY

(U) Russian secret writing first appeared in twelfth- and thirteenth-century manuscripts as simple letter-for-letter substitutions. Serious political cryptography coincided with the reign of Peter the Great in the early eighteenth century; the best available evidence comes from English records showing the solution of a Russian cipher system in 1719. Ciphers remained primitive, however, until about 1754, when Russian cryptology blossomed under Peter's daughter, Elizabeth. The deciphering side of this cryptologic coin emerged early in the nineteenth century when Tsar Alexander I gave credit to Russian cryptanalysis for helping to defeat Napoleon in 1812. Black chambers (where diplomatic and terrorist-enciphered written correspondence was analyzed) were established in post offices across the land later in the nineteenth century under the Okhrana, the notorious secret police.[5]

~~(SC)~~ According to Friedman, by 1915 Imperial Russian diplomatic cryptography was outstanding, "far ahead of anything anybody else had at that time."[6] Rather involved substitution and additive-based systems with very elaborately concealed indicators were employed.[7] These systems were also described as "frequently cumbersome in appearance, [but] adroit and cleverly devised."[8]

(U) In contrast to his country's diplomatic cryptographic prowess, the last Tsar's military cryptography was so feeble as to be disastrous. This failing was aptly demonstrated by Russian fortunes in World War I during the Battle of Tannenberg. The Imperial Russian Army lost 100,000 men or more directly because German and Austrian commanders had detailed and absolutely reliable information on the disposition and movements of Russian troops and strategic plans from reading unenciphered or poorly enciphered Russian military communications.[9]

~~(SC)~~ Following the overthrow of Imperial Russia in 1917, the Bolshevik successors, in an apparent eagerness to reject all vestiges of tsarism, initially abandoned the complex and relatively secure diplomatic systems. Government bureaus, military headquarters, police, etc., compiled their own codes and ciphers, and, until 1923, employed mostly primitive substitution and single transposition systems.[10] Involved, complex indicators seem to be the only phenomenon they retained.[11]

~~(TS)~~ In general, Soviet cryptographers have heavily favored substitution systems over transposition systems. In the very early days after the revolution, however, they frequently employed transposition systems,

> especially during the troubled years of 1920 and 1921, bearing with what might seem almost counter-revolutionary whimsy such names as the erudite SALAMBO, the political SPARTAK, the classical VULCAN, the grave SERIOZA, and folk names as TATIANA, MARTA, BAZIL. Other system names of this period are VIOLET, RAYON, KONGO, etc.[12]

Moreover, primarily the Latin alphabet and not Cyrillic script was used in these early systems.[13] In 1921, the Soviets began to make their cryptographic systems more complicated by combining transposition methods with substitution.[14]

~~(SC)~~ After 1923, some correspondents reverted to additive-based systems employing reusable key. In 1927, after the British Foreign Office published a white paper containing some deciphered Soviet telegrams, the functions of compiling and distributing cryptographic materials were again centralized, this time under a special department of the OGPU (a forerunner of the KGB). Shortly thereafter, systems and techniques originally developed in prerevolutionary times were revived and modernized to reflect current advances in cryptographic art, including the use of one-time pads. Also, extensive cryptographic training of carefully selected Communist party members was introduced.[15]

~~(SC)~~ On the military side, the Red Army made little use of radio before 1937, as approximately 70 percent of all radiograms intercepted by the Germans were originated by various NKVD (formerly OGPU) organizations, chiefly the Border Troops. Before 1937, the Red Army, and its subordinate air forces, confined most radio communications to the Military District level, using simple systems in effect for only short periods of time. Radio was usually observed only when units were deployed for out-of-garrison activities or during maneuvers and communications practice sessions. Little is known of Soviet Navy communications practices in the 1930s. This is because there was relatively little interest by foreign COMINT organizations, except for the British, who themselves did not work on Soviet naval systems between 1935 and 1939 because collection sites were diverted to intercepting traffic related to the Italo-Abyssinian war.[16]

~~(S-CCO)~~ As might be expected, most of what we know about Soviet cryptography during this period comes from the British, who had varying levels of interest, and from German records acquired after World War II. Before we address the British interest, let's answer the timeless questions of what the United States knew and when it knew it.

EARLY AMERICAN CRYPTANALYTIC EFFORTS AGAINST RUSSIA AND THE SOVIET UNION

(U) In his book *The American Black Chamber*,[17] Herbert O. Yardley, America's first modern cryptanalyst, discussed the Russians mainly in a chapter on deciphering a coded letter (a transposition cipher in the German language), prepared in 1919 by a Russian spy in Berlin, apparently intended for his superiors in Moscow and found in the wreckage of a plane that crashed in Latvia. Yardley's book puts far greater emphasis on the U.S. attacking the ciphers of Germany and Japan. Moreover, French and Spanish and even British ciphers get equal time. In fact, he claims his operation broke the diplomatic ciphers and codes of twenty countries, among which both Imperial Russia and the Soviet Union are listed, but not prominently.[18]

~~(SC)~~ According to another source,[19] however, Yardley's Cipher Bureau, Department 8 of the Military Intelligence Division (MI-8), which was established at about the same time as the Bolshevik Revolution of 1917 unfolded, received until April 1919 "a moderate quantity of Russian diplomatic intercepts," including cipher messages composed of five-digit groups and five-letter groups to ten-letter groups, of which apparently none was solved. In fact, the following statement was made in 1945: "The only Russian system ever solved by any American cryptanalyst prior to the Second World War was a transposition system using the German language."[20] That, of course, was the letter written by the Russian spy in Berlin.

~~(S-CCO)~~ In May 1920, Yardley's Black Chamber in New York apparently planned to work on the traffic of five governments, among which was Russia, albeit last in importance.[21] By 1921, however, as an apparent consequence of changes in U.S. foreign policy, American interest in Soviet traffic became "considerable." Soviet messages were divided into thirteen different categories, including plaintext traffic in French or English, Moscow-Berlin messages, traffic bearing either discriminants or key words, and a variety of three-, four-, five-, six-, and ten-digit and letter traffic.[22]

~~(SC)~~ As indicated earlier, none of these systems was solved by American cryptanalysts, despite work done on them and despite the availability of an interesting variety of collateral information such as the following:

a. details of the Comintern "cipher code," surreptitiously acquired from Stockholm, Sweden, in 1923;

b. similarly acquired explanation of a Soviet dinomic system in 1925;

c. [redacted]

(b)(1)
OGA

DIA

d. copy of a cipher system used by the Soviet Communist Party and its conduit for espionage, the AMTORG Trading Corporation in New York City, in 1928; and

e. details of what was thought to be a Bolshevik code used in Java in 1928, acquired by the Office of Naval Intelligence from Dutch authorities.[23]

~~(SC)~~ When Yardley's Black Chamber was closed in 1929, the Russian traffic was turned over to the Army's Signal Intelligence Section (SIS) (a forerunner of the Army Security Agency), staffed at the time with only five cryptanalysts (Friedman and his four assistants, Messrs. Rowlett and Hurt, and Doctors Kullback and Sinkov). A brief attempt was made to solve this and subsequently acquired Russian traffic, but with no success.[24]

~~(SC)~~ The AMTORG Trading Company was the focus of cryptanalytic attention again in 1931 when Representative Hamilton Fish of New York conducted an investigation into Communist propaganda in the United States. A congressional committee subpoenaed about 3,000 code messages from the cable companies and submitted them to the Navy's Code and Signal Section, itself composed at the time of only two cryptanalysts (Commander Safford and Lieutenant Wenger). When the analysis was unsuccessful, the messages were turned over to the army, with its five experts. All efforts proved fruitless, despite a great deal of work being done. Mr. Friedman even conveyed Representative Fish's offer to Mr. Yardley of payment of $100 per week for a few weeks to work on them. Friedman clearly anticipated Yardley's lack of interest ("I told them that your peg was higher up . . ."). Yardley was then at work on his articles on *The American Black Chamber*, which were about to be published in *The Saturday Evening Post* before appearing in book form.[25]

Frank B. Rowlett

~~(S-CCO)~~ If one is looking for another "origin," Frank Rowlett, one of those army civilians who emerged as a major leader in the postwar cryptologic undertaking against the Soviet Union, recalled that the AMTORG operation was the first formal U.S. effort to solve a Russian cryptosystem.[26]

~~(S-CCO)~~ Consequently, in Rowlett's view, in the 1930s three nations stood out from all others in the list of priorities, and Russia was not one of them. Exposing America's Pacific focus, Japan was by far the highest ranked, followed by Germany and Italy.[27]

~~(S-CCO)~~ Russia was not totally ignored, however, as Rowlett remembered:

> Several times between 1935 and the outbreak of World War II we [SIS] examined the Russian materials available to us; however, this examination was cursory and no serious effort was started in this period.[28]

(U) During the period 1939–1941, the Soviet Union was truly an enigma, neither friend nor foe. Americans had no love for the USSR, but their closest allies, Great Britain and France, were courting Stalin. From April to August 1939, with Austria, the Sudetenland and Czechoslovakia having fallen into German hands, Britain and France tried to negotiate a peace treaty with Russia in hopes of blocking further German aggression. But Stalin had other ideas. He was flirting with Nazi Germany during the summer of 1939, with an eye on acquiring land himself – the Baltic states, Finland, parts of Poland. The Soviets would have to fight for the West. They would only have to stay neutral for Hitler. On 23 August 1939, the Soviet-German Nonaggression Pact was signed. The Soviet Union took on the trappings of a foe.

(U) Those trappings were ripped off rather dramatically on 22 June 1941, however, when Nazi Germany invaded the Soviet Union. Suddenly, Soviet Russia, if not a beloved friend, was turned into a beleaguered ally of the two English-speaking democracies. President Roosevelt, squirming out of the neutrality legislation and bucking the American public's isolationist sentiments, quickly made promises of aid, as did the British.

~~(S-CCO)~~ British COMINT relations with the Soviet Union also changed dramatically (as we'll see below). But America, not yet at war, continued to concentrate cryptanalytically on Japan.

~~(SC)~~ After Pearl Harbor and America's entry into the war, apparently there was considerable discussion in American COMINT circles as to whether cryptanalytic resources should be diverted to the Russian problem, among others. It was decided that some effort should be put on the diplomatic systems of Russia, Spain, Vichy France, and others, because discussion of peace terms and the status of Germany's progress in the war might be found in such traffic.[29]

~~(S-CCO)~~ Rowlett also recalled that it was in "late 1942"[30] when a small section in SIS's General Cryptanalytic Branch was formally established to organize the intercepted Russian traffic and to attempt a diagnosis of the Russian cryptosystems under the strictest compartmentation. A group made up of five analysts in early 1943 was gradually expanded to twenty-five persons by 1 January 1944 and to seventy-five by V-J Day.[31]

SIS cryptanalytic operations at Arlington Hall Station during World War II (Person to right center is Ann Caracristi).

~~(SC)~~ During this period, there were three major sources of Russian traffic. The most important, in Rowlett's view, was the Washington-to-Ladd Field, Alaska, landline, which the Soviet government had been allowed to use and to which ASA had surreptitious access.[32]

~~(SC)~~ Another important source were the American telegraph companies. Until the end of World War II, wartime censorship laws allowed military intelligence access to copies of most telegrams leaving the United States.[33]

~~(SC)~~ Rowlett recalled that the third source was diplomatic traffic on foreign-controlled radio circuits copied by surplus communications operators of the cable companies, under contract. There was also low-priority coverage by army and navy intercept operators.[34]

~~(SC)~~ It was probably navy captain Joseph Wenger (who rose ultimately to the rank of rear admiral and who during World War II was head of OP-20-G, the Navy's cryptologic section) who remembered that the U.S. Navy began an attack on Soviet (probably naval) traffic in August 1943, but little seems to have been accomplished until the BOURBON project got under way in 1945.[35]

Captain Joseph Wenger, USN

~~(S-CCO)~~ After V-E day (May 1945), the ASA intensified the buildup of its Russian effort. Skilled technicians, freed up from the German effort, were assigned to the Russian section. The growing importance of the Soviet problem was indicated by the fact that these technicians were being carefully selected from the best of the population that had worked on the German effort.[36]

~~(SC)~~ One episode which created the suspicion (if there were none before) in the ranks of the army and navy that Russia was not to be trusted, was Stalin's behavior at the Potsdam Conference (17 July–2 August 1945). A few weeks before the conference opened, a series of most important Japanese diplomatic messages was deciphered. The messages contained instructions to the Japanese ambassador in Moscow to approach Stalin with a view of having Stalin intercede with the Allies for negotiating an "honorable peace." In simple form, the terms proposed were tantamount to an unconditional surrender, the only caveat being that "the integrity of the Imperial Household be maintained." Ultimately, the ambassador was unable to see Stalin and was given the diplomatic brush-off by the Soviet foreign minister. Stalin apparently showed himself to be less than forthright with Truman and Churchill (and later, Atlee), who were all aware of the Japanese initiative through the decrypts, by not revealing the Japanese proposal during the conference.[37]

~~(SC)~~ The Tokyo-Moscow messages also served to persuade both the army and navy cryptologists that the war would be over within the next few weeks, and that it was time to begin planning for the future. One of the earliest postwar plans implemented was the establishment of the BOURBON arrangement.[38]

(U) Now, let's take a brief look at the third main player in this cryptologic triangle, Great Britain.

EARLY BRITISH CRYPTANALYTIC EFFORTS AGAINST IMPERIAL RUSSIA AND THE SOVIET UNION

(U) As mentioned earlier, Great Britain had been reading Russian secret diplomatic messages since at least 1719. And because the German government, whose communications had been Britain's focus during World War I, had reverted after the war to the impregnable one-time pads, the absence of any useful German signals to intercept allowed the newly created Government Code and Cipher School (GC&CS) to begin concentrating its efforts on Soviet military traffic in about 1920; specifically, the British Army monitored the Soviets, and the Royal Navy handled Japanese signals.[39]

(U) GC&CS (the forerunner of today's GCHQ) had a leg up on most SIGINT organizations targeting the Soviet Union: a Russian refugee named Ernst Fetterlein. Nigel West, in his *The Sigint Secrets*, describes Fetterlein as "the eccentric Russian emigré who . . . before the October Revolution . . . had been employed by General Jilinski's Russian cipher service."[40]

~~(S-CCO)~~ Brigadier John Tiltman (about whom more later) was more specific. "Fetterlein," he wrote, "had been Chief Cryptanalyst of the Russian Tsarist Government and held the ranks of both admiral and general" prior to the revolution. He had come to work for GC&CS and easily mastered early Soviet codes.[41]

(U) Soviet decrypts provided the British with "invaluable insights into Soviet foreign policy," particularly evidence of Soviet attempts to subvert India and provide financial support to socialist extremists in England. In fact, in August 1920 the intelligence was so revealing of Soviet skullduggery that Prime Minister Lloyd George allowed some of the more incriminating decrypts to be published in the press in hopes of embarrassing the Soviet government into more acceptable behavior. Some cabinet members and Alistair G. Denniston, director of GC&CS, were appalled. As might be expected in these circumstances where sources (if not methods) were revealed, in December 1920 all Soviet radio traffic disappeared. It was replaced by a system of couriers. Soviet transmitters resumed operations in March 1921 in a more secure cipher. GC&CS broke the new codes within a matter of weeks, however, and the decrypts (forwarded to the cabinet with a cautionary note: "If intelligence is used for publicity it will be lost to us") showed that the Soviet government had no intention of honoring certain clauses of a new treaty in which Britain had formally recognized the Soviet Union.[42]

(U) In 1923, the British government again deliberately compromised the decrypts in a note of protest to the Soviet foreign minister. Additional changes in Soviet coding practices followed, culminating in the introduction of one-time pads later in the year.[43] Fetterlein reportedly broke the new Soviet ciphers at the end of 1925, allowing GC&CS to provide important decrypts to the British government until his retirement in April 1938.[44]

(U) In 1930, military service sections were introduced into what had been primarily a civilian-based GC&CS. Here the name of Brigadier John H. Tiltman first appears. Tiltman, who was in 1930 a retired major from the King's Own Scottish Borderers, was placed in charge of the Army Section at GC&CS.[45] After Fetterlein, Tiltman became the best-known British cryptanalyst of Russian systems (he was ultimately promoted to brigadier after being recalled to service in World War II).

~~(S-CCO)~~ Tiltman had studied Russian as a young military officer. Upon graduation in 1920, he was placed on temporary attachment for two weeks to GC&CS to attack a growing backlog of untranslated Russian diplomatic messages. Those two weeks grew into a year, and he never did return to his regiment. Initially, he worked for Fetterlein, learning cryptanalysis through on-the-job training. The British interest in Russian cryptosystems is not better demonstrated than by the fact that in 1921 Tiltman was posted to the intelligence branch of the British General Staff in Simla, India, where he then worked on Soviet diplomatic cipher systems for the next eight and one-half years.[46]

Brigadier John H. Tiltman

~~(S-CCO)~~ Until 1936, GC&CS's chief concern was illicit communications emanating from the Soviet Union.[47] Tiltman wrote that during the years 1931 through 1934, his primary preoccupation was with the study of Comintern cipher systems. Although the systems were complicated, the messages were virtually all read.[48] He explained:

> Starting about 1929, the Communist International set up a world-wide clandestine radio network to carry the intercommunications of the various national Communist parties with Berlin (not Moscow) as control. During 1930, our intercept consisted almost exclusively of telegrams between:
>
> a. Kompartei, Berlin and Komintern [*sic*], Moscow and
>
> b. Kompartei, Berlin and Comparty, London, known by us as 'Komintern' and 'Comparty' respectively.
>
> Both classes of intercepts were sent in 5-figure groups and were shown to have concealed indicators.[49]

~~(S-CCO)~~ Meanwhile, also in 1929, the British Army was keeping watch on foreign air traffic for the Royal Air Force, intercepting in particular Italian and Russian traffic from Sarafand in Palestine and from India. By 1932, the Waddington field station had accumulated a considerable amount of Russian air material.[50]

~~(S-CCO)~~ In 1936, Russian air traffic was still one of four requirements levied by GC&CS, the others being Spanish Revolution, Italian air, and German air.[51] And in 1940, although discussions took place on how to acquire Russian air traffic from the Transcaucasus to support British Middle East intelligence needs, apparently no traffic was collected.[52]

~~(S-CCO)~~ Turning to the Russian naval target, by 1937 the naval Y station (i.e., intercept site) at Scarborough was taking Russian, along with German traffic.[53] But there was a definite lack of purpose in the cryptanalytic work done on Soviet naval codes and ciphers until 1935, at which time all study was abandoned entirely until the outbreak of World War II. Limited traffic analysis was then resumed, supplemented in 1940 by the work done by a party of Polish analysts. Information was exchanged with the Finns; incidentally, the British cooperated with both the Finns and the Poles in SIGINT exploitation of Russian until 1941.[54] Several minor naval systems were broken into, and the decrypts were circulated, but they were too fragmentary to be of much interest. In September 1941, the Russian Naval Section was disbanded.[55]

~~(S-CCO)~~ Despite the lack of analysis at GC&CS, Russian naval traffic was being included, along with German, Italian and Spanish, in the intercept of the Y section of [redacted] (b)(1) from September 1939 until at least April 1940.[56]

~~(S-CCO)~~ Also in 1940, the British were reading five Russian weather codes.[57] It was the effort on these codes which brought about an interesting development following the German invasion of the Soviet Union in June 1941. In the minds of some, as we know, the Soviet Union had thereby become an ally. Therefore, it was not a SIGINT target but a potential collaborator in SIGINT matters.[58] Consequently, in early July 1941 the head of the air section at GC&CS wrote to the air ministry in connection with the meteorological problem. "It seems a pity," he penned, "that we should have to spend time breaking the cypher of a friendly power. Given an approach through the right channels, the Russians could surely be persuaded to hand over their cypher."[59] Inquiries were made, but with no success. After meeting with the Russians on the subject in September 1941, a British Army officer reported, "The greatest difficulty I experienced was the fact that no Russian officer can answer a question when it is put to him. Everything must be referred to the Kremlin for a decision." Negotiations continued into 1942,[60] but when the Russians requested information about British success with the high-level German cryptographic (Ultra) material, the British backed away,[61] and, like Lenin's view of the future of Soviet state power, British Army COMINT liaison with the Russians "was to wither away."[62]

~~(S-CCO)~~ In contrast to the army experience, British and Russian collaboration in the area of naval SIGINT briefly showed promise. In July 1941, Russia consented to the establishment of a small British naval Y unit at Polyarnoe near Murmansk. The station produced valuable intercept – 60 percent unique by one account – on the communications of German U-boats operating out of northern Norwegian fjords. But there were reporting timeliness problems and concerns over sharing the material with the Russians. In the first instance, the station had great difficulty transmitting the intercept results back to United Kingdom because of unpredictable ionospheric conditions in the northern latitudes interfering with radio communications. In addition, the British knew that the Germans were reading Russian ciphers and feared that their collaboration with the Russians would be discovered by the Germans. The station was closed in 1944.[63]

~~(S-CCO)~~ As World War II wound down, the Russian target reemerged slowly. By April 1945, the (b)(1) [redacted] Y station's collection tasks included Russian along with Italian, French, Spanish, Portuguese, Swedish, and German, including merchant shipping frequencies.[64]

~~(S-CCO)~~ Also by 1945, all British liaison with the Russians had effectively collapsed, and Russian material was again being analyzed, with plans for an expansion of Russian coverage. On 23 May 1945, the military services were instructed to make 643 radio sets available for Russian interception, and Y station commanders were to be informed that the new effort was to be treated as an "exotic" task, a label placed on any target except Germany and Japan.[65]

~~(S-CCO)~~ After the German surrender, intercept positions became available at all British Army stations for "exotic" tasks hitherto slighted. Foreshadowing the future: "Reports show how the operations were extended; shortly afterwards, directions were received to take up Russian problems on a larger scale."[66]

~~(S-CCO)~~ Related so far have been the individual efforts of the United States and Britain against Russia and the Soviet Union. Before BOURBON, however, there was also a history of Allied collaboration against the Germans in World War I and against both Nazi

Germany and the Empire of Japan in World War II, cooperation that eventually segued into BOURBON.

EARLY ALLIED CRYPTOLOGIC COLLABORATION

~~(S-CCO)~~ Over the years British COMINT authorities actively collaborated with a variety of counterparts in other countries. GC&CS liaised with the French during World War I, with the Poles and the Finns before World War II, and even in a limited fashion with the Russians during World War I and, as we have just seen, in World War II.

(U) Initial collaboration between Britain and its allies during World War I began in 1914, with the sharing of German naval codebooks; the Russian Imperial Navy offered the British Admiralty such a book recovered from a German cruiser run aground on Russian territory, and the Australians provided the British with a package of photographed German documents, among which was another naval codebook.[67] Subsequently, French military cryptanalysts began sharing German SIGINT information with the British Directorate of Military Intelligence (MI1).[68] In 1916, French direction-finding stations were apparently sharing with the British tracking information on German Zeppelin reconnaissance flights.[69]

(U) In the fall of 1917, the Americans provided the British with a codebook retrieved from a downed Zeppelin. In a note of thanks from Admiral Hall to Pershing's staff, the British promised that "any information therein which will be of value to the United States forces will be at once communicated to them."[70]

(U) The British, of course, had already made good in spades on that promise in the diplomatic arena. In February 1917, the British Foreign Office shared a translation of the famous Zimmermann telegram (which, incidentally, they had intercepted from a State Department landline) with the American ambassador to England. British motives for sharing this information were not altogether altruistic: They wanted the United States to enter the war, and they were successful.[71]

(U) The British also urged the American government to improve its methods of encoding War Department cablegrams, to protect them from German intercept and decipherment. Collaboration between Yardley and British cryptographers took place during his official visit to London in August 1918. This trip was in conjunction with Yardley's attendance at the Paris Peace Conference and his assignment to liaise with the French and the British in an attempt to learn all he could about the cryptologic methods of the Allies.[72] It was during this trip, by the way, that Yardley became aware that the British were probably reading all American diplomatic and military correspondence,[73] a favor the Americans returned to a limited extent over the next decade.[74]

(U) Eventually, Yardley was allowed to study all the methods of the British Military Cipher Bureau,[75] and he was invited to visit the Cipher Bureau at British General

Headquarters in France.[76] Yardley was also given extensive access to French cryptologic practices except their work on diplomatic ciphers in *La Chambre Noire*.[77]

(U) In addition, at least by 1918 the American and British fleets maintained close liaison, which included maintaining radio communications between their units and, consequently, sharing of cryptographic systems between their navies.[78]

~~(S-CCO)~~ Formal discussions on COMINT collaboration between the U.S. Army and the British began in the summer of 1940. Early in 1941, a mission made up of two Army and two Navy officers went to London, taking with them two Purple machines (analogs of cipher equipment that permitted the timely American decryption of certain high-level Japanese diplomatic communications) and associated materials. In exchange, the British provided much valuable information on German and Italian systems. Active collaboration began soon thereafter and reached the point where in 1944 the army was communicating continuously by radio with GC&CS. The U.S. Navy was in similar, but separate, communications with GC&CS. In separate agreements between GC&CS and the army, and between GC&CS and the navy, a division of effort was arranged whereby the U.S. would have primary responsibility for COMINT activities in the Pacific, and the U.K. would have similar responsibility in the Atlantic and in Europe, with intelligence and technical data exchanged freely.[79]

~~(S-CCO)~~ This arrangement would provide the basis for U.S. and British collaboration against the Russian target in 1945. But in the early days (circa 1943) little or no Russian intercept nor technical results of its long-established Russian effort were provided by the British to cryptanalysts at ASA. The American military intelligence offices (the army's G2 and the navy's Office of Naval Intelligence) received on a limited distribution basis certain information developed by GC&CS, but the ASA technical effort was denied the advantage of British technical results until about the end of the war.[80]

EARLY ARMY-NAVY COLLABORATION ON THE RUSSIAN AND SOVIET UNION TARGET

(U) Finally, American collaboration with the British against the Soviet Union in BOURBON involved extensive cooperation between the United States Army and the United States Navy. Before BOURBON, that was not the case.

~~(S-CCO)~~ To be concise about it, William Friedman wrote:

> Except for a brief collaborative effort to solve a large batch of AMTORG messages submitted by a member of Congress to the Navy in 1930 (both Services were unsuccessful, however), there was no collaboration in COMINT activities in the years 1920–1935, but only a more or less friendly rivalry in the solution of test messages.[81]

CONCLUSION

(U) Before World War II, the Soviet Union was neither a military superpower nor a significant COMINT target. It was nonetheless cryptanalytically challenging. Before BOURBON, Russia's diplomatic ciphers were relatively difficult to break; its military ciphers were relatively easy to read, a pattern that would continue well into the BOURBON period.

(U) Collaboration was limited before BOURBON, but precedents were set, seeds were sown that took root and blossomed during BOURBON. Clearly, British cryptanalysis was more advanced than America's, at least against the Soviet Union. The British seemed to be reading almost everything; the Americans, virtually nothing. So, collaboration, given British cryptanalytic expertise, initially benefited the United States, which eventually paid its bill many times over in terms of resources applied to the target and information shared.

(U) From the beginning, and well into the BOURBON period, collection was a sometime thing. Telegrams, acquired by hook and by crook mostly from the cable companies, comprised the bulk of raw traffic.

(U) Moreover, the cryptanalyst was king. COMINT exploitation meant cryptanalytic exploitation; the skills of traffic analysis and plain language processing played important but supporting roles. This relationship would change after 1948, when the analysis of communications externals and plain text began to provide greater value for money. Still to be heard from were the signals analysts and processing specialists, and ELINT, [redacted] and telemetry analysts, as well as the computer programmers and analysts, who in the 1940s were not even yet waiting in the wings, not required to join the cast and bring their act on stage until the 1950s and after.

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

(U) But the extraordinary American performances by Friedman and his team in the Army Security Agency, and by the navy's OP-20-G cryptanalysts led by such stalwarts as Safford and Wenger, against Imperial Japan, and the equally outstanding work done by Britain's GC&CS against Nazi Germany, set the standard for the next fifty years of collaborative COMINT effort against the Soviet Union. It was the skilled and dedicated people, trained and tested in the cryptologic battles of World War II, who became the leaders of the BOURBON project against the Soviet Union. With that kind of support, could BOURBON be anything but successful?

(U) That's another story.

NOTES

(All materials are available at the Center for Cryptologic History (CCH), in the Cryptologic Archival Holding Area, or in the NSA Library.)

1. A history of the Soviet problem, from the BOURBON days of 1945 through 1948, when most of the readable Soviet cipher systems disappeared and the character of the effort changed, is in preparation in the CCH.

2. *The Friedman Legacy: A Tribute to William and Elizebeth Friedman* (U), NSA/CSS, United States Cryptologic History, Sources in Cryptologic History Number 3, 29.

3. Ibid., 75–119.

4. Ibid., 121.

5. David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: The Macmillan Co., 1973), 614–618. Chapter 18, "Russkaya Kriptologia," 614–671, is one of the most comprehensive and interesting accounts of early Russian and unclassified Soviet cryptology available.

6. Quoted in *Data on Soviet Cryptographic Systems 1917-1933*, Serial TRQ-77 (hereafter cited as TRQ-77) (Washington, D.C.: Army Signal Security Agency, 1945) (TSC), 2; Cryptologic Archival Holding Area, Accession No. 6600, box CBMN61, NSA.

7. Tony Naples, *Soviet Manual Systems* (Unpublished Manuscript, drafted circa 1974), Part II, (TSC), 1. CCH General Collection.

8. ~~(C)~~ Burton Phillips and Suzanne Snook, "A Brief History of Russian Cryptographic Systems," circa 1946 (TS); Cryptologic Archival Holding Area, Accession No. 42572, box G03-0205-1, NSA.

9. *Friedman Legacy*, 164: Mr. Friedman says Russia "lost 100,000 men in the three-day battle. . ." Kahn, 627, writes that 100,000 men were taken prisoner, with an estimated 30,000 dead or missing.

10. Naples, 1.

11. Phillips.

12. Ibid.

13. Ibid.

14. Ibid.

15. Naples, 2.

16. Ibid., 7.

17. Herbert O. Yardley, *The American Black Chamber* (Indianapolis: Bobbs-Merrill Co., 1931), 239–249.

18. Ibid., 332.

19. TRQ-77, 3.

20. Ibid., 5.

21. Ibid., 6.

22. Ibid., 7.

23. Ibid., 9-13.

24. Ibid., 8.

25. Ibid., 14-17.

26. (U) Frank Rowlett, "Recollections of Work on Russian," 11 February 1965 (TSC), CCH Collection, Series VII.83, 1.

27. Ibid., 2.

28. Ibid.

29. Ibid.

30. Ibid., 2-4. ((FOUO) Robert L. Benson, however, in his forthcoming cryptologic history, placed the start as 1 February 1943.)

31. (U) ASA Memorandum for Col. Solomon, U.S. Army, at Pentagon, "History of BOURBON Problem," 12 March 1946 (TS); Cryptologic Archival Holding Area, Accession No. 5333, box CBNI21, NSA.

32. Rowlett, 4.

33. Ibid.

34. Ibid.

35. (U) Undated, unsigned typed note, with a handwritten annotation that it was "From a desc[ription] of cryptanalytic situation in Feb. 1946 in Wenger files," (SC); CCH Collection, Series IVAA.6.

36. Rowlett, 5.

37. Ibid., 6.

38. Ibid.

39. Nigel West, *The Sigint Secrets: The Signals Intelligence War, 1900 to Today* (New York: William Morrow and Company, Inc., 1988), 100.

40, *Ibid.*, 101.

41. (U) John H. Tiltman, "Experiences 1920-1933," (TSC) *NSA Technical Journal*, Summer 1972, 1.

42. West, 101–103.

43. Ibid., 104.

44. Ibid., 117.

45. Ibid.

46. Tiltman, 1–9.

47. West, 118.

48. (U) John H. Tiltman, "Some Principles of Cryptographic Security," (TSC) *NSA Technical Journal*, Summer 1974, 17.

49. (U) John H. Tiltman, "The Development of the Additive," (TSC) *NSA Technical Journal*, Fall 1963, 2.

50. (U) GC&CS history: ARMY & AIR FORCE SIGINT, Vol. IV – The Organization and Evolution of British Air Force SIGINT - I (TSC), 27. CCH General Collection.

51. Ibid., 35.

52. Ibid., 84-85.

53. (U) GC&CS history: NAVAL SIGINT, Vol I - The Organization and Evolution of British Naval SIGINT, Part 1 – The Making of SIGINT (TSC), 17. CCH General Collection.

54. (U) GC&CS history: ARMY & AIR FORCE SIGINT, Vol. IV - The Organization and Evolution of British Air Force SIGINT - I (TSC), 201. CCH General Collection.

55. (U) GC&CS history: NAVAL SIGINT, Vol. I - The Organization and Evolution of British Naval SIGINT, Part 1 - The Making of SIGINT (TSC), 222. CCH General Collection.

56. (U) GC&CS history: NAVAL SIGINT, Vol. II, The Organization and Evolution of British Naval SIGINT, Part 1 (Continued) - The Making of SIGINT (TSC), 32. CCH General Collection.

57. (U) ARMY & AIR FORCE SIGINT, Vol. IV (TSC), 137. CCH General Collection.

58. Ibid., 50, 75.

59. Ibid., 99.

60. Ibid., 100–104.

61. Ibid., 162.

62. Ibid., 135.

63. (U) NAVAL SIGINT, Vol. II (TSC), 40–45. CCH General Collection.

64. Ibid., 36.

65. (U) GC&CS history: ARMY & AIR FORCE SIGINT, Vol. II - The Organization and Evolution of British Army SIGINT - II (TSC), 348. CCH General Collection.

66. Ibid., 362.

67. West, 62.

68. Ibid., 57.

69. Ibid., 70.

70. Ibid., 83.

71. Ibid., 88-92.

72. Yardley, 203–209.

73. Ibid., 212.

74. ~~(S)~~ *Remarks on British Cryptographic Systems (1917-1932).* (Washington D.C., Signals Security Agency, 2 May 1945), (S); Cryptologic Archival Holding Area, Accession No. 3985, box CBNI16, NSA.

75. Yardley, 217.

76. Ibid., 219–220.

77. Ibid., 221–230.

78. Ibid., 201.

79. (U) Friedman memorandum for Mr. Grant Hanson, "Brief History of U.S. COMINT Activities," 20 February 1952, (TS), 10; CCH General Collection. Also "Review of Current U.S.-British Collaboration in the Communications Intelligence Field," August 1947, 1-12, (TSC); Cryptologic Archival Holding Area, Accession No. 1377, box CBPB57, NSA.

80. Rowlett, 7.

81. Friedman memo, 7.

(C) ~~(FOUO)~~ Mr. Peterson is currently a historian at the Center for Cryptologic History (E324). He began his career as an intercept processing specialist in the U.S. Air Force (1959-63). After his discharge, he transferred to NSA, first working as an intelligence analyst in A32 (1963-66) and later as section chief in A74 (1966-71). Subsequently, Mr. Peterson served as A Group product control officer, NSOC (1972-73); cryptologic staff officer in A8 and V5 (1973-74); cryptologic staff officer [redacted] (1974-76); branch chief in A23 (1976-83); deputy chief, Current Watch Operations, A11 (1983); chief, Plans and Programs, on the A Group Programs and Budget Staff, A043 (1983-85); deputy chief, A44 (1985-88); and chief, A65 (1988-92). In 1972 Mr. Peterson was awarded [redacted] His article "The Church Cryptogram: Birth of Our Nation's Cryptology" appeared in the Summer 1987 issue of *Cryptologic Quarterly*; a second article, "Maybe You Had to Be There: The SIGINT on Thirteen Soviet Shootdowns of U.S. Reconnaissance Aircraft," was published in the Summer 1993 issue. Mr. Peterson is a certified Special Research Analyst, Traffic Analyst, and Editor/Writer.

(b)(1)
(b)(3)-P.L. 86-36

(b)(6)