The Origins of the Soviet Problem: A Personal View

OLIVER R. KIRBY

The following has been adapted from a presentation made by Mr. Kirby at the second Cryptologic History Symposium on 14 November 1991. We have consolidated Mr. Kirby's prepared remarks and additional statements made at the symposium. Oliver R. Kirby became involved in the cryptologic profession while enrolled in ROTC at the University of Illinois. During World War II he worked on the German problem and participated in the TICOM project, a joint Anglo-American search for Nazi Germany's cryptologic personnel and equipment. After a progression of supervisory positions in the Armed Forces Security Agency (AFSA) and NSA, he became the first civilian Assistant Director of Production (equivalent to DDO) in 1966. He retired from NSA in 1968, although he returned to serve on the NSA Advisory Board in 1972. Mr. Kirby makes no pretense of providing either a complete or a balanced account of the early days of the Soviet problem in the cryptologic community. As he told the symposium audience, "I make no apologies – these are my highlights." Nevertheless, Mr. Kirby has much of value to say to the cryptologic community of today, not only about the past he witnessed but about the professional future we will experience.

DAVID A. HATCH
Center for Cryptologic History

My career in the signals business began at the University of Illinois in the fall of 1939 when I enrolled in the Friedman cryptanalysis correspondence course in ROTC.[1] I think a number of the early people around here came in through this course, so Billy Friedman had a good idea after all. After Pearl Harbor, I completed undergraduate work, then gave up a deferment that would have permitted graduate study in chemistry at Cornell. After I was commissioned in the U.S. Army Signal Corps in 1943, I came to Arlington Hall Station and was assigned with Dr. Pettingill, who was a linguist on the German problem. In January 1944, I joined the U.S. team working on the ENIGMA problem at Bletchley Park.[2]

The assignment at Bletchley Park was the "grand transfusion" where a lot of things took place. I'm not sure how much we contributed to them, but they contributed much to us, through everyone who had the experience of working there.

[1] Presumably "Elementary Military Cryptography," using Special Text No. 165 of the same title. The Center for Cryptologic History holds a copy of the 14-lession, 31-hour course dated 1940–41, with the 1935 edition of the text – presumably that used by Mr. Kirby.

[2] The central location for the British cryptanalytic effort against the German codes and ciphers.

The opinions expressed in this article are those of the author(s) and do not represent the official opinion of NSA/CSS.

In May 1945 I was attached to a British Royal Marine commando unit as a member of a Target Intelligence Committee (TICOM) operation in North Germany. Our main task was finding Germans who had worked on the Russian SIGINT programs; I thought it was strange but interesting. Through TICOM I had my first contact with the Soviet SIGINT problem when we interrogated members of the several SIGINT organizations of the Third Reich. Through this operation, designed to locate scientists and other former enemy specialists, I not only began my education in future work, but met and worked with several future officials of the Ministry of Defense and other government agencies of the Federal Republic of Germany. We discovered that they had developed some equipment to handle a special problem called "non-Morse," which was a BAUDOT teletype system. We didn't find the equipment, but we knew it existed; one of the other TICOM teams in southern Germany found it.

When I returned to the U.S. in July 1945 and began my tour at the Army Security Agency, I found I was looking at a different world – massive demobilization, military and industrial; Congress and country in disarray. We had just done what we were supposed to do – win a war – now where did we go from there?

No longer did we have a clear-cut mission and defined targets. The Naval Security Group (NSG) had concentrated very heavily on wartime Japanese and German Navy COMINT and was in effect without a COMINT job, just a COMSEC mission. The Army had taken on many worldwide nonmilitary targets, but no national authority had decided on the national intelligence value of the ongoing programs. With military and industrial demobilization and pink slips being passed out to wartime civilian employees of government agencies, we had no certain future for our business!

Fortunately, an effort was already under way at Arlington Hall on Soviet traffic. High-level diplomatic and trade messages filed with the U.S. Office of Censorship during the war years had been duplicated and copies were sent to the Army organization. Some of the traffic had been processed and subjected to the tried and true cryptanalytic attack used in enciphered code messages. Enough success had been achieved to demonstrate that this was not one-time pad encryption of code (as probably intended by the Russians) and that there was additive reuse – therefore there was a possibility of matching traffic and exploiting this target.

The Army G-2 always provided the intelligence guidance, and the Army G-2 Special Branch under then Colonel Carter W. Clarke identified some early fragments of recovered and decoded messages as possibly pertaining to Soviet espionage activities. Believing this would be of interest to U.S. policy makers, the cryptanalytic unit was encouraged to increase the effort on this body of traffic, and at the same time, precautions were taken to reduce the possibility of compromise.

Clarke was amazing. He gave me my first lesson on how to operate in this business. He pointed out that not everything was clear in terms of regulations. The rule we followed was simple. If it is not specifically prohibited, by law and written regulation, you charge – but you don't get caught! That was the rule we followed in a lot of the things we did.

With specific guidance from Colonel Clarke and Chief of Staff Omar Bradley, selected officials in U.S. departments and agencies were contacted and briefed on the initial program results. The fragmented data and presidential declaration that Russia was a great wartime ally resulted in our receiving little expression of interest from anyone but our own immediate boss, Frank Rowlett, and Colonel Clarke in G-2. We continued to work hard on this traffic.

Carter Clarke

Dissemination was very simple – we took it around by hand to the recipients and briefed them on what we had. In this case, the person we lined up to take the blame for whatever might happen was a guy named Omar Bradley, Chief of Staff, Army. I believe a lot of people don't know the procedure. We went to Bradley to get all our guidance on what we should do. He and Carter Clarke selected the potential recipients of this material. We took around a few grubby, scrappy items of information. We didn't have a case, we didn't know what it really applied to, but it was agent stuff: there were cover names, there was stuff about reports, but just fragments. We took this around to several places.

I think I have the distinction of being the only person who got kicked out of some of the highest offices in Washington. I was a lowly first lieutenant coming around from an agency nobody had heard of. Remember, we were operating under the anonymity of ULTRA, and it really succeeded; nobody knew who we were or what we were – we just didn't exist. This young fellow was coming around with stuff that didn't make sense and saying "I think this is Russian spy activity, probably right here in our own backyard, in Washington, D.C." At that point I was reminded that the president of the United States had declared that these were our glorious wartime allies, and I'd better be real [*sic*] careful who [*sic*] I talked to.

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

However, Carter Clarke and company still believed this was good stuff, so we in effect compartmented it. We selected the people we would talk to. There was very little interest expressed in the material.

During 1947 an ambitious and ingenious FBI analyst/agent, Robert Lamphere, discovered our fragmentary decrypts, and an exciting and productive interaction was initiated between the FBI and the small but highly skilled cryptanalytic unit headed by Meredith Gardner.[3] Successful matching of traffic in different codes sent months or years apart eventually resulted in decodes which enabled the FBI to identify active agents and build cases based on investigations and surveillance.

From our TICOM interrogations and later contacts with foreign SIGINT specialists, we became aware of Russian use of radio teletype. We also knew that they used BAUDOT teletype code rather than the more common international code, which added to the problem. [redacted] Our senior SIGINT bosses, faced with more demands than funds, also showed little interest in funding a program which in their view would "add to the growing stack of unprocessed intercept."

We began to intercept them using Hellschreiber undulator tape.[4] Anyone coming into this burgeoning unit learned the Cyrillic alphabet transcribing undulator tape by hand.

As a young officer convinced of the need to intercept this traffic which we knew carried some enciphered versions, and intending to return to my interrupted chemistry studies, I wrote a short but convincing paper on the need to address Soviet non-Morse traffic collection. It turned out to be a shocking paper. The opening line read, "There is a deplorable lack of understanding on the part of U.S. officials of the importance of the Soviet non-Morse program" – and it got worse from there! Distributed directly to U.S. users, to NSG, and to the U.K. liaison, the report came as a surprise to my superiors, two unpardonable sins.

Oliver R. Kirby

[3] This story has been told in Robert J. Lamphere & Tom Shachtman, *The FBI-KGB War: A Special Agent's Story* (New York: Random House, 1986). This is a personal narrative that contains many interesting insights, but, as the authors themselves admit, Lamphere and Shachtman did not have access to the full documentation; thus it should be used with care.

[4] German paper tape, predecessor to plastic recorder tape; manufactured by the German firm Hellschreiber.

The U.K. folks thought it was a funny but useful piece, my bosses didn't think it was funny at all, and while the Navy folks approved the idea, they said, "We're glad you said it, not us." I survived somehow, and the report did get action.

After the Navy and Army organizations received something over $200,000 between them, they pooled funds and set up a manufacturing program to build the needed [redacted]

[redacted]

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

During 1947 there was a dire need for qualified Russian linguists in the Navy and the Army organizations. On the Army side we discovered a small, select group of former OSS [Office of Strategic Services] linguists still working in the old State Department building in Washington. They realized they had a dead-end job and would be out of work soon. We eventually hired several of the most qualified, [redacted]

[redacted]

One of the acquisitions was Olin Adams, a musician and linguist well versed in Soviet military and industrial organization and philosophy. [redacted]

[redacted]

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

[redacted] [redacted] From mid-1948 for several years, this was an important and unique contribution to our users and a strong source of support for our growing COMINT program.

This was an early bread-and-butter problem. Along with the [redacted] this had high visibility, although we were also building a picture of their armed forces. Our object was to get attention at least at cabinet level, perhaps above, so we could get funding. We made pitches at high levels to get the people we needed to do the job better and give them more information. The military support was fine, but we needed the other to get the big money we were looking for.

The cooperation between the U.K. and the U.S. must rank high in the factors contributing to long-term program success. The 1948 London conference made the detailed agreements which became the UKUSA Agreement and formed the bases for the later Canadian and Australian agreements.

Of the results of the UKUSA Agreement, I believe the most important was the creative/productive contribution. Through interaction among long-term, wartime-experienced personnel with a variety of hard-to-find specialties, amazing new approaches and "least expensive, most cost-effective" solutions were generated. I believe the secret of success was the unusual situation of developing a new program and a new organization. The period of 1948 to 1964 in the U.S. SIGINT effort came quite close to the normal situation in competitive industry. There were more successes than failures, but the future hung on year-to-year responsiveness. Protection of the boundaries of the realm was low on the list of requirements which would justify continued existence; hence U.S./U.K. interaction to find ingenious and better solutions were welcomed by all involved.

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

In this period, in addition to the work on high-level cryptanalysis, [redacted] [redacted]

5. ~~(TS-CCO)~~ [redacted]

[redacted]

was unbelievable. We did believe our opponent could do unbelievable things if only mass were involved.

By 1948, after considerable debate on centralization and anonymity considerations, Secretary of Defense Louis Johnson adopted a plan to merge existing Army, Navy, and Air Force SIGINT and COMSEC functions under the Armed Forces Security Agency (AFSA).[6] The plan placed AFSA under the Joint Chiefs of Staff and established an AFSA Council intended to provide guidance. The AFSA members, however, had greater concern with individual service prerogatives than effectiveness of the functioning of AFSA. During the Korean conflict, the performance of the fractionate U.S. SIGINT effort was extremely and noticeably poor.

In the end, the results were so deplorable that it was evident the system was not working and must be fixed. We had to spend inordinate amounts of time trying to figure out how to get something done within the system.

As an example of how bad it was, we had roving intelligence consumer representatives running all through the place, and since they felt we couldn't process the stuff fast enough, they would take raw data and issue reports. They were often 180 degrees out of phase – greater, if that's possible! Not only were the results reprehensible, but the methodology and system just did not work. The only good thing to say about it was that everybody knew it was broken and had to be fixed.

Sooner or later, you had to invent NSA. However, it took quite awhile to do it.

President Truman in December 1951 directed Secretary of Defense Robert Lovett and Secretary of State Dean Acheson to form a committee to investigate the U.S. SIGINT establishment and to recommend remedial action to the cabinet members. From this directive was born the high-level committee headed by George Brownell. Some six months after establishment, the Brownell Committee submitted its conclusions and recommendations. These were the bases for a new National Security Council Intelligence Directive No. 9, as well as a presidential order establishing the National Security Agency. The consolidation of national-level SIGINT and COMSEC must rank as the most important factor in establishing and maintaining a viable, first-class cryptanalytic effort, as well as ensuring the highest-quality COMSEC effort.[7]

The consolidation and continuation of high-level cryptanalysis was basic, which made the Agency worthwhile, but it was not the only thing. Another was having the Agency manage the SIGINT information and see that national and tactical data got to consumers when they needed it.

Signal Discovery is a more descriptive term for what we sometimes call Search and Development. From the beginning of the Soviet program, extensive Signal Discovery

[6] A good source for information on the centralization of cryptologic activities after World War II, the formation of AFSA, the Brownell Committee, and the transition to NSA is Thomas L. Burns, *The Origins of NSA, 1940–1952* (Center for Cryptologic History, 1990).

[7] Ibid.

operations were a top priority in planning collection tasking. Detection, sampling, analyzing, and determining information values are the lifeblood of any dynamic SIGINT program. They are also the only viable means of identifying function and detailed characteristics of signals and systems as they are adapted to meet requirements of target users.

Initially and through much of the early development of the program, at least one fourth of our assets were dedicated to location and value analyses of target signals. This was the key to [redacted] to selective coverage, and to avoiding surprise, and was strongly supported by the SIGINT community. From time to time we even shifted assets to survey new geographical areas and to catalog signals for future reference. Had we experienced the tentative support which became commonplace in the later years, we could not have implemented a systematic and reasonably successful attack to find, collect and exploit signals providing priority information to customers.

There are what I term "baseline signals" in all time periods, with more today than at any time in our history. Early baseline signals were often limited to geographical areas. [redacted] systems. *Collecting, analyzing, and cataloging for* possible future emergencies appear to be as essential today as in any past time. As preparation for responsiveness to surprise requirements, I would consider this to be a national center function and responsibility.

The situation today is more akin to the pre-World War II situation than 1945. In 1945 we had experience and had demonstrated the value of SIGINT, which had been an important factor in winning the war. Resources were hard to come by, but not as hard as in the prewar era when the real pioneers fought their battles.

As you look forward, you have to do what is key to this time period – you must be responsive. If you don't provide something to make people think you are needed, you are not needed. That's your challenge.

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