DRAFT

Soviet Sophistication in Communications Security and Communications Intelligence.

Any design as to what safeguards must be provided the US COMINT effort against USSR and Satellite signal communications should consider the following related factors:

a. Soviet sophistication in cryptographic security: how "good" are their cryptographic systems; what security against cryptanalysis are they designed to afford; and, what security have they been found to afford in practice.

b. Soviet sophistication in communications intelligence: what they consider their own communications intelligence can produce; what they know enemy COMINT has produced against them in the past; what they expect their own communications systems to provide in terms of security against enemy analysis.

A. Soviet Sophistication in Cryptographic Security:

Soviet cryptographic security should be traced to its historical origin which may be inferred from the clandestine nature of the terrorist and subersive organizations of Czarist Russia from among which the Bolshevik party emerged. Cryptographers and historians of the Czarist Secret Police have published monographs on the cipher systems which these 19th century groups employed for their private correspondence.

It is interesting to note that the official Soviet "History of the Communist Party" approved by Stalin includes as an exhibit an enciphered message passed by the Bolshevik committee to the Communist group in the Czarist fleet at Leningrad. (St. Petersburg). Unfortunately not too much is known about Czarist cryptographic practices beyond the fact that the cryptographers had the reputation of competence in the cryptographic practices of the day. Practically nothing is known as to whether any Czarist cryptographic personnel continued to serve under the Soviets after the October Revolution, and in any event present day Soviet cryptography is a far cry removed from the systems reported from German and Austrian records as having been used in World War I.

After World War I the head of the Austrian cipher bureau, General Maximillan Ronge published a world famous book on the activities of his organization and the intelligence produced from monitoring Czarist and Bolshevik radio communications. Subsequent to World War I the Bolshevik invasion of Poland directed by Trotsky was decisively defeated due to the success of French and Polish cryptanalysis in reading the Red Army communications. The details of this success were recorded in an official Polish Signal Corps monograph. Both this Polish monograph and Ronge's book are cited and quoted by Russian lecturers on cryptographic security. The lessons to be derived from these past failures of Russian cryptographic practices are apparently basic in present day Russian thinking and training for cryptographic security.

After the first Russian-Finish war during the early period of World War II, the cipher section of the general staff of the Red Army published a series of lectures on cryptographic security which cited both the Polish monograph and Ronge's book, and further included an analysis of bad cryptographic security by their troops in the first Finish campaign. These lectures specifically pointed out cases in which cryptographic materials were mishandled, instances in which code books were captured and their loss not reported, and examples of improper message handling. Further available from German captured documents are the regulations of the Red Army and of the NKVD for the security of crypt rooms and cipher materials dating from approximately 1939 - 1941 and manuals for radio communications in the Red Army (includes the Air Forces of the Red Army), and the Red Navy dating in 1944 are available. From all of these the Russian philosophy both in communications procedures and cryptographic security is revealed. It is clear that they expect their tactical communications to be intercepted and compromised by loss or capture. The lectures on cryptographic security clearly indicate the time limit for which they expect these tactical cryptographic systems to provide protection. The regulations for code and cipher security also indicates the priority in which cipher materials are to be destroyed in the event that capture of a code room is expected.

Significantly first priority is assigned to destruction of additive, second to plain text of transmitted messages, and third to code books. The record of German cryptanalysis of all Russian cryptographic systems during World War II, and the continuing effort of the U.S. since World War II is well known and no one should have any delusion as to the fact that the Russians know what secure cryptographic systems are and employ them regularly and carefully. It is therefore pertinent at the present time to note that the Russians themselves assume that their tactical communications will be intercepted and their intentions in designing these systems is to provide security for only a limited period of time.

B. Russian Sophistication in Communications Intelligence:

We noted above in reference to the lectures on cryptographic security that the Russians were aware of foreign cryptanalysis and its present success against their own communications. It should be noted that the Russians have carefully studied the Pearl Harbor report and all of its implications. The Biblography of the lectures on cryptographic security in addition to the two works mentioned also refers to many of the standard international writers in this field. Actual knowledge of the Russian communications intelligence organization is extremely limited. However, during World War II German and Finish reports cited instances in which Russian COMINT had been used for tactical operations. A captured Russian Operational Order for Russian troops in the Ukrain cited without particular emphasis radio intelligence as among the intelligence sources forming the basis for this order and other instances of this sort of tactical or operational COMINT have been mentioned in German interrogation of Russian prisoners of war. Finally the Red Army manual on Radio Intelligence issued in 1944 and beginning with an appropriate quotation from Stalin on the value of radio intelligence is available and in the opinion of US radio intelligence experts is an excellent manual on tactical radio intelligence.

From defector reports obtained since 1946 there is evidence including in some cases copies of the reports prepared of the activities of Russian radio intelligence units monitoring the traffic of the U.S. and British occupation troops. It is noteworthy that all of the defector and captured document evidence available only reveals low level direction findings, traffic analysis, and plain text exploitation. The absence of cryptographic analysis above the R.I. Company level is striking. Finally the manual for Signal communications in the Red Air Force of 1944 provides that the Battle Headquarters of the Air Army shall have "intercept receivers for listening to the communications of the enemy Air Force."

There have been a few indications that the Soviets have interests in German cryptanalysis and intercept operators to the extent of questioning some of them, and more recently offering them employment.

During World War II the British attempted to set up an exchange in Signal intelligence with the Russians. While complete details of what was accomplished have never been revealed by the British it is known that the British delegates felt that the Russians were well on the way to, if not already successful in, cryptanalysis of the German cipher machine, Enigmas. In this regard it is interesting to note that when a U.S. and British team visited the German factory which had produced Enigmas they learned that a Russian Army team had preceded them, and of greater interest in the opinion of the German factory personnel, the Russian Army Officer had seemed completely familiar with the German Army model but had been more interested in the German Navy model which did differ in certain details from the German Army machine.

Conclusions:

While the above is intended to outline information available on Soviet sophistication in communications security and COMINT, it is clear both from the evidence listed above and from our knowledge of Russian communications, and the results of our studies that the Russians are highly sophisticated in both matters. It is suggested therefore, that a detailed study of all of the above evidence be initiated if not already under way in AFSA. It is also the opinion of the writer that in view of the Russian philosophy and cryptographic practices in regard to their tactical communications that they expect a large scale effort against these communications and have no illusion as to their ultimate cryptographic security. Therefore, it is believed that U.S. policy for work in this category of Russian communications is provided by Category "D" as presently proposed by the USCIB Security Committee.

THOMAS A. MILLER
USAFSS, Member
Security Committee