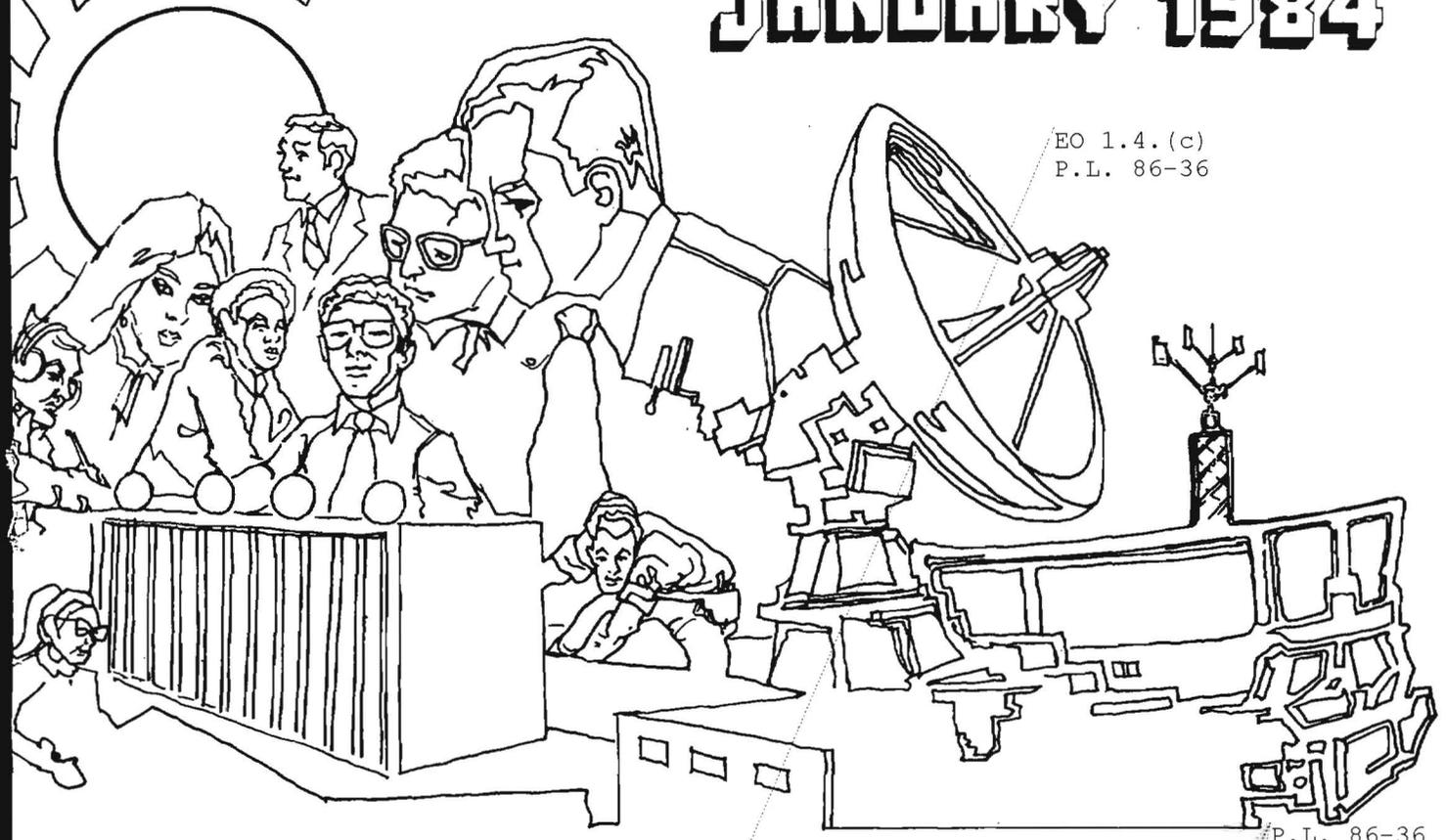


NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JANUARY 1984



EO 1.4.(c)
P.L. 86-36

P.L. 86-36

COMMUNICATIONS INTELLIGENCE AND TSARIST RUSSIA (U).....	[REDACTED]	1
PRESENT STATUS AND FUTURE DEVELOPMENT OF CHINA'S TELECOMMUNICATIONS (U).....	Zhu Gaofeng.....	13
1983 CISI ESSAY AWARDS (U).....	[REDACTED]	17
1983 CISI ESSAY ABSTRACTS (U).....	[REDACTED]	19
THE LANGUAGE PROBLEM AT NSA (U).....	[REDACTED]	24
[REDACTED].....	[REDACTED]	25
NSA-CROSTIC NO. 52.....	[REDACTED]	28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating~~
~~Agency's Determination Required~~

CRYPTOLOG

Published by Pt, Techniques and Standards

VOL. XI, No. 1

JANUARY 1984

PUBLISHER

[Redacted]

BOARD OF EDITORS

Editor..... [Redacted] (963-3045s)
 Asst. Editor... [Redacted] (963-1103s)
 Production..... [Redacted] (963-3369s)

Collection..... [Redacted] (963-3961s)
 Computer Security
 [Redacted] (859-6044)
 Cryptolinguistics. [Redacted] (963-1103s)
 Data Systems..... [Redacted] (963-4953s)
 Information Science
 [Redacted] (963-5711s)
 Mathematics..... [Redacted] (968-8518s)
 Puzzles..... David H. Williams (963-1103s)
 Special Research..... Vera R. Filby (968-7119s)
 Traffic Analysis.. Robert J. Hanyok (968-8418s)

For subscriptions
 send name and organization
 to: [Redacted], P14

P.L. 86-36

To submit articles or letters
 by mail, to: Pt, Cryptolog

via PLATFORM mail, send to:
 cryptolg at barlc05
 (bar-one-c-zero-five)
 (note: no '0' in 'log')

Editorial

~~(S)~~ Some years ago, during the early stages of the Vietnam War, one of the things we had on our wishlist was a way to get good, precise direction-finding fixes on the many VC targets we kept continuity on. Somebody theorized that what we really needed was an airborne direction finder, one we could put into an aircraft. However, we were assured that, for a variety of technical reasons, it couldn't be done.

(U) Of course, it could be done, because some time later, it was done. However, the thing that interested me most was that once someone had done it, there suddenly appeared a half dozen schemes for doing it. At least two principal methods came into general use at almost the same time, and they both delivered consistent and accurate results. It is a tribute to how well they worked that control of these new "assets" became a major political issue within the community at that time.

(U) The key to all this development and the sudden emergence of a new technique was, quite simply, knowing it could be done.

(U) Some time later, after our own systems were operational, we happened to learn that the French had managed to do it first, and also in Vietnam. Suppose we had known that from the first! I have always wondered what we could have done--and how much earlier--if we had known that it could be done, because someone had already done it.

WES

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.



COMMUNICATIONS INTELLIGENCE & TSARIST RUSSIA^(U)

by



P.L. 86-36

INTRODUCTION

This article explores the early development and use of communications intelligence by the Tsarist Russian regime through World War I and the importance attached to it, especially by the Russian Navy. The article is UNCLASSIFIED in its entirety.

Western publications in recent years have been providing frequent revelations about the use of communications intelligence (COMINT) by major nations of the world.[2] The one notable exception, at least in English-language publications, has been Russia. At the logical source, the natural secrecy attached to COMINT information in general, combined with the traditional obsession with secrecy throughout its society, has held discussion of the subject to a minimum. Outside the USSR, such imperial Russian failures in communications security as Tannenberg in World War I have contributed to the impression that the Russians must have known little about COMINT. Despite these constraints, however, since the early 1960s several rather specific articles concerning COMINT organizations and operations under the Tsars[3] and even on the early development on radio intelligence service in the Soviet Army[4] have appeared in Soviet journals. When supplemented with information available from non-Soviet sources, a general picture emerges of an early Tsarist COMINT effort approaching similar efforts in the West. This article is an initial attempt to shed some historical light on this little-known area of Tsarist intelligence.

It should be noted that the absence of any discussion in the present article concerning Russian Army COMINT activities before World War I or Ministry of Internal Affairs COMINT operations during WWI itself does not necessarily mean such activities did not exist, but merely that insufficient documentation was available from which to draw any conclusions. It should also be noted that the early Russian COMINT efforts apply to communications in their broadest sense, including secret or coded written messages.

Ministry of Foreign Affairs (MID)

Traditionally, communications intelligence involving foreign governments and their representatives fell within the purview of the Ministry of Foreign Affairs (MID). This tradition has been traced back at least to the reign of Peter the Great.[5] The methods used, of course, involved gaining access to the diplomatic correspondence, opening it (perlustration), and (if found to be encrypted) either purchasing the necessary cryptographic materials from a willing employee or actually engaging in operational cryptanalysis to exploit the document. Even so wily a statesman as the "Iron Chancellor," Otto von Bismarck, while serving as Prussian Ambassador to St. Petersburg (1859-1863), fell victim to MID's reading of Prussian ciphers.[6] MID was aided in its COMINT efforts by the so-called "Black Cabinets" of the Imperial Russian Postal Service.

Black Cabinets were set up at the post offices in major cities of the Russian Empire. One of their important functions appears to have been opening suspect correspondence, photographing the contents, and disseminating the information to the appropriate ministry:

- [] information of "general State interest," usually comments about the Imperial Family made by segments of Tsarist nobility, to the Minister of Internal Affairs;
- [] "political" correspondence to the Department of Police;
- [] "diplomatic" correspondence to the Minister of Foreign Affairs; and
- [] "espionage" correspondence (presumably during wartime) to the Army and Navy General Staffs.

According to one former Black Cabinet official, there was never much of a problem gaining access to or photographing the contents of foreign diplomatic pouches. When the diplomatic correspondence was found to be encrypted, it was not worked on at the Black Cabinet itself but sent to a "similar establishment attached to the Ministry of Foreign Affairs." Copies of all encrypted telegrams sent and received by embassies in St. Petersburg were delivered to this MID organization. In important cases, even copies of reports carried in locked leather briefcases by special diplomatic couriers were forwarded to this same unit.[7] As most couriers and embassy employees were underpaid by their governments, they could be prevailed upon for a small bribe to allow the contents of their briefcases to be photographed by Black Cabinet specialists.

The fact that diplomatic documents were encrypted only served to intensify MID's efforts to discover their contents. One Black Cabinet official described the ease with which foreign cryptographic materials could be obtained, even on the open market, in the following manner:

"Codebooks were acquired not only with the assistance of embassy employees but also in the cities of Brussels and Paris, where well-known persons engaged directly in the open trade of foreign codebooks for a fixed price.[8] The situation was completely identical in both cities. Codebooks which were of less interest to us, e.g., Greek, Bulgarian and Spanish, and could be obtained rather easily, cost 1,500 to

2,000 [rubles]. Such codebooks as those of the Germans, Japanese or U.S.A. cost several tens of thousands. The prices for the remaining countries fluctuated between 5,000 to 15,000. It was possible with this trading in codebooks to place an order for this or that new codebook, and these orders were filled within a short period of time."[9]

The "similar establishment" of the Ministry of Foreign Affairs to which the encrypted diplomatic correspondence was sent by the Black Cabinets was, of course, the main COMINT organization within MID responsible for diplomatic cryptanalysis. Little information is available on the specific structure and operations of this organization. Before World War I, purportedly, it could read the encrypted correspondence of at least France, Great Britain, Turkey, Austria-Hungary, and Sweden. According to one source the following additional countries' diplomatic correspondence was being read by MID cryptanalysts during WWI itself: Italy, Japan, Bulgaria, Romania, and Greece. Shortly before World War I this cryptanalytic organization was reorganized by Aleksandr A. Savinskij, Chief of the MID Cabinet (1901-10), and brought directly under control of the foreign affairs minister himself.[10]

Ministry of Internal Affairs (MVD)

Like the Ministry of Foreign Affairs, the Ministry of Internal Affairs (MVD), through the cryptanalytic organization of its Department of Police, was an important component of the Tsarist Russian COMINT community. The internal security and surveillance functions of the MVD, including the monitoring of communications of both anti-Tsarist revolutionary groups and the general populace of the Empire as a whole, have been rather well documented elsewhere.[11] What is not generally well-known is that, at least for a short period of time, the MVD expanded its jurisdiction to include monitoring the communications (as well as the movements) of foreign ambassadors, ministers, and military attaches based in Russia. This extension of the MVD into an area normally under sole control of the Ministry of Foreign Affairs occurred between 1904 and 1906. Included among those whose communications were being monitored by the MVD was the US Ambassador.

The monitoring of US diplomatic communications, according to the former chief of this self-described "Top Secret" MVD bureau, Colonel Mikhail Stepanovich Komissarov, had "enormous significance for Tsarist diplomatic initiatives." On 4 May 1917, in testimony before the Extraordinary Investigating Commission of the Provisional Government, [12] Komissarov stated:

"During the Portsmouth Treaty (Conference), we knew all the American conditions (positions) earlier than the American Ambassador [13] in Petrograd." [14]

This statement may have been only post-Revolutionary bluster on the part of Komissarov, but it might be added that the principal Russian delegate to the Portsmouth Conference, Sergei Witte, received the title of "Count" from the Tsar upon his return to Russia specifically for his work at Portsmouth. Thus, the Portsmouth Treaty Conference may not have been the major Russian loss or Teddy Roosevelt's personal victory, as it has so often been portrayed by historians.

Army Radio Intelligence

The integration of radio communications into the military forces of the major world powers at the beginning of the 20th century greatly expanded the horizons of COMINT in obtaining information on one's adversaries. It is unknown precisely when a radio intelligence service was first established in the Russian Army, but it undoubtedly was influenced by the successful radio intelligence set up in the Baltic and Black Sea Fleets during the 1911-14 period. [15] Although there was no centralized control of intelligence, COMINT or otherwise, within the military command structure overseeing both Army and Navy operations, according to a former Soviet Communications Service chief close cooperation did in fact exist between the Army radio intelligence services of Russia, Great Britain, and France. This cooperation included frequent exchanges of information on the operating characteristic of enemy radio stations, call sign constructions, and signal codes. [16]

In the Russian Army, at each Army Headquarters, radio intelligence operations were controlled by the chief of Army Communications through his Assistant for Technical Matters. Each Army's radio battalion had a radio intelligence squad or section, which operated two

radio stations: one station monitored the radio waves for enemy communications and, when it detected some, the other station then recorded them. Presumably, the radio direction-finding (RDF) stations also located at each Army Headquarters were controlled by the Assistant for Technical Matters too. (See Chart I.)

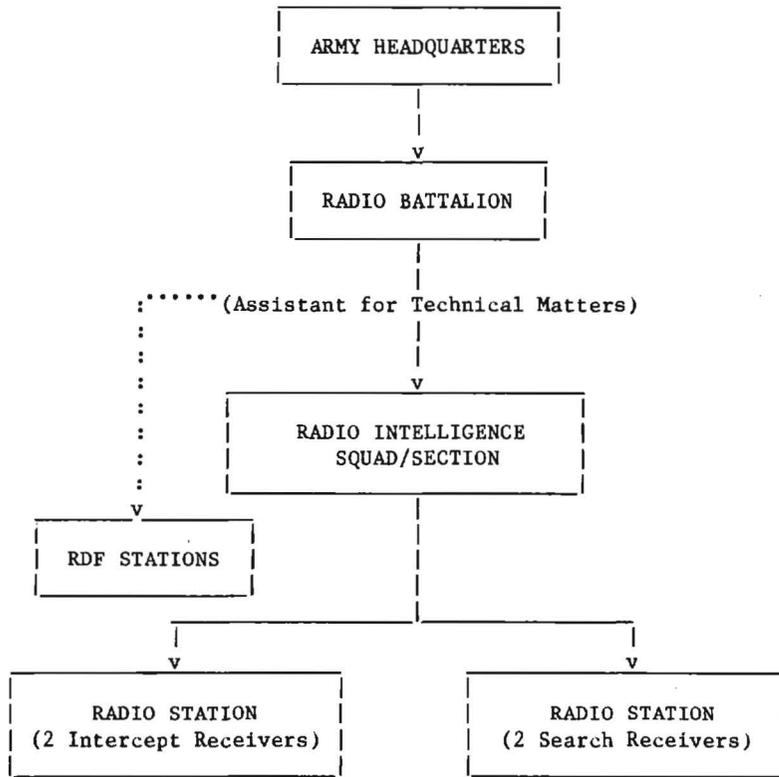
Although information on Russian Army radio intelligence operations is almost nil, one example can be cited. Between February and April 1915, on the eve of the German breakthrough in Galicia, Russian Army COMINT-provided information revealed the appearance of several new German Corps at the front, including a Guards Corps which had just been transferred from another area in Galicia. The radio intelligence service had discerned this information on the basis of certain peculiar operating characteristics of these corps' radio stations and by the distinctive "fists" of their radio operators. Russian RDF stations were also being used extensively at this time. [17]

By the end of 1915 the encrypted German Army radio messages were being intercepted on at least the Northern Front and sent to a "special bureau of the Main (Operations) Directorate of the General Staff" (SPETSIAL'NOE BYURO GLAVNOGO UPRAVLENTYA GENSH TABA) in St. Petersburg for cryptanalysis. According to one former high-ranking Tsarist intelligence officer, however, tangible results of this bureau's work were not passed on and the radio work itself was poorly organized in the Army, when compared to similar work in the Russian Navy. [18]

Navy Radio Intelligence

If communications intelligence was organized and operated poorly in the Army, the exact opposite was the case in the Russian Navy. In fact, the organizational structure of the radio intelligence service was so thoroughly developed during World War I in the Baltic Sea Fleet that operations undertaken by the fleet were almost always successful. Like the Baltic Sea Fleet, the Black Sea Fleet also had an effective, if somewhat less well-developed, radio intelligence effort. From available evidence, it appears that each fleet's radio intelligence service was independent and responsible ultimately only to its respective fleet headquarters.

BASIC COMINT STRUCTURE IN A RUSSIAN ARMY (circa 1915)



..... Postulated Control

——— Actual Control

(from Peresypkin, op. cit., p. 56)

CHART I

The decision to set up radio intelligence services in the Navy can be traced to the debacle suffered by the Russian Navy during the Russo-Japanese War of 1904-05 and the decision of young Russian naval officers never to allow such an occurrence to happen again. Restructuring of the Navy became the order of the day. In 1911 the Commander-in-Chief of the Baltic Fleet, Admiral Nikolaj Ottovich von Ehsen, appointed Captain 1st Rank (later Vice Admiral) Adrian Ivanovich Nepenin[19] to be Chief of Communications Service, Baltic Fleet. This appointment was to have enormous consequences on the development of COMINT in the Russian Navy.[20]

Nepenin immediately set about reorganizing the Communications Service to support the Baltic Fleet Command, not only with better communications but also with effective and accurate intelligence information. To this end Nepenin placed his closest assistant[21] in key Communications Service positions and the staffed the Service with only well-trained personnel. To further enhance the skills of enlisted personnel, Nepenin set up several Communications Service schools with special attention given to training "radiotelegraphic intercept operators" (RADIOTELGRAFIŠTISLUKħACHI).[22] Although it is unknown precisely when land-based radio intercept operations began in the Communications Service, according to the official Soviet history, radio intercept operations were carried out by Russian Baltic Fleet ships during training exercises held prior to the outbreak of World War I.[23] By the beginning of the war the communications service was well-organized and ready for action. However, it was only with recovery of the German radiotelegraphic codebooks from the cruiser MAGDEBURG, which had run aground near Oldensholm (now Osmussar) Island in the Baltic Sea on 26 August 1914, and the subsequent use to which they were put that the radio intelligence service really came into its own and became quite effective.[24]

Before going into specific examples of the use of COMINT information by the Russian Navy, let's look at the overall radio intelligence structure as it was set up in the Baltic and Black Sea Fleets.

At the beginning of the war the Baltic Fleet Communications Service was divided into three regions:

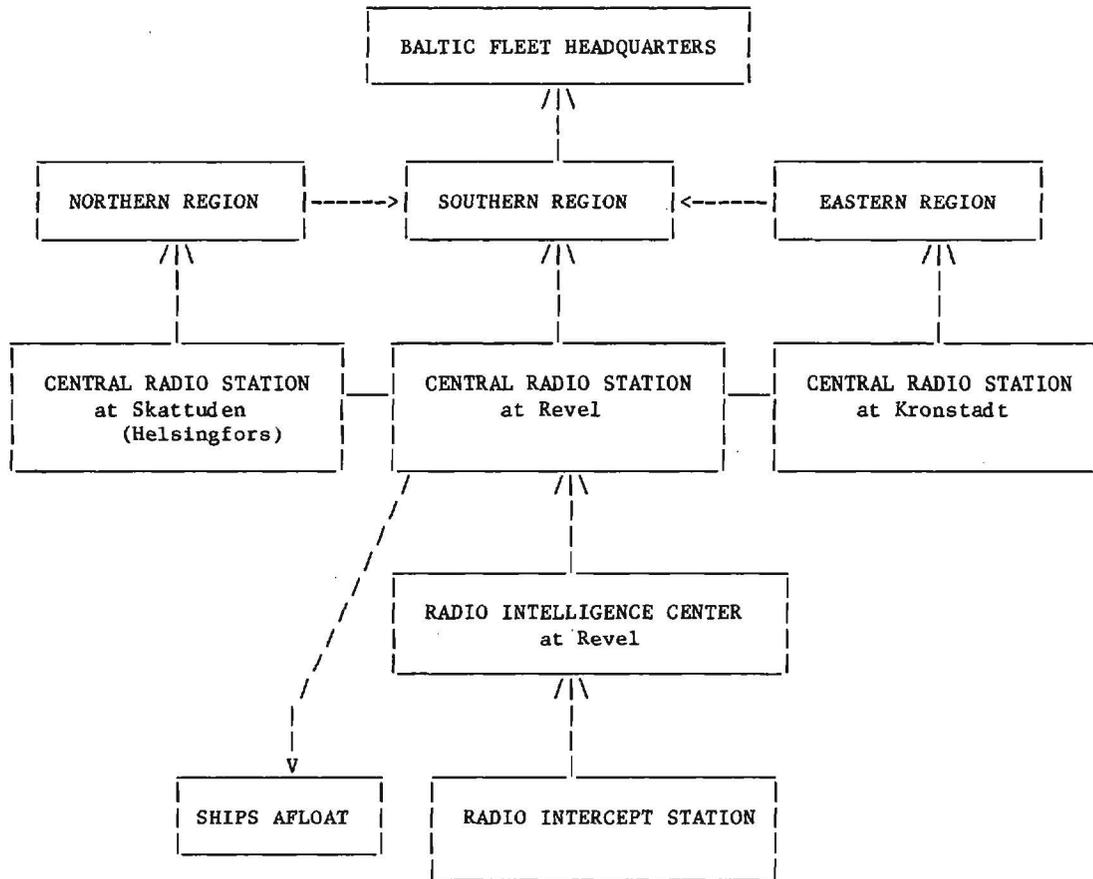
1. Northern, stretching from Helsingfors (now Helsinki, Finland) to the Abo-Åland Islands;

2. Southern, from the Kunda Inlet in the west to the German border; and
3. Eastern, covering the Gulf of Finland east of Helgoland Island.

Each of these regions had a Central Radio Station (CRS) attached to it which provided communications support to the fleet and received intelligence information from aerial reconnaissance and shore-based observation posts in addition to radio intelligence from intercept and RDF[25] stations. Except for the Southern Region, which served as the headquarters for the Chief of the Communications Service, it is unknown when the other regions first set up their COMINT stations. By the autumn of 1916, however, the Northern Region had five RDF and five radio intercept stations in operation, while the Southern Region had expanded its operations to five RDF and four radio intercept stations. It is possible that the Eastern Region did not have a COMINT effort at all or that the effort was only of limited duration. In March 1915 a so-called "Radio Intelligence Center" was set up at Revel (now Tallin), subordinate to the CRS of the Southern Region. This "Center" was probably connected with all radio intercept and RDF stations within the Southern Region by underground cable. It is possible similar "Centers" were established within the other regions to deal strictly with COMINT-related data before forwarding the information on to their respective CRSSs. Once the COMINT information reached the CRS, if it was time-sensitive and extremely urgent, it would be transmitted immediately to commanders of Russian ships operating in the Baltic. (See Chart II.)



EARLY DEVELOPMENT OF THE COMINT SERVICE IN THE BALTIC FLEET
(circa 1915)



— Probable reporting flow (From Zernov & Trukhin, *op. cit.*, p. 107;
 Yankovich, *op. cit.*, p. 116;
 Timirev, *op. cit.*, p. 46;
 Steblin-Kameskij, *op. cit.*, p. 620; &
 Dudorov, *op. cit.*, May 1959, pp. 35-36)

- - - - Postulated reporting flow

CHART II



accomplish this task by logically comparing facts and conjectures, which had been provided to him by Communications Service posts, both on the basis of decrypted German radio messages and bearings obtained by radio direction-finding stations. His predictions of enemy movements, sometimes very bold and apparently with little basis, almost always were vindicated. ... Not one operation was undertaken [by the fleet] without first receiving a detailed and almost always correct interpretation (of information) on the requested area from Nepenin."[31]

The importance of COMINT to the Russian Navy was not limited to officers of the Baltic Fleet. The chief of a special British military intelligence liaison mission in Russia, Sir Samuel Hoare, was also most impressed with the Russian Naval COMINT effort:

Although the Black Sea Fleet's radio intelligence organization was somewhat similar to the Baltic Sea Fleet's, there are fewer details available.[26] The Communications Service was divided into a northern region, stretching from the mouth of the Danube to Feodosiya, and an eastern region extending from Feodosiya to Batumi. Except for one known radio intercept station set up at Sevastopol' early in the war,[27] it is unknown if or when other similar stations were established. (See Chart III.)

"I was on intimate terms with certain officers of the Russian Naval General Staff and I learned many interesting details about secret codes and ciphers. In this branch of intelligence the Russians excelled. Their experts could unravel almost any cipher in an incredibly short period of time. One of them implored me as a friend and ally to ask the British Foreign Office to change a cipher that he could read almost as easily as his daily paper."[32]

It might be added that while some of the equipment for the radio intelligence services was provided to the Russians by foreign firms,[28] some of it was constructed by specialists of the Russian Navy Department itself,[29] possibly associated with the Naval Ministry's own radiotelegraphic equipment factory (now called the "COMINTERN" factory).[30]

The information provided by the radio intelligence service under Nepenin's direction was looked upon with such favor by the Russian Naval Command that it was one of the reasons why Nepenin was designated as Commander-in-Chief of the Baltic Fleet in September 1916. Nepenin was succeeded as Chief of the Communications Service by Captain 1st Rank Davydov,[33] the head of the Communications Service's analysis and reporting section. Davydov may himself have been succeeded by Captain 1st Rank Novopashennyj,[34] who was noted as Chief of the Baltic Fleet Communications Service in 1917,[35] and Novopashennyj by Captain 1st Rank Rengarten.[36]

The use of COMINT information by the Russian Navy during the war, especially in the Baltic Sea Fleet, proved to be very effective. Part of the reason for this effectiveness, according to a former high-ranking Tsarist Baltic Fleet officer, lay in the analytical judgments of Captain Nepenin as chief of the Baltic Fleet Communications Service:

"Nepenin had developed to the highest degree the gift of establishing a complete picture of the movements of enemy ships and from this determining the plans and intentions of the enemy. Nepenin was able to

In the Baltic Fleet, the first operation known to have been taken on the basis of COMINT information[37] took place on 14 February 1915, when the Russians learned in advance the scheduled times for the arrival and departure of a German cruiser at the port of Libau (now

Liepaya). A Russian submarine was immediately dispatched and sank the cruiser as it left Libau. COMINT information also played a major role in mine-laying operations involving German ships in the Baltic. On 14 May 1915 the radio intelligence service decrypted a message from the German mine-layer DEUTSCHLAND revealing the location of a German minefield in the area of the Bogsher-Dagerort islands, thus allowing the Baltic Fleet Command to take corrective measures.[38]

Another example of the utilization of time-sensitive information derived from COMINT by Russian ships afloat occurred on 1 July 1915. A detachment of Russian cruisers, while in transit to bombard German targets in Memel (now Klaipeda), received a report on the location of a scheduled rendezvous between the cruiser AUGSBURG and a group of other German ships. The Russian detachment then broke up the rendezvous by forcing the German ships to retreat.[39]

The high point in the operations of the Baltic Fleet's radio intelligence service was reached on 31 July 1915, when the Russians gained foreknowledge of the German Navy's proposed forcing of the Gulf of Riga in conjunction with the German Army's seizure of the city of Riga. Information obtained by cryptanalysis, as well as from aerial reconnaissance and shore-based observation posts, provided the proposed time and date of the offensive, including the deployment of enemy forces. When the German Navy attempted to carry out the operation on 8 August, ships of the Baltic Fleet were already in place and broke up the attack.[40] By May 1916, however, the Germans began to restrict their use of radio communications in the Baltic and the Baltic Fleet Communications Service had to rely more on aerial reconnaissance for advanced warning of German activities.

As a result of its operations, the official Soviet history of the Russian Navy in WWI rated the Baltic Fleet intelligence effort very highly:

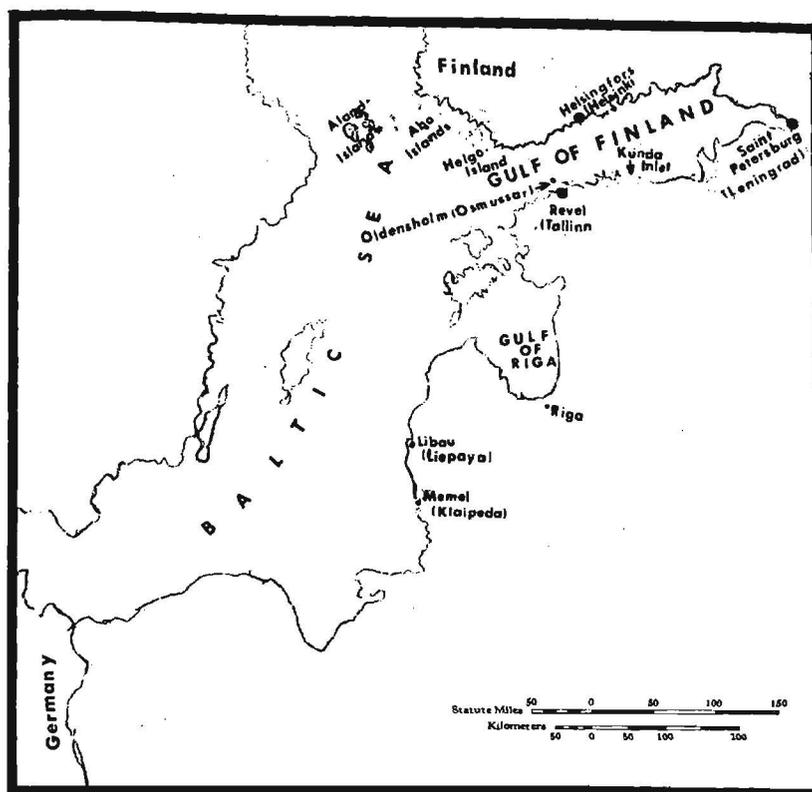
"The organization of operational intelligence in the Baltic Fleet reached a very high level of development during the First World War. Fleet Headquarters received timely, precise, reliable information on the activities and intentions of the enemy. Thanks to this, the Fleet Command right up to the end of the war had the opportunity to be both forewarned about enemy operations and to organize in a timely manner countermeasure.

"In carrying out reconnaissance activities in the Baltic Theater of Military Operations (TMO), Baltic Fleet Headquarters used agents, submarines, naval air reconnaissance, radio-technical [SIGINT] facilities, a widely developed network of NIS (Observation and Communications) posts, and on certain rare occasions, surface ships. For purposes of reconnaissance, an especially high value was placed on the use of radio-technical facilities.

"Radio-technical intelligence in the Baltic Fleet during the period of 1914-1915, in essence was the primary type of intelligence in that TMO."
[41] [Emphasis added. TRH]

The earliest known example of an operation undertaken by the Black Sea Fleet based on COMINT occurred in September 1916, although undoubtedly there must have been earlier operations.[42] The Russians were aided in the Black Sea Fleet radio intelligence effort by the Turkish Navy's reliance on the Germans for cryptographic material, which the Russians already had in their possession. On 15 September 1916 Black Sea radio intelligence elements (subunits) intercepted information from a shore-based Turkish radio station regarding the sweeping-up of Russian mines obstructing the approaches to the Bosphorus. A large Turkish transport ship was to pass through the swept area with a cargo of coal from Zonguldak. Russian ships were quickly sent to relay mines and the Turkish ship was sunk. In December 1916 the Russians decrypted an order for a German submarine to return to Constantinople along with the coordinates of the mine-swept channel through which the submarine was to pass. Torpedo boats were immediately dispatched from Sevastopol' to mine the area. It was learned by the Russians within 48 hours through another decrypted message that the submarine had been sunk by the mines. This was the last German submarine to embark for the Black Sea during the war. Up until the last days of WWI Black Sea Fleet radio intelligence facilities played a key role, in conjunction with aerial reconnaissance, in informing the Black Sea Fleet Command of the German battleship BRESLAU's departure to sea.[43]





Conclusion

It is clear from the above that communications intelligence was an important and integral part of information-gathering under the Tsars. The invention of radio and its integration into the military forces of the major world powers at the turn of the century also opened up a new horizon for Tsarist COMINT activities, although the Russian Military Command appears to have been somewhat slow in recognizing the possibilities inherent in using the radio for intelligence purposes. Nevertheless, Tsarist Russia, whatever faults it may have had, was not totally inept in intelligence-gathering, as implied by some historians; and, despite its slowness, it did achieve some success, at least in the Navy, with its use of COMINT.

FOOTNOTES

1.



2. Kahn, David, The Codebreakers, New York: Macmillan, 1967; Winterbotham, F. W., The Ultra Secret, New York: Harper & Row,

1974; Beesly, Patrick, Very Special Intelligence, London: Hamish Hamilton, 1977; and Montagu, Ewen, Beyond Top Secret Ultra, New York: Coward, McCann & Geoghegan, 1978, to list just a few.

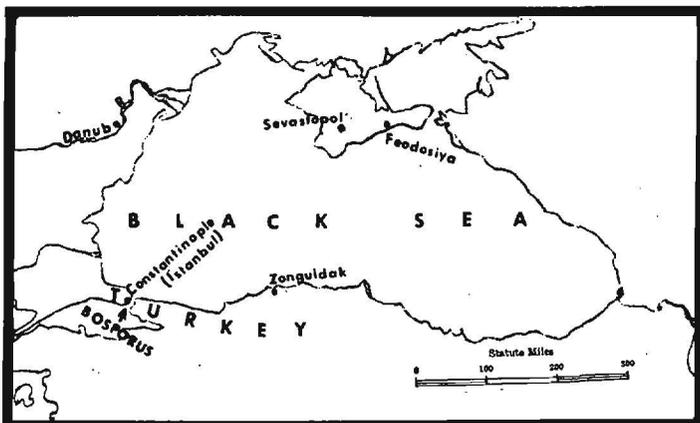
3. Yankovich, V., "On the Origins of Radio Intelligence in the Russian Navy," Voenno-Istoricheskij Zhurnal (Journal of Military History), Moscow, February 1961; Peresyepkin, Marshal I. T., Voennaya Radiosvyaz' (Military Radio Communications), Moscow: Voenizdat, 1962; Zernov, M., & N. Trukhnin, "The Communications Service in the Russian Navy during World War I," Voenno-Istoricheskij Zhurnal, March 1966; and Pavlovich, N. B. (editor), Flot v Pervoj Mirovoj Vojne (The Navy in World War I), 2 vols, Moscow: Voenizdat, 1964.

It is interesting to note that the Soviet articles began appearing approximately at the same time as similar articles in the Russian naval emigré press. See, for example, Rear Admiral Boris Petrovich Dudorov's articles on Admiral Nepenin in the emigré journal Morskije Zapiski (The Naval Records), New York, April 1956-April 1962.

4. Ural'skij, Yu., "The Organization and Combat Use of Radio Intelligence during the Civil War," Voenno-Istoricheskij Zhurnal, November 1972. (A translation of this article appeared in Cryptolog,

- September 1978, under the title "Soviet COMINT and the Civil War: 1918-1921.")
5. For instance, see Kahn, op. cit., p. 614.
 6. Cited in Richard W. Rowan's Secret Service, New York: Literary Guild, 1937, p. 699.
 7. Majskij, S., "Black Cabinet: Recollections of a Former Tsarist Censor" in Byloe (The Past), Paris: July 1918, p. 191.
 8. Probably a reference to the so-called "International Secret Service Bureau" with pre-WWI headquarters in Brussels and described by some as a semi-private business available to the highest bidder. Russian intelligence was known to have had extensive dealings with this bureau during the pre-WWI era. See Graves, Armgard Karl, The Secrets of the German War Office (New York: McBride, Nast & Co., 1914), p. 28 and Ludecke, Winfried, The Secrets of Espionage, Philadelphia: J. B. Lippincott, 1929, p. 227.
 9. Majskij, op. cit., p. 192.
 10. Swedish cryptanalyst Yves Gylden, quoted in Kahn, op. cit., p. 621, and Gottlieb, W. W., Studies in Secret Diplomacy during the First World War, London: George Allen & Unwin, Ltd., 1957, passim.
 11. For example, Kahn, op. cit., pp. 618-621. Anti-Tsarist revolutionary groups even used COMINT activities against the MVD itself by, on at least one occasion, obtaining a copy of the Department of Police's own cipher with which it communicated with subordinate elements throughout the Empire. See "The Department of Police Cipher" in Byloe, November-December 1909, pp. 189-190.
 12. The Extraordinary Investigating Commission was set up by the Provisional Russian Government after March 1917 to take testimony from former Tsarist Russian officials on the functioning of the old regime. Its operations were ended with the Bolshevik Revolution.
 13. George von Lengerke Meyer served as US Ambassador to Russia from 8 March 1905 to 26 January 1907. He later served as US Postmaster General (1907-09) and Secretary of the Navy (1909-13). According to the US State Department, US diplomatic communications were encrypted by 1905.
 14. Cited in "The Revolution of 905-06 in the Reports of Foreign Diplomats" by M. G. Fleer in Krasnyj Arkhiv (Red Archive), Moscow, Vol 3 (16), 1926, p. 220. The Portsmouth Peace Conference (August-September 1905) which took place at Portsmouth, NH, ended the Russo-Japanese War of 1904-05. President Theodore Roosevelt won the Nobel Peace Prize for his mediation efforts at the conference. It is also interesting to note that Colonel George Fabyan, later William F. Friedman's boss at Riverbank Laboratories, was a member of the US delegation at Portsmouth.
 15. See "Navy Radio Intelligence," the next section of this article.
 16. Peresytkin, op. cit., p. 57. The existence of Russian Army COMINT liaison with the COMINT services of Great Britain and France has not heretofore been acknowledged in any western publication concerning Allied COMINT activities in WWI.
 17. Peresytkin, op. cit., p. 57, and Ocherki Vneshej Politiki Rossii: 1914-1917 (Studies of Russian Foreign Policy: 1914-1917) by V. A. Emets, Moscow: Nauka Izdar., 1977, p. 165, footnote 441.
 18. Batyushin, General-Major Tajnaya Voennaya Razvedka i Bor'ba s Nej (Secret Military Intelligence and Combat with It), Sofia: Nov'zhivot Press, 1939, p. 73. See also General Batyushin's articles "Cryptography in World War I," Ratnik (Soldier), Belgrade, June-July 1928, and "Radiotelegraphic Intelligence," Vestnik Voennykh Znaniy (Herald of Military Knowledge), Bosnia (Yugoslavia), January-March 1931.
 19. Captain Nepenin will be the subject of another article by [redacted] in a future issue of Cryptolog. P.L. 86-36
 20. Dudorov, op. cit., July 1958, p. 39.
 21. According to Dudorov, op. cit., December 1958, pp. 17-22, Nepenin's chief assistants included Mikhail Platonovich Davydov, who was in charge of all critical analysis and intelligence reporting based on all-source data received by the Communications Service resources; V. P. Orlov, who as Chief Engineering Officer was in charge of all engineering and mechanical support to the Communications Service; Anatolij Koval'skij, who was in charge of the Central Radio Station (CRS) at Revel and later chief of the Southern Region of the Communications Service; and B. P. Dudorov, who set up and operated the first aerial reconnaissance wing of the Communications Service.
 22. Dudorov, op. cit., December 1958, p. 38.
 23. Pavlovich, op. cit., Vol 1, p. 79.
 24. An article by [redacted] about the MAG-DEBURG incident will appear in a future issue of Cryptolog. P.L. 86-36
 25. Ivan Ivanovich Rengarten, a leader in Russian radiotelegraphy and RDF, had set up two RDF stations by September 1914: one on Osel (now Saaremaa) Island and one at Libau. See Dudorov, op. cit., March 1960, pp. 50-51, and "On Radio Communications in the Navy" by I. I. Rengarten, Morskoj Sbornik (Naval Collection), Moscow, Jan-Mar 1920, pp. 32-33.
 26. Even the official Soviet history of the Navy in World War I (Pavlovich) does not credit the Black Sea Fleet with any substantial intelligence activity.

27. Steblin-Kamenskij, Senior Lieutenant Ivan Ivanovich, "Mine Warfare in the Black Sea," La Revue Maritime (Naval Revue), Paris, Nov 1932, p. 620.
28. There was some cooperation between the British firm of Marconi and the Russian firm of R.O.b.T.i.T. (Russian Company of Wireless Telephone and Telegraphy) in building accurate RDF stations, according to Rengarten, op. cit., p. 33, and Peresyphkin, op. cit., p. 31.
29. Ural'skij, op. cit., p. 84.
30. Zernov & Trukhnin, op. cit., p. 107, and "Obituary of I. I. Rengarten," Morskoi Sbornik, Jan-Mar 1920, pp. 1-5.
31. Timirev, Rear Admiral Sergej Nikolaevich, Vospominaniya Morskogo Ofitsera (Recollections of a Naval Officer), New York: American Society for Russian Naval History, 1961, pp. 14-15. On the non-emigré side, the official Soviet history of the Russian Navy in World War I, while condemning Nepein's brief tenure as Commander-in-Chief of the Baltic Fleet (1916-17), complimented him on his intelligence foresight and ability:
 "The Communications and Observation Service in the Baltic Fleet was excellently organized by Rear Admiral A. I. Nepein for operational intelligence. ... A. I. Nepein was also one of the first admirals of the Russian Navy to appreciate the significance of naval aviation as a most important means of reconnaissance."
 See Pavlovich, op. cit., pp. 75-76.
32. Hoare, Rt. Hon. Sir Samuel, The Fourth Seal, London: William Heinemann, Ltd., 1930, p. 57.
33. Dudorov, op. cit., p. 100.
34. According to one source, Captain 1st Rank P. A. Novopashennyj was later chief, intelligence/counterintelligence department, White Russian Naval Directorate in support of White Armies fighting in northwest Russia during the summer of 1919. See A Short Survey of White Forces under the St. Andrew Flag by Lieutenant N. Z. Kadesnikov, New York: private printing, 1965, p. 41. This is probably the same Novopashennyj who "had rendered good service during World War I in the imperial Russian Navy" and from 1922 on served as a senior assistant to the chief of a German cryptanalytic organization. See War Secrets in the Ether by Wilhelm F. Flicke, Laguna Hills: Aegean Park Press, 1977, Vol. II, pp. 292-293.
35. Timirev, op. cit., p. 165.
36. "Obituary of I. I. Rengarten."
37. Although this is the first known operation, the Baltic Fleet radio intelligence service was active before this time. For example, daily consolidated radio intelligence summaries (based on Communications Services assets information, foreign broadcast transmissions, and weather forecasts) were regularly being compiled in Oct-Nov 1914 when the Baltic Fleet first began active operations in the southern part of the Baltic Sea. See Pavlovich, op. cit., pp. 104 & 109-110, and Zernov & Trukhnin, op. cit., p. 107.
38. Chernomor, Volnyj Baltiki: 1914-1915 (Waves of the Baltic: 1914-1915), Riga: Dlya Vas, 1939, pp. 275-276.
39. Zernov & Trukhnin, op. cit., p. 107; Yankovich, op. cit., p. 117; and Pavlovich, op. cit., pp. 169-171.
40. Korostovetz, Vladimir, Seed and Harvest, London: Faber and Faber, Ltd., 1931, pp. 220-221; Monasterov, Nestor, & Sergej Tereschenko, Histoire de la marine russe (History of the Russian Navy), Paris: Payot, 1932, pp. 289-297; Dudorov, op. cit., Aug 1960, pp. 34-35; Yankovich, op. cit., p. 117; Zernov & Trukhnin, op. cit., p. 108; and Pavlovich, op. cit., pp. 175-6 & 225.
41. Pavlovich, op. cit., p. 311.
42. On 25 January 1915, for example, Black Sea Fleet ships were intercepting communications of enemy cruisers. See Pavlovich, op. cit., p. 470.
43. Steblin-Kamenskij, op. cit., pp. 621-622; Zernov & Trukhnin, op. cit., p. 110; & Pavlovich, op. cit., p. 470.



电信业务

PRESENT STATUS AND FUTURE DEVELOPMENT OF CHINA'S TELECOMMUNICATIONS (U)

by ZHU GAOFENG,
Vice Minister of Posts and Telecommunications,
People's Republic of China

INTRODUCTION

Scope

The subject matter will be covered as follows:

1. China's telecommunication services;
2. China's telecommunication industries and scientific research;
3. Main development targets for the next 20 years;
4. Some factors affecting the development of telecommunications infrastructures; and
5. Measures to be taken for developing communications.

CHINA'S TELECOMMUNICATION SERVICES

China's earliest telecommunications facilities were set up in the 1870s in the latter part of the feudal Qing dynasty (1644-1911). But up to 1949, when the People's Republic of China was founded, there were only 736 urban telephone exchanges; of these only 59, or 8 percent of the total, were equipped with automatic telephone connection. The total capacity of these was 712,000 lines, among which 208,000, or less than one third, were automatic. Thirteen provinces and municipalities had no automatic telephone exchanges at all. The limited telecommunications equipment was concentrated in the coastal regions and the handful of larger inland cities. There

The following paper was presented at TELECOM 83 (see CRYPTOLOG, October 1983, pp. 12-15).

were no telecommunications services whatsoever in the vast rural areas. Before 1949 shortwave circuits were the main transmission medium for long-distance telecommunications. Open wires were miserably scarce. There were only about 2,000 transmission lines for long-distance telephone and they were mainly single-channel and three-channel carriers. Throughout the nation, the postal and telecommunications offices numbered only some 25,000.

Over the past 34 years since the founding of the People's Republic, post and telecommunications systems have developed rapidly. Equipped with open wires, cables, microwave and shortwave circuits, a network of telecommunications, with Beijing as the hub, has been built. This network links up cities and towns with the vast rural areas. The first 1,800-channel coaxial cable carrier system from Beijing to Shanghai went into operation in 1967. The experience gained in building this project provided the basis for developing more big-capacity trunk networks of telecommunications. Construction of another trunk cable system for telecommunications, the Beijing-Wuhan-Guangzhou 1,800-channel coaxial cable carrier system is in full swing. When completed in 1985, this will form another big north-south telecommunications artery. More than 10,000 kilometers of trunk cables have been built and a series of new ones are under construction. Over 14,500 kilometers of

microwave links with 600- or 960-channel capacity have been completed. These form a nationwide network linking 26 provinces, autonomous regions, and municipalities so that telephone calls, telegrams, facsimile transmission, radio, and television programmes can be exchanged between them.

In 1982, the number of urban telephone offices were four times as many as in the early days of liberation. Of these, the number of those with automatic equipment rose by 20 times, with a total capacity of 8.3 times as much as that in early 1949. Before 1949 telephones were unknown in the rural areas. Now there are over 2.4 million lines there. There are 26,000 long-distance telephone circuits, 9 times the figures in the early days of liberation. The national number of post and telecommunications offices has reached nearly 50,000, a 90 percent increase over 1949. Through the use of cables and microwaves, automatic or semi-automatic long-distance telephone service is available in 24 of the provincial capitals. The growth of post and telecommunications services in the countryside and border regions of the national minorities is even more remarkable. Now 95.8 percent of the people's communes (townships) and 53.9 percent of the brigades (villages) have access to a telephone. In Qinghai province, an area of 700,000 square kilometers, there were only five post offices and one telecommunications office before liberation. Today there are more than 200.

All these achievements made in the past three decades were unthinkable in the old China.



CHINA'S TELECOMMUNICATION INDUSTRIES AND SCIENTIFIC RESEARCH

In the past 34 years following the policy of taking the initiative into our own hands and self-reliance, we have built through our own efforts a comprehensive post and telecommunications industry and made big progress in scientific research in this field. Twenty-eight affiliated factories, two institutes, and a dozen research units have been established under the Ministry of Posts and Telecommunications.

We have now basically mastered the switching technique of analogue telecommunications and large-capacity transmission. A fairly big production capacity for these has been reached. We have also formed the basis for developing the digital communications technique. We are able to produce cross-bar local telephone exchanges with a capacity of more than 10,000 lines, coded cross-bar toll telephone exchanges with medium or large capacity, 1,800-channel coaxial cable carrier systems, and 960-channel microwave systems. 30-channel and 120-channel PCM systems have already gone into operation. Apart from these, scientific research and the trial manufacture of modern telecommunications equipment is also underway. Trial operation of an 1,860-channel microwave system and a 4,300-channel Cazler system will soon be completed.

We can now manufacture earth stations for satellite communications and are testing under actual operating conditions a short wavelength optical fibre system. A stored program controlled automatic message transmitting system of medium capacity, electronic teleprinters, and group 2 subscriber-to-subscriber facsimile machines are being publicized.

MAIN DEVELOPMENT TARGETS FOR THE NEXT 20 YEARS

The experience gained from our own endeavours over the past 34 years and from advanced countries shows that telecommunications are an important infrastructure of modern society and should develop in harmony with, or quicker than, the growth of the national economy. Yet in present day China, posts and telecommunications is one of the weak links in our national economy. As is known to many, China has set herself the goal of quadrupling her gross annual value of industrial and agricultural production by the year 2000. In our struggle to attain this goal, we have recognized the necessity for telecommunications to

develop at a slightly higher rate than national economy as a whole. The Central People's Government and People's Governments at all levels are giving higher priority to telecommunications in investment and other forms of support. All these mean that telecommunications are entering a new phase of development. Based on progress in science and technology, by 2000 China will have gradually built a modernized posts and telecommunications network which will be able to provide high-quality, highly efficient services to the customers. This is the starting point in drawing up our strategy for development.

Concrete targets are as follows:

Telephone network

A telephone network is the main emphasis for development. We shall employ, step-by-step, SPC digital telephone exchanges and digital transmission equipment in the big cities and use cross-bar toll telephone exchanges for the medium-sized and small cities and other areas. By 2000 the national figure for telephones will increase several times. The urban and county telephone exchanges will be largely automated.

For long-distance telephones, a complete network with multiple tandem centres and multiple functions suitable for normal direct connections, will be gradually built and many alternative routes will be formed. Long-distance telephone circuits and automatic exchanges will increase considerably. Inter-city long-distance calls will have automatic or semi-automatic dialing.

Transmission media

Before 2000 new-type local telephone cables, long and short wavelength optical fibre systems will be introduced in a big way. Apart from bigger capacity carrier cables and microwave system, optical fibre cables, satellite communications and digital transmission technique will be employed in long-distance services.

Data communications

Data communications will be developed on a large scale. Medium-speed data communications are now available in telex networks and public automatic telephone networks. Later, a better

data transmission network will be established which will be suited to packet switches and will enable the use of computers and other terminals with different bit rates, codes, and protocols to interwork. A state public data communications network will also be built.

Satellite communications

As China has a vast territory, complicated topography, and varied climates, we will space-lift our own communications satellites and thereby step-by-step build a satellite communications network for domestic use. In the near future we shall lease transponders from Intelsat so as to meet the communications needs of our border areas and other regions where earth networks cannot easily reach. The transponders will also serve the special duty communications of different sectors of the national economy.

SOME FACTORS AFFECTING THE DEVELOPMENT OF TELECOMMUNICATIONS

Infrastructures

Though China's telecommunications has developed greatly in the past 34 years, they still fall short of meeting the growing needs of the national economy and the social life of our people. The main problems here are as follows: Switching equipment and transmission lines are seriously inadequate, thus service capacity is far from sufficient. This is particularly evident in the state of urban telephone systems. The national percentage of telephone availability for per hundred inhabitants is very low. Even in Beijing, the capital, the percentage is only 4.2. In many big cities there are long lists of people and units waiting to have telephones installed. Quality and efficiency of service is not satisfactory. Communications equipment is little and technology low. For instance, one third of the urban telephone exchanges (mainly in counties) are manually operated. Manual operation also prevails in long-distance telephone service. As a result, efficiency is low. This situation has hindered domestic and international telecommunications service. In the recent years, as China has adopted an open-door foreign policy and aimed at bringing her national economy into full swing, the gap between the rising demands for telecommunications services and their low capacity becomes wider. Responsible for such a situation are the following: weak foundation, low investment, backward technology, and faulty management.

MEASURES TO BE TAKEN
FOR DEVELOPING COMMUNICATIONS

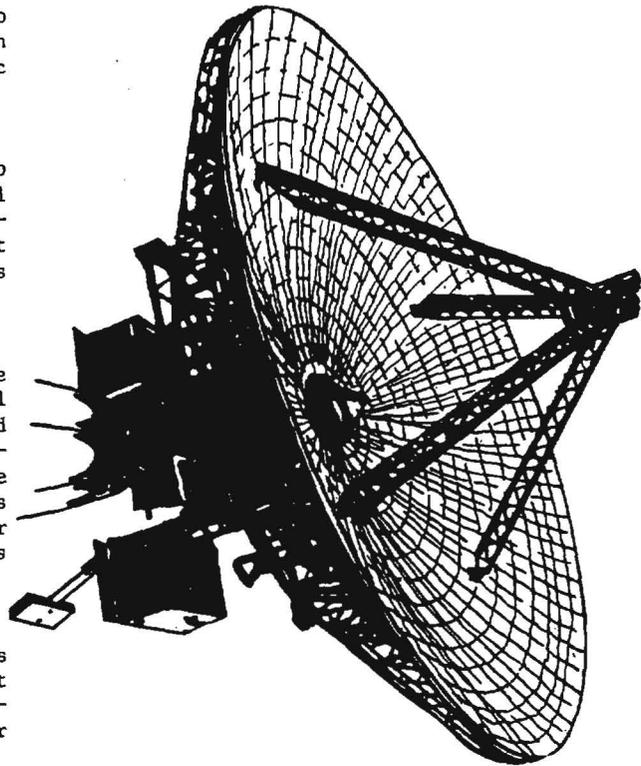
In order to change the backwardness of our communications service as soon as possible so as to meet the needs of modernization, the Government has made telecommunications one of its major strategic emphases in its general development plan. To speed up the process, we have adopted several measures:

- [] Beginning from 1982, the State has increased the proportion in its total investment for post and telecommunications construction and increased the percentage of services profits and foreign exchange revenues to be retained by the post and telecommunications administration so that it can have greater financial resources for equipment and upgrading technology.
- [] The national banks are to grant low-interest loans to the post and telecommunications administration so that it can import stored program-controlled telephone switching equipment and other advanced devices for use in the transformation of existing networks or building new ones.
- [] The Government has approved a proposal to lease Intelsat transponders and establish new earth stations to provide domestic satellite communications.
- [] The Government is giving full support to the initiatives of various governmental departments, enterprises, and local authorities to coordinate the development of special service telecommunications networks.
- [] Greater attention is being paid by the Government to the development of rural communications facilities. Under unified planning and technical standards, localities and departments are expected to take the initiative in building rural networks with investment from local authorities or collective donation by the subscribers and peasants.
- [] Profits from urban telephone services need not be turned over to the State, but are kept by the post and telecommunications administration as special funds for expanding telephone services.

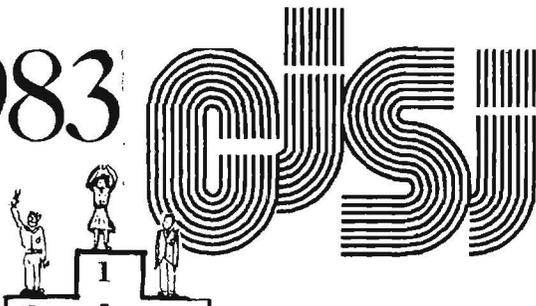
[] Construction of urban telephone facilities is framed into the overall development plans of cities so that the investment required can be drawn from both the Central People's Government and the local authorities.

[] New subscribers will be charged for the installation of telephones and the revenue from this set aside as supplementary funds for construction of urban telephone systems.

We have now realized that in a country with a vast territory and huge population such as ours, to carry out the task of modernizing telecommunications, we should rely mainly on our own efforts. At the same time, following our foreign policy, we will import advanced technology and equipment from abroad. We will also strengthen economic ties and technical cooperation with friendly foreign countries and undertake joint ventures with them. Friends and our colleagues in telecommunications, industrial and commercial circles abroad are welcome to cooperate in our efforts to accelerate China's telecommunications development.



1983 CISI ESSAY AWARDS ^(U)



by R53

P.L. 86-36



(U) In 1982 I was newly elected as a Member-at-Large of the CISI Board. During discussions for the 1982 CISI Spring Conference, there was some sentiment for not having a paper competition coupled with the conference, as it had been for the past several years. I suggested that CISI should run a totally separate essay awards competition in the fall, as other NSA professional organizations did. The CISI Council agreed wholeheartedly with my idea and promptly appointed, elected, or maybe railroaded me into the job of organizing and running such a competition for 1982. As you may remember, we had a very successful 1982 competition with 15 papers submitted in three categories and five cash prizes were awarded. Most of these papers were published in a very nice (but somewhat late, due to size and color printing) special issue of Cryptolog. This was billed by me as the "First Annual CISI Essay Awards Competition."

(U) When 1983 rolled around, I once again was asked to organize and run the essay awards competition for 1983. (However, this time I had volunteered to do so.) As you will see below, we had another good year in this, the "Second Annual CISI Essay Awards Competition." After the 1983 version was completed, when I was cleaning up my documentation for both 1982 and 1983 to file it for CISI posterity, I asked the CISI secretary where I should file all this material. She handed me the CISI Essay Contest file folder (as yet not seen by me). Inside, I discovered memoranda and notes dating from 1969 to 1972, which showed that the truly FIRST annual CISI essay contest was

held in 1969, not 1982. My apologies to anyone offended by my renumbering efforts. One interesting discovery on my part was that most of my judges for 1982 and 1983 had been entrants in these much earlier contests. Some of them had even won awards.

(U) The main purpose of the CISI Essay Awards competition is to encourage NSA employees to share their expertise and experience in computer and information sciences with the NSA community. CISI feels that publishing papers from the competition in Cryptolog and elsewhere helps further this purpose, especially for papers that might not receive wide distribution otherwise. The secondary purpose of the competition is to reward NSA employees for excellent technical writing with cash prizes. We hope that these prizes stimulate papers to be written which might not otherwise make it to hard copy.

(U) Papers submitted for a CISI Essay Awards competition need not be written specifically for the Awards. Any paper on an appropriate topic written during the previous year may be entered. Papers written for work-related purposes, for classes, or for professional certification (especially those designated Honors Papers) may be acceptable entries. Papers may be classified up to Top Secret Codeword. All authors of papers submitted to this competition must be NSA employees. Papers published or accepted for publication in outside technical journals are not automatically excluded from this competition.

However, only the author's final draft as originally submitted for outside publication will be accepted for this competition.

(U) For the 1983 competition, papers were solicited in the following three general categories:

- [] Systems Software
- [] Applications Software
- [] Systems Design and Hardware

(U) Nineteen papers were received in all. Each category had its own panel of judges who refereed (i.e., decided which papers should be published) and judged (decidin which ones der-served prizes) each paper in that category. Judging criteria included relevance to the field, quality of writing, completeness, and significance to NSA.

(C) After hard work on the part of our three panels of judges, the following prizes were given as the 1983 CISI Essay Awards:

Category I: Systems Software

- [] First Prize: [redacted] of W196 for "Logical and Structural Conflicts"
- [] Second Prize: [redacted] of B613 for "A Computer Graphics Data Base Design Aid Package"

Category II: Applications Software

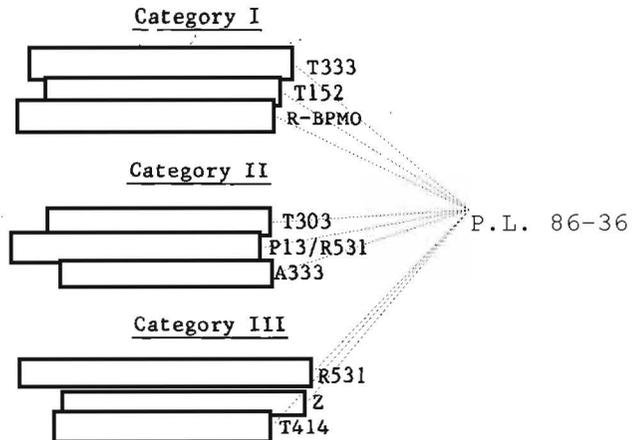
- [] First Prize: [redacted] of G622 for "Computer Scripting of Arabic: Not the Impossible Dream"
- [] Second Prize: [redacted] of R531 for "INTERROGRAPH: An Information Tool for Counter-Terrorism Intelligence Centers"

P.L. 86-36

Category III: Systems Design and Hardware

- [] First Prize: [redacted] of A215 and [redacted] of T443 for "Designers vs Users: Bridging the Communication Gap"
- [] Second Prize: [redacted] of G331 for "The Apollo DOMAIN Network: An Integrated Approach to the Networking of Powerful Personal Computers"

(U) I would especially like to thank our nine judges, several of whom also served as judges last year:



(U) Our publication procedures will be different this year. Rather than wait a very long time for an extremely big, special issue of Cryptolog, the abstracts of all successfully refereed papers will be published in THIS issue of Cryptolog. A number of these papers are already scheduled to be published in a special issue of the NSA Cryptologic Quarterly (due out in February or March) and those abstracts will be so noted. The editors of Cryptolog will work with the remaining authors and will publish their papers in various issues of Cryptolog during the coming year. This procedure will allow you to very quickly see all of the abstracts and to fairly quickly read those papers which require little or no editing.

(U) I hope you enjoy reading the results of the 1983 CISI Essay Awards competition. It's not too early to begin thinking about a paper for the next competition. Many of this year's entries AND winners began as a class term paper or as a paper for professional certification.

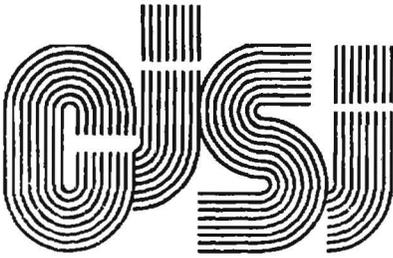
SOLUTION TO NSA-CROSTIC No. 51

[NSA] Safety Hazard Notice, dated 12 Jan 84.

"Failure to use a three-prong plug with this equipment [may] cause operator shock. Every user should contact the Occupational Health and Safety Office to obtain labels which should be affixed to the equipment."

~~CONFIDENTIAL~~

P.L. 86-36



ABSTRACTS (U)

Category I: Systems Software

Conflicts Between Logical
and Supporting Structures:
Concern for Computer Software Professionals

by [REDACTED]

(U) Visual constructs and documentation used by human analyzers of computer source language documents often conflict with the logical structures that they support. Basic types of conflicts are identifiable as well as their causes. Techniques are given for detecting discrepancies. The function and form of coding constructs can be controlled to ensure correctness of the ancillary structures. Changes to existing programming tools are suggested which could reduce the probability of conflicts being generated.

A Computer Graphics Data Base
Design Aid Package
(Cryptologic Quarterly)

by [REDACTED]

(U) The most important phase of data base development is the design phase. A poorly designed data base may not be able to handle important applications in a timely and efficient manner. In fact, a costly and possibly prohibitive redesign may become necessary if new applications not originally envisioned are suddenly needed. Because data base design is the most difficult and time-consuming phase when done properly, the temptation is to avoid expending the necessary amount of time in this phase. One solution to ease this temptation is to automate the design process using computer graphics. The designer can input his design at a terminal and allow the computer to analyze it, enabling him to quickly spot weaknesses and flaws. This paper presents the man-machine interface for such an interactive graphics data base design tool running on a powerful personal computer.

NOS/BE To NOS 2 Conversion:
Significant Differences
from a User's Perspective

by [REDACTED]

(U) The purpose of this paper will be to evaluate if the change from the Network Operating System / Batch Environment (NOS/BE) to the Network Operating System, version 2 (NOS 2) on the METEOR complex will have a major impact on its users. Conversion is tentatively scheduled for November 1984. Significant differences in the two systems from a user's perspective will be outlined. Where these are reductions in current capability, proposed or available compromises will be presented. This paper should serve as a useful guide in assisting users converting to NOS 2.

P.L. 86-36

C Programming Using UNIX System Calls

by [REDACTED]

(U) UNIX system calls are a way of interfacing between C programs and the operating system. These system calls can be subdivided into several categories which include: I/O calls, Process Management calls, and File System calls. The purpose of this paper is to provide additional explanations and examples of the system calls found in Chapter II of the PWB/UNIX documentation manuals in order to aid C programmers. This paper is a supplement to the manuals, which present a brief description of the calls but do not explain how to implement them or why they may be needed in C programs.

Category II: Applications Software

P.L. 86-36

Computer Scripting of Arabic:
Not The Impossible Dream
(Cryptologic Quarterly)

by [REDACTED]

(U) Agency nonvoice linguists are tasked with extracting intelligence by translation, working under a variety of conditions ranging from mildly inconvenient to near crippling. This paper will concentrate on those difficulties that result from conflicting transliteration systems imposed on an already foreign language, while examining the question of computer scripting of Arabic with output in soft and hard copy. It will then address solutions to these problems, using as examples descriptions of the work done in private industry on Arabic scripting. A complete

~~CONFIDENTIAL~~~~HANDLE VIA COMINT CHANNELS ONLY~~

scenario of how such a system should look to the working linguist at NSA is also presented.

(U) Although current technology is available to generate computer scripting of Arabic, other factors, including limitations on personnel and monetary resources, would probably preclude implementation of such scripting at the Agency in the immediate future. However, given the rapid strides made in computer technology in recent years, together with declining relative costs, computer scripting of Arabic might well be a reality at NSA in the not too distant future.

INTERROGRAPH: An Information Tool for Counter-Terrorism Intelligence Centers (Cryptologic Quarterly)

by [redacted]

(U) A user interface design for a Spatial Data Management System for the retrieval of information on international terrorism is outlined. After a discussion of the benefits of using graphics to interact with a data base, the concept of SDMS is briefly described. The qualities that make SDMS an appropriate system to use in conjunction with a terrorism data base are mentioned. Several examples of possible incidents involving terrorists and how questions arising from these incidents could be answered by INTERROGRAPH show the efficacy of the system for a watch center.

M(A)T: Method from Madness

by [redacted]

(U) This paper discusses the field of machine translation in general and my own theory in particular. Chapter I introduces the terminological distinction between machine translation (MT) and machine-assisted translation (MAT) and considers the most important US groups currently doing MT. Chapter II explores the three-way nature of the problem: language, theoretical linguistics, and computer science and traces the history and development of linguistic science, especially those recent treatments rigorous enough to be simulated by computer. Chapter III deals with the nitty-gritty of translation at the syntactic level and the kinds of abstract structures that need to be created and manipulated by any serious MT system. Chapter IV considers the specific strategies of syntactic description required by MT. Chapter V describes and flowcharts my computational implementation in SNOBOL4. Chapter VI cites recent literature in support of the methods adopted and proposes a schedule for an NSA feasibility study.

P.L. 86-36

Top-Down COBOL Management

by [redacted]

(U) Having a set of standards guarantees neither efficient coding practices nor the staff's willingness to apply them to module development. Design considerations and management decisions can affect the rate at which code is produced and the correctness of the executable code. These factors also affect the amount of time spent during any one phase of the program development to correct for design errors.

(U) This paper details an approach to software design and development which defines elemental activities in the design and production of COBOL code at the module level. The definitions are then used as tools in the technical and managerial aspects of module production.

(U) An outline of adjunct COBOL coding standards will be presented which stresses naming conventions. Most importantly, all development documentation is an integral part of the delivered product, thereby eliminating redundancy and the conflict that can occur between internal and external documentation.

(U) Suggestions on how the phases in this methodology can be PERTed or used in other resource management techniques will be offered.

Ada and Cryptanalysis

by [redacted]

(U) Ada is the new computer language developed by the Department of Defense. After a brief introduction to Ada and the concept of staged testing in cryptanalysis, this paper takes a look at the advantages and disadvantages of using Ada in the cryptanalytic environment. The paper tries to decide how best to use Ada in cryptanalytic applications, if at all.

A Graphic User Interface for the Transcriber-Analyst (Cryptologic Quarterly)

by [redacted]

(U) Designers of new computer systems are placing increasing emphasis on user friendliness, specifically on the ability of non-ADP professionals to gain quick and easy access to their data and data base systems. Two of the newest and most intriguing systems, from the intelligence analyst's point of view, are the

Xerox Star and the Computer Corporation of America's Spatial Data Management System (SDMS). Both systems use visual/graphic approaches to data storage and retrieval and are based on the principle of having the user select files and data from graphical menus/directories, rather than rely on often complicated query languages. This paper will detail how these state-of-the-art systems could be used by transcriber-analysts here at NSA.

CRITICOMM Management
A User Interface
(Cryptologic Quarterly)

by

(C) As NSA moves into the 80s and the age of increasing automation of data-collection facilities, the human beings who are called on to interpret that data become more and more inundated by the sheer volume. T13, for example, receives large volumes of data daily, only part of which is used because of a lack of resources to organize it into information. Some means must be found to convert more of the data into information which can be used by a person sitting at a desk or a terminal. One concrete example of this data explosion is circuit management of the CRITICOMM network. This is accomplished through monthly statistical reports (NSA-760s) which are sent to T133 from the stations of the network and are incorporated into the monthly CRITICOMM Operational Summary (COS) prepared by T133. Circuit management is also accomplished on a near real-time basis through the CRITICOMM Systems Management system (CSM). As a result of Project TREEHOPPER, a manual data entry system for the NSA-760 monthly statistical report was converted to an automated system using GENED and SPECOL to manage the data base, but even this advance left the analyst with hard-to-understand reams of alphanumeric data.

(U) This paper illustrates how interactive graphics techniques can be used to convert the present follow-on reports to the NSA-760 report into a pictorial format in order to clarify the information. It suggests report formats to make use of data in the NSA-760 report not now used--as well as formats which tie together data from the NSA-760 reports and other data bases. Applications of interactive graphics to the time-sensitive work of the CSM are also presented.



Category III: Systems Design and Hardware

Designers vs. Users:
Bridging The Communication Gap
(Cryptologic Quarterly)

by

(U) The communication gap that has existed between users and designers of computer systems has widened with the introduction of new terminology and new methods of user interaction. A design technique known as "mock-ups" was eventually devised to improve communication with users during the requirements specifications and design phases of new graphics projects. This paper presents a detailed example of the mock-up strategy. For those individuals interested in composing a design using this technique, some instruction has been provided, including a section on an automated mock-up maker.

The Apollo DOMAIN Network:
An Integrated Approach to the Networking
of Powerful Personal Computers

by

(U) One of the most exciting new data processing technologies to emerge in the past couple of years is the local area network (LAN). The continued maturation of this technology has opened the door to a host of innovative and economical approaches to distributed processing, resource sharing, and high-speed local communications. Still in its formative years, the LAN industry currently consists of a large number of vendors offering a wide variety of LAN devices and systems designed for an equally wide variety of applications.

(U) One of these applications involves the use of the local network to build a system of linked microprocessor-based workstations which share a pool of common resources, such as disk files and printers, via the local net. Such local network resource sharing is a very cost-effective mechanism for greatly enhancing the processing environment available to the user of a microprocessor. Examples of such systems are the Corvus Omninet and the Xerox 8000 Network System.

(U) Another company to incorporate this concept into a system design is Apollo Computer. In addition to utilizing current LAN technology, Apollo has taken advantage of other state-of-the-art hardware and software technologies (high-density RAM, 32-bit VLSI processors, interactive high-resolution graphics with bit-mapped interfaces, Winchester

disks, and high-level object-oriented operating systems) to develop a very sophisticated system of powerful personal computer workstations integrated into a high-speed resource sharing local network. This network, called DOMAIN (Distributed Operating Multi-Access Interactive Network), presents the scientific and engineering professional with a promising processing alternative to current timesharing and dedicated systems.

(U) This paper outlines the concepts behind the Apollo DOMAIN network, describes the integrated design approach and the primary architectural features of the DOMAIN and its associated nodes, discusses some of the advantages and disadvantages of this type of system, and briefly looks at potential applications for the Apollo and Apollo-like systems at NSA.

Cartography in The Electronic Age
Paper vs. Display Screen

by [redacted]

(U) Maps have been an invaluable tool of communication since earliest time. Although the basic nature of maps is relatively uniform, the characteristics of individual maps are dictated by the use for which the map is created. Static paper maps have been common for centuries. Today, however, the availability of computer technology has caused the advent of dynamic electronic maps. This paper discusses the characteristics of maps and compares and contrasts paper maps to electronically generated ones. It then examines the various factors involved in designing flexible, detailed, and portable map display systems and compares the current technologies available for creating such systems. Finally, an evaluation of the potential for future use of these interactive map display systems, together with NSA implications, is presented.

Management of TDY Funds:
A Graphical Approach
(Cryptologic Quarterly)

by [redacted]

(U) A manager's primary resource is time. He has only so much time in a day to absorb information relevant to his immediate decision-making responsibilities. Managers therefore prefer graphic displays which reduce large amounts of complex information into readily understood pictorial form.

(U) This paper addresses the area of computer graphics for management applications. An example of this application is presented,

P.L. 86-36

displaying the management of TDY funds. A systems design is provided on a computer graphics system for the Travel Program at NSA. The present system and its shortcomings are described, and requirements for a new graphics system and examples of the desired outputs are presented. Fortunately for NSA, this requirement can, by and large, be satisfied with an off-the-shelf "turnkey" system recently announced by the Xerox Corporation. The graphics system, Xerox Star workstations linked by the Ethernet communications facility, is then described, and the TDY application is demonstrated. An additional NSA application for this computer graphics system, the Stock Fund program, is also described. Computer graphics systems, like the one referred to in this paper, will provide managers with a means to quickly analyze and respond to complex information. Satisfying such Agency requirements with off-the-shelf equipment will also reduce the burden on NSA's data system personnel.

Optical Disk Technology:
The Future of Mass Data Storage

by [redacted]

(C) Optical disk technology is still a relatively new field. Consumer products have been on the market for approximately five years and have been fairly slow to catch on, mainly because they lack the record/play flexibility of video tape recorders. This disadvantage on the consumer front becomes a real advantage on the data processing front as government agencies and private industry explore their needs for long-term archival storage of large amounts of data. Optical disk storage capacities are in the terabyte region, and their relative low cost and indestructibility make them the logical choice for this use. This paper covers the types and capacities of various optical disks, discusses NSA's research and development effort in that field, and the objectives of the contract NSA has let for the acquisition of a prototype system. In addition, commercial applications and NSA applications for optical disks will be explored.

Replace RACE

by [redacted]

(U) RACE is the name given to a computer system operated by T154, the goal of which is to provide signals data base and management support to Management and Signals Conversion Technicians. It is no secret that over the past few years this system, with respect to its task effectiveness, has been declining. Also the workload being placed upon it has

increased to such a degree that the time has arrived for management to take an objective look at the prospect of replacement. RACE is, after all, an essential tool in the fulfillment of the mission of the Agency.

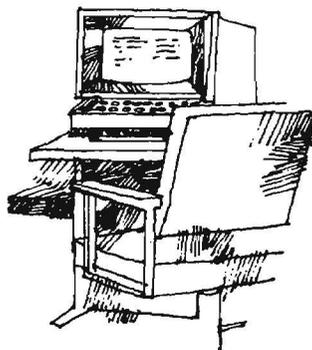
(U) This paper addresses RACE in its past and present operating environments, while examining its functions, capabilities and requirements. It attempts to show that there is a limited future for RACE in its present working environment mainly due to its single job processing and low-level assembly language characteristics. The author will demonstrate that RACE is slow, outdated, and inadequate based on today's demands and has outlived its usefulness within the T organization. Also, it will be shown that the operational elements supported by RACE critically need a replacement computer.

(U) This paper will also discuss and summarize the results of research into the UNIVAC 90/30 computer system, a prime candidate for replacement of the present RACE equipment.

Excellence Must Be Cultivated Corporately:
Some Ideas For Improving Productivity

by

(U) This paper focuses on the issue of excellence, excellence in terms of products, people and the management of both. We will consider several perspectives on what excellence is and means, why it is especially important now and how it might apply to NSA in general, and to computer and information science in particular. Next we will address the theme of this paper, that excellence must be cultivated corporately and what that implies. Then we will learn about what others are doing to cultivate excellence. We will also consider the need to generate more feedback in order to effectively apply what others have learned to NSA. Finally, a number of specific suggestions will be proposed which could significantly improve the productivity of our products, our people and our management process, if we corporately commit ourselves to the cultivation of excellence.



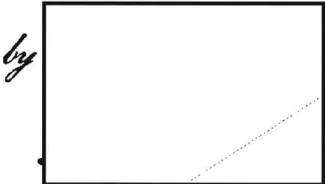
P.L. 86-36

P.L. 86-36



**WE ARE ALWAYS
LOOKING FOR
ARTICLES, COMMENTS,
NOTES, LETTERS,
THAT WOULD BE
OF INTEREST TO
OUR READERS**

The LANGUAGE PROBLEM at NSA

P.L. 86-36

(U) In February 1976 the US Air Force's Foreign Technology Division invited NSA and other agencies to send a representative to a Conference on Translation. The purpose of the conference was to share mutual translating problems and interests. Representatives were asked to present a brief introductory (and unclassified) statement about the language problems at their respective agencies. Ms. [redacted] were NSA representatives, and [redacted] was tasked with presenting the introductory statement, which is reproduced here.

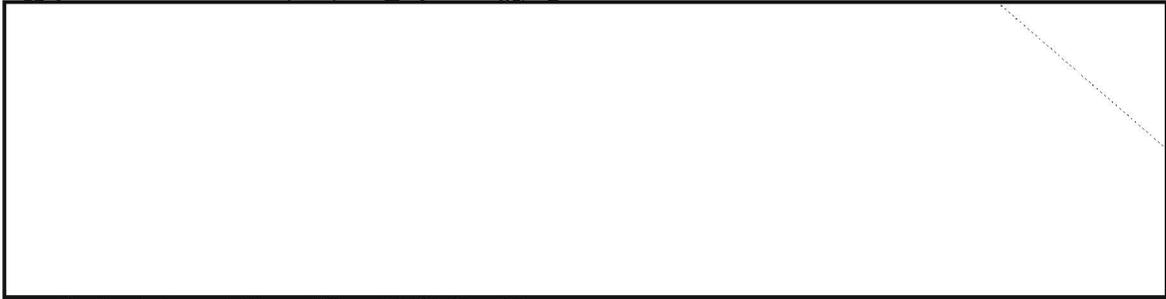
P.L. 86-36

(U) There is no language problem to speak of at NSA. Let me phrase that another way: there is a language problem at NSA, but we don't speak of it in mixed company. If I were to speak of it, I would state that the language manager at NSA is looking for a language specialist

- * who at the time of hiring has a native understanding of the subject language (or better yet, of several languages);
- * who is a rapid reader and a prolific writer;
- * who is well-versed in the subject language culture;
- * who understands various specialized jargons equally well in English and the subject languages;

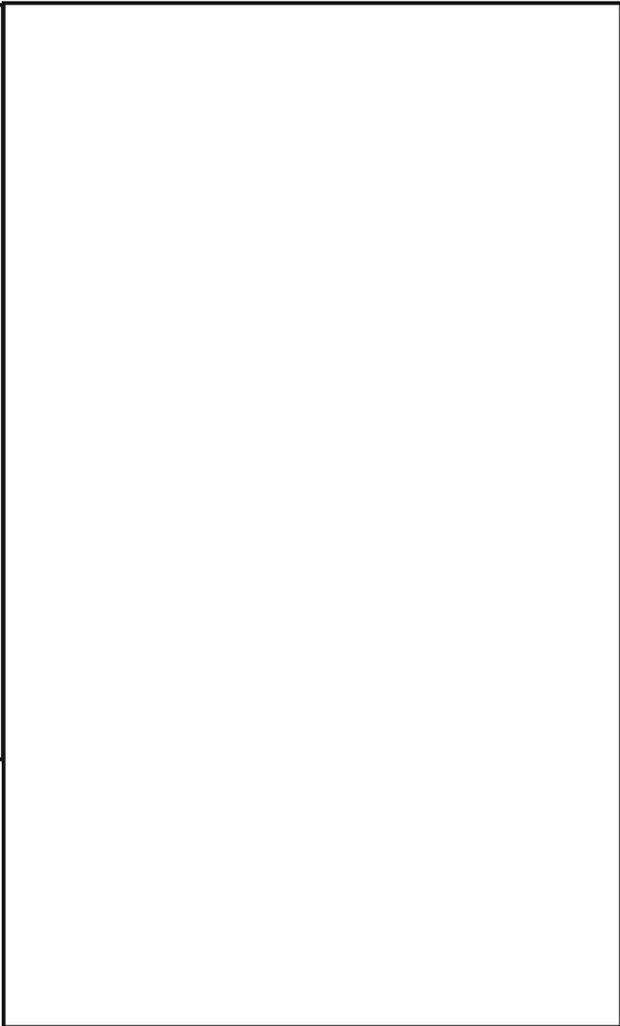
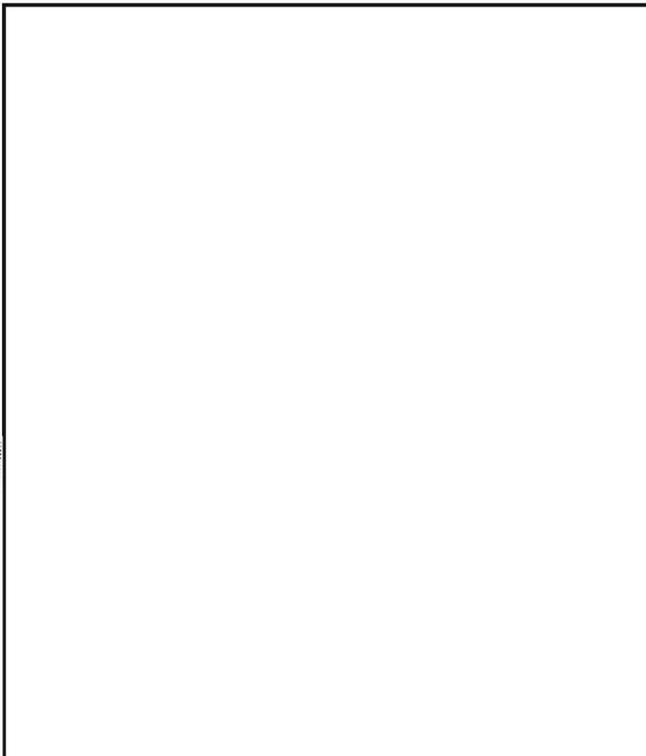
- * who is a top-notch intelligence analyst;
- * who is a native-born, loyal American citizen who has never traveled abroad;
- * whose command of English is superb;
- * who enjoys the opportunity to learn exotic or low-density languages in spite of the poverty of tools available about that language;
- * who spends his or her spare time maintaining these skills without making contact with any foreign nationals;
- * who enjoys taking--or teaching--courses to improve proficiency (with no decrease in production chargeable to class time);
- * whose private life is above reproach (and especially blackmail);
- * whose needs are simple and whose wants are few;
- * who enjoys the challenge of maddeningly incomplete or imprecise text from which an accurate translation is to emerge; and
- * who is imaginative and creative in tackling hard problems as well as a stickler for accuracy in translation.

(U) Those language managers also expect this person's name to be Legion--but Nemo is more apt.



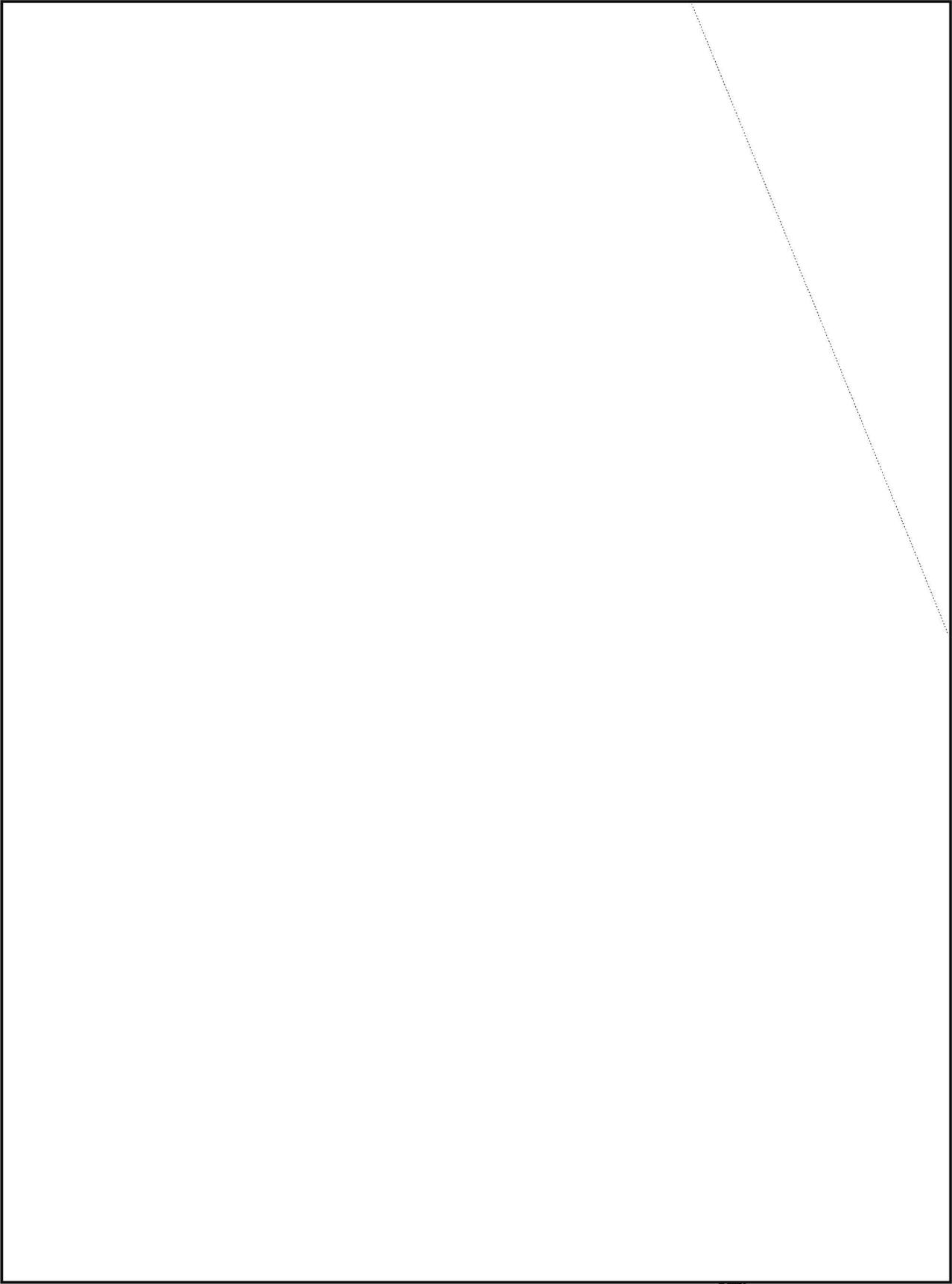
G61

P.L. 86-36





I keep six honest serving-men
 (They taught me all I knew):
 Their names are What and Why
 and When
 And How and Where and Who.
 --Rudyard Kipling

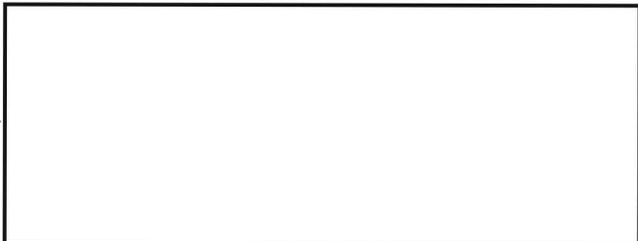


P.L. 86-36

To: [redacted] Editor
Fm: [redacted]



(S) I found the article in the Sept 83 issue of Cryptolog entitled PARPRO (beginning on page 15) most informative and interesting.



To [redacted]

To: [redacted] P14
From: [redacted] A3111

(FOUO) In regards to your "I Remember JFK" in the Nov 83 issue of Cryptolog, I was here at the Agency on the day President was shot. I was working in A2 at the time ... [in] Room 3E039.

Re: Subscribing to the CRYPTOLOG

(FOUO) For your information, there were 2 announcements made over the loudspeaker system. The first one said "Ladies and gentlemen: The President of the United States has been shot and is in critical condition." The second one in a very solemn voice (male) simply said "Ladies and gentlemen, the President of the US is dead."

(U) Please add me to the subscribers' list for CRYPTOLOG. I have discovered that some of the articles (like the one on ELINT notations in the October 1983 issue) are so useful that I clip them and save them, or else I stash the thing in my desk and the rest of the branch is deprived of the chance to read it. Clearly I need my own copy!

(FOUO) You may or may not have been informed by the people who were here at the time. If so, sorry for the inconvenience.



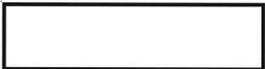
1. (FOUO) Per our phone conversation ..., this is to inform you that the following two articles from the October 1983 CRYPTOLOG were reproduced and disseminated to selected [redacted] employees:

[redacted] replies:

- a. "Tips on Topical Reporting"
- b. "Banners, Cowboy Hats, & ELINT Notations"

2. (FOUO) [redacted] recipients were advised of the requirement to keep the articles within the cryptologic community. ...

(FOUO) If [redacted] says he heard two announcements, I won't argue with him. But I stand by my original statement that the folks in the office where I was working on that day (Room 2C-something-or-other) didn't hear even one. I'm fairly sure that I wouldn't forget any announcement that started off with "Ladies and gentlemen" instead of the standard "May I have your attention please!" (especially if it happened twice).



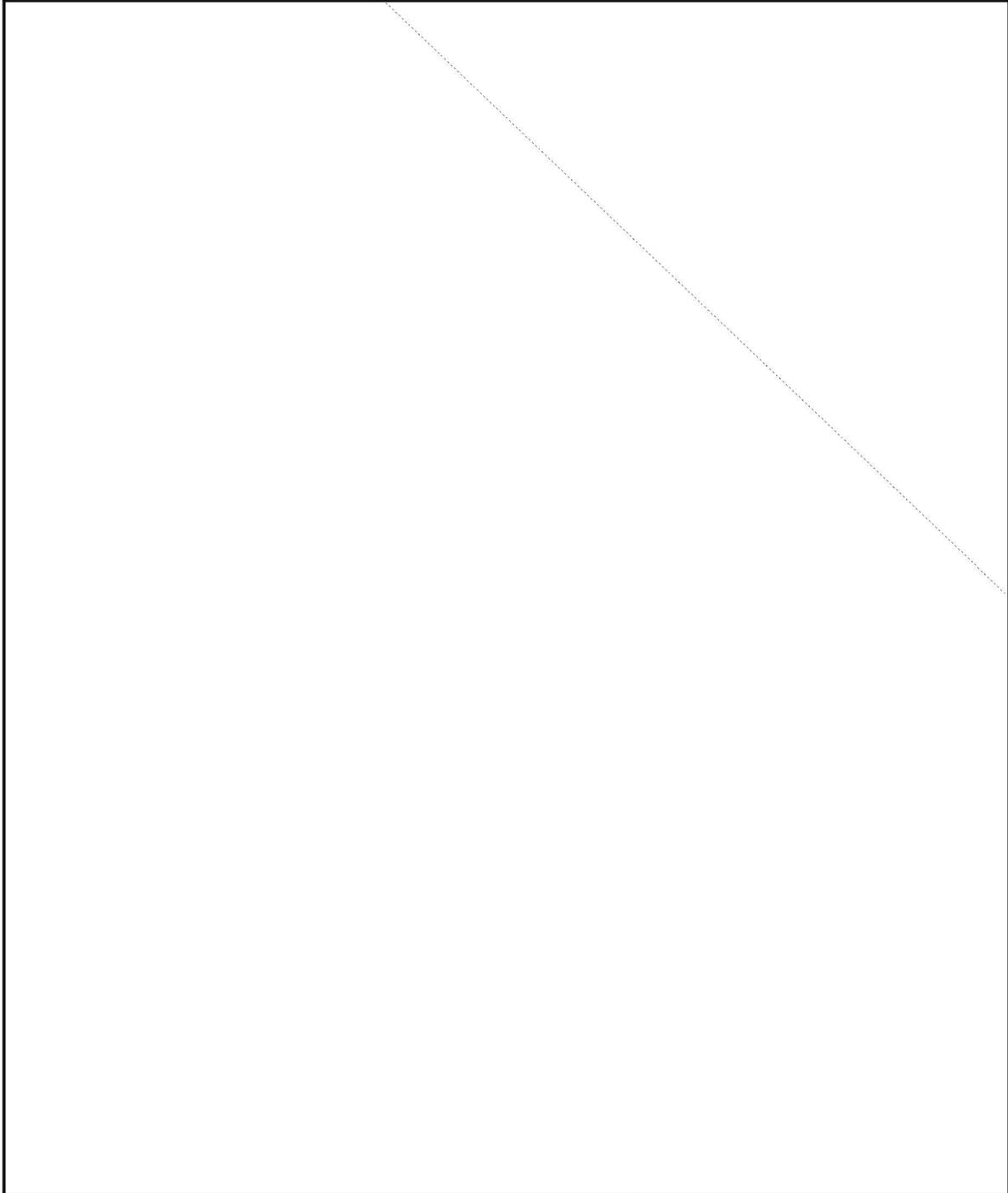
HGR

P.L. 86-36

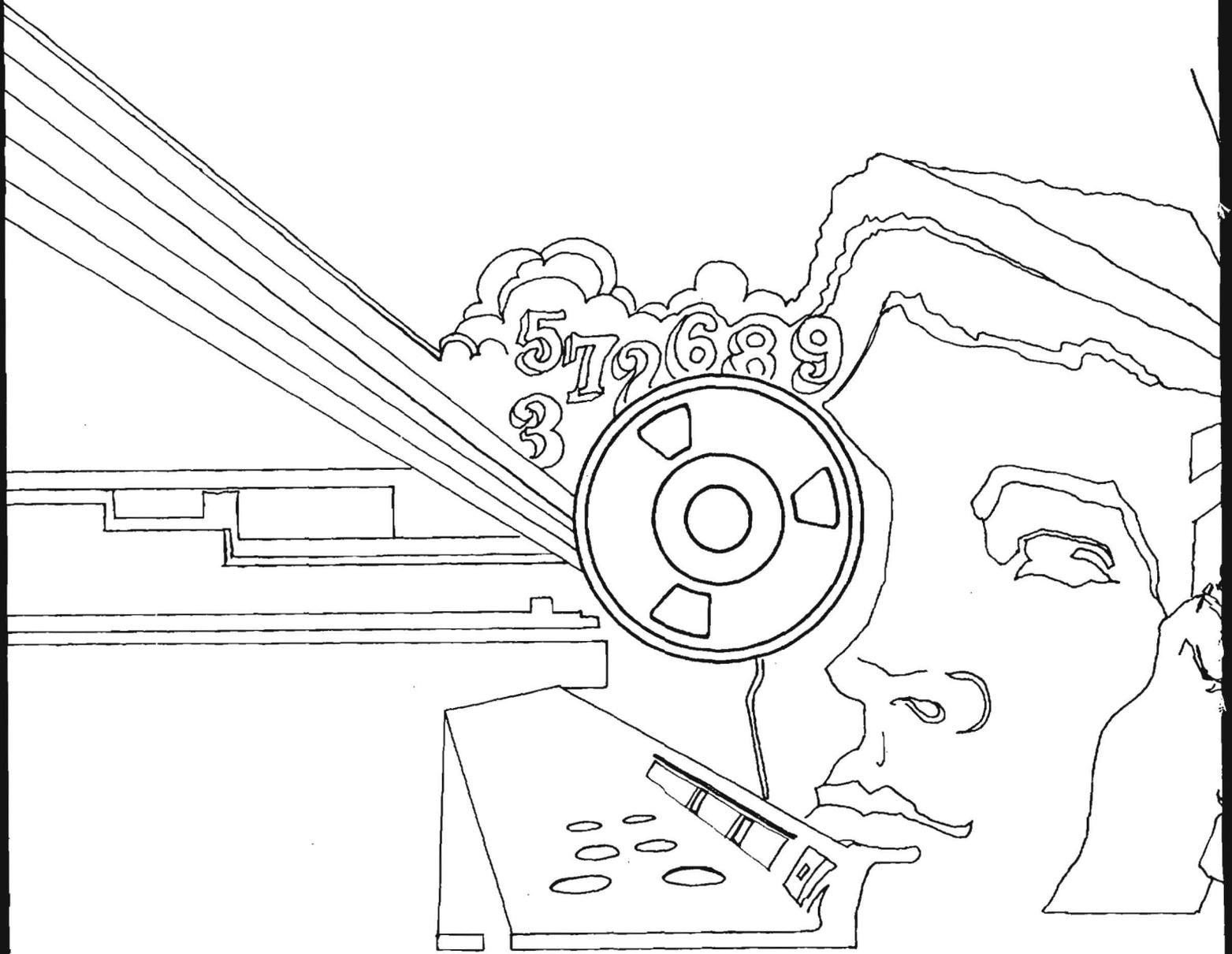
P.L. 86-36

NIA Crostic No. 52

this month's
Guest Acrostician, crafted
this fine first effort over
a weekend, because "I just
wanted to see if I could
do one."







~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~