This report includes all systems current on 31 December 1954 and all systems under study in NSA-712 at any time during the calendar year 1954.

DISTRIBUTION:

- External - 2# copies
- NSA-712 - 15 copies
- NSA-7121 - 1 copy
- NSA-7122 - 1 copy
- NSA-7123 - 1 copy
INTRODUCTION

The two principal targets of NSA-712 during 1954 were the Diplomatic and Military problems. There are about____ persons assigned to the Diplomatic problem and about_____ to the Military.

The most significant developments during the past year were as follows:

1. An attempt by the____ to tighten up security in both Diplomatic and Military cryptographic systems. This trend reached its peak in June and July after which time security consciousness decreased somewhat.

2. The introduction of two voice scrambler systems in_____ the Single-Side-Band, 4-cycle AZ-13 and the Double-Single-Side-Band, 5-band system (the other side of which carries radio-printer traffic.

Generally speaking, the overall situation in NSA-712 during 1954 reflects conditions that have continued now for several years: inadequate numbers of cryptanalytic and linguistic personnel to carry out properly its mission. From a personnel strength of_____ in Jan 58 the Branch has been reduced to an average strength of about_____ people during 1954. This has been due, principally, to levies placed on Branch personnel to support higher-priority problems such as_____. The inevitable cost to consumers has been fewer translations and a decrease in their timeliness. The intelligence yield to consumers represents only about____ of its potential _______ Diplomatic and_____ Military.) In addition to this, the manning of extra shifts in response to special consumer priority requests, the establishment of a swing shift of arbitrary size, management surveys, periodic furniture reshuffling have all contributed to further limit the Branch's production.

-1-
## Production Statistics

<table>
<thead>
<tr>
<th></th>
<th>Oct-Dec 1954</th>
<th>Oct-Dec 1953</th>
<th>Year 1954</th>
<th>Year 1953</th>
<th>Year 1952</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orig Cipher Mags Rec'd</td>
<td>51,551</td>
<td>34,238*</td>
<td>213,427</td>
<td>137,693*</td>
<td>162,896*</td>
</tr>
<tr>
<td>Dupe Cipher Mags Rec'd</td>
<td>21,135</td>
<td>37,781</td>
<td>198,498</td>
<td>126,618</td>
<td>138,428</td>
</tr>
<tr>
<td>Total Cipher Mags Rec'd</td>
<td>72,686</td>
<td>72,019*</td>
<td>411,925</td>
<td>264,311*</td>
<td>291,314*</td>
</tr>
<tr>
<td>Cipher Mags Decrypted</td>
<td>21,633*</td>
<td>19,568</td>
<td>87,988*</td>
<td>82,666</td>
<td>59,163</td>
</tr>
<tr>
<td>Cipher Mags Translated</td>
<td>4,733*</td>
<td>4,556</td>
<td>21,137</td>
<td>21,743</td>
<td>21,573</td>
</tr>
<tr>
<td>Cipher Mags Summarized</td>
<td>494</td>
<td>644</td>
<td>2,649</td>
<td>2,619</td>
<td>738</td>
</tr>
<tr>
<td>P/L Mags Trans or Summ</td>
<td>594**</td>
<td>644</td>
<td>1,401**</td>
<td>2,848**</td>
<td>714**</td>
</tr>
<tr>
<td>Code Meanings Recovered</td>
<td>2,363</td>
<td>5,554</td>
<td>14,252</td>
<td>15,544</td>
<td>22,561</td>
</tr>
<tr>
<td>Aver Number Personnel</td>
<td>118</td>
<td>138</td>
<td>132</td>
<td>129</td>
<td>122</td>
</tr>
</tbody>
</table>

## Intercept/Traffic Analysis

Although the Production Statistics indicate that the volume of original messages received for 1954 is about the same as it was for 1953, there has been a downward trend in receipts since June. The loss of a large volume of traffic (B-211 machine encipherment of high-level military traffic) between May and August as a result of a change from Morse and Teletype transmission to Double Single Side Band was a major factor in this decrease. Although U5M-9 began to intercept on the DSSB in August, the traffic volume remains low because difficulty has been experienced in acquiring all the equipment necessary to intercept this new type of transmission and because of the loss of and the consequent decrease in the amount of traffic sent by the

In 1953, it was estimated that cipher traffic received was passed on the

percentages have not changed much for 1954, except that there has been some increase in radio-printer traffic as a result of the installation of the

in October 1953 and a corresponding decrease in Net traffic.

* 1952 and 1953 figures for cipher messages do not include a large number of unsolved messages, the volume of which is estimated to be per month.

** Plain-language messages received are not counted. It is estimated that about are received and scanned quarterly. Plain-language messages used in reports are included in these figures.
From the standpoint of exploitability and consumer interest, the importance of pet traffic cannot be too highly stressed. Intercept receipts have remained fairly steady for this year with about [ ] of the total sent being successfully intercepted compared with [ ] in 1953. The recent loss of [ ] traffic both in quality and quantity is regrettable and it is hoped that it will not cause too great harm to the [ ] problem.

This loss, in addition to the complete loss of cover at Station USM-18 during the year, made it seem essential to provide for [ ] cover to the extent of 3 positions located on the continent. NSA-712 was successful in having one position at STATION USM-6 assigned to this problem at the end of November with very favorable results based on one month's take.

A new attempt is being made at Station USM-6 to intercept [ ] traffic passing between [ ] which is thought to be sent by means of the "True-Tone" system. Since both [ ] and the Air Force are interested in this traffic, it is hoped that all possible effort will be made this time to obtain the proper equipment and personnel to intercept this traffic which NSA-712 has desired for so long.

During the last half of 1954 the AZ-13 and the 5-band voice scramblers came into general use. Shortly after the fall of [ ] Hanoi started using the AZ-13 almost exclusively although the hand-morse and teleprinter circuits were kept open. This caused a drop of about [ ] traffic.

In July the second voice scrambler (5-band) in use in [ ] was identified. It is passed on one side of a Double Single Side Band system, the other side of which was found to carry the [ ] traffic which had been missing since May 54. USM-9 is now intercepting some of the traffic passed in these systems. However, lack of proper equipment has prevented full interception and exploitation of the two scrambler systems and the DSSB. The partial intercept of the Double Single Side Band transmissions restored some of the [ ] traffic but the volume is still far below normal.

CRYPTANALYTIC DEVELOPMENTS

I. MACHINE SYSTEMS

The readability of this [ ] in 1954.* Difficulties encountered in solution were the lack of workable depths as a result of [ ]

* See Attachment A.
There were several important highlights in solution during the year.

1) Electrical forwarding of USM-8®E traffic by NSA-13.

2) Special processing at both ends of NSA-13's circuits. Among other things, this involved a

3) A special Courier forwarding arrangement which cut the average delivery time of hard copy from 7 to 1½ days.
Solution of these systems has progressed slowly since the

Little is known about this series.

However, it is felt that more groups are involved in each of the indicator systems, although recent studies, including a

have not revealed them.

Most of the solution work on ______, the assumed predecessor of the ______ series, was accomplished during the first few months of 1954. When work was abandoned.

3. The ______

Solution and exploitation of this series of ______

In August, the ______

-5-
A small effort was directed during the year to conferences, and to which started during the lanes and is slowly dying out. It is believed that these systems use one-time pads.
RESEARCH AND MACHINE AIDS

1. Computer Programs

The following computer programs were designed for use on ATLAS II.

2. Machines

INTELLIGENCE PRODUCTION

From the Production Statistics it will be noticed that.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>1,834</td>
<td>1,625</td>
<td>1,616</td>
<td>1,598</td>
<td>1,459</td>
<td>1,190</td>
<td>1,045</td>
<td>1,034</td>
<td>1,382</td>
<td>1,543</td>
<td>1,889</td>
<td>2,591</td>
<td>17,726</td>
</tr>
<tr>
<td>Units</td>
<td>56</td>
<td>36</td>
<td>124</td>
<td>107</td>
<td>134</td>
<td>.3</td>
<td>26</td>
<td>9</td>
<td>1</td>
<td>28</td>
<td>77</td>
<td>14</td>
<td>616</td>
</tr>
</tbody>
</table>

Total 17,726 616 4,956 268 3,633 534 2,142 362 16,714 82 13,798 97 25,221 894 84,187 2,793 (3.3%)