

~~TOP SECRET TRINE~~

22



NATIONAL SECURITY AGENCY  
FORT GEORGE G. MEADE, MARYLAND 20755

Serial: N 0668  
13 May 1968

~~TOP SECRET TRINE/NOFORN~~  
~~LIMITED DISTRIBUTION~~

MEMORANDUM FOR USIB PRINCIPALS

A 808914

SUBJECT: Assessment of the Loss of the USS PUEBLO (C)

1. This report is being provided to the Members of USIB for their information.

2. Attached is an impact assessment statement concerning the capture of the USS PUEBLO (AGER-2) on 23 January 1968 and the loss which may result from the compromise of an unknown amount of SIGINT technical support material, communications equipment and SIGINT collection equipment carried aboard the vessel.

3. In NSA's judgment, based on "worst case circumstance", which is normally part of the evaluative procedures surrounding cryptographic and COMINT compromises, the overall loss and long term effect on the U.S. SIGINT effort is assessed to be very severe. If the technology and doctrine which may have been made available through the capture of the PUEBLO were to be applied to Soviet, KORCOM and CHICOM communications there is little doubt that the U.S. would suffer a serious and costly loss of intelligence. The recent revelation by the North Koreans that they possess TOP SECRET codeword, SECRET codeword and Handle Via COMINT Channels documents dramatically points up the possible severity of our loss. With regard to this latter development, [redacted]

[redacted]

~~SPECIAL HANDLING REQUIRED NOT~~  
~~RELEASABLE TO FOREIGN NATIONALS~~

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

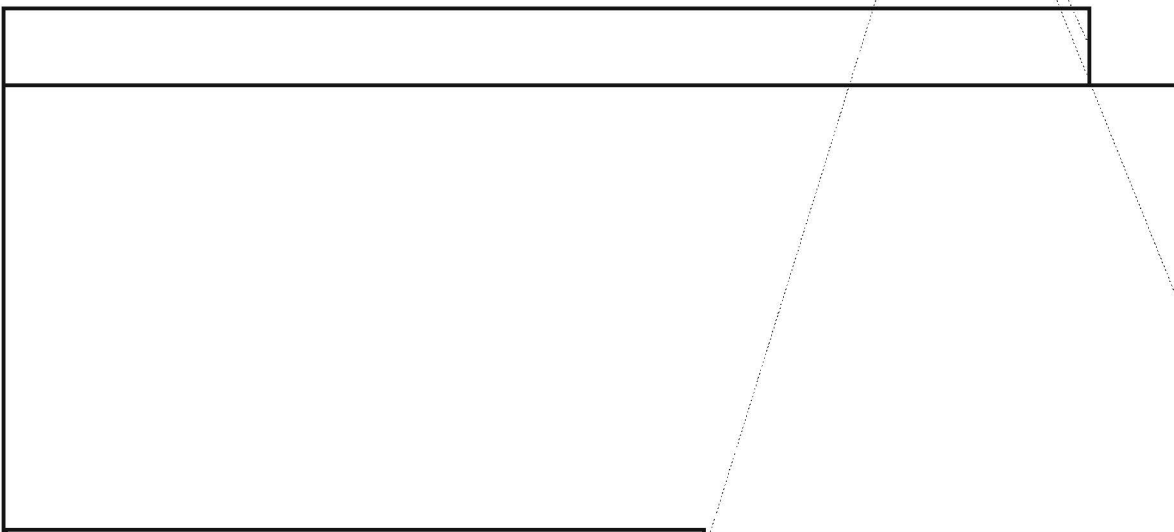
23

~~TOP SECRET TRINE~~

d/m 8-5

~~TOP SECRET TRINE~~(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36~~TOP SECRET TRINE/NOFORN~~  
~~LIMITED DISTRIBUTION~~

Serial: N 0668



The contents of the SICRs identified involve two main ingredients: first, the nature of the desired information on the subject mentioned in the title; and second, a review of the known information on the subject. The known information, in most cases, reflects a compendium of data from several sources (not limited to SIGINT). In addition to revelations of specific areas of interest, the method of generating and addressing SICRs affords a clear insight into the relationships and capabilities of various member agencies of the U.S. Intelligence Community.

4. There were 30 Navy Security Group personnel on board the ship (29 enlisted and 1 officer), all of whom were cleared and indoctrinated for Category III COMINT. The Commanding Officer, Executive Officer, Operations Officer and Communications Officer were also COMINT-indoctrinated. Several of the NSG personnel were also knowledgeable in various compartmented problem areas. For example, 4 personnel held [redacted] clearances, one of whom also held a [redacted] clearance, and 3 held SPO TALENT/KEYHOLE clearances. In general it can be stated that the NSG personnel on the PUEBLO were fully qualified signals intelligence technicians and that their past assignments have covered a wide range of geographic

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

~~TOP SECRET TRINE~~~~TOP SECRET TRINE/NOFORN  
LIMITED DISTRIBUTION~~

Serial: N 0668

areas and targets in the field of SIGINT. Collectively these men would be able to describe the world-wide mission of the U.S. SIGINT collection and production effort, including most of the overt collection sites and their subordination, as well as many key NSA and Service Cryptologic Agency personnel. They could be expected to be completely knowledgeable of the state of the art in the fields of SIGINT collection, processing, reporting techniques and successes, including our effort on the Soviet Union, Communist China and North Korea. Depending on the duress to which these men may be subjected and the amount of information they may recall, a serious compromise could ensue from their involuntary revelation of the scope of the U.S. SIGINT effort.

5. Similarly, the entire U.S. SIGINT collection, processing and reporting procedures could be compromised through the depth of the technical support material carried on the PUEBLO. These documents expose our SIGINT objectives, our techniques in attacking those objectives, the results (at least in part) of our years of effort, and provide a broad insight into the entire operating structure of the U.S. and some allied SIGINT establishments, and the intelligence interests of the U.S.

6. At this juncture, there still remain a number of critical unknowns regarding the extent to which classified information and equipment may have been jettisoned or destroyed by the crew of the USS PUEBLO. For lack of more definitive information other than that presently available concerning the specific identification of the documents and equipment which may have fallen into the hands of the North Koreans, our damage assessment must be couched in foreboding tones. If some of the more sensitive documents were actually captured, as now seems to be the case, the translation and interpolation of the information contained therein would require extensive study before the results of their analysis could be detected in effective counter-measures. Ultimately, however, it can be anticipated that communist efforts in communications security will be greatly increased in those areas specifically covered by

~~TOP SECRET TRINE~~

~~TOP SECRET TRINE~~~~TOP SECRET TRINE/NOFORN  
LIMITED DISTRIBUTION~~

Serial: N 0668

the captured documents, and we can also anticipate an overall concentration of Soviet, KORCOM (and perhaps CHICOM) communication security endeavors, even in areas of communication activity not covered by the captured documents. Moreover, it is reasonable to postulate that Soviet, KORCOM and CHICOM efforts to strengthen communications security practices throughout the entire Communist Bloc will be undertaken. Should this in fact occur, the general level of SIGINT information now available to the U.S. Intelligence Community could be reduced. Exactly how much, in what areas, or for how long, we cannot say at this time.

7. Although the possible loss of the communications security equipment or materials in no way will compromise U.S. communications, it nonetheless has this serious aspect:

The capture of the modern U.S. communications security equipments or the maintenance and operations manuals, could stimulate one or another of these countries (or possibly Communist China) to make major changes in their communications security equipment and practices.

8. NSA has provided as interim notification and preliminary assessment of the loss of the USS PUEBLO to GCHQ, CBNRC and DSD. NSA has been advised by the Senior United Kingdom Liaison Officer (SUKLO) that verbal reports concerning the loss of the ship have been made to the JIC and also to the LSIC Security Committee by the Director, GCHQ. We are presently providing an official COMINT compromise report to GCHQ in accordance with paragraph 44(a) Appendix B, of the UKUSA Agreement and are reviewing with them the desirability of replacing the present COMINT codewords. The Board will be advised later of the results of this review.


~~TOP SECRET TRINE~~

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

~~TOP SECRET TRINE~~~~TOP SECRET TRINE/NOFORN~~  
~~LIMITED DISTRIBUTION~~

Serial: N 0668

9. In anticipation of the possible release of the crew of the USS PUEBLO, NSA has established a "fly away" team to interview COMINT personnel in Hawaii, in order to obtain as promptly as possible detailed knowledge concerning the extent of loss of COMINT material and communications equipment. In the interim, NSA will continue to closely observe communications activity of North Korea, the Soviet Union and Communist China and report to the Board any reflection of changes which can be possibly attributed to the capture of classified documents from the USS PUEBLO.

  
MARSHALL S. CARTER  
Lieutenant General, U. S. Army  
Director

Incl:  
a/s

Copies Furnished:

Chairman, SIGINT Committee, USIB

Chairman, United States Communications  
Security Board

*ASD 8915*

~~TOP SECRET TRINE~~

~~TOP SECRET~~~~TOP SECRET/NOFORN~~

Serial: N 0668

cc: DIR (3)	D33	G/SSO
L2	P04	K/SSO
Reading File	M55	
D12 (5)	M501	
ADN	S13	
ADP	GC	
ADPM	IG	
ADC	A/SSO	
D32	B/SSO	

M/R: The instant memorandum for the Members of USIB provides an impact assessment statement based upon the capture of the USS PUEBLO and possible compromise of an unknown amount of SIGINT technical support material, communications equipment and SIGINT collection equipment.

The SIGINT impact statement being provided the Board has been extracted from data used in a 15 February 1968 PFIAB presentation made by the Director, NSA concerning the PUEBLO. The COMSEC impact statement was provided to D12 by S1 (Mr. W. Ryan).

Comments concerning NSA review of COMINT documents appearing in photographs recently released by North Korea were provided by P04 (Mr. Snow) at D12 request. P04 advises that cognizant elements of A, B and G Groups affirm that to date the capture of the USS PUEBLO has had no adverse affect on the COMINT effort.

The Board is also being apprised of earlier action taken by NSA (D33) to advise GCHQ (and CBNRC/DSD) of the PUEBLO capture and that NSA is providing an official COMINT compromise report to them in accordance with paragraph 44(a), Appendix B, of the UKUSA Agreement.

CONCUR: P04, Mr. Snow	D1, Col. Halloran
M501, Mr. Nix	D32, Mr. Croskery
<span style="border: 1px solid black; display: inline-block; width: 150px; height: 15px;"></span>	S13, Mr. Ryan
DADPM, Mr. Price	
D33, Mr. Braley	

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

~~HANDLE VIA COMINT CHANNELS ONLY~~~~TOP SECRET~~

~~TOP SECRET TRINE~~~~TOP SECRET TRINE/NOFORN~~  
~~LIMITED DISTRIBUTION~~

SUBJECT: Assessment of the Loss of the USS PUEBLO

The Following is an impact assessment statement concerning the loss of the USS PUEBLO and the possible damage resulting from the compromise of SIGINT technical support material, communications equipment and SIGINT collection equipment aboard the vessel.

SIGINT Impact

The USS PUEBLO carried SIGINT technical documents and equipments tailored to support the intelligence mission assigned. The mission included target communications of North Korea and the USSR. Message traffic from the PUEBLO as well as the North Koreans indicated that a destruction effort had taken place on board the vessel before she was captured. Since the exact destruction of SIGINT materials cannot be ascertained until members of the SIGINT team are returned and interrogated, the following assessment describes the damage which may accrue to the intelligence effort if all SIGINT documents and equipments were captured intact.

The Technical support documentation would reveal both in its detail and its over-all effect our general mastery of techniques to collect, analyze, and exploit most foreign target communications. Specifically, the material directly reveals or implies: (a) the extent and positioning of intercept collection resources worldwide which for the most part are already revealed or inferred; (b) the intensity and relative priority assigned each effort; (c) the depth of our understanding of target techniques and capabilities; (d) our ability to construct complex intercept equipments to match target emissions; and (e) some successes against foreign cryptographic methods.

~~SPECIAL HANDLING REQUIRED NOT~~  
~~RELEASABLE TO FOREIGN NATIONALS~~

ENCLOSURE

~~TOP SECRET TRINE~~

~~TOP SECRET TRINE~~

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

~~TOP SECRET TRINE/NOFORN~~  
~~LIMITED DISTRIBUTION~~

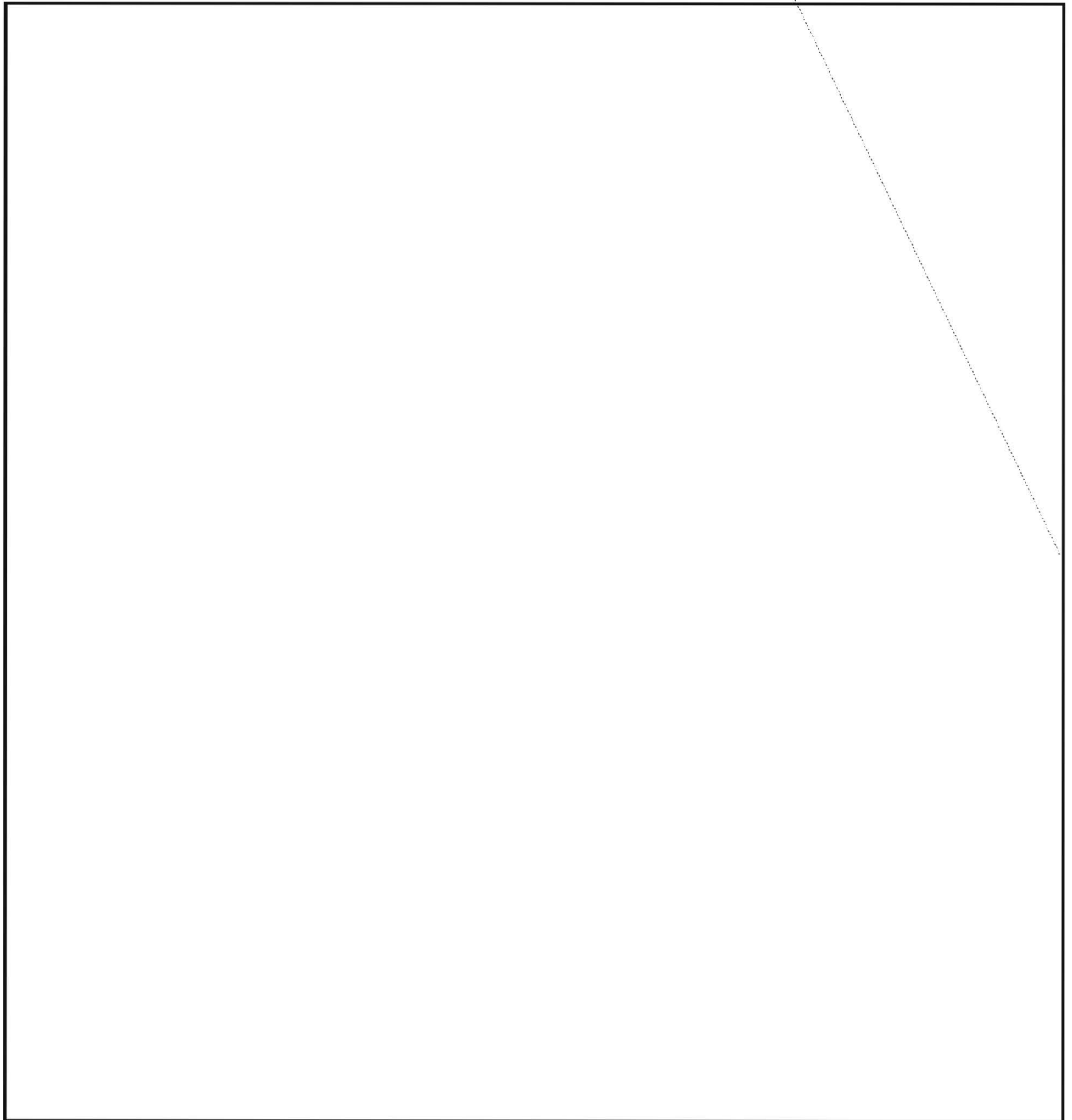
The information that could be gleaned from a complete reconstruction of the technical materials on board would vary between the target countries involved and with the cryptologic methods used. In assuming the worst possible situation, that is no destruction of SIGINT material took place, the following would be the situation.

~~TOP SECRET TRINE~~



(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-19 USC 798  
(b) (3)-P.L. 86-36

~~TOP SECRET TRINE/NOFORN~~  
~~LIMITED DISTRIBUTION~~

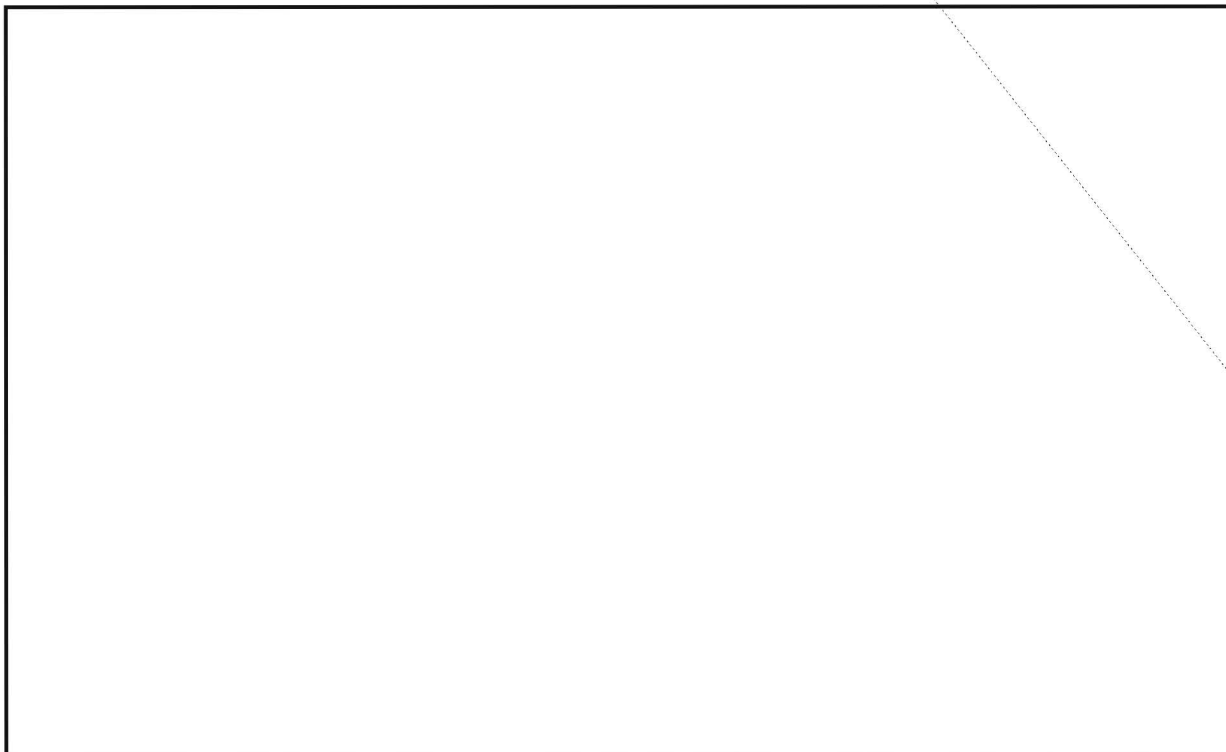


~~TOP SECRET TRINE~~

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

~~TOP SECRET TRINE/NOFORN~~  
~~LIMITED DISTRIBUTION~~

Korean Communists



Communications Security Impact

The estimated loss of COMSEC materials is considered to have resulted in minor damage, mostly temporary, to the security of U.S. Communications. The types of COMSEC equipment on board were the KW-7 (an on-line electronic tactical teletypewriter cipher machine,) the KWR-37 (an on-line broadcast receiver) with associated KG-14 (key generator) equipment, and the KL-47 (a literal cipher machine). Other cryptographic materials aboard included variable keying material (such as key lists or key cards) for the above-mentioned equipment, plus two operational codes and an authentication system.

~~TOP SECRET TRINE~~

~~TOP SECRET TRINE~~~~TOP SECRET TRINE/NOFORN~~  
~~LIMITED DISTRIBUTION~~

The variable keying materials are of critical importance to the security of the machine systems. These variables change frequently, usually daily, and with each change, the cryptography of the system is reconstituted. Compromise of the equipment causes negligible damage to U.S. COMSEC if the variables are kept secure. If the variables are also compromised, only that traffic which had been encrypted by means of those particular variables would be subjected to compromise.

As a precaution, all of the jeopardized variables were taken out of use and superseded as soon as possible. The facts now available, and the inferences which may be drawn from them, indicate that most of the variables aboard the USS Pueblo may have been destroyed, with the strongest supporting evidence being the messages from the ship describing this destruction effort.

The facts also indicate that the logic of the equipments may have been compromised because of ineffective or incomplete destruction of the hardware or maintenance manuals. Damage to the machine systems, therefore, is tentatively assessed as follows:

a. Security of messages transmitted in systems held by the USS Pueblo was jeopardized only to the extent that undestroyed copies of some of those messages remained aboard the ship itself. No other direct damage to U.S. COMSEC resulted.

b. Indirect damage to U.S. COMSEC is confined largely to that which may have resulted if the North Koreans furnished the USSR with new information on the details of the logic of the newer crypto-equipments aboard and detailed information on U.S. cryptographic nets as may have been acquired from captured supporting documents. The potential damage to U.S. COMSEC in these two areas is judged serious because each may enhance Soviet capability to exploit captured keying materials and to perform traffic analysis. North Korea probably would not be able to exploit materials in those two areas without help from the USSR.

~~TOP SECRET TRINE~~

~~TOP SECRET TRINE~~~~TOP SECRET TRINE/NOFORN  
LIMITED DISTRIBUTION~~

In view of widespread use of the operational codes and the authenticator system, immediate supersession was not possible, but all holders were warned of possible compromise, and ordered to limit usage until the materials could be replaced.

#### Equipment Loss Impact

The PUEBLO carried a sufficient amount of collection gear to enable her to monitor North Korean communications and radar facilities on the East Coast as well as some of the [REDACTED]

[REDACTED] Out of 100 pieces of equipment, 4 items have been identified as classified not higher than CONFIDENTIAL; but the use to which the equipment itself could be put and the results derived therefrom are of course classified. It is very possible that if the equipment was undamaged, a reasonably precise reconstruction of the PUEBLO's intelligence mission could be accomplished.

In addition to the collection equipment the PUEBLO carried a substantial number of technical publications and analytical aids required to enable her to discharge her intelligence collection mission. If these items were captured intact, they would give the North Koreans precise information on the extent of U.S. knowledge of their communications techniques, usage, and radar equipments. The technical publications also reveal a more limited U.S. knowledge of general Soviet communications practices and [REDACTED]

[REDACTED] This information would stimulate either of the two nations to change their communications practices, supersede their callsign systems and/or modify their operational codes.

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

~~TOP SECRET TRINE~~