~~TOP SECRET~~

National Security Agency

Fort George G. Meade, Maryland

CRYPTOLOGIC/CRYPTOGRAPHIC DAMAGE ASSESSMENT

USS PUEBLO

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~LIMITED DISTRIBUTION~~

~~NOFORN~~

~~TOP SECRET~~

~~TOP SECRET~~

National Security Agency

Fort George G. Meade, Maryland

CRYPTOLOGIC-CRYPTOGRAPHIC

DAMAGE ASSESSMENT

USS PUEBLO, AGER-2

23 January - 23 December 1968

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

TABLE OF CONTENTS

PREFACE

This report constitutes a review and assessment of the Cryptologic - Cryptographic damage resulting from the North Korean capture of the USS PUEBLO (AGER-2) and the eleven month internment of her crew. The information utilized to prepare this report was derived from the debrief of USS PUEBLO crewmembers which led to a determination of what sensitive information and equipment is, or is assumed to be, in the possession of, at least, the North Koreans.

All previously published reports estimating the possible Cryptologic - Cryptographic damage resulting from the assumed compromise of information and equipment aboard the USS PUEBLO are herewith superseded. This report is a final overall review of the Cryptologic - Cryptographic damage resulting from the North Korean capture of the USS PUEBLO and her crew.

BACKGROUND

The USS PUEBLO (commissioned as AGER-2 in mid-1967) departed the Sasebo Naval Base at 2100Z on 10 January 1968 for her first intelligence collection patrol which was to be in the Sea of Japan, primarily off the coast of North Korea. The operational deployment areas for the USS PUEBLO were designated by CINCPACFLT. The primary mission of this direct support patrol as expressed by CINCPACFLT, was to:

a. Determine the nature and extent of naval activity in the vicinity of the North Korean ports of Chongjin, Sonjin, Mayong Do, and Wonsan.

b. Sample the electronic environment of the east coast of North Korea, with emphasis on intercept/fixing of coastal radars.

c. Intercept and conduct surveillance of Soviet Naval units operating in the Tsushima Straits in an effort to determine the purpose of the Soviet presence in that area since February 1966.

d. Determine the Communist reaction to an overt intelligence collector operating near the periphery of North Korea and the Soviet Union and conduct surveillance of their naval units.

e. Report any deployment of North Korean/Soviet units which might indicate a change in the WESTPAC threat level.

f. Evaluate the USS PUEBLO (AGER-2) capabilities as a naval surveillance ship.

The USS PUEBLO arrived on station off the coast of North Korea at 1430Z on 12 January 1968. From that date until her capture on 23 January, the USS PUEBLO conducted an intelligence surveillance patrol off the North Korean

coast. However, from 12-22 January the USS PUEBLO operated under radio silence and therefore did not report her position to any U.S. Naval authority during this period of time. The crew debriefs indicate that the USS PUEBLO had proceeded northward along the North Korean coast and was on a return route along the coast when she arrived off the Wonsan harbor area where the North Korean capture occurred on 23 January 1968.

Subsequent to the capture, the crew of the USS PUEBLO were detained for a period of eleven months in North Korean detention camps. During this eleven month period the North Koreans conducted extensive interrogations of the Communications Technicians assigned to duty aboard the USS PUEBLO.

On 23 December 1968, the crew of the USS PUEBLO was released to U.S. authorities. During the period 26 December 1968 through 10 January 1969 these crewmembers were provided the opportunity of a privileged intelligence debriefing (conducted under the title "BREECHES BUOY") in order to assist in the assessment of the Cryptologic - Cryptographic damage incurred as a result of the USS PUEBLO capture.

I. CRYPTOLOGIC DAMAGE ASSESSMENT

A. INTRODUCTION

The Naval Security Group Detachments (NAVSECGRUDET) aboard the USS PUEBLO possessed the Signal Intelligence (SIGINT) documentation and equipments considered necessary to accomplish their assigned mission. Although the mission was targeted against various entities in North Korea and the USSR, the NAVSECGRUDET material inventory included general cryptologic publications and technical support documents which relate to various aspects of the total National SIGINT Effort. Additionally, on the date of the USS PUEBLO capture, a record copy of the Western Pacific Navy Operational Intelligence (OPINTEL) Broadcast for the period 5-23 January was on board. The information in this OPINTEL record pertained in depth to the U.S. SIGINT efforts and successes throughout the Far East/Pacific area and in particular contained a large amount of sensitive information relating to Southeast Asia SIGINT targets. And finally, on board were some 90 DIA Specific Intelligence Collection Requirements (SICRs) which provide detailed background information (including intelligence successes) and SIGINT collection needs on various Soviet, North Korean and Communist China SIGINT targets.

The SIGINT collection equipments operated by the NAVSECGRUDET personnel are not considered classified. However, the combination of different types of equipment into an intercept position configuration in conjunction with its assigned mission reveals specific SIGINT interests. As a result of the USS PUEBLO capture and the verbal disclosures of her crew, all of the intercept position configurations aboard the USS PUEBLO are considered compromised.

The potential damage inflicted on a given SIGINT target area (e.g., North Korea, USSR, etc.) varies relative to the amount of documentary or verbal information obtained. The volume and type of information acquired by North Korea represents an excellent cross-section view of the overall

effort and success of the U.S. cryptologic community. Consequently, effective exploitation and dissemination of this information could prompt costly communications security changes to signal methods and procedures by certain foreign countries (i.e., North Korea, Communist China, North Vietnam, and the USSR) for the next ten years. The estimates of this damage are obviously contingent upon a successful translation and interpretation of the information obtained.

In summary, it can be concluded in all probability that at least the North Koreans are well aware of:

a. The extent and positioning of U.S. SIGINT collection and processing resources worldwide (particularly the Naval Security Group Stations);

b. The intensity and relative priority assigned various SIGINT target efforts;

c. The depth of our understanding of SIGINT target techniques and capabilities;

d. Our ability to construct complex intercept equipments to collect sophisticated SIGINT target emissions;

e. Some of our successes against foreign cryptographic methods and;

f. Our ability to analyze and disseminate intelligence derived from SIGINT on a near real-time basis.

B. SUMMARY OF THE CRYPTOLOGIC DAMAGE ASSESSMENT

1. CLASSIFIED DOCUMENTS

Classified cryptologic material was maintained in two areas aboard the USS PUEBLO prior to the incident which led to her capture. These spaces were: (1) the Research Operations room, occupied by the Naval Security

Group (NSG) Detachment, and (2) the Administrative Office used by the NSG Detachment Officer-in-Charge as the main office for NSG matters and the prime storage area for organizational files as well as excess or duplicate documentation not required on-hand in the Research Operations room. These two areas were limited access spaces and were considered to be "secure". Therefore, documents were not always stored in safes or files.

Emergency destruction of this classified material was conducted during a 20 to 40 minute period immediately prior to the boarding of the USS PUEBLO by the North Koreans. Although the order to "prepare for emergency destruction" was given fairly early in the incident, actual implementation of destruction was withheld until the North Koreans opened fire. In the Research room, physical destruction of material commenced some five to six minutes prior to the receipt of an order from the bridge. The destruction that actually occurred was accomplished in almost total confusion and in a highly disorganized fashion.

Attempts were made to burn classified documents in two or three trash cans which were placed in the passageway outside of the Research room. Almost all of the material from the Administrative Office and some material from the Research room were placed in weighted bags with the intent that they would be jettisoned; however, only one unidentified bag was actually thrown over the side. An insufficient number of weighted bags were available for the amount of classified material on-board and therefore, laundry bags and mattress covers were also filled with material. Some documents, message rolls and other classified material were torn into pieces and scattered about the deck.

At the time of the boarding of the USS PUEBLO by the North Koreans, all efforts directed toward emergency destruction ceased, even though destruction was far from complete. Estimates of the percentage of the classified documents, known to have been on-board the USS PUEBLO, that are now in the possession of the North Koreans range from

50 to 80 percent. This wide range in percentage results from the unknown degree to which the North Koreans were able to recover that material which was torn or ripped.

2. EQUIPMENT

The individual intercept equipments aboard the USS PUEBLO were not classified, although in the past certain tuners of the WLR-1 ELINT receiver were considered to be CONFIDENTIAL. Any sensitivity in regard to intercept equipment results from the integration of various equipments into an intercept "position" and the assigned mission of that "position". The tasks performed by an intercept "position" using various equipment combinations as well as the signal targets assigned can divulge specific SIGINT interests. With this perspective, considering the knowledge of SIGINT collection operations displayed by the North Koreans and the information obtained from various crewmembers, the SIGINT missions of all intercept positions aboard the USS PUEBLO are considered compromised.

Although crewmembers have stated that they did their best to destroy all intercept equipments aboard the USS PUEBLO, it is estimated that only about 5% of the total equipments was destroyed beyond repair or usefulness. Even this 5% estimate cannot be viewed with optimism in view of the number of related maintenance manuals and spare parts captured intact as well as the knowledge gained from interrogations of the USS PUEBLO crewmembers.

The destruction of equipments, as attempted, is best described as confused and disorganized. The disorganization may have stemmed from the lack of training in emergency destruction, the inadequacy of (or unfamiliarity with) an emergency destruction bill, and as a result of the primitive tools available for use in destroying equipments. There was a total of eleven crewmembers in the Research spaces at various times during the destruction period. The limited number of fire axes and sledgehammers available to the crewmembers, and the small area involved, prohibited effective destruction of rack-mounted equipments and added to the disorganization and confusion.

There is no evidence available to indicate that equipments (except for a small piece of unidentified test equipment) were removed from the racks. The damage to the front panels was extensive but resulted in "locking" the equipments in place. Once it was realized that very little damage to internal components was being accomplished, an unsuccessful attempt was made to remove the equipments for further destruction. The debriefing of various crewmembers indicated that in a few instances, however, the internal components of some equipments were destroyed or damaged.

It is assumed that the North Korean capture of the intercept equipments advanced their knowledge of U.S. SIGINT interests and interception equipment technology. The damage impact of any destruction to the intercept equipments was probably negligible because of:

a. Spare parts, undamaged equipments, equipment and facilities book and related maintenance manuals captured intact.

b. Information on the mission of individual positions as divulged to the North Koreans by the crewmembers during interrogations.

3. VERBAL DISCLOSURES

During the detention of the crew of the USS PUEBLO classified Special Intelligence-associated information was disclosed to the North Koreans through several media. Classified information was divulged during the formal interrogations and other interviews and conversations. Additional classified information was also disclosed in various "confessions" and letters which were written by the crew during detention. Finally, some information may have been disclosed through intra-crew discussions of classified data in areas vulnerable to North Korean electronic eavesdropping.

The interrogation and written material provided the North Koreans detailed information not otherwise available. This is particularly true in the area of previous experience, jobs, training schools and prior assignments. Another portion of the oral and written material was already available to the North Koreans from the captured documents and equipment aboard the USS PUEBLO. These latter disclosures were probably beneficial to the North Koreans for assisting in the interpretation and understanding of the captured material and determining the degree of cooperation of the individual crewmembers.

A significant portion of the information was disclosed in a piecemeal fashion (i.e., a number of items on a certain subject were derived from a number of crewmembers or the same crewmembers during different interrogations). Although divulged piecemeal, the compilation of this material could easily provide a comprehensive summary of a number of subjects which were of interest to the North Koreans.

An encountered difficulty regarding completeness and accuracy of what was disclosed both orally and in written confessions is the fact that this information is dependent upon the individual crewmember's recollection of what were at times extended discussions which took place at various intervals over a period of eleven months. There were a number of confessions written by the crewmembers which were never released by the North Koreans. It has been established that a number of these confessions were detailed and contained Special Intelligence information.

The North Koreans displayed particular interest in SIGINT collection units around the world to include collection equipment and the previous duties of the communications technicians of the USS PUEBLO. The degree to which information was elicited was apparently related directly to the degree of knowledge the Koreans held on a particular subject or the previous assignment/training of a given crewmember as revealed in his captured service record.

Although it can be established that a great deal of information was provided the North Koreans in both oral and written form, various factors (e.g., crewmembers' ability to recall information) tend to reduce the probability of a comprehensive evaluation of information disclosed.

4. MAJOR SIGINT TARGET AREA ASSESSMENTS

North Korea - There were approximately 397 separate SIGINT documents on board of which 55 are directly or indirectly related to SIGINT exploitation of North Korea. This documentation, in addition to some forty separate North Korean-related items contained in the Operational Intelligence Broadcast and crewmember disclosures, reveals the full extent of U.S. information on North Korean Armed Forces communications activities and

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

USSR -

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

Communist China - The material reviewed for the overall assessment of damage to the U.S. SIGINT effort against Communist China includes [redacted] of on board SIGINT information from the Operational Intelligence Broadcast System, MUSSO documents and other miscellaneous publications. The totality of SIGINT information which has been compromised at least to the North Koreans concerning the collection, processing and reporting operations/techniques of the U.S. against the Chinese Communist target is extensive and without precedent. [redacted]

[redacted]

North Vietnam (Vietnamese Communist) - The damage assessment of the U.S. SIGINT effort against North Vietnam was derived primarily from a review of approximately 3500 messages transmitted on the West PAC Operational Intelligence Broadcast System. [redacted] the application of traffic analytic techniques to produce SIGINT and the successes of all relevant airborne, seaborne and landbased collection efforts was compromised. This information, used in conjunction with the information in the MUSSO documents and miscellaneous publications on board the USS PUEBLO, reveals the completeness of the U.S. exploitation of North Vietnamese communications, the use of these results in support of tactical operations and a complete and accurate picture of U.S. SIGINT posture in Southeast Asia.

[redacted]

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

II. CRYPTOGRAPHIC DAMAGE ASSESSMENT

A. INTRODUCTION

When the USS PUEBLO departed Japan in January 1968, the critical communications security materials which she carried included four types of cryptographic equipment, associated keying materials, maintenance manuals and operating instructions, and the general COMSEC publications necessary to support a cryptographic operation of the scope envisioned for the USS PUEBLO.

Prior to the USS PUEBLO's departure from Japan, she was directed by COMNAVFORJAPAN to off-load various cryptographic systems in view of the sensitive nature of her mission. The material she was to have kept aboard was considered to have been essential by COMNAVFORJAPAN to maintaining secure communications, while simultaneously subjecting a very minimum of cryptographic material to compromise in the event of emergency. The material to have been kept aboard included one KL-47 for off-line encryption, two KW-7s for on-line teletype encryption, three KWR-37s for receiving the Navy Operational Intelligence Broadcast, and four KG-14s which are used in conjunction with the KW-37 for transmitting and receiving the Fleet Broadcasts. The remainder of the prescribed inventory included repair kits for the equipment, seven maintenance manuals, three operating instructions, fifteen single-page printed key lists effective for January, February and March 1968 for five communication networks, six books of key cards (34 cards per book) effective in January, February, and March 1968 for the Navy Operational Intelligence Broadcast and eleven classified general instructional documents.

During the Special Intelligence debriefs conducted at San Diego in December 1968 and January 1969, it was discovered that there was superseded keying material for the months of November and December 1967 still aboard the USS PUEBLO. It was also determined during these debriefs that the destruction effort for the equipment, keying material, and general instructional publications was ineffective to the extent that most of the material was compromised.

The damage resulting from the loss of the superseded keying material is complicated by the absence of any action taken at the appropriate level to review traffic for November and December 1967 at the time of the USS PUEBLO incident. The failure to initiate all-encompassing traffic reviews resulted from the presumption in January 1968 that all superseded material aboard the USS PUEBLO had been destroyed as required by Naval Directives. In accordance with Navy practice, an authorized destruction list was forwarded to the USS PUEBLO for the November and December 1967 material but was returned by the U.S. Post Office with a notation that it was undelivered to the addressee. However, Navy Directive (RPS-4), held by the USS PUEBLO, requires that in the event the list is not received, destruction of superseded material will be effected by the 15th day of the month following its effective period with an appropriate report being forwarded to higher headquarters.

With respect to the cryptographic equipment which was aboard, it should be noted that the USS PUEBLO was directed by COMNAVFORJAPAN to retain four KG-14s with associated repair kits. The keying material and operating instructions for these equipments were removed from the USS PUEBLO since they were not on the list of materials to be retained on board. There was, therefore, no operational requirement for the KG-14s to be aboard and, in fact, the USS PUEBLO did not have the keying capability to receive the KG-14 broadcasts.

In summary, cryptographic damage incurred by the capture of the USS PUEBLO can be attributed, in part to the extensive amount of superseded and excess crypto-material aboard. Had it not been for the existence of this material, the destruction effort probably would have been more effective. In particular, if the superseded keying material had not been lost, the possibility of compromise of any United States traffic, other than the undestroyed record copies of messages on board the USS PUEBLO at the time of capture, would have been negligible.

Following the USS PUEBLO's capture, selected qualified cryptographic technicians were interrogated intensively by

special and apparently highly competent North Korean electronics experts regarding the technical principles of the cryptographic equipment, the equipment operating procedures, and the relationship of the associated keying material to the cryptographic equipment. It is noted that the North Koreans neither displayed any of the captured cryptographic material to the crew (except for some equipment diagrams) nor publicized the material for propaganda purposes. When contrasted with the international publicity given to the capture of other highly classified Special Intelligence documents, the fact that cryptographic material was not displayed or publicized would indicate that they thoroughly understood its significance and the importance of concealing from the United States the details of the information they had acquired.

B. SUMMARY OF CRYPTOGRAPHIC DAMAGE ASSESSMENT

1. EQUIPMENT

Ineffective maintenance manual and equipment destruction resulted in the compromise of the cryptographic principle of the KL-47, KW-7, KWR-37 and KG-14. The loss of these equipments provides no appreciable advantage to the Communists (e.g., North Korea, USSR, Communist China) in the exploitation of United States or Allied communications beyond the point that it provides them with a clear understanding of the crypto-principles employed in the electrical encryption of U.S. communications. While such an understanding would be of abstract benefit in planning possible future cryptanalytic attacks on U.S. communications, if the state of the art ever leads to the development of suitable computational capacity, the fact that they have detailed knowledge of the U.S. cryptographic principles employed does not in itself aid in the exploitation of U.S. communications. In order to readily exploit U.S. communications using the captured crypto-equipments, assuming they successfully reassemble one or more units, the Communists would have to have or recover the cryptographic key. Although this is a contingency which appears unlikely, it must be recognized as a possibility considering the keying material targetting information which appears in various U.S. general informational publications captured by the North Koreans. Thus, in summary, the absolute threat to U.S. communications resulting from the loss of cryptographic equipment ranges from zero to minimal.

In assessing the compromise of the various equipment cryptographic principles, consideration has been given to the assistance provided by USS PUEBLO technicians during North Korean interrogations. It is concluded that the information provided by the cryptographic equipment operators, while probably detailed and accurate, did little beyond confirming what was already available to the North Koreans. The operating techniques employed for the equipment are simple and clearly outlined in the operating instructions, which are presumed to have been captured, thus any information provided by the operators would have been of little value from a technological standpoint. Conversely, the detailed technical explanations provided by USS PUEBLO's cryptographic maintenance technicians are regarded as having been significantly helpful to the North Koreans in analyzing both the hardware and maintenance manuals. While it is difficult to assess accurately the precise advantage in terms of time, considering the probable technical competence of the special interrogation teams and the detailed knowledge of the USS PUEBLO technicians, it is estimated that from three to six months of technical diagnostic analysis were saved by the North Koreans through interrogation of the crewmen. However, no information apparently was provided by the technicians which could not have been eventually obtained through analysis of technical data available to the North Koreans from the captured hardware and maintenance manuals.

2. KEYING MATERIAL (SUPERSEDED)

All traffic encrypted by any holders in the November and December 1967 keying material which was aboard the USS PUEBLO was subjected to compromise by virtue of the probable capture of the related keying material. The North Korean Government probably does not possess a sophisticated COMINT effort which would be required to intercept and file all of the types and volumes of U.S. communications encrypted in the cryptographic systems in question. The USSR, however,

probably has such a capability and effort. Consequently, if the USSR has acquired the captured material they will be able to match the captured key to intercepted traffic.

While some limited amounts and types of keying material were destroyed prior to the USS PUEBLO being captured, the crew's inability to identify specifically the items which were destroyed necessitates the presumption that all of the cryptographic keying material may have been captured. Following is a summary of the types of cryptographic systems lost for which the related traffic is subject to compromise:

a. The KW-37 Operational Intelligence Broadcast (GOPI) for November and December 1967.

b. Eight KW-37 Fleet Broadcasts for November 1967.

c. Eight KG-14 Fleet Broadcasts for November 1967.

d. Five and two KW-7 systems for November and December 1967, respectively.

e. Twelve and three KL-47 systems for November and December 1967, respectively.

f. A One-Time Pad System. (Pages destroyed as used; unused pages of no value.)

In addition to the major systems listed above, two tactical operations codes for November and December 1967, four authentication systems, and five other miscellaneous cryptographic items effective during November 1967 may have been lost. These minor systems are used for and are capable of providing only real-time or very short-term protection to tactical communications and consequently their loss at the time of the USS PUEBLO capture did not result in any appreciable damage.

3. KEYING MATERIAL (JANUARY 1968)

The January 1968 keying material for the KW-37 Operational Intelligence Broadcast, two KW-7 systems, and three KL-47 systems were compromised. In addition, five cryptographic items of lesser significance, including two tactical voice codes, one tactical authentication system, and two other minor systems were compromised. On 24 January 1968, all holders of the KW-37, KW-7, and KL-47 materials were directed to discontinue use of the systems immediately. Holders of the tactical does and authentication systems were directed to minimize usage until replacement materials could be provided. The traffic passed in these systems for the period 1 through 24 January 1968 was subjected to compromise as a result of this keying material loss. With regard to the KW-37 Operational Intelligence Broadcast, loss of the keying material was incidental since the traffic itself for the period 5 through 23 January 1968 was on board the USS PUEBLO and is presumed captured.

4. KEYING MATERIAL (RESERVE ON BOARD)

The future months' keying material aboard the USS PUEBLO for the KW-37 Operational Intelligence Broadcast, two KW-7 systems, and three KL-47 systems was replaced by new material; thus, no related traffic was jeopardized. As in the case of the January material, the holders of the tactical systems were directed to minimize usage until replaced. Replacement of these systems was effected by 1 March 1968.

5. GENERAL PUBLICATIONS

All general publications aboard the USS PUEBLO are considered to have been captured by the North Koreans. There were eleven such documents aboard and, cumulatively, they provide a detailed description of the United States physical security structure for the protection of cryptographic material. These documents also define the U.S. Navy cryptographic order of battle. The following are the types of information available in these captured documents:

a. The cryptographic netting structures of all material used by the U.S. Navy and those systems used jointly with the U.S. Army, U.S. Air Force, the National Security Agency, NATO, SEATO, and [redacted]

b. The short title, long title, effective period and effective date of each system. Also, the destruction date, classification, addresses of reserve material stock points, and the identity of associated materials, e.g., equipment, rotors, etc., can be derived from the publications.

c. The specific structure of the COMSEC material distribution and accounting system including authorized physical transmission media, frequency of inventories, method of inventory, etc.

No direct damage to the U.S. cryptographic effort should result from the loss of these general publications. However, with the detailed knowledge of COMSEC material distribution channels, and systems usage which these publications provide, it can be anticipated that Communist attempts to physically acquire U.S. cryptographic materials can be intensified and carried out in a more systematic and effective manner than in the past.

(b)(1)
(b)(3)-P.L. 86-36

III. CONCLUSIONS AND OBSERVATIONS

In summary, it is concluded that the compromise, to at least the North Koreans, of information concerning the Cryptologic Community collection, processing and reporting operations/techniques on a worldwide basis is without precedence in U.S. cryptologic history. The threat to U.S. communications resulting from the loss of the cryptographic equipment aboard the USS PUEBLO is minimal. The fact that this loss provides nations, other than the U.S., a clear understanding of the crypto-principles employed in the encryption of our communications does not in itself aid in the exploitation of U.S. communications. They would have to acquire the cryptographic keys used in conjunction with the equipment in order to exploit U.S. communications. If U.S. crypto-principles are adapted and used by other countries in their communications, the threat to the U.S. intelligence effort would be serious. Although there is no firm evidence that the North Koreans have passed the "PUEBLO PAPERS" to any other Communist power, it seems only reasonable to assume that the North Koreans have, or will in the future, provide the USSR, Communist China and North Vietnam that information which pertains to their communications.

Distinct from any assessment of the overall compromise, is an estimate of the potential damage to any particular SIGINT target area. Communications of most SIGINT targets are normally in a state of evolution. Because of this, attribution to the USS PUEBLO loss of any particular modification in a SIGINT targets methods or procedures is extremely difficult. The options open to any of the effected nations in possession of the "PUEBLO PAPERS" are numerous. Thus any definitive prediction of the potential impact on any given SIGINT target would be hypothetical at this time.

There are observations that should be made concerning factors that impact on the seriousness of the cryptologic and cryptographic compromise:

a. Technical support materials were provided the USS PUEBLO from many sources independently. The cryptologic damage was heightened by the presence of multiple copies of support materials and a liberal interpretation of the technical information required to support the mission by these many sources.

b. The fact that the USS PUEBLO was "home base" for the crew required that materials concerning personnel records, technicians workbooks from previous assignments, classified advancement in rate training materials and other general documentation were on board. These documents were used to direct the interrogation of the crew and to provide a generalized framework for better interpretation and understanding of the specific technical information revealed.

c. Destruction of classified materials was not a well organized, preplanned operation. Destruction devices did not match the size or complexity of the materials to be destroyed. These factors contributed to the enormous loss of highly classified documents and equipments.

d. Maintenance of historical message files and communications circuit monitor requirements compromised significant information of a timely nature that was completely unrelated to the USS PUEBLO area of activity.

e. The distribution and retention of daily and weekly intelligence summaries compromised a measure of methods and successes not otherwise available on the USS PUEBLO.

f. The inclusion in intelligence reports of not only required intelligence information, but also unnecessary details of the source and SIGINT techniques and successes used to produce the information significantly added to the cryptologic damage inflicted.

g. The unnecessary capture of excess equipment and materials was the most significant loss sustained in the cryptographic area.