~~TOP SECRET~~

28 FEB 1969

SECTION V

CRYPTOGRAPHIC DAMAGE ASSESSMENT

USS PUEBLO, AGER-2

23 January - 23 December 1968

Declassified and approved for release by NSA on 12-20-2006 pursuant to E.O. 12958, as amended. MDR 42513

25603 0252

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

DOCID: 3075790

TABLE OF CONTENTS

		PAGE
A.	INTRODUCTION	
B.	SUMMARY OF CRYPTOGRAPHIC DAMAGE	4
	1. Equipment	4
	2. Keying Material (Superseded)	5
	3. Keying Material (January 1968)	6
	4. Keying Material (Reserve On Board)	7
	5. General Publications	7
C.	RECOMMENDATIONS	9
D.	EQUIPMENT	10
	1. Location	10
	2. Destruction	11
	3. Conclusions	15
E.	DOCUMENTS	17
	1. Location	17
	2. Destruction	19
	3. Documents Observed	23
	4. Conclusions	23
F.	INTERROGATIONS	25
G.	EQUIPMENT AND MAINTENANCE MANUALS	32

		PAGE
H.	INVENTORY OF EQUIPMENT, MANUALS AND PARTS	36
I.	KEYING MATERIAL	39
J.	INVENTORY OF KEYING MATERIAL	43
K.	GENERAL PUBLICATIONS	55
L.	INVENTORY OF GENERAL PUBLICATIONS	57

A. INTRODUCTION

1. 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.

2. Prior to the 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. She was also directed to hold repair parts 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 one Naval broadcast system, and eleven classified general instructional documents.

3. At the time the word was received of the PUEBLO's capture on 23 January 1968, it was presumed she had off-loaded material as directed. However, during the Special Intelligence debriefs in San Diego in December 1968 and January 1969, it was discovered that there was superseded material for the months of November and December 1967 still aboard the PUEBLO. It was also determined during the debriefs that the destruction effort for the equipment, keying material, and general instructional publications was ineffective to the extent that a majority of the material was compromised.

4. The damage resulting from the loss of the superseded keying material is complicated by the absence of any action taken at the National level to review traffic for November and December 1967 at the time of the PUEBLO incident. The failure to initiate traffic reviews results from the presumption being made in January 1968 that all superseded material aboard the PUEBLO had been destroyed as required by Naval Directives. It should be noted that in accordance with Navy practice, an authorized destruction list was forwarded to the 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. It should also be noted, however, that a Navy Directive (RPS-4) requires that superseded material will be destroyed on the 15th day of the month following its effective period, and while the procedures provide for a destruction list to be sent to each COMSEC account by the Navy Central Office of Record in Washington, RPS-4 states specifically that in the event the list is not received, the responsible custodian will effect destruction by the 15th of the month and execute the appropriate report to higher headquarters. Because this instruction was available to an experienced custodian, it was assumed in January 1968 that all material was destroyed as required.

5. With respect to the cryptographic equipment which was aboard it should be noted that the PUEBLO was directed by COMNAVFORJAPAN to retain four KG-14s with associated repair kits. The keying material and operating instructions for these equipments were off-loaded by the PUEBLO as directed. There was, therefore, no operational requirement for the KG-14 to be aboard and, in fact, the PUEBLO did not have the keying capability to receive the KG-14 broadcasts.

6. In summary, the damage incurred by the capture of the USS PUEBLO can be attributed, in part, to the extensive amount of superseded and excess cryptomaterial aboard. Had it not been for this material, it is believed that the destruction effort 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 PUEBLO at the time of capture would have been negligible.

7. Following the 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 did not display any of the captured cryptographic material to the crew, except for some equipment diagrams, or otherwise publicize 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 this 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

1. Equipment

a. 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 (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 cryptoprinciples employed in the electrical encryption of U. S. communications. While such an understanding would be of abstract benefit in planning cryptanalytic attacks on U. S. communications, 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 exploit U. S. communications using the captured crypto-equipment, assuming they have been able to reassemble one or more units, the Communists would have to have the cryptographic key, a contingency which while unlikely, 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 is minimal. The threat to the U. S. intelligence effort through the adaptation of U. S. cryptographic principles to the Communist cryptography is covered elsewhere in this report.

b. In assessing the compromise of the various equipment cryptographic principles, consideration has been given to the assistance provided by the 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 available to and easily understood by 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 to the North Koreans. Conversely, the detailed technical explanations provided by the PUEBLO's cryptographic maintenance technicians are regarded as having been significantly helpful to the North Koreans in analyzing both the hardware and maintenance manuals in their possession. 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 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. It should be noted, however, that no information was provided by the technicians which could not have been eventually obtained through analysis of technical data available to the North Koreans from either (or both) the captured hardware or maintenance manuals.

2. Keying Material (Superseded)

a. All traffic encrypted by any holders in the November and December 1967 keying material which was aboard the PUEBLO on 23 January 1968 was subjected to compromise by virtue of the probable capture of the related keying material. The North Korean Government does not possess the capability to mount a sophisticated COMINT effort sufficient to intercept and file U. S. communications of the types and volumes encrypted in the cryptographic systems in question. The USSR, however, has such a capability and is engaged in a massive collection effort; consequently, the possibility exists that: (1) the USSR acquired the captured material and (2) is technically capable of matching the captured key to intercepted traffic.

b. While some limited amounts and types of keying material were destroyed prior to the 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 was subjected to compromise:

(1) The KW-37 Operational Intelligence Broadcast

(GOPI) for November and December 1967.

(2) Eight KW-37 Fleet Broadcasts for November 1967.

(3) Eight KG-14 Fleet Broadcasts for November 1967.

(4) Five and two KW-7 systems for November and December 1967, respectively.

(5) Twelve and three KL-47 systems for November and December 1967, respectively.

(6) 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 systems are used 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 PUEBLO capture did not result in any appreciable damage.

3. Keying Material (January 1968)

The January 1968 keying material for the KW-37 GOPI 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 codes 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 GOPI broadcast,

loss of the keying material was incidental since the GOPI traffic itself for the period 5 through 23 January 1968 was on board the PUEBLO and was presumably captured.

4. Keying Material (Reserve On Board)

The future months' keying material aboard the PUEBLO for the KW-37 GOPI 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

a. All general publications aboard the PUEBLO on 23 January 1968 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. In addition to describing the measures for protecting cryptographic material, the documents also define the U. S. Navy cryptographic order of battle. Following are the types of information available in the captured documents:

(1) 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] EO 1.4.(d)

(2) 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.

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

b. No direct damage to the U. S. cryptographic effort resulted from the loss of the 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 acquire physically U. S. cryptographic materials will be intensified and carried out in a more systematic and effective manner than they have in the past.

C. RECOMMENDATIONS

All recommendations contained in this report have been consolidated in Section III.

D. EQUIPMENT

1. Location of Cryptographic Equipment

The following COMSEC equipments, spares, and manuals were aboard the PUEBLO when she was captured by the North Koreans on 23 January 1968. The equipment and repair parts kits were located in the CRYPTO Room, and the maintenance manuals were in the maintenance area of the research spaces:

a. One TSEC/KL-47 equipment

b. Two TSEC/KW-7 equipments

c. Three TSEC/KWR-37 equipments

d. Four TSEC/KG-14 equipments

e. One KWQ-8 Kit (spare elements for the KW-7)

f. One KWQ-4 Kit (spare elements for the KWR-37)

g. One KG-14 Kit (spare elements for the KG-14)

h. One KAM-3(A), Repair and Maintenance Manual for KL-47

i. One KAM-78(A), Repair and Maintenance Manual for KWR-37

j. One KAM-79(A), Repair and Maintenance Manual for KWR-37

k. One KAM-143(B), Repair and Maintenance Manual for KW-7

l. One KAM-144(B), Repair and Maintenance Manual for KW-7

m. One KAM-145(A), Repair and Maintenance Manual for KW-7

n. One KAM-179(A), Repair and Maintenance Manual for KG-14

2. Cryptographic Equipment Destruction

a. The destruction was far from complete. No COMSEC equipments, spare parts, or KAMs were jettisoned. A few unidentified printed circuit boards from the COMSEC equipments were jettisoned through a porthole. It has been established that approximately 30 - 45 minutes were available for destruction of these items. The primary method of destruction for the equipment was to knock modules and electrical components from the printed circuit boards and let the parts fall to the deck. Some mechanical damage was inflicted to chassis and cabinets. The cabinets and chassis of at least one of each type of the COMSEC equipments (with the exception of the KL-47) were captured practically intact. There was no destruction at all attempted on the spare parts kits (KWQs) for the COMSEC equipments due to the lack of time. Some of the KAM manuals were destroyed by tearing. No burning of the remains was accomplished. A more detailed description of the destruction of specific equipment follows.

b. The following describes the destruction of specific equipment:

(1) KL-47 - Four sets of rotors for the KL-47 were broken up and the pieces left on the deck of the crypto space (two sets of KAR-460A and two sets of KAR-463A). The plastic rotor bodies and notch rings were broken and in some instances the wiring was cut apart. A sledgehammer and a fire axe were used to smash the keyboard, stepping unit, and printing unit. The stepping unit was reportedly smashed with a fire axe in the blade down position. Parts were still recognizable but badly bent and smashed. Approximately 15 - 20 minutes were devoted to smashing the KL-47 and the

four sets of rotors. It is the opinion of a crewman that the North Koreans could not put the KL-47 back into operating condition. Two PUEBLO personnel witnessed and confirmed the physical damage inflicted to the KL-47.

(2) KW-7 - There were two KW-7s aboard. The destruction of each proceeded as follows:

(a) One KW-7 was disconnected from its KWF-1 slide mount and set on the deck in the CRYPTO Room. The top cover was removed from the KW-7 and all of the printed wiring boards were removed from the KW-7. All the modules were knocked off of the printed wiring boards. No further attempt was made to destroy the modules or the bare printed wiring boards. The A1 and A2 boards, which contain the Tetrahedral key combining logic and Fibonacci shift register stages, were not removed from this equipment. The two KWK-7s from this KW-7 were smashed with a hammer. The degree of actual destruction is difficult to ascertain, however, it would be questionable at best since the pieces were left on the floor of the CRYPTO Room. After the modules were knocked off of the printed wiring boards on the first KW-7, the chassis and front panel were smashed rather extensively. The pointed end of a fire axe was used to knock holes all over the front panel. An attempt was also made to smash up the interior of the equipment, card slots, etc. The bottom cover was not removed -- no wiring harnesses were cut or severed. No blows of a fire axe or sledge were directed to the bottom of the KW-7. A crewman felt that the first KW-7 was pretty thoroughly smashed.

(b) The second KW-7 was the last thing in the CRYPTO Room that the crewmen attempted to destroy before the PUEBLO was captured. This destruction effort took place after the North Koreans had actually boarded. All the printed wiring boards, except the A1 and A2 boards, were removed from the second KW-7 and thrown against the opposite bulkhead. The modules were not knocked off of these boards because the crewmen could not find a sledge, fire axe, or chipping hammer. An attempt was made to break some of the

patch cords on the A1 and A2 boards by pulling against them while they were still attached to the KWX-10. It is doubtful if any of the patch cords were broken. The KWK-7 plug boards from the second KW-7 were smashed with a hammer. No damage was inflicted on the KW-7 chassis. A crewman feels this KW-7 could be put back into operating condition, minus the KWK-7 permuter. No destruction of the KWQ-8 was attempted because of lack of time and the location of the kit.

(3) KWR-37 and Spares

(a) The classified boards were removed from the three KWR-37s. The equipments were opened, the drawers pulled out and all the classified boards were removed and put in a pile on the deck. The unclassified elements were left in the equipment. The destruction was accomplished by placing the boards on the deck in the area of the KW-37 where they were pounded with a sledgehammer and a fire axe. At first an attempt was made to completely break the parts and printed circuit boards into pieces, but because of the number of people within the limited open space of the CRYPTO Room, the sledgehammer or fire axe could not be used effectively. A chipping hammer was therefore used to smash the tubes and knock the components off the boards. No further attempt was made to continue breaking up the printed circuit boards. Some KWR-37 boards were broken up with a ballpeen hammer on the raised portion of the hatchway which leads from the research space into the CRYPTO Room. There was no attempt made to destroy the unclassified elements.

(b) The card readers on the KWR-37s were unlocked, and the KAW-1A CRIBs were removed. They were then put on the hatchway ledge and broken by pounding with the ballpeen hammer. The printed wiring matrix was then peeled away from the metal backing plate to which it is glued and both sections of each CRIB were pounded with the hammer again. This is considered to be an incomplete destruction, since the pieces were left in the CRYPTO Room and the matrix could be reconstructed from these pieces. A sledgehammer was used in

the attempt to destroy the card readers on the KWR-37s. The plunger contact panel on one of the card readers was hit with several blows of the sledgehammer. The card readers on the other two KWR-37s were closed when hit with the sledgehammer. It is reported that the outside of the readers were badly bent.

(c) An attempt was made to damage the cabinets and drawers of two of the KWR-37s. Two of the KWR-37 drawers were damaged with blows from the sledgehammer; however, one drawer and cabinet were almost intact, except for the damage inflicted on the card reader.

(d) The KWQ-4 spare parts kit for the KWR-37 was not destroyed. No destruction was attempted because of the lack of time and the fact that they were stowed under the operating position where the communications circuit between the PUEBLO and Kami Seya was being maintained.

(e) It was confirmed that the KWR-37 printed circuit boards were smashed and broken up, but it was not possible to identify the specific classified elements of the KWR-37 which may have been broken up by the crewmen.

(4) KG-14 and Spares

(a) All of the classified and unclassified printed circuit boards were removed from the four KG-14 equipments. Small hammers were used to knock off all the modules from all the boards. Some of the modules were reportedly smashed into pieces, and an attempt was made to break the bare boards into pieces. A chipping hammer was used by a crewman to knock all of the modules off of the boards, but he did not attempt to further destroy either the boards or the modules.

(b) An attempt was made to smash the card readers on the top two KG-14s with a sledgehammer. The card readers were closed. The card readers on the bottom two KG-14s were not damaged.

(c) An undetermined amount of damage was inflicted to two of the KG-14 front panels with a sledge-hammer. Two of the KG-14 chassis and front panels were not touched. The power supply chassis on the four KG-14s were not damaged at all. It is the opinion of a crewman that two of the KG-14s were captured in very good condition. The spare parts for the KG-14 equipments were not destroyed. No destruction of the 14 spares was attempted because of lack of time and the fact that they were also located under the operating position where the circuit with Kami Seya was being maintained.

(d) No one can corroborate or verify the actual destruction of any specific classified element of the KG-14s.

(5) Seven COMSEC KAMs were on board the PUEBLO when she left Japan. These KAMs were located on a shelf in back of the workbench located in the research spaces, because there was no room to stow them in the CRYPTO Room. Three CTs were involved in the destruction of the KAMs. The method of destruction was by ripping pages from the KAMs, tearing the pages into strips or small pieces, and throwing the pieces on the floor. No burning was accomplished. One of the CTs estimates that approximately three to three and one-half KAMs were destroyed in this manner. None of the three crewmen involved in this effort could identify specifically which KAMs were destroyed. During the period of detention a crewman was shown pages from both KAM-143 and KAM-144 (manuals for the KW-7); accordingly, it is highly probable that these manuals were not torn up.

3. Conclusions

a. The cryptographic logic and cryptographic principles for the KL-47, KW-7, KWR-37, and KG-14 have been compromised.

b. It is highly probable that by utilizing the printed wiring boards and spare parts which were not destroyed, the North Koreans can repair and assemble at least one model of the KW-7, KWR-37, and KG-14 equipments.

c. The rotors for the KL-47 were all broken and smashed to the extent that it would be very difficult to reconstruct an operational set of rotors from their remains.

d. The KL-47 was extensively damaged; however, not to the extent that the basic principles of operation could not be ascertained and the equipment possibly reconstructed.

e. An undetermined number of the KAMs were captured intact. (Evidence tends to indicate that KAM-143 and KAM-144 for the KW-7 are in the hands of the North Koreans.)

f. For the short time available and the tools at hand a very concentrated and noteworthy effort was made by the crewmen involved to destroy the COMSEC equipment.

E. DOCUMENTS

1. Location of Cryptographic Documents

Following is the location of cryptographic documents and keying material aboard the USS PUEBLO during the patrol.

a. The following material was located within the research spaces:

(1) CRYPTO Room:

KAK-936	(JL)
KAK-1639	(HK)
KAK-2590	(FK)
KAK-2669	(BB)
KAK-2684	(AS)
KAL-11	(GS)
KAO-27	(B)
KAO-34	(C)
KAO-83	(D)
KAY-T-2000	(Y) Day 23

(2) Maintenance Area:

KAM-3	(A)
KAM-78	(A)
KAM-79	(A)
KAM-143	(B)
KAM-144	(B)
KAM-145	(A)
KAM-179	(A)

b. The following material was located in the RPS safe in the passageway outside the Officer's Ward Room:

AMSP-158	(CT)
AMSP-298	(CF)
AMSP-617	(CQ)
KAA-29	(EC)

KAA-33	(DD)
KAA-38	(CE)
KAA-60	(AT)(AU)(AW)(AX)(AY)
KAC-132	(QY) through (TF)
KAC-138	(BK)(BL)(BN)(BO)(BP)
KAK-588	(JF)
KAK-646	(JL)
KAK-930	(JL)
KAK-932	(JJ)
KAK-935	(JL)
KAK-936	(JJ)(JK)(KA)(KB)(KC)
KAK-1403	(HI)
KAK-1409	(HI)
KAK-1639	(HI)(HJ)(HL)
KAK-1753	(JD)
KAK-1817	(HD)
KAK-2590	(FI)(FJ)(FL)
KAK-2645	(AL)
KAK-2647	(AG)
KAK-2667	(AI)
KAK-2669	(AZ)(BA)(BC)(BD)(BE)
KAK-2684	(AQ)(AR)(AT)
KAY-T-2000	(W)(X)(Y days 1-22 and 24-31)(Z)(AA)
KAY-S-2014	(E)
KAY-S-2016	(AB)
KAY-S-2017	(AA)
KAY-S-2018	(AA)
KAY-S-2023	(M)
KAY-S-2025	(J)
KAY-S-2029	(F)
KAY-S-2073	(B)
KAY-S-3054	(Z)
KAY-S-3056	(Y)
KAY-S-3059	(Z)
KAY-S-3079	(S)
KAY-S-3090	(F)
KAY-S-3091	(F)
KAY-S-3092	(F)
KAY-S-3115	(S)
KAP-EB	
KAG-1C	
KAG-18-1	

KAG-27A
AFSAG-1248
CSPM-1E
CSPM-1F
CSPM-3H
CSPM-3J
CSPM-3J RPMCO1
CSPM-3J RPMCO2
CSPM-3J RPMCO3
CSPM-3J RPMCO4
RPS-4G
RPS-10B
RPS-31E
RPS-32D
RPS-36E
ATP-1A VOL 1
ATP-1A CH 5
ATP-1A RPS I

c. The following material was located in the radio shack:

KAA-60	(AV)
KAC-138	(BM)
KAL-15	(CU)

2. RPS Material Destruction

a. The order to commence emergency destruction was given immediately following the PUEBLO receiving the first salvo of North Korean small arms fire. The emergency destruction bill did not designate ship's personnel to conduct emergency destruction of the contents of the RPS safe; consequently, no crewmembers proceeded to this area for duty. The course of events within the RPS safe area developed as follows: The RPS custodian was in the operating spaces at the time the emergency destruction order was given. He remained in this area for approximately ten minutes after which time he proceeded to the passageway adjacent to the Officer's Ward Room where the RPS safes were located. In

the meantime, the communications technicians were attempting to burn material within the operating spaces but their efforts were largely unsuccessful as a result of excess smoke and lack of ventilation; therefore, the containers used for burning (standard Navy waste cans) were moved from the operating spaces to the weather deck where the destruction effort resumed. This effort was now located within a few feet of the RPS safes. When the RPS custodian reached the RPS safe he reports that he removed all key lists from the safe and personally destroyed them by burning. There are conflicts with respect to what actually occurred at this particular time; however, it appears that some key lists were probably destroyed. He also removed two safe liner jettison bags of material and left them lying on the deck. These bags were never jettisoned. Following the custodian arriving at the scene, several ship's crewmen who were assigned General Quarters Station within the vicinity of the RPS safes began to assist in emergency destruction. Most of these men were General Service (GENSER) personnel whose duties excluded them from the ship's research spaces. None of them, including the communications technicians, was familiar with the identity of cryptomaterial. The point at which the remainder of the cryptomaterial in the RPS safe, including the superseded material, was removed cannot be definitely determined. It appears, however, that some of the ship's crewmen (GENSER) were removing this material, tearing it up, and burning some. One of the primary people involved in this activity was FN D. D. Hodges, who was subsequently mortally wounded. The destruction activity of the RPS material continued for about 15 - 20 minutes (about 10 minutes of burning) from the time that the safes were opened until the North Koreans wounded several of the crewmen. Approximately 30 minutes elapsed from the time the men were wounded until the ship was finally boarded; however, the destruction activity came to a virtual halt at the time the men were wounded and it never resumed to any effective extent. While one crewman indicates that he destroyed a considerable amount of material after the North Koreans opened fire in the area of destruction, statements from other crewmen and officers would suggest that his activity was minimal if indeed he was in the area at all.

b. In summary, emergency destruction of RPS material began approximately 10 - 15 minutes following the order to effect emergency destruction. It continued for a period of approximately 15 - 20 minutes, 10 minutes during which material was being burned. The people engaged in destruction were totally unfamiliar with cryptomaterial, thus their efforts in identifying what was destroyed are largely ineffective. Their description of what was ultimately destroyed follows:

(1) Quite a few pubs -- yellow cover, four-number series, 3/4" x 18" x 8"

(2) One CONFIDENTIAL pub on ADONIS system

(3) Pads (reference is to JOVE. No indication as to how many. Torn only.)

(4) One pad

(5) One booklet CRYPTO cards

(6) KAP-EB

(7) CRYPTO document

(8) Two long gray paperback documents

(9) One pack CRYPTO keying material (key cards)

(10) White envelopes from RPS safes

(11) "Couple" key lists

c. The reference to the yellow cover, four-number series publications is believed to be JOVE pads. It is estimated that somewhere from between four and eight of these were destroyed of a total of 13 aboard. Of the 36 books of key cards aboard, two books are identified as being destroyed with probably a portion of one other. The white envelopes referred to are believed to be key lists -- It is significant that this particular activity took place

after the men were wounded which would have been a considerable period of time after the RPS custodian indicated that he had destroyed all key lists. There were 22 key lists aboard; however, no estimate can be made of the number destroyed. There is no indication as to what the "long gray paperback documents" or the "CRYPTO document" may have been.

d. Simultaneous with the activity described above, the cryptographic keying material and manuals located in the CRYPTO Room were being handed out of the area for destruction. Since the paper material ended up with that being removed from the RPS safe, its ultimate disposition is equally uncertain, thus it is considered compromised. The material known to have been in the CRYPTO Room includes:

(1) the 23 January 1968 key for the KW-37 (KAY-T-2000)

(2) KAK-2684 (AS)

(3) KAK-1639 (HK)

(4) KAK-2590 (FK)

(5) KAK-2669 (BB)

(6) KAK-936 (JL)

(7) KAL-11 (GS)

(8) KAR-460 (A)

(9) KAR-463 (A)

(10) KAW-1 (D)

(The details of the destruction of KAR-460(A), KAR-463(A), and KAW-1(D) are covered elsewhere in this report.) In addition to the above material, it is believed that equipment operating instructions KAO-83(D) for the KW-7, KAO-34(C)

for the KWR-37, and KAO-27(B) for the KL-47 were also in the CRYPTO Room, were passed out for destruction and were captured by the North Koreans.

e. The cryptographic equipment maintenance manuals KAM-179(A), KAM-143(B), KAM-144(B), KAM-145(A), KAM-78(A), KAM-79(A), and KAM-3(A) were located in the maintenance area of the research spaces. Three and one-half unidentified manuals are reported to have been torn up with none of them being burned. It is presumed that those which were torn up were reconstructed by the North Koreans, thus, all of the maintenance manuals were captured.

f. At the time the North Korean harassment began, the January editions of KAC-138(BM), KAA-60(AV), and KAL-15(CU) were located in the radio shack. When the emergency destruction order was given, these documents were lashed to a tool box and jettisoned.

3. Documents Observed in North Korea by Crewmembers

Equipment diagrams from the KW-7 maintenance manuals (KAM-143 and KAM-144) were observed in the possession of the North Koreans by one crewman. One other crewman believes he saw a document which was either a key list or a PALLAS key square; however, the identification is not positive. All other cryptographic information observed was either hand-drawn or compiled by the North Koreans or by the crewmen themselves. The seriousness with which the North Koreans viewed their capture of cryptographic equipment and material is best demonstrated by their unwillingness to display it to crewmembers or otherwise use the material for propaganda purposes.

4. Conclusions

a. The cryptographic document destruction ceased and never resumed when one man was mortally wounded and several were wounded by the North Koreans. The total amount of time effectively devoted to the destruction effort was from 10 - 15 minutes. While some of the key lists, key cards, and one-time pads were effectively destroyed by burning,

the absence of positive identification leaves no recourse but to presume all of the material to have been captured. The only documents positively identified as having been destroyed were the January editions of KAC-138(BM), KAA-60 (AV), and KAL-15(CU).

b. While the lack of time and the hostilities of events precluded effective destruction of material, the over-riding fact is that the crewmembers were faced with destroying a significant amount of superseded material which should not have been aboard. Further, there had been no prior planning for such events either by specific emergency personnel assignments or by practicing emergency destruction. Had only authorized material been aboard the PUEBLO and had the ship's personnel been assigned and drilled in emergency destruction, the damage to U. S. cryptography would have been negligible.

F. INTERROGATIONS

1. The PUEBLO cryptographic maintenance and operator personnel were subjected to intensive interrogations by the North Koreans, who concentrated their efforts primarily on the operational characteristics and the theory of operation of the COMSEC equipments carried aboard the PUEBLO. These intensive sessions were conducted by a North Korean electronics expert who demonstrated a capability to understand the information elicited from the crypto personnel. During early interrogations some of the crypto personnel attempted to convey erroneous or incomplete information to the North Koreans; however, these areas were corrected later by the crypto personnel when they were confronted with the accurate information.

2. Diagrams and sketches of the COMSEC equipments and of the cryptographic logic, which were provided to the North Koreans by the crypto personnel, were of sufficient detail in most cases to explain completely the theory of operation of the COMSEC equipments. In most of these cases, great detail was provided to the North Koreans concerning the Koken and Fibonacci registers, key combining logic, and combiner permutations. This information fully described the cryptographic principles of the COMSEC equipments. On a few occasions the North Korean interrogators produced pages from the KW-7 KAMs at the interrogation sessions and asked the crypto maintenance personnel for technical explanations or clarifying information. There is no doubt that the information obtained through these interrogations greatly reduced the time it would normally have taken for the North Koreans to gain a complete understanding of the COMSEC equipment which they captured aboard the PUEBLO.

3. The North Koreans also attempted to obtain information from the crypto personnel concerning COMSEC equipments which were not aboard the PUEBLO. Some of the equipments mentioned were the CSP 2900, CSP 3000, KW-2, KW-26, KY-1, etc. It is assumed that these equipment short titles were obtained by the North Koreans from documents captured aboard

the PUEBLO. Since the PUEBLO crypto personnel were not intimately familiar with most of these equipments, the North Koreans did not obtain much, if any, detailed information concerning the operational characteristics or cryptographic principles of these equipments.

4. Following is a detailed description of the COMSEC information revealed to the North Koreans during interrogations:

a. A crewman was interrogated intensively by the North Koreans regarding the overall and theoretical operation of the KW-7. He was interrogated frequently by a North Korean "electronics expert" who has been described as "sharp". During the first North Korean interrogation he drew simplified block diagrams of the KW-7 leaving out many details and containing errors which were not detected by his interrogators. During subsequent sessions with the electronics expert these errors and lack of detail were pointed out to him, and he was told to draw better diagrams of the KW-7. When the crewman claimed to have a poor memory concerning the primary and secondary key generator portions of the KW-7, the North Korean electronics expert produced the logic diagrams of the primary and secondary key generators contained in KAM-143B and asked him to explain the theory of operation and the symbols and abbreviations on the logic diagrams. He states that much time was spent with the North Korean electronics expert in the area of key generation and combining, and he told the North Koreans what he knew about it. During these sessions on the KW-7, he was also shown timing diagrams from KAM-143B and asked to explain them. He drew sketches of KWK-7 programming plug and explained how the combiner permutations were accomplished. He made a sketch of the key list for the KW-7 and explained to the North Koreans how and when the KW-7 key changes were made. During one of his interrogations by the North Korean electronics expert he was shown a page from KAM-144B which explains a trouble-shooting technique for the KW-7 key generator section, and he was also shown a print-out which was different from the one in KAM-144B. The crewman was asked

at that time if he could tell what was wrong with the KW-7 if such a print-out occurred. He did not help them in this area. Another crewman explained in detail the operating procedures for the KW-7 including how the KWK-7 plug boards were set up from the key list.

b. Two crewmen were interrogated by the North Koreans regarding the design and operation of the KL-47. One crewman drew sketches of the KL-47 which showed the location of the controls, keyboard, printer, stepping unit, and rotor basket. As an example of the detail that the North Koreans insisted be put in these sketches, they wanted the location of every key on the keyboard. He drew sketches for the North Koreans of the KL-47 electrical circuits in the stepping unit and described how the notch rings on the rotors depressed the leaf spring contacts in the stepping unit and caused the stepping pawls to be activated. He told the North Koreans that the KL-47 had one stationary and six or seven moving rotors. He told the North Koreans that the rotors moved once for each character and did not rotate continuously. The North Koreans questioned the purpose of the 500 letter check on rotors. He could not tell the North Koreans because he didn't know; however, he did describe the routine maintenance check which he normally made, which was 1000 letters or more. From time to time the North Koreans described mechanical parts from the KL-47 and asked what they were and what they did. A crewman drew sketches of the KL-47 rotors showing the rotor body, notch rings, and contacts. He claims the North Koreans did not ask and he did not volunteer the number of contacts on the rotors. Both of the crewmen were interrogated at length about the operational procedures for the KL-47 and how the rotors were set up each day from the key list. Other crewmembers were interrogated by the North Koreans about the compatibility of the KL-7 and KL-47, but they claimed ignorance of such compatibility.

c. One of the crewmen was interrogated intensively by the North Koreans concerning the operational characteristics

and the logic design of the KWR-37. He was interviewed frequently by a North Korean "electronics expert". An indication of the knowledge and technical capabilities of this electronics expert was demonstrated on occasions when he would start to explain a basic logic function or basic electronics theory to the expert and the expert would interrupt the discussions and say that he knew that in detail; to go on. In later interrogations the expert would tell him it was not necessary to cover technical areas that had been previously discussed. The crewman was not shown any portion of the KAM manuals for the KWR-37 during his interrogations by the North Koreans. During the North Korean interrogations the crewman described in great detail the complete theory of operation for the KWR-37. He drew diagrams and described in detail the logic contained on each printed circuit element in the KWR-37. He drew overall block diagrams of the KWR-37 so as to tie the individual functions together. He described the late entry capability of the KWR-37. Sketches of the KWR-37 card reader and key card were drawn and he explained in detail how the card reader and key card accomplish the daily permutations of the Koken stages to the key combiners. He described the traffic flow security characteristics of the KWT-37. Another crewman provided, in detail, the function of the front panel switches, lights and clocks, the length of crypto period, and the operating procedures for the KWR-37.

d. One of the crewmen was intensively interrogated by the North Koreans concerning the operational characteristics and the logic design of the KG-14. He had many interrogations on the KG-14 with an "electronics expert". The technical capabilities of this expert have been previously described in the KWR-37 summary. He was not shown any pages from the KG-14 KAM by the North Koreans. Initially he drew block diagrams of the logic contained on each type of printed wiring element contained in the KG-14, relating this logic back to the overall block diagram of the equipment. He explained how the KG-14 was an ancillary key generator, which used the raw key stream from the KWR-37 to generate an

independent key stream in the KG-14. This explanation of KG-14 key generation involved detailed explanation of the theory of operation of the non-linear sequence generator and cyclic shift registers. He described the function of all controls on the KG-14. He described the function of the alarm circuits and explained the KG-14 high speed, low speed, and facsimile modes of operation. He explained the traffic flow security principles of the KG-14.

e. During the North Korean interrogations there were many attempts to elicit information about COMSEC equipments not carried on the PUEBLO. The North Koreans possessed a listing of undetermined origin which contained an unidentified number of COMSEC equipments. Various crewmembers were interrogated about their knowledge of equipments on the list. Interviews conducted during the SI debrief of the PUEBLO personnel have revealed that the following equipments were mentioned:

(1) CSP 2900

(2) CSP 3000

(3) TSEC/KL-7

(4) TSEC/KW-2

(5) TSEC/KW-26

(6) TSEC/KY-1

(7) TSEC/KY-8

(8) SSM-33

(9) AN/FGQ-1 (131 B2 table)

One crewman drew rather incomplete sketches for the North Koreans of the CSP 2900, CSP 3000, and TSEC/KW-2 showing the equipments to be rotor type machines. He attempted to show

the number and placement of rotors, but stated during his SI debriefs that the information provided them was very vague and general in nature. His sketches showed three rows of five moving rotors and one row of five fixed rotors. He does not recall if his sketch of the KW-2 indicated two or three rows of rotors. He drew sketches of the KW-26 equipments racked up and identified the configuration as having a KW-26T, KWR-26, and two KW-26 power supplies, but was not able to provide the North Koreans with any more detail than the crude sketch. Another crewman also provided the North Koreans with a sketch of the KW-26 front panel, but could not provide specific detail on theory of operation since he was not knowledgeable. Apparently the North Koreans did not press for detailed information on COMSEC equipments when they became convinced that the crewmember was not knowledgeable of the equipment. The North Koreans apparently were aware of cryptographic compatibility of the KL-47 and KL-7 equipments, but it is undetermined if this was confirmed to them. They were told that the KY-8 was a voice encryption system; a crewman explained to the North Koreans that he didn't think the 131 B2 system was used anymore by the U. S. He explained that the SSM-33 worked like the 131 B2 table.

f. In addition to interrogation of the cryptographic maintenance technicians, the PUEBLO radioman was interrogated by the North Koreans who exhibited considerable interest in the manner in which challenge and replies are derived by use of the TRITON authenticators. The process was explained to them in detail including a hand-drawn sketch of the TRITON grille (KLI-12). The fact that the radioman gave them the information they were seeking is incidental, since they captured the TRITON authenticators which contain detailed instructions. It is assumed that the North Koreans (1) have copies of KAA-29, KAA-33, KAA-38, and KAA-60, (2) know the details of how they are employed, and (3) know the geographical areas in which each is used.

5. Conclusions

a. The North Koreans made an intensive effort and succeeded in obtaining information which gave them a

very good understanding of the theory of operation and the cryptographic principles of the KL-47, KW-7, KWR-37, and KG-14.

b. The information elicited by the North Koreans from the PUEBLO crypto personnel greatly reduced the time it would have taken them otherwise to become familiar with and understand the principles embodied in the COMSEC equipment that was aboard the PUEBLO.

c. With the information obtained by the North Koreans from the PUEBLO crypto personnel and the incomplete destruction of the COMSEC equipments and spare parts, it is highly probable that they now have at least one working model of the KW-7, KWR-37, and KG-14 equipments in their possession.

G. DAMAGE ASSESSMENT OF CRYPTOGRAPHIC EQUIPMENT AND MAINTENANCE MANUALS

Following is the damage assessment of the compromise of the cryptographic principles of the equipment aboard the PUEBLO considering the two extremes of acquisition by the USSR and North Korea. The value of the principles to other Communist nations, for example Communist China or North Viet Nam, would be in proportion to their technological development.

1. The KG-14, a relatively new addition to the U. S. inventory, is a versatile and efficient equipment incorporating advanced electronic techniques. Used in conjunction with the KW-37, it provides high security to multi-channel teletypewriter or facsimile broadcast transmissions. There is no record of its previous compromise through physical loss or exposure to a known defector, and it has been released only to the UK, Canada, and Australia. Its acquisition by Soviet Russia is of value since it permits them to bypass the diagnostic phase of cryptanalysis which would otherwise consume years of costly and painstaking labor through pure cryptanalytic study. With the equipment logic known, a competent SIGINT activity can, by acquiring any KG-14 key card used by the U. S. in the future, read all traffic encrypted with that key card, provided the related KG-14 cipher transmission along with the KW-37 cipher transmission which controls its operation has been intercepted and identified. It is also possible that the Soviets will use some of the logic (or its embodiment) to improve or modernize some of their own systems to the detriment of U. S. SIGINT effort. One feature which would be of great benefit to the Soviets is the heavy use of alarm circuitry characterizing the KG-14, an area to which the USSR has paid insufficient attention until recently. USSR access to the KG-14 will undoubtedly accelerate its engineering efforts in alarm circuitry development.

2. The same considerations as described for the KG-14 generally apply to the KW-37 with the exception that:

a. The KW-37 is released to Germany, Netherlands, France, Italy, Norway, Denmark, Greece, Turkey, Belgium, Portugal, Canada, Australia, and UK and is, therefore, more likely to have been previously compromised, although no reports to that effect have been received.

b. The KW-37 uses a secondary variable (CRIB) limited to U. S. holders only, thus the acquisition of both the key card and CRIB is required for immediate exploitation of traffic.

c. The KW-37 logic is embodied in subminiature tubes, an obsolete technique for U. S. electronic crypto-equipments.

3. The KW-7 is probably the best crypto-equipment for encryption of tactical teletypewriter traffic in the world. It is small, efficient, and secure. As in the case of the KG-14, loss of the equipment itself or of its logic has no direct effect on U. S. COMSEC, but provides an immediate means to exploit any key lists the enemy may acquire. It should be recognized that the KW-7 was specifically designed as a tactical equipment for use in forward echelons where physical loss through capture has been anticipated. Its logic has been or is being provided to all NATO countries and has been provided to Australia and New Zealand as well. Since being placed into operation in Southeast Asia, eight KW-7s have been lost with four presumed compromised; however, the PUEBLO incident is the only absolutely substantiated loss and accompanied as it was by the loss of the related manuals and technical explanations is certainly the most complete. It is reasonable to expect that the Communists will eventually adapt some of the features to their own cryptography.

4. Indirect damage to COMSEC which may have occurred through USSR acquisition of the details of the techniques, principles, or procedures used in the KL-47 is judged to be negligible. Although the information would have been of great value to them had they not previously acquired it, there is a very high probability that they already possess

the information. This is almost certainly true because many thousands of equipments have been in use world-wide for more than a decade, including about 10,000 functionally identical KL-7 equipments held by NATO countries. The equipment, associated maintenance manuals, and operating instructions have been exposed to possible compromise a number of times over the years. In recent intelligence operations, the USSR has made efforts to obtain key lists and rotors, but have shown no interest in the equipment itself or its supporting documents. Damage to SIGINT interests as a result of loss of the KL-47 to the USSR is also judged to be negligible. There is no evidence that they have found it necessary or desirable to adopt KL-47 principles or techniques in their own systems. The system is old, electromechanical, obsolescent, and relegated primarily to back-up use by the U. S.

EO 1.4.(c)

5.

nation's traffic. It is presumed, however, that with the capture of the cryptomaterial aboard the PUEBLO, the Koreans now have sufficient knowledge of the four U. S. machine systems involved to permit them to exploit any future traffic in these systems provided they can intercept it and physically acquire the specific keying variables used. It is possible, therefore, that they may make a concentrated attempt to acquire some of these key lists and key cards by subversion or physical penetration, although such efforts will probably be limited for some time to come by both economic and technological constraints.

cryptographic equipment. During the interrogations by the North Koreans of the PUEBLO crew, however, it became apparent that the special teams brought in to conduct cryptographic interrogations were highly competent in the field of electronics. They were also critically interested in the technological aspects of the cryptographic equipments aboard the USS PUEBLO. While it is possible these special teams were, in fact, representing the interests of the USSR, it must be acknowledged that the interest and competence being displayed may have been North Korea's and thus machine cryptography may soon begin to appear on the scene in North Korea. While it is presumed that at this time they do not now have the manufacturing base to commence immediate manufacture of precision parts required for an equipment such as the KW-7, with their understanding of the general electronic principles of the KW-7, it is assumed that an equipment of less sophisticated engineering design but incorporating some of its cryptographic features could be constructed by the North Koreans. It is concluded, therefore, that within a matter of years, the electronic data and hardware acquired through the capture of the PUEBLO will result in increased sophistication of North Korean cryptography.

H. INVENTORY OF CRYPTOGRAPHIC EQUIPMENT AND RELATED MANUALS AND PARTS

	SHORT TITLE	COPIES	CLASS	LONG TITLE/DESCRIPTION
1.	TSEC/KL-47	1	CC	Electromechanical Literal Cipher Machine (ADONIS System)
	KLK-47	2	CC	Stepping Unit for KL-47
	ENG 00347	2	U	Spare Parts Box for KL-47
	KAO-27B	1	CC	Operating Instructions for KL-47
	KAM-3A	1	CC	Repair and Maintenance Instructions for KL-47
2.	TSEC/KW-7	2	CC	Electronic Tactical Teletypewriter Security Equipment
	KWQ-8	1	CC	Spare Parts Kit for KW-7
	KW-7 ERP Kit	1	U	Emergency Repair Parts for KW-7
	KWK-7	4	U	Programming Plug for KW-7 and KG-22
	KWF-1	2	U	Slide Mount for KW-7
	KWL-4A	2	U	Loop Adaptor for KW-7
	KWX-8	1	U	Function Remote Unit for KW-7
	KWX-10	2	U	Permuter Adaptor Unit for KW-7
	ONO 8757	2	U	Stop Switch - Plain - KW-7
	KAO-83D	1	CC	Operating Instructions for KW-7

	SHORT TITLE	COPIES	CLASS	LONG TITLE/DESCRIPTION
	KAM-143B	1	CC	Repair and Maintenance Instructions for KW-7, Vol I
	KAM-144B	1	CC	Repair and Maintenance Instructions for KW-7, Vol II
	KAM-145A	1	CC	Repair and Maintenance Instructions for KW-7, Vol III
3.	TSEC/KWR-37	3	CC	Electronic Broadcast Teletype-writer Security Equipment
	KWB-6	3	U	Frame Assembly for KWR-37
	KOI-1A/TSEC	3	U	Card Reader for KW-37
	KWQ-4	1	CC	Emergency Repair Parts for KWR-37
	KOI-1A Mod Kit	3	CCNF	CRIB Mod Kit for KWR-37 Card Readers
	KAO-34B	1	CC	Operating Instructions for KW-37
	KAO-34C	1	CC	Operating Instructions for KW-37
	KAM-78A	1	CC	Repair and Maintenance Instructions for KWR-37, Vol I
	KAM-79A	1	CC	Repair and Maintenance Instructions for KWR-37, Vol II
4.	TSEC/KG-14	4	CC	Accessory Key Generator
	KOI-4A	4	U	Card Reader for KG-14
	KG-14 Spares	2	CC	Spare Parts Kit for KG-14
	KG-14 Mod Kit	4	U	Mod Kit for KG-14

	SHORT TITLE	COPIES	CLASS	LONG TITLE/DESCRIPTION
	KAM-179A	1	CC	Repair and Maintenance Instructions for KG-14, Vol I
5.	TSEC/HL-1	1	U	Tape Reader Attachment for KL-47
	ENG 00337	1	U	Repair Kit for HL-1
	CE 094050	6	U	Card Reader Repair Kit
	CSP 1750A	1	U	Radio Call Sign Cipher Device - MK2
	KLI-12	1	U	Authentication Grille with Table Holder