~~TOP SECRET UMBRA~~

28 July 1969

Report on the Assessment of Cryptographic
Damage Resulting from the Loss of the USS PUEBLO (AGER-2) (U)

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

2. The critical communications security materials carried by the USS PUEBLO on her mission 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 commensurate with the mission. The materials included (after off-loadings made preliminary to sailing) one KL-47, two KW-7s, three KWR-37s (receivers), four KG-14s, repair kits, seven maintenance manuals, three operating instructions, single-page key lists for January, February, and March 1968 for five communications networks (15 in all for the KW-7 and KL-7), six books of key cards (34 to a book) for January, February, and March 1968 for the Navy operational intelligence broadcast, tactical and authentication codes, and eleven classified general instructional documents. In addition, it was determined that the destruction effort for the equipment, keying material, and general instructional publications was ineffective and that most of the material was compromised. The USS PUEBLO had retained aboard four KG-14s (key generators) even though there was no operational requirement nor were keying materials available for use. There also was superseded keying material for November and December which will be mentioned later in this report.

3. The cryptographic damage incurred by the capture of the USS PUEBLO can be attributed in part to the extensive amount of superseded and excess crypto-material aboard. The absence of the material might have made the destruction effort more effective. In particular, the possibility of compromise of U.S. traffic would have been negligible. It is also recognized that selected qualified cryptographic technicians

Inclosure

Approved for Release by NSA on 05-28-2013, FOIA Case # 63391

of the USS PUEBLO were extensively interrogated by special and apparently highly competent North Korean experts on cryptographic principles, operating procedures, and the relationship of keying materials. The materials were neither displayed to the crew nor used for propaganda purposes. This is not the case for a variety of other highly significant intelligence materials. It appears that the North Koreans thoroughly understood the significance and importance of these materials and the concealment of the details of the acquisition from the United States.

4. Ineffective maintenance manual and equipment destruction resulted in the compromise of the cryptographic principles embodied in the KL-47, KW-7, KWR-37, and KG-14. This would lead to a clear understanding of the principles of electrical encryption used by the United States. The absolute threat to future U.S. communications in these systems resulting from the loss of the equipment is zero. However, it is estimated that the assistance provided by USS PUEBLO crewmen saved the North Koreans three to six months of technical diagnostic analysis. During debrief, it was determined that superseded keying material for November and December 1967 was aboard the ship. Therefore, November and December 1967 traffic encrypted by any holder of the keying material must be considered compromised. No action was taken at the time of capture to review traffic for November and December 1967 since the presumption in January 1968 was that all material had been destroyed as required by Naval Directives. By the time of the crew release and discovery of the existence of superseded keying materials much of the broadcast material had been destroyed and hence no damage evaluation could be made.

5. It is not believed that the North Koreans have sufficient capability to accomplish an attack against this old traffic. The USSR does have the capability assuming they acquired the keying materials and had recorded the traffic in a time-accurate format. January 1968 keying material must also be considered compromised, and traffic passed in them from 1-24 January was also compromised. This compromise is largely academic, however, since the decrypted messages apparently were captured intact. Holders were directed to cease use on 24 January of the systems compromised as well as to minimize use of tactical codes and authentication systems until replacement could be achieved. All reserve keying material was replaced by 1 March 1968.

~~TOP SECRET UMBRA~~

6. There were also general publications captured on board the USS PUEBLO. Cumulatively, they provide a detailed description of the United States physical security structure for protection of cryptographic materials, and the U.S. Navy cryptographic order of battle. While this loss caused no direct damage, it can be assumed that the information would provide targeting aid in attempts to penetrate the U.S. cryptographic establishment.

7. The over-all threat to U.S. communications resulting from the loss of the cryptographic equipment aboard the USS PUEBLO is minimal. The fact that the loss provides a clear understanding of United States communications techniques and principles does not, in itself, aid in the exploitation of the communications. All U.S. machines have been specifically designed to withstand attacks using such information. The detailed knowledge of U.S. cryptographic practices would, however, greatly facilitate exploitation of key acquired from clandestine procurement if the circuit could be identified and the enciphered traffic made available in the correct time-accurate format. Adaptation and use of U.S. COMSEC techniques and principles by other countries would cause serious problems in the U.S. exploitation of their communications for intelligence purposes. In the long run then the major potential loss appears to be in the areas of intelligence loss rather than any weakening of U.S. cryptography or danger of successful attack on it as a result of the PUEBLO losses.

sgd/ Louis W. Tordella

LOUIS W. TORDELLA
Deputy Director
National Security Agency