DOCID: 4092108

~~SECRET~~

~~SECRET - NOFORN - LIMITED DISTRIBUTION~~

TALKING PAPER

SUBJECT: National Security Agency Assessment of Communications Security Loss in the USS PUEBLO Incident

1. In accordance with the National Security Council Directive 5711, 25 April 1957, I am concerned with the production of cryptographic materials for use in the Federal Government. In the case of the PUEBLO, cryptographic materials aboard the ship were manufactured by the National Security Agency. Once manufactured, the cryptographic materials are turned over to the individual service for operational deployment and use in accordance with nationally developed regulations and service instructions. Long-standing regulations and instructions provide for stringent protection and use of cryptographic materials.

2. The Navy, realizing the sensitive nature of the operations in shallow waters contemplated in the case of the PUEBLO, issued instructions to that ship on 4 January, well before sailing, to temporarily remove all cryptographic materials excess to operational requirements prior to departure from Yokosuka, Japan. The USS PUEBLO complied with these instructions.

3. In general, the cryptographic materials held on board were special purpose machine and manual systems rather than general service cryptographic materials. Consequently, this loss did not affect general Pacific Fleet encrypted communications, or communications of the Army, Air Force, or the Defense Communications System.

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

~~SECRET~~

Approved for release by NSA on 01-13-2014, Transparency Case# 63391

4. Cryptographic materials of major significance carried aboard the USS PUEBLO in terms of machine systems were the TSEC/KL-47, TSEC/KW-7, and the TSEC/KWR-37 with associated TSEC/KG-14. These equipments were designed under a concept which contemplated their possible loss in operations. For example, the TSEC/KW-7 is used in South Vietnam today under this tactical deployment concept. The TSEC/KL-47 principle is widely distributed to NATO nations and others, as is the TSEC/KWR-37. So long as the cryptographic keys are not generally compromised and may be replaced, message traffic in these machine systems will remain secure.

5. Cryptographic materials of lesser significance carried aboard the USS PUEBLO also included two low-level operational codes, and an authentication system. They are specifically designed for tactical deployment, and while in wide use, their loss will have no more than transitory effect.

6. Cryptographic instructions require the establishment of emergency destruction procedures. According to information from the USS PUEBLO at the time of the incident, emergency destruction was initiated at least one hour prior to final communications contact. The emergency destruction procedure requires that cryptographic keying material be destroyed as a first priority. Destruction of the keying materials would require approximately fifteen minutes. Destroying the equipment is the next order of priority and would take a longer period of time. It appears possible that most of the keying material, consisting of approximately three months supply, was destroyed and no traffic in the systems was compromised. As

a precautionary measure, however, new keying material was brought into effect and traffic previously enciphered in these systems ordered held for review. Due to the widespread usage of the low-level codes, immediate replacement was not possible. However, all holders were directed to minimize use pending replacement. Detailed information is not available to positively state that all cryptographic materials were destroyed prior to capture, and will not be available until interrogation of the crew is possible. Nonetheless, all measures dictated by previous experience have been taken to minimize effect of the loss.

7. In my judgment, based on "worst case circumstance" as is normally part of the evaluative procedures surrounding cryptographic compromises, the probable compromise of the logic of these modern electronic cryptographic equipments is a major intelligence coup without parallel in modern history.

If the technology and doctrine made available through this probable compromise were applied to Soviet Bloc communications, there is little doubt that we would suffer a dramatic loss of intelligence. In other words, while we have most likely been successful in minimizing losses in terms of specific messages, the technology and doctrine loss may well have major long-term effect.

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