

1 February 1968

*Technical*  
SUBJECT: Possible Damage Resulting from Compromise of Equipment  
or Personnel of the PUEBLO

*Support obtained and collection equipment on*  
The "Bill of Destruction" covering the equipment of the PUEBLO

provided for destruction of key cards and key lists, then of the equip-  
ment, then codes and authentication materials, and finally maintenance  
and operating manuals. While it is theoretically possible to have elec-  
tronic automatic detonation gear, the PUEBLO was not so equipped.  
The hazards of automatic detonation equipment on board a ship are  
weighed against other methods of destruction and the possible damage  
from compromise and are generally considered unacceptable.

For the past 30 years it has been the general U.S. practice  
that, where possible, security of U.S. communications will not depend  
solely on physical protection of the equipment used to encipher and de-  
cipher the messages. During the past 20 years no equipment has been  
produced without variable elements which depend upon keying elements,  
usually key lists or key cards, for their primary security. In particular,  
all the communication security equipments which the PUEBLO carried  
depended upon either key lists or key cards. Loss of a particular equip-  
ment with the keying element would not jeopardize any other traffic en-  
ciphered by similar equipments using different keying elements. As soon  
as notification of the capture of the PUEBLO was received in Washington,  
steps were taken to supersede all keying elements which she carried and  
new ones were prescribed.

The key list enables the user to establish a unique machine set up for a crypto period which is not longer than 24 hours. The key card is a card punched with a specified pattern and is inserted into the machine by means of a card holder. The key card and holder permit feeler pins to make contact through randomly positioned holes and effectively rewire the cipher machines, again not less often than each 24 hours. The number of combinations resulting from a card system is astronomical and a message which is transmitted through a machine using a particular keying element can only be read at the other end by a machine with an identical keying element.

National Security Agency activities are centered about two major purposes: One is to maintain the security of the United States communications, and second is to take advantage of the communications of target nations. It is the National Security Agency's judgment that no degradation to the security of U.S. communications can result from this compromise even if the equipment and the key lists were captured intact, since steps were taken immediately to supersede all of the keying materials. In the worst possible case, the few messages to and from the PUEBLO could be read if all materials and equipment were captured intact.

DOGID: 3997629

Message traffic from the PUEBLO, as well as from the North

Koreans, indicated a destruction effort on board the vessel by fire as well as jettisoning. From her communications, it may be inferred that the bulk of her key material, perhaps all, and as much equipment as possible was destroyed, but that several publications were probably compromised.

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

[REDACTED] This equipment was generally unclassified (we are still checking 2 pieces) but the use to which the equipment could be put and the results derived therefrom are classified. It is very possible that if the equipment was undamaged a reasonably precise reconstruction of the PUEBLO's intelligence mission could be accomplished.

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

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

DOGID: 3997629

general Soviet communications practices and a [redacted]

[redacted] This information, if compromised, would stimulate either of the two nations to change their communications practices, supersede their call sign systems and/or modify their operational codes.

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

[redacted]

[redacted] The capture of the modern U.S. communications security equipments or the maintenance and operations manuals could stimulate one or other of these countries (or possibly Communist China) to make major changes in their communications security equipment and practices. This could very seriously hamper the extensive U.S. signals intelligence production on these nations.

There were 30 (29 enlisted and 1 officer) Navy security personnel on board the ship. Most of these men and officers were highly skilled and represented several years of experience in the business. Some of them had intimate knowledge of a number of sensitive Navy

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

collection and analytic efforts and a few of them had some knowledge of one or two sensitive National Security Agency projects. Depending on the duress to which they may be subjected and the amount they may recall, serious compromise of several highly classified projects could ensue from their involuntary revelation of the scope of the U.S. signals intelligence effort. This could result in defensive measures by the Soviets to deny the U.S. further information.

However, no damage to our own communications security would follow even from the forceful extraction of information from captured personnel.