THE SECRETARY OF DEFENSE
WASHINGTON, D. C. 20301

FILE

#20C

9 MAR 1978

MEMORANDUM FOR THE PRESIDENT

SUBJECT: Questions Brought up at the Presidential Visit to the National Military Command Center

At the session in the National Military Command Center in January, you requested more information regarding U.S. missile warning systems, communications to the National Emergency Airborne Command Post and communications checks with the Presidential Party.

The attached is a response to that request.

Harold Brown

Attachment

VULNERABILITY OF DSP SATELLITES TO LASERS

Questions:

- Can the Soviets blind ours with lasers? If not, what is their projected capability for doing so?
- How can we protect ours against Soviet laser blinding (or whatever other action they may be capable of taking)?
- Suppose the Soviets do blind one/some of our DSP satellites, what can we do, on short notice, to protect ours (quick fix)?
- What are we doing to develop a capability to blind Soviet warning satellites? (Include discussion of their current ICBM warning capability, both present and projected.)

Background: The Defense Support Program (DSP) consists of three satellites stationed at geosynchronous altitude (19,323 nm) each equipped with an Infrared (IR) sensor for detecting and tracking missiles in powered flight. One satellite in the Eastern Hemisphere, with a dedicated ground station in Australia, provides coverage of Soviet and Chinese ballistic missile complexes. Two satellites, with a dedicated ground station in CONUS, provide coverage of SLBM launch areas. [redacted]

NRO 25X1

Vulnerability to Lasers: The Soviet Union is not believed to possess lasers sufficiently powerful and accurate to physically damage the DSP satellite structure or permanently blind the IR sensors on the DSP satellites. [redacted]

NRO 25X1

NRO 25X1

NRO 25X1

NRO 25X1

Soviet exploitation of the vulnerability of the DSP system to laser jamming would also require a surveillance system capable of detecting and tracking satellites at geosynchronous altitudes. The existing Soviet space surveillance system consists principally of ground-based radars and optical trackers. It is not known whether the radars are capable of detecting and tracking satellites at geosynchronous altitudes. The optical systems, however, are believed to have the capability to search for, detect, and track the large, stationary DSP satellites. This capability is limited to cloud free, nighttime conditions when the satellite is illuminated by the sun. NRO 25X1 [redacted] The DSP satellites are launched into geosynchronous orbit with a Titan IIIC boost vehicle from Cape Kennedy, which has only one active launch pad. Presently, four spare Titan IIIC boost vehicles are available. With current procedures, however, a minimum of 45 days is required to put a replacement satellite into orbit. This assumes that there is no other satellite and booster on the launch pad. If the launch pad were occupied, it is estimated that it could take up to 61 days to put a replacement DSP satellite into orbit.

Soviet Missile Surveillance Capability: The Soviet missile surveillance system is believed to consist of ground based radars and IR satellites. The radars include 8 conventional phased-array radars (6 VHF Henhouse, 1 UHF Dog House and 1 UHF Checkhov (also called Cat House)) and 2 over-the-horizon (OTH) radars.

The Soviets are believed to have launched 4 IR surveillance satellites into inclined, elliptical 12 hour orbits with the last satellite launched into orbit in June 1977. Only two are currently operational. As a result. coverage is restricted to about 13 hours per day on the U.S. ICBM fields and the North Atlantic SLBM operating areas. The 4 satellite system would have provided continuous coverage.

NRO 25X1 NRO 25X1

[redacted] 06 59[illegible]/78

25X1

Approved For Release 2005/02/18 : NLC-8-4-7-18-3

PAVE PAWS SLBM WARNING SYSTEM

Question: Please provide a report on the status of our phased array radars for SLBM warning. Discuss current capabilities and weaknesses, the role to be played by the phased array radars already programmed, and projected IOC's for the latter.

Background: The PAVE PAWS system consists of two modern phased array radars for SLBM warning, one on the East Coast at Otis Air Force Base, Massachusetts, and one on the West Coast at Beale Air Force Base, California. The expected operational dates are April 1979 for the East Coast site and April 1980 for the West Coast site. The currently operational FPS-85 SPACETRACK radar at Eglin Air Force Base has been modified to also detect SLBM launches and will be integrated into the PAVE PAWS system.

Present Status: The PAVE PAWS program is on schedule. Full system capability is expected to be achieved by April 1980. 25X4

[redacted]

Contribution of PAVE PAWS: The PAVE PAWS radars will provide significant improvements over the 474N radars in terms of coverage, reliability and attack assessment. The radars cannot be overflown by either the SSN-6 or

SECRET

the SSN-8. The expected system availability is about 95 percent. They are designed to handle SLBM raid densities of up to 100 missiles per minute and predict their impact points with an accuracy of 25 nm. When they are operational, radar coverage of most potential SLBM launch areas will be provided. The 474N radars would then be phased out. A four site PAVE PAWS phased array radar system is also under consideration. This would provide essentially complete coverage of SLBM launches against CONUS.

Summary: The two PAVE PAWS phased array radars will be operational in April 1979 and April 1980. They will provide a significant improvement over the present 474N system in terms of reliability, coverage, capacity and attack assessment. With the DSP system, dual radar/IR coverage of most potential SLBM launch areas will be provided.

06 593 /73

SECRET

SECRET

#20F

MISSILE WARNING SYSTEMS FALSE ALARMS

Question: How many false alarms have we experienced within the NMCS since the inception of our early warning capabilities.

Background: Threat reports from the missile warning systems are automatically processed and displayed in the command centers of the National Military Command System (NMCS). Alarms for each system are generated at North American Air Defense (NORAD) Headquarters. CINCNORAD assigns a confidence of "No", "Medium", or "Hi" to an alarm. There are three alarm levels which are defined as follows:

Alarm Level Three: This is the lowest state of alarm and is generated when the number of threat reports has reached a level that would rarely be reached unless a missile attack were in progress. The average false alarm rate is calculated to be less than one per year.
Alarm Level Two: This represents a greater likelihood that a missile attack is in progress. The false alarm rate is calculated to be less than one per 10 years.
Alarm Level One: This is the highest state of alarm and is almost certainly caused by a missile attack. The false alarm rate is calculated to be less than one per 25 years.

Operational Experience: The false alarm history of the five operational missile warning systems is as follows:

a. Defense Support Program - IOC 1971

Date	Cause	Alarm Level
28 August 1976	US Polaris Launch	3
13 December 1976	Computer Hardware	1

The CINCNORAD assessed confidence was "No" in both cases. The system deficiencies which caused these false alarms have been corrected by hardware and software changes at the DSP ground stations.

b. Ballistic Missile Early Warning System (BMEWS) - IOC 1960

Date	Cause	Alarm Level
5 October 1960	Moon	3
3 November 1964	Computer Software	3
30 March 1966	Multiple Satellites	3
18 March 1975	Personnel Error	1

The CINCNORAD assessed confidence was "No" in all cases. The system deficiencies which caused these false alarms have been corrected by hardware and software changes at the BMEWS radar sites.

25X1 [redacted]65922/78

SECRET

c. <u>Coastal SLBM Radars (474N) - IOC 1970</u>

The 474N system has generated no false alarms over the past five years. It is scheduled to be replaced by the PAVE PAWS system in 1980.

d. <u>FPS-85 SLBM Radar at Eglin AFB, Florida - IOC 1975</u>

Since the FPS-85 radar has been converted to detect SLBM launches in 1975, no false alarms have been generated by this system.

e. <u>Perimeter Acquisition Radar Characterization System (PARCS) - IOC 1977</u>

The PARCS has generated no false alarms.

<u>Summary</u>: Since the activation of the first missile warning system (BMEWS) in 1960, seven false alarms have been experienced within the NMCS. There have been no false alarms since December 1976.

SECRET

#20G

IMPROVED SECURE COMMUNICATIONS WITH THE NEACP

Question: What are the plans for overcoming the narrow band to wide band secure voice conferencing problem with the NEACP? (In a recent exercise, it was impossible to bring the NEACP into a conference with the CINCs).

Background: During the 28 January 1978 exercise, the President (at the NMCC) was unable to get a secure voice link with NEACP. The cause was failure of the HY-2 narrow band secure voice equipment. The HY-2 has not been noted as having an unusual non-availability record. It just broke down at the wrong time.

Present Status: At present, the NMCC has a secure, wide band (KY-3) link with the NEACP alert facility. However, when the NEACP is airborne, a narrow band link (HY-2) is employed.

Future Status: Actions are underway to assure direct, wide band secure voice between the NEACP and the ground-based AUTOSEVOCOM Network.

a. KY-3 wide band secure voice equipment will be installed on all three E-4A NEACP aircraft. (This has no serious space, weight, power, etc., repercussions.) Aircraft modification cost is about $200,000. Installation is scheduled to begin not later than 1 June 1978 and will require approximately three weeks including Operational Test and Evaluation. However, an FOC of 9 June 1978 may be possible with an expedited implementation.

b. To supplement the present ground entry points at Hillsboro, Missouri, and Offutt AFB, Nebraska, ground entry points at the Alternate National Military Command Center near Fort Ritchie, Maryland and at Norfolk, Virginia will be configured by May 1978 to provide AUTOSEVOCOM access from and to the NEACP. This improved capability requires leasing of several 50 kbps telephone lines plus a radio modification at Norfolk.

c. Therefore, by late June 1978, all E-4A aircraft will have both narrow band (KY-2) and wide band (KY-3) secure voice capability. The E-4B aircraft will also have both narrow band and wide band secure voice capability.

d. The wide band secure voice links will provide voice-recognition-quality secure communications, and are a major improvement over narrow band secure voice.

Summary: The narrow band/wide band secure voice conferencing problem will be solved by late June 1978. The solution will be the installation of wide band secure voice equipment aboard NEACP.

25X1 NRO

06592[illegible]/78

SECRET

Approved For Release 2005/02/18 : NLC-8-4-7-18-3

SECRET

COMMUNICATIONS CHECKS WITH THE PRESIDENTIAL PARTY AWAY FROM WASHINGTON

Question: What procedures have been established for the Secretary of Defense to conduct communications checks in the clear with the Presidential Party away from Washington? Some checks should be made with the President himself.

Checks with the Presidential Party: Communications checks with the Presidential Party can be accomplished through the White House Communications Agency (WHCA) Trip Officer. Within 24 hours of the arrival of the President at a trip location, the WHCA Trip Officer offers the National Military Command Center (NMCC) the opportunity to initiate a communications check to the WHCA Trip Officer.

Checks with the President: NMCC-WHCA procedures can accommodate direct calls from the Secretary of Defense to the President. Since the Secretary of Defense is on the direct access list to the President, prior clearance is unnecessary. In order to avoid interference with the Presidential schedule, however, it is recommended that communications tests with the President be cleared in advance with the duty military aide who can determine the availability of the President.

Summary: NMCC-WHCA procedures have been established for the Secretary of Defense to conduct communications checks with the Presidential party or the President through the White House Communications Agency.

06500[illegible]/78

SECRET