

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

~~TOP SECRET~~

A53-

# NSA TECHNICAL JOURNAL

VOL. XII

FALL 1967

NO. 4

[Redacted line]

Military Oceanography ..... J. A. MEYER 17

Portion identified as non-responsive to the appeal

[Redacted content]

Portion identified as non-responsive to the appeal

### WARNING

This Document Contains CODEWORD Material

~~TOP SECRET~~

DECLASSIFIED UNDER AUTHORITY OF THE INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL, E.O. 13526, SECTION 5.3(b)(3)

ISCAP APPEAL NO. 2008-032, document no. 5  
DECLASSIFICATION DATE: October 14, 2015

# SIGINT Implications of Military Oceanography

BY J. A. MEYER

~~Top Secret Trine~~

Expansion of oceanographic programs by many nations raises many new problems in COMINT and COMSEC.

25X3, E.O.13526

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

An appendix reviews

the contribution of [redacted] to the wartime enigma problem.

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

INTRODUCTION 25X3 and 6, E.O.13526

Cipher machines can be recovered from ships and aircraft sunk in the ocean depths by deep submergence vehicles and apparatus of the kind used in the H-Bomb search off Palomares. Although deep ocean search and recovery capability is only marginally operational at present, the technology is being developed rapidly, [redacted]

[1].

The facts of World War II cryptanalysis show that captures [redacted] were absolutely essential to give a start on many systems [2]. Even the German Enigma problem had a long history [redacted] sometimes overshadowed in reminiscence by the notable cryptanalytic work, but [redacted] in summarizing the problem, remarks:

[redacted]

Although some of the [redacted] captures from trawlers and submarines were accidental, [redacted] points out that:

[redacted]

Deep submergence vehicles are not exclusive to the U. S. The diving record of 36,000 feet is held by the French submersible *Archimede*, and U. S. vehicles such as *Trieste I* are capable of working at 30,000 feet. Seven U. S. vehicles currently or soon to be operational can work at depths of 6000 feet or more, and the H-Bomb recovery from 2850 feet of water off Palomares has demonstrated search and recovery opera-

25X3 and 6, E.O.13526

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

tions in embryonic form. The deep submergence capability of Russia and China is not fully known.

25X3, E.O.13526

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

A few of the major SIGINT and COMSEC topics will be described in this paper.

*Deep Submergence and Recovery.*

25X3, E.O.13526

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

25X3, E.O.13526

Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)

25X3, E.O.13526

Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)

25X3, E.O.13526

Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)

The practical and legal problems of operating in or near territorial waters of unfriendly nations have been brought into prominence by the Palomares incident [5].

25X3, E.O.13526

Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)

25X3, E.O.13526

Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)

*Warning Systems.*

Anti-submarine warfare warning systems, to be effective, must report probable target detections by electrical or electromagnetic means, and this implies signals and communications. A problem of deep concern is that any nation which discovers a new physical method of propagating energy through the sea may be able to make the oceans transparent to detection systems, and thus change the strategic balance of weapons systems.

25X3, E.O.13526

Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)



25X3, E.O.13526

Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)

25X3, E.O.13526

Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)

25X3, E.O.13526

Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)

25X3, E.O.13526

Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)

*Recommendations.*

25X3, E.O.13526

Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)

25X3, E.O.13526

Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)

25X3, E.O.13526



Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)

16. A symposium on SIGINT implications of military oceanography should be organized and held at NSA to review and forecast the whole spectrum of problems and developments.

25X3 and 6, E.O.13526

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

APPENDIX

Summary of Enigma [redacted]

On the German Enigma problem, rare and unique events— [redacted] led to the solution of the system, and the changes. Sustaining events— [redacted] formed the kernel of the exploitation. [redacted]

Polish cryptanalysts used [redacted] the keys in 1937 to recover the wheels (p. 124). The [redacted] in April 1940, was an enemy trawler which yielded stecker and grundstellung. [redacted]

In Feb. 1941 the [redacted] captured keys for the complete month of Feb. 1941 (p. 135). Then keys for June and July 1941 were captured; though slow progress was being made by Banburismus (p. 139), the keys gave information not available from cryptanalytic recovery.

[redacted] On 30 October 1942, the *Wetterkurzsignalheft*, complete with indicator tables, was captured in the Mediterranean from U-559 [redacted] making the weather signals suddenly readable (p. 159). At the same time the *Kurzsignalheft 41* and *Kenngruppenheft* were captured—without which B-Bar U-boat signals would have been unreadable (p. 163).

The wiring of new wheels introduced in July 1943 had previously been captured in North Africa [redacted] so the wirings were broken the hard way.

[redacted] The introduction of a new basket of wheels for the U-boats would have stopped the reading of the traffic for some time. Even with [redacted] a known machine, it took about 4 years under wartime pressures (1937-1941) to get the problem opened up.

25X3 and 6, E.O.13526

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

## REFERENCES

25X3 and 6, E.O.13526

- [1]. PSAC, *Effective Use of the Sea*, G. P. O., 1966.
- [2]. [REDACTED]
- [3]. [REDACTED]
- [4]. National Council on Marine Resources and Engineering Development, *Marine Science Affairs—A Year of Transition*, G. P. O., 1967.
- [5]. CNO Technical Advisory Group, *Aircraft Salvage Operation Mediterranean*, Dept. of the Navy, 1967.
- [6]. Oceanographer of the Navy, *4th U. S. Navy Symposium on Military Oceanography*, May 10-12, 1967, Washington, D. C.
- [7]. V. M. Albers, *Underwater Acoustic Handbook*, Pennsylvania State University Press, 1960.
- [8]. D. G. Tucker and B. K. Gazey, *Applied Underwater Acoustics*, Pergamon Press, 1966.
- [9]. H. A. Wheeler, "Radio Wave Propagation in the Earth's Crust," *Journal of Research*, National Bureau of Standards, March 1961, pp. 189-191.
- [10]. Data Staff Analysis, "Man Committed to Exploration of the Oceans," *Data*, March 1967, pp. 13-18.
- [11]. Encyclopaedia Britannica, Vol. 7, pp. 694, 1964 edition.
- [12]. Larry L. Booda, ASW Research, *Undersea Technology*, November 1966, pp. 43-50.
- [13]. Navy IOIS integrated airborne search project.

Withheld from public release under  
§6 of the National Security Act of 1959,  
50 U.S.C. 3605 (P.L. 86-36)