~~TOP SECRET~~

APPENDED DOCUMENTS CONTAIN CODEWORD MATERIAL

USCIB: 23/18

~~U.S. EYES ONLY~~

13 July 1951

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Portuguese Communication Security.

The attached report, prepared in accordance with USCIB decision at the 65th Meeting, 22 June 1951, is forwarded for consideration.

H. D. JONES
J. W. Pearson
Secretariat, USCIB

Inclosure 1 Report by the Coordinator to USCIB, dated 13 July 1951.

USCIB: 23/18

~~APPENDED DOCUMENTS CONTAIN CODEWORD MATERIAL~~

~~U.S. EYES ONLY~~

~~TOP SECRET~~

~~TOP SECRET SUEDE - U.S. EYES ONLY~~

REPORT OF THE USCIB COORDINATOR
TO THE
UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD
ON
PORTUGUESE COMMUNICATION SECURITY

THE PROBLEM

1. To study and evaluate Portuguese communications security and its bearing on the security of North Atlantic Treaty Organization (NATO) and U.S. classified information.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. See Enclosure.

CONCLUSIONS

EO 3.3(h)(2)
PL 86-36/50 USC 3605

3. It is concluded that:

Enclosure with USCIB 29.18/8 dated 13 July 1951

d. The Portuguese authorities responsible for the production and use of its cryptosystems show great ignorance and naivete in the whole field of cryptology. In fact, they appear to be not only wholly unaware that their communications are open to rather easy reading by cryptanalytic processes, but also there is reason to believe that certain high officials are completely unaware of the existence of such a science as cryptanalysis.

[redacted]

f. Portuguese communications insecurity may soon become a matter of serious concern as NATO develops and the Portuguese become more involved in NATO affairs, because of (1) their failure to take adequate COMSEC precautions to safeguard NATO information in their national communications, (2) their insecure practices in connection with the use of the TYPEX machines furnished them by the U.K., thus jeopardizing not only their own TYPEX NATO communications but also the TYPEX communications of other NATO members, and (3) their suspicions with regard to British issuance of TYPEX and keys thereto, which suspicions lead them to transmit certain NATO information in their own insecure national system.

g. The Portuguese people and the Portuguese Government so lack an understanding of the need for physical and personnel security measures necessary for safeguarding classified information that even if technically

sound COMSEC materials were provided them, there would be no assurance that the U.S.S.R. could not obtain those materials by clandestine means, thus obviating their need for cryptanalysis of Portuguese communications.

h. In the absence of exact knowledge of the practices which now apply (1) to the use by NATO holders of TYPEX and its associated crypto-materials and (2) to the various types or categories of NATO or national classified information which may be encrypted by TYPEX, there is no assurance that all available and authorized ways and means have been applied toward a solution of this problem.

i. In view of h above neither (1) the extent of the present danger to classified information of NATO and the U.S. which is inherent in the insecurity of Portuguese communications nor (2) the general insecurity of the Portuguese Government would justify exceptional, direct action toward improvement of Portuguese communications security at this time.

RECOMMENDATIONS

4. It is recommended that:

a. The conclusions of this study be approved as the present USCIB view with regard to the problem.

b. The U.S. Delegation to the U.S.-U.K. Conference on French communications security be continued as an ad hoc body to ascertain the exact extent to which present NATO practices may provide secure ways and means, within the framework of these practices, to solve the Portuguese problem.

c. Further consideration of exceptional, direct action to improve Portuguese communications security be deferred pending (1) completion of the study recommended under b above and (2) NSC and USCIB decisions whether such action is to be taken vis-a-vis the French Government.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

GENERAL STATEMENT

1. Intelligence may be derived from crypto-communications by any or all of the following methods:

a. By obtaining physical possession of the exact texts or the substance of the communications (hereafter called Method 1);

b. By obtaining physical possession of the crypto-material (key-lists, code books, etc.) necessary for direct reading of the intercepted traffic (hereafter called Method 2);

c. By interception and cryptanalysis of the communications (hereafter called Method 3).

PL 86-36/50 USC 3605
EO 3.3(h)(2)

2. With respect to intelligence derivable from present Portuguese communications, the U.S.S.R. is in a position to employ all three methods, [redacted] Denial of Methods 1 and 2 to the U.S.S.R. will depend ultimately upon physical security as well as the reliability and discretion of those who are responsible for handling and safeguarding classified information in the Portuguese Government, and especially in the Cryptographic Service of the Portuguese Ministry of Foreign Affairs (M.F.A.).

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

4. The cryptosystems used by Portuguese military and naval attaches employ the Hagelin C-38 cipher machine. Since this machine and its usage by other agencies of the Portuguese Government will be treated below, no further remarks on this phase of the problem will be made in this section.

5. It is true that Portugal has furnished a contingent of troops to the U.N. for service in Korea but no information is available at this time regarding the communications of these Portuguese forces in Korea, what cryptosystems they are using, if any, and how they are being used.

PORTUGUESE DIPLOMATIC COMMUNICATIONS

6. There is unquestionable technical evidence that the cryptographic systems and practices recently and currently employed by the Portuguese Government in its diplomatic and colonial communications are such that practically all of those communications, if intercepted, could be read by any properly staffed and equipped communications intelligence (COMINT) organization.

7. The naivete of the Portuguese with regard to communications security is quite evident from their laxity in regard to the physical protection of crypto-materials; their ignorance of cryptologic techniques is established by very faulty cryptographic practices in connection with use of their own national ciphers as well as of the TYPEX machines furnished them by the British for NATO communications.

8. a. Some almost incredible breaches of security in the use or handling of Portuguese crypto-materials have been reported by Portuguese diplomats themselves and although these incidents were attended to by the Foreign Ministry in due time, these cases indicate only too clearly that Portuguese diplomatic personnel are not well indoctrinated in the handling of classified material.

b. The instructions in the prefaces of available Portuguese code books contain no general precepts on the subject of security. Although some of their cryptographic systems are fundamentally and potentially good, these are made vulnerable either through misuse or through compromise. Almost every type of violation in the gamut of COMSEC insecurity practices is to be found in Portuguese crypto-communications,

d. Their attitude toward the TYPEX machine and system is fostered by an unwarranted faith in the inviolability of their own national systems and involves a clearly stated suspicion that all Portuguese messages enciphered by TYPEX will be available to the British.

e. The foregoing statements are supported by evidence given below.

PORTUGUESE ATTITUDE TOWARDS SECURITY OF CRYPTO-MATERIALS

9. Some almost incredible breaches of security have been reported in recent years by Portuguese diplomats in important European posts. The Ambassador in London, in January 1950, discovered a discrepancy between inventories of 1943 and 1946, and found no record of the disposition of missing cipher material. Two years elapsed before the Portuguese Minister in Bern informed Lisbon that cipher material was missing as a result of robbery. Worst of all was the case of the Portuguese Minister to Copenhagen, who left his codes with the Brazilian Ambassador during a trip to Lisbon.

10. It is true that these incidents received official attention: the Minister at Bern was promptly relieved; the Copenhagen codes were quickly retrieved; and the Ambassador in London proposed suitable changes in procedure. Nevertheless, these cases indicate only too clearly that Portuguese diplomats are not well indoctrinated in the handling of classified material.

PORTUGUESE COLONIAL CRYPTOGRAPHIC SYSTEMS

PORTUGUESE USE OF TYPEX MACHINES

13. a. There are sound indications that the Portuguese are wary of using TYPEX because they fear that their traffic will be readable by the British, who furnished the TYPEX machines.

b. Such a fear is not unfounded when consideration is taken of the failure on the part of the Portuguese to avail themselves of the possibilities provided by NATO arrangements for the use of TYPEX in purely national communications, by means of keys and machine settings compiled by each nation itself, rather than by means of those provided by the British.

c. Failure to compile their own keys and machine settings leads the Portuguese [redacted] This practice, if continued, will be most detrimental to the security of NATO classified information.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

STATUS OF PORTUGUESE CRYPTOLOGY

14. There is no evidence that the Portuguese make any concerted effort to monitor their own communications for the purpose of observing or controlling COMSEC. [redacted]

15. There appears to be no tradition of COMINT in Portugal, and only one book on the subject is of Portuguese origin, written about 60 years ago. Although recent and usually reliable information indicates that there exists within the International and State Security Police, Policia Internacional e de Defesa do Estado (PIDE), a section which is concerned with communications as well as with cryptography and cryptanalysis, it certainly cannot be active, or well informed, or in a position to bring about improvement in Portuguese [redacted]

16. Except for the fact that "Listening (interception and monitoring)" is listed as a source of information for the Portuguese Army Intelligence Section (3a Reparticao), there is no information on the cryptologic activities of the Portuguese Ministries of the Army and Navy.

CONSEQUENCES OF INSECURITY OF PORTUGUESE COMMUNICATIONS

17. a. From the strictly military standpoint, there is little question that Portuguese traffic presents the greatest problem to NATO security. The

20. It is true that currently the Portuguese are not made privy to the more sensitive NATO policies, decisions, and information. However, the situation might become more serious as NATO develops, the Portuguese receive more extensive and more sensitive information, and become more involved in NATO affairs.

CONSIDERATIONS AS TO PORTUGUESE INTERNAL SECURITY

21. It is obvious that even if technically sound cryptosystems and associated procedures were employed by or furnished the Portuguese by the U.S., it is still necessary to insure that another government, and especially the U.S.S.R., could not obtain copies of the cryptomaterials employed for those systems, because such an outside government is then obviously in a position to obtain the classified information by applying Method 2 (see paragraph 1b above). Therefore, this report must consider the Portuguese situation from this point of view.

22. Appendix 1 to this enclosure deals with the status of Portuguese internal security. It indicates very clearly that the Portuguese people and the Portuguese Government so lack an understanding of the need for physical and personnel security measures necessary for safeguarding classified information that even if technically sound COMSEC materials were employed by them, or provided them by the U.S., there presently would be no assurance that the U.S.S.R. would not obtain those materials, thus obviating any need on their part to obtain Portuguese classified information by Method 3.

POSSIBLE REMEDIAL MEASURES

23. Consideration could be given to an approach to the Portuguese Government with a view toward improving the security of its communications, just as is now being considered in the case of the French Government. This however, is premature, since no decision has yet been made by the National Security Council in regard to the proposed approach to the French Government.

24. At its sixty-fifth meeting, on 22 June 1951, USCIB "explored the possibility of instituting safeguards in the form of a note to recipients of sensitive NATO information, stating that before information is released there must be assurances that it will preferably not be forwarded by any electrical communication means; but if necessary to forward, that secure courier service would be utilized." However, before making a recommendation along these lines to NATO governments it would be necessary to study the practicability of instituting such a safeguard by all the NATO members. Such a study would require considerable time by the Security Coordinating Committee of the Standing Group of the NATO Council.

25. Detailed information is lacking as to the practices which now apply (a) to the usage being made, by NATO holders, of TYPEX and its associated crypto-materials, and (b) to the various types or categories of NATO or national classified information which may be encrypted by TYPEX. There is therefore no assurance that all available and authorized ways and means for attaining COMSEC have been applied toward a solution of the problem of insecurity of Portuguese communications. Such detailed information would probably be very useful in devising remedial measures, within the framework of present authorized procedures, which might materially assist in rectifying the situation as regards the insecurity of Portuguese communications, as well as of those of certain other NATO governments.

26. In connection with the subject of possible remedial measures, attention is invited to the fact that such measures are also being currently studied by the Security Coordinating Committee of the Standing Group of NATO*. In particular, the following action is being considered by that Committee:

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

"8. It is submitted that the following action is necessary:-

(a) To ensure that when Typex Mark II machines have been issued, they are brought into use with the least possible delay.

(b) Since the Council of Deputies was set up after the allocation of Typex Mark II machines, (SGS-200-50 of 20th July, 1950), to draw the Council of Deputies' attention to the regulations regarding cryptographic channels in order to determine whether the allocation is sufficient to meet their requirements.

(c) To issue further guidance to NATO agencies, making it clear that telegraphic traffic involving not only 'Cosmic' interests but also other communications related to North Atlantic Treaty interests must be sent by the approved cypher system."

"RECOMMENDATION

"9. That action should be taken along the lines of paragraph 8 above."

27. Until the foregoing possibilities for remedial measures have been explored, a direct approach to the Portuguese Government is not indicated and would be unwise.

9 July 1951

Memorandum on Portuguese Internal and Personnel Security

1. The Portuguese Government places security emphasis on safeguarding the Regime as a political entity. In so doing, machinery for the protection of classified information in the hands of politically reliable persons is virtually ignored. The instrument used by the government to check political reliability is the International and State Security Police (Policia Internacional e de Defesa do Estado - PIDE). Besides its routine duties of border control and control of movement of foreigners in Portugal, the PIDE places informants in Government departments and into opposition groups including the Communists. The main emphasis in PIDE activity is placed on the suppression of internal subversive elements.

2. The PIDE reports that it is placing effective curbs on the Portuguese Communist Party (PCP). By action taken in late 1950, the PIDE claims to have reduced the membership of the PCP from 4,500 active members and 7,000 sympathizers in 1949 and 1950 to 2,500 active members and 5,000 sympathizers in early 1951. There is no supporting evidence to serve as a check against the PIDE claims.

3. The Communist Party of Portugal is considered illegal; therefore no measure of its strength is available. Its effectiveness in evading police action was demonstrated by the inability of the PIDE to capture the Secretary General of the PCP, Dr. Alvaro CUNHAL. CUNHAL was finally arrested in March 1949 after having been hunted by the PIDE for more than three years. A comment by a PIDE inspector, in September 1948, [redacted] perhaps explains CUNHAL's ability to elude the PIDE. The Inspector said that he was reasonably sure that there were communist agents in the ranks of the PIDE. More recent success on the part of the PIDE in neutralizing communist activities in Coimbra and in the capture of a leading Central Committee member could indicate that possible leaks from the PIDE to the PCP had been eliminated.

Appendix to Enclosure.

4. The PIDE thoroughly investigates all potential PIDE recruits. After recruitment, the new member is held on probation for one year. After the end of the probationary period, spot checks are made on the permanent members.

5. The PIDE is lax in the physical security of its premises. Entrance past a door guard is usually easily made. Before entering the interior restricted area, a visitor has to fill out a form at a guard desk indicating who he is and the nature of his business. However, once he becomes known, a visitor, even if a foreigner, can pass from the guard desk to one of several waiting rooms unattended. Papers frequently are left on desks of empty offices in the restricted area. The Portuguese seem to take it for granted that the visitor would not be present unless he had a right to be there. Identification passes are not required of employees. There is no evidence that there is any greater emphasis on security in other government departments.

6. The Portuguese Foreign Office and Portuguese Defense establishment show an attitude toward Spain that clearly reflects the concept that the destinies of Portugal and Spain are immutably linked. This concept has led, according to unconfirmed reports, to the submission of reports acquired by the Portuguese government as a member of NATO to Spanish authorities. In an August 1950 interview, Prime Minister SALAZAR stated that "Portugal's contribution to Europe's security hinged on the role to be played by Spain." In this connection, Defense Minister, Lt. Col. SANTOS COSTA, frequently confers with Spanish authorities on the question of the defense of the Iberian Peninsula.

7. The temper of the Portuguese people, a garrulous group in a country where security has been no problem, does not lend itself to restrictions followed in countries where the presence of an enemy is more acutely felt.

8. Even when the presence of an enemy is pointed out, the Portuguese Government appears to take a benevolent rather than a severe attitude in meeting the threat. This attitude is indicated in the Government's treatment of the PCP. When CUNHAL came to trial, as a member of a supposedly outlawed political group, the judge hearing the case gave a comparatively light sentence on grounds that Portuguese law failed clearly to place the Party in an illegal status.

9. While the potential of the PCP to acquire information through infiltration of the Government is great, there is no evidence to show that the Party is properly organized to make the most of this advantage.

10. The relationship of Portugal to Spain is such that there would be little moral compunction on the part of the Portuguese to deter them from giving military and political secrets to the Spanish. This is particularly true if the Portuguese felt that by such action they would further the case of security of the Iberian Peninsula.

11. To summarize, the Portuguese people and the Portuguese Government so lack an understanding of the need for physical and personnel security measures in regard to the safeguarding of classified information that a hazard exists in providing them with such information. If that Government is to function properly in its role as a member of the North Atlantic Treaty Organization, it appears clear that measures will have to be taken to indoctrinate the Portuguese on security practices required in the handling of classified information which is either already in their possession or which may be given to them in the future.