REF ID:A66942
TOP SECRET CANOE
Security Information

13 Feb 1953

TOP SECRET CANOE SECURITY INFORMATION

SECURITY OF ALLIED COMMUNICATIONS

1. Lack of adherence by Allied Nations to NATO Communications Security regulations has been in the past a matter of grave concern to USCIB. The danger to U. S. and NATO security, resulting from the susceptibility of certain Allied cryptographic systems to attack by cryptanalysis, demanded that active remedial measures be adopted.

2. With the concurrence of LSIB, USCIB authorized the U. S. Ambassador to Portugal to approach President Salazar to tell him that the U. S. was aware of certain violations of NATO regulations governing the transmission of COSMIC material. This conversation took place on 20 December 1951; Ambassador McVeagh reported that his presentation had been well-received, and that President Salazar had issued instructions for strict and literal compliance with NATO security regulations. An offer of U. S. technical assistance was, however, politely refused.

3. Concurrently, the problem of French communication security was under consideration by LSIB and USCIB. It was eventually agreed in January 1952 that, because of the state of general internal security in France, an approach to the French Ministry of Foreign Affairs on communications security would not be made until the Tripartite Report on general security had been approved by the French, and the French Government had undertaken definite, implementing action. Although the Tripartite Report has been approved by the three governments, apparently no definite action has thus far been initiated by the French. Therefore, no U. S. and U. K. action in the premises has been made.

4. That the Turkish Government is occasionally aware of its shortcomings in the matter of communications security is evidenced by their approach to the U. S. State Department to obtain cipher machines which would assure the inviolability of Turkish correspondence. Negotiations for the provision of Combined Cipher Machines to the Turks have been suspended temporarily. On this subject, LSIB has expressed its regret that it was not notified of the initiation of these negotiations; correspondence with LSIB on the matter is in progress.

5. Recent developments indicate that Allied communications continue to be a serious hazard to security.

6. The Portuguese introduced certain changes, presumably in response to the U. S. demarche, in an attempt to increase the security of their cipher systems.

[redacted]

7. Turkish communications are so insecure that the Swedish Government, provoked by leakage of information regarding business negotiations between the two governments, notified the Turks that the latters' cryptosystems were readable. Because Sweden was apparently unable to convince Turkey of this fact, the Swedish Minister appealed to the U. S. Ambassador for support.

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

Declassified and approved for release by NSA on 06-02-2014 pursuant to E.O. 13526

TOP SECRET CANOE SECURITY INFORMATION

The State Department does not plan at this time to reply to the Swedish Minister's request. The Turks, like the Portuguese, have attempted to increase the security of their communications, but because of their lack of knowledge of sound cryptographic procedures, and their abuse of inherently secure cryptosystems, their efforts have been unsuccessful.

8. It is recommended that USCIB again consider the problem of Allied communications security with a view towards initiating more positive remedial action where necessary.