

Op-20/B k
(SC)A8
Serial 0009P20

NAVY DEPARTMENT
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON 25, D.C.

1 SEP 1948

~~TOP SECRET GLINT~~

MEMORANDUM FOR THE SECRETARY OF THE NAVY:

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

Subject: Brief on attached NSC Item.

1. All agree that there is no completely satisfactory answer to the problem. The important point is that when a decision is made by NSC, that those making it should know the results that may be expected regardless of which course is selected.

2. The answer is - "Should the [redacted] endeavor to prevail on 'Western Union' Powers particularly [redacted] to increase security of their rapid communications, by having the [redacted] provide a secure cryptographic system - and thus try to prevent the U.S.S.R. from decrypting and reading messages about Western Union plans and intentions?" Naturally, the Secretary of State and the British Prime Minister wish to insure security of such communications.

3. If a common cryptographic system were proposed by [redacted] and was accepted by [redacted] and other Western Union Powers - then

(a) Some improvement in communication security might result, but this would remedy but one defect in the

[redacted]

(b) Because the [redacted] make this proposal, the [redacted] and others concerned will believe that the [redacted] are able to read [redacted] encrypted messages and will change and improve their codes and ciphers to our obvious disadvantage.

(c)

[redacted]
several months and possibly forever - whereas the U.S.S.R. probably would continue to get considerable intelligence as at present from their agents within

[redacted]

poor at this time.

- 1 -

~~TOP SECRET GLINT~~
~~TOP SECRET GLINT~~

NAVY DEPARTMENT
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON 25, D.C.

Op-20/Bk
(SC)A8
Serial 0009P20

1 SEP 1948

~~TOP SECRET~~ ~~CONFIDENTIAL~~

Subject: Brief on attached NSC Item.

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

4. The CNC (Op-20) recommends that -
- (a) No action be taken to improve [redacted] (or other weak ally) cryptographic security, in peacetime.
 - (b) The U.S. recommend to U.K. the adoption of this (a) as a combined [redacted] policy.
 - (c) [redacted] be considered before releasing any classified cryptographic information to the [redacted]
 - (d) No action be taken by [redacted] that might curtail [redacted]
 - (e) The U.S. insist that only "pouch by courier" be used for transmitting all "Western Union" information.
 - (f) [redacted] discreetly advocate moving headquarters of "Western Union" discussions from [redacted] as a means of reducing number of communications that the [redacted] must send.
 - (g) If, despite the grave disadvantages which will ensue, it should be decided that the [redacted] propose [redacted]
 - (h) No unilateral action be taken by the U.S. as the [redacted] has an equal interest and only combined action should be taken.

5. The CNC (Op-20) strongly supports the Army and CIA position (as opposed by State and Air Force), and recommends -

That the Secretary support CIA and Army unless he personally decides that the State Department must be supported even though the cost to U.S. interest by reason of such support will be great; and even though that course may prove ineffective.

Earl E. Stone
Respectfully, Rear Admiral, USN

~~TOP SECRET~~

~~TOP SECRET~~ ~~CONFIDENTIAL~~

Copy to: Op-32
Op-20-2

~~TOP SECRET INT~~~~TOP SECRET GLINT~~

31 August 1948

MEMORANDUM FOR THE NATIONAL SECURITY COUNCIL:

- Subject: Security of Communications Relating to International Diplomatic Activities Participated in by the United States.
- Reference: (a) NSCID #9.
- Enclosure: (A) TOP SECRET Memorandum for the Executive Secretary, NSC from the Chairman, USCIB dated 31 August 1948.

1. There is attached a memorandum from the Chairman, USCIB to the Executive Secretary enclosing majority and minority reports on a TOP SECRET matter referred to USCIB by the Secretary of State.

2. Because of the need for special security safeguards in the handling of this matter it is necessary to depart from established procedures for handling NSC reports. The facilities of USCIB therefore are being employed to limit the distribution of the material relating to the subject problem.

3. USCIB members have been charged with the responsibility of assuring that the heads of the departments represented by them are furnished full background information prior to Council consideration.

4. This item has not been placed on the agenda for the NSC meeting September 2 but in view of the urgency of the matter the Council may desire to consider the subject at that meeting.

SIDNEY W. SOUERS
Executive Secretary

~~TOP SECRET GLINT~~~~TOP SECRET GLINT~~

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

~~TOP SECRET~~

31 August 1948.

MEMORANDUM FOR THE EXECUTIVE SECRETARY, NATIONAL SECURITY COUNCIL

Subject: Security of Communications Relating to International Diplomatic Activities Participated in by the United States.

Reference: (a) NSCID #9

Enclosure: (A) USCIB Majority Report dated 31 August 1948.
 (B) USCIB Minority Report dated 31 August 1948.

1. The Secretary of State has requested USCIB to determine a method for insuring the security, against decryption by the USSR, of rapid communications among the

USCIB was unable to reach a unanimous agreement on a solution of this problem.

2. In accordance with the provisions of reference (a), the enclosed reports are forwarded for consideration by the National Security Council at the time of its meeting on 2 September 1948.

3. In connection with the consideration of the subject problem by the National Security Council, attention is invited to the requirement that all participants be indoctrinated for dealing with communication intelligence matters.

FOR THE UNITED STATES COMMUNICATION INTELLIGENCE BOARD:

THOS. S. INGELIS
 Rear Admiral, U.S. Navy
CHAIRMAN

~~TOP SECRET~~ GLINTMEMORANDUM

TO: The Executive Secretary
National Security Council

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

SUBJECT: Views of USCIB Minority on the Solution to the Problem of Western Powers Communication Security.

1. On August 25 the U. S. Communication Intelligence Board (USCIB) met at the request of the Department of State to consider how the [redacted] can continue doing business with the western powers in the light of the latter's communication insecurity. The Board was advised of the predicament facing the [redacted] Secretary of State and of their request that a solution be reached as a matter of urgency. The Board appointed an ad hoc committee of technical experts to consider the problem and devise a plan.

2. On August 27 the Board met again. The ad hoc committee reported that a plan had been prepared which it believed would have the effect of insuring secure communications among the western powers

[redacted]
telecommunication net on which the Western Union nations -- and the U. S. -- will use a one-time tape system for all communications involving matters affecting the national security of any of the participating nations. Each nation would encipher its messages in its own systems which then would be super-enciphered in jointly-managed message centers and transmitted in the secure system.

3. The Board debated two questions: (a) whether, in these circumstances, the policy of providing cryptographic assistance to other nations should be adopted; and (b) if so, whether the plan proposed by the ad hoc committee is feasible and accomplishes the desired end. When the first question was put to vote, four of the nine members (State, two Air members and one Navy) voted "yes"; and five (two Army, two CIA and one Navy) voted "no." On the second question, the plan of the ad hoc committee was approved unanimously by the Board.

4. The minority of USCIB is convinced that this Government must provide cryptographic assistance to other powers, if necessary to assure the security of strategic information affecting the plans and intentions of this Government; and it proposes that the plan

~~TOP SECRET~~ GLINT

~~TOP SECRET~~ ~~GLINT~~

-2-

devised by USCIB be implemented for the following reasons:

a. Recent and foreseeable developments between the Western Union powers and the U. S. require that this Government be free to negotiate with those powers in matters of critical strategic importance. Such negotiations must assume the character of direct and intimate participation with those governments, and their success is predicated upon complete security which, in turn, will be no stronger than the protection afforded by any one participating power.

b. In formulating a plan to meet this situation, the U. S. Government must consider whether its need to negotiate freely and the degree of attainable security outweigh the risk to its own communication security and [redacted]

c. The USCIB minority believes that the need to negotiate freely is paramount. Moreover, the plan proposed by the ad hoc committee and approved by USCIB will permit free and secure negotiations.

d. The specific cryptographic assistance recommended in this plan does not endanger U. S. cryptographic security.

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

e. As proposed and if effectively executed,

[redacted]
powers.

f. The position taken by the majority of USCIB can only be

[redacted]
with the western powers. The argument that the plans and intentions of the western allies may reach the USSR by other means of penetration certainly does not justify taking no action in a field in which it must be assumed that such leaks are occurring every day. This would be in impressive contrast to the situation in areas controlled by the

~~TOP SECRET~~ ~~GLINT~~

~~TOP SECRET~~ GLIN+

-3-

USFR where immediate and firm measures were taken to protect the security of Soviet operational planning through the establishment of controls over satellite telecommunications.

Thomas B. Inglis
Rear Admiral, USN
Chairman, USCIB

CPC

Charles F. Cabell
Major General, USAF

RL

Ray H. Lynn
Colonel, USAF

PA

W. Park Armstrong, Jr.

~~TOP SECRET~~ ~~SECRET~~

TBSI

Comments on proposal to improve [redacted]
Cryptographic Security

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

1. The proposed course of action may result in some probable improvement in the security of [redacted] government communications bearing upon western Union matters. The cryptographic weakness requiring correction, however, while serious in nature, is but one defect of many of equal gravity in the over-all security of the [redacted] governmental structure.

[redacted]

[redacted]

intelligence is highly sensitive in nature and reacts to the slightest alarm. It is important to note that once attention is directed to a particular communication link indicating vulnerability to cryptanalytic attack, the ensuing reforms usually result in loss of the specific

[redacted]

[redacted]

intelligence sources. Their loss as a source is a practically certain sequel of the proposed action. Such loss would doubtless be irreversible in nature.

5. [redacted] structure is, as a considered opinion, so generally below minimum essential standards

[redacted]

in this field have been consistent and reliable. These nations have placed little emphasis, therefore, on covert activities within [redacted] Government. The USSR is believed, on the other hand, to be in a sufficiently favorable position in operation of other intelligence activities to obtain significantly the same amount of information and lose nothing of consequence.

~~TOP SECRET~~

6. It is more than possible, considering limitations of communication intelligence activities imposed upon them by scarcity of qualified personnel, procurement of equipment and the ceiling above which internal security of activities even inside the "Iron Curtain" is no longer practical, that the USSR has neglected exploitation of [redacted] as a source. If coverage from other intelligence activities has been adequate it is quite a logical probability that her COMINT strength has been concentrated on her major targets — the U.S. and the U.K.

7. [redacted] other security risks involved in passing information to [redacted]

b. Indiscretion of officials.

g. Personal disloyalty of officials or employees of the Government having access to classified information. This is disloyalty arising from personal or political opposition to [redacted] or Western Union collaboration. Without any pro-communist slant it can result in serious breaches of security by disclosure of information with intent to embarrass political or personal opponents or handicap opposed policies.

g. Poor physical security. It is notorious that employees of the [redacted] are poorly paid and many who have access to files and information within [redacted] may be vulnerable because of economic conditions.

g. The demonstrated cryptographic weakness is prima facie evidence of lack of over-all security. It is so glaring that it is highly incredible that the [redacted] are unaware of its existence. The government lacks the will or intention, or both, to correct it.

f. Penetration by other, non-communist, national interests.

g. Access of [redacted] press to files.

h. Disclosure of information by [redacted] Government to insecure individuals for political expediency.

8. It is therefore strongly urged that:

a. No action be taken designed to improve [redacted] cryptographic security.

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

~~TOP SECRET~~ ~~SECRET~~

~~TOP SECRET~~ ~~GLINT~~^{TOP SECRET}

f. That the United States recommend to the [redacted] adoption of a common policy on the matter.

g. That full consideration be given to the overall security risk, of which the subject cryptographic security weakness is but one facet, before authorization to release any classified cryptographic information to the [redacted]

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

[redacted]

They are currently and in all probability will indefinitely remain both a unique and important source of intelligence.

10. The above opinions and recommendations have the concurrence of the Director, Intelligence Division, United States Army, the Chief, Army Security Agency, the Chief of Naval Communications, and the Director, Central Intelligence Agency.

K. H. MILLERSON, JR.
Rear Admiral, USN
Director of Central Intelligence