Report on the Problems with and Solutions to Special Operations Executive Signal Ciphers

Source: https://www.arcre.com/soe/soesciphers

Category: Cryptography Published: Saturday, 05 January 2013 23:31 Hits: 12736

The following document is taken from the Special Operations Executive official Signals history. It discusses what went wrong with SOE cipher procedures and the piecemeal steps taken to perfect greatly enhanced cipher security for field agents. It can be seen that problems with ineffectual security checks in the early SOE missions no doubt contributed to such disasters as wrought in the Netherlands, the Abwehr's so-called Englandspiel which wiped out SOE circuits in the country.

S.O.E. FIELD CIPHERS

I. PERIOD 1942

What was wrong

1). Agents were using emergency phrases for their main cipher system.

2). Identity checks were 99% useless; their security was negligible, and they were almost totally invalidated by morse mutilation.

3). THERE WAS NO ORGANISED AGENTS' TRAINING. Agents appeared for cipher training when and if they could spare the time, and when and if they felt like it.

4). Officers available for the training of agents in field cipher knew almost as little about the cipher systems as the trainees themselves.

5). Coders at the Base Station were given only the scantiest instructions on how to code before being put onto operational messages.

II. WHAT WAS DONE ABOUT THIS

1). Original poems were issued instead of emergency phrases.

2). Security precautions for double transposition brought into use.

3). An analysis was made of all incoming and outgoing S.O.E. traffic and the following conclusion was drawn from it:- DOUBLE TRANSPOSITION WAS THE WRONG TYPE OF CIPHER FOR S.O.E. TYPE OF CLANDESTINE COMMUNICATIONS.

Long stereotyped questions demanding long stereotyped answers mingled with long stereotyped comments were rules of the day. Dropping points – moon periods – containers – money – could be anticipated in almost all the outgoing and incoming agents' messages. In 1942 S.O.E. agents' traffic was an anagrammer's paradise.

4). An attempt was made to make the texts less stereotyped by using more than one language in the same message, but Country Sections did not have time to cooperate.

5). Immediate research was begun into alternative methods of cipher. In the meantime, agents were provided with a number of original poems, each of which was used up to a depth of approximately 15 messages each way and no more.

6). Training officers were first trained in London and then despatched to cipher training school. Each training officer was shown briefly the enemy's methods of attacking transposition.

7). Each training officer was shown briefly the best psychological approach to training.

8). The closest scrutiny of the process of the training officer as well as the progress of his trainees was kept.

9). All coders were made to undergo special coding courses, and shown the enemy's methods of attacking double transposition.

10). Country Sections were warned that to cope with their increase in stereotyped type of traffic, major changes in cipher policy were imminent.

11). Country Sections were warned that no reliance could be placed in existing identity checks. THAT ALL AGENTS IN THE FIELD MIGHT BE UNDER DURESS AS FAR AS WE KNEW.

III. CONCLUSION. 1942

Transposition systems based on poems or emergency phrases carried in the agent's head are a complete failure as the main system for S.O.E. type clandestine traffic.

IV. WHY ARE THEY A FAILURE

1). Because if an agent is caught and tortured, he will almost certainly reveal the details of his poems – thus enabling the enemy to decipher all of his traffic which they have intercepted. This consideration is of paramount importance.

2). Low grade security is afforded when stereotyped messages are sent in transposition.

3). Under emotional stress the agent cannot remember his poems without difficulty, and when he can remember them he has not the time to use the code with the accuracy it requires.

4). After about 15-20 messages have been passed on a poem, the agent has a tendency to repeat the indicators he has previously used. If he is instructed to retain the list of indicators he will also retain his list of en clair messages; if he is instructed to destroy his messages, then it is a psychological certainty that he will revert to using indicators which have been tried and proven.

THE UNCONSCIOUS MIND HAS A TENDENCY TO REVERT TO WHAT IT BELIEVES TO BE SAFE.

"If Indicator 123 has been cleared by the Home Station once, let us use it again and take no chances."

V. 1943. WHAT WE DID

1). W.O.K.'s [Worked-Out Keys] were introduced.

2). A higher grade of identity checks was introduced.

3). Cipher training was put on a scientific basis.

4). Higher grade cipher officers were sought and made "S.O.E. minded".

5). Country Sections were instructed in detail about the dangers of stereotyped texts.

6). Coders at Home Station were more closely supervised.

VI. WHY WE DID IT

1). As soon as an agent has used his W.O.K. transposition keys, he must cut them away and destroy them. The advantages of this are so manifold as not to need elaboration.

2). An agent can code very much more quickly with a W.O.K. than any other form of transposition.

3). With W.O.K. the percentage of indecipherable messages fell by 85%.

4). The confidence of agents in their ciphers arose enormously. Other advantages of W.O.K.'s are so manifold as not to need elaboration.

5). Identity checks. The first major advance in identity checks was the provision to agents of individual secret numbers, by means of which, they could change pre-arranged indicator groups.

6). It was observed that to be a successful training officer, especially in cipher, required certain pronounced characteristics.

7). The standard of cipher personnel was raised very considerably by means of a selection based on the rule of thumb "psychological measurement" of the characteristics required.

8). It is important that the coder is fully aware of what is going on in the field. An agent's coding convention gives her a mental picture of the agent. Every coder has her favourite agent, even though she has never met him. If she is told the latest news from the field about this agent, she is given an extra fillip and added capacity for concentration. EVERY AGENT HAS HIS FANS: this fact should be exploited for the gain of the agent. This fact was exploited.

9). Clandestine cipher requires great flair from the Base Station coder, who must be made to identify herself with the agent and to retrace his thought processes when coding. This enables the coders to anticipate the type of errors the agents are most likely to make. The errors were anticipated and indecipherables quickly broken by reference to card indexes.

10). One Time Pads. Apart from obvious security value, letter one time pads enabled the agent to get off the air with a minimum of 3 groups. This was invaluable. Letter one time pads also hid from the enemy the language which the agent was using. This was useful.

VII. CONCLUSIONS 1943

1). Letter one time pads are ideal for S.O.E. type of clandestine communications providing:

a). They are clearly printed.

b). They are produced in several sizes so that the agent may choose which size he prefers.

c). They are well camouflaged.

d). The agent is offered as many varieties of one time pads as possible so that his mind is deflected from the problem of whether he wants it or not into the problem of what type he wants.

e). W.O.K. is an excellent reserve to the one time pad.

2). At the end of 1943 the average agent was sent into the field with the following cipher equipment:-

a). MAIN SYSTEM. Letter One Time Pad.

b). RESERVE. W.O.K.

c). RESERVE (extreme emergency only) – 26 word phrase.

d). HIGH GRADE IDENTITY CHECKS ON MAIN AND 1 ST. RESERVE SYSTEMS.

VIII. 1944/1945. REAL ADVANCES

1). Agents were now sent into the field with 12 page Letter One Time Pads on silk.

2). W.O.K. or Code 53 on silk.

3). Crack Signal One Time Pad on silk.

4). Broadcast One Time Pad on silk.

5). High Grade Identity Checks.

Sounds a lot? – It is a lot – but so was the volume of traffic agents were required to send. Compared with the large space occupied by agents' wireless sets, the cipher section's demands on operators are very slight. A few sheets of silk are all we ask him to carry.

1944 saw the development of the principle that just as an agent needs a wireless set to transmit messages, he needs a tangible cipher in which to code them.

The closest liaison was established between training officers and Base Station coders. Every fault the agent made in training was recorded in special files and sent to the Home Station for future reference.

The application of mental systems was introduced, including mental One Time Pads, mental Code 53. These are discussed under "Systems".

During 1944, the number of people employed at the London H.Q. alone, making, checking and distributing agents' ciphers was 89. Only when Cdr. Dudley Smith through B.P. [Bletchley Park] assisted us by making machine made W.O.K.'s were we able to steadily reduce this figure. Amongst the 89, were 15 high grade instructresses.

IX. CONCLUSIONS. 1944/1945

1). The more field cipher systems at the disposal of an organisation like S.O.E. the better.

2). Cipher systems to be individually tailored for the agent.

3). There were several forms of transposition available to the agent – W.O.K., Code 53, etc. – we would decide which type would be most useful to him and try to guide him into it.

4). Seeing a lecture on the breaking of ciphers gives the average section head a fright. Telling a person that a code can be broken is not as effective as making him break it for himself.

5). S.O.E. Identity check systems were proved extremely reliable if properly used. (Cricket and Swale in Holland; Bolero in France, etc.)

X. WHAT WENT WRONG

1). Many agents (50%) did not cut away and destroy their one time pads or tangible ciphers.

Whose fault was this? Ours. If an agent fails to destroy and cut away his tangible cipher it is the fault of the person who has briefed him.

2). All that goes wrong with ciphers in England goes 3 times as wrong in ciphers abroad.

S.O.E.'s field cipher security abroad was a mess from 1942 to the middle of 1943; from 1943 to 1945 it was put on a sound basis, but the rot was so embedded that some agents were using in 1945 conventions with which they had been issued in 1942.

XI. SYSTEM BY SYSTEM

1). W.O.K.'s. How many issued. – 2283.

Each W.O.K. consisting of 240 pairs of keys; 120 In and 120 Out. Details are as follows:-

Country Sections		**Missions Abroad**	
Belgian	39	Australia	217
Czech	2	Cairo	310
Danish	5	India	773
Dutch	3	Force 399	133
D/F (Land Line)	1	Maryland	69
French	94	Massingham	132
Fighting French	335	S.O.M.	8
Norwegian	8		
Polish	7		
X Section (German)	2		

Special Commitments	
Bardsea	19
Jedburgh	121
Special Forces	5

W.O.K.'s were printed in 4 different sizes; the offset lithographic process giving the clearest and quickest results; it was also the cheapest method.

2). One Time Pads, Clandestine. How many issued. – 3052. Details as follows:-

Country Sections		**Missions Abroad**	
Belgian	271	Australia	53
Czech	6	Berne	20

Danish	270	Cairo	143
Dutch	130	Force 399	77
D/F (Land Lines)	30	Gibraltar	1
French	316	India	751
Fighting French	332	Istanbul	29
German	31	Lisbon	1
Norwegian	343	Maryland	83
Polish	43	Massingham	63
X Section (German)	28	S.O.M.	18
		Stockholm	13

3). Code 53. Very popular with agents as it is less bulky than W.O.K. How many issued – 1089. Details are as follows:-

Country Sections		**Missions Abroad**	
Belgian	14	Australia	96
Czech	8	Force 399	7
Danish	3	India	770
Dutch	17		
French	44		
Fighting French	17		
German	48		
Norwegian	41		
Polish	20		
X Section (German)	4		

4). Broadcast One Time Pads. This system was a great success and less complaints were received about it from agents in the field than any other system.

5). Mental One Time Pads. This system was cumbersome, slow, and difficult to master. It was issued to 54 agents as a reserve system, and to 5 agents as a main system. Of the 54 agents, 18 used it and the other 36 never had occasion to. Of the 18, 4 used it successfully, passing respectively approximately 30-90 groups each without sending any indecipherable messages. Between the 4 agents a total of about 450 groups were passed. Of the other 14, one agent's messages were never deciphered and we had to go on ordinary transposition; the other 13 used it with considerable success marred only by slight morse mutilation on the indicator.

The Mental Pad could only be taught to a low grade agent by a high grade trainer. It should not be used as a permanent reserve system. Mental W.O.K.'s and One Time Pads were used to a considerably less degree and no more than 50 groups were passed on this system, primarily because the need for them never arose.

For comparisons and specimens of all this traffic please refer to the file which will be in Cdr. Dudley Smith's keeping.

XII. TRAINING

To cover this enormous subject would require volumes: it would also require that the reader has at least a working knowledge of the current principles of psycho-analysis – for it was upon certain of these principles that S.O.E.'s cipher training technique was finally evolved.

Briefly, psycho-analysts maintain that (a) behind almost every conscious intention there lingers in the unconscious a deep seated resistance, and (b) Emotion is ambivalent – two sided – what we feel in our conscious mind has its exact opposite in, our unconscious: behind a display of enthusiasm lurks a desire for lethargy – behind a display of affection lurks dislike – behind a display of nausea lurks desire, etc.

The way to discover the existence in the average person of (a) and (b) is through his slips of the tongue, lapse of memory, dreams, gestures, laughter, etc. THIS HOLDS GOOD FOR AGENTS.

The theories of (a) and (b) affect agents in the following ways:-

(1) AGENTS RESENT BEING TRAINED. (This resentment is unconscious).

(2) ENTHUSIASTIC AGENTS DO NOT REALLY WISH TO GO INTO THE FIELD. (This reluctance is unconscious).

(3) AGENTS SEE IN THEIR TRAINING OFFICERS "PARENT IMAGOS" AND REACT ACCORDINGLY. (The fact that the TRAINING OFFICERS are taken as *parent imagos* is unconscious as far as the agent is concerned, but SHOULD NOT BE as far as the training officers are concerned.

(4) Carelessness, Indolence, Stupidity, or Careless Talk on the part of the agents during training – and indeed afterwards – may be due to UNCONSCIOUS causes.

(5) TRAINING MUST AIM AT THE UNCONSCIOUS OF AN AGENT and not merely to the conscious, otherwise mighty forces may, in the end, bring the most carefully planned training to nought – and an otherwise competent agent may be the despair of his training officer simply because of unconscious trends which no-one has attempted to control.

(6) For further details of the psycho-analytical approach to agents' training, see Appendix entitled "Ciphers, Signals and Sex".

Every agent should go through a post graduate course. It is not enough for an agent to know his ciphers consciously, they must be burned into his unconscious mind so that in moments of acute tension they will be recalled to him with the facility of an instinct.

Constant repetition is imperative. An agent must be told something so often that he begins to react by mimicking his instructor. It is not enough to tell an agent 3 or 4 times about his identity checks, it may not be enough to tell him 30 to 40 times; it is his unconscious mind that must be instructed. Agents should be disturbed at all hours and made to code. Their reactions under intense fatigue should be watched. Paper, spectacles, and electric lights should be removed, and they should be made to improvise methods of coding and decoding traffic. Agents should be grilled before departure to the field. A mock Gestapo session should be set up in which their reactions should be noted. The technique of rebuffing psychological questions should be explained to the agent.

The time it takes to train an agent.

15 hours at a training school.

Post Graduate Course. This consists of every spare second the agent has. Each agent is given his own instructress whose timetable is so arranged that she can be available whenever he requires instruction in cipher. This is a point of psychological importance.

Types of Instructresses. Primarily the extraversive type is best: the dreamy, poetic, aesthetic type was of little use in instructing agents in cipher: the ultra-sophisticated type is even worse. Personable manner, striking or restful appearance are important qualifications for the coding instructress. An agent at a time of intense emotional strain will react far more favourably to a set of characteristics that attract him rather than to the opposite.

Ciphers should be sold to the agent; cipher training is a sales campaign; instructresses should be chosen of the same types as would be used for saleswomen.

A brilliant coder is not necessarily a brilliant instructress in cipher; a brilliant instructress is not necessarily a brilliant coder.

[FINAL PAGE OF REPORT WITHHELD UNDER SECTION 3(4) OF THE PUBLIC RECORDS ACT 1958]

[Source: TNA HS 7/41, transcribed by www.arcre.com]