



British Intelligence Superiority, 1939-1948, Based on Breaking Haganah Ciphers

Version 1.02

The Association for the Commemoration of the Fallen Soldiers of the IDF Signal Corps, 2025

Colonel (Ret) Daniel Rosenne

Background

British Deciphering of Haganah Ciphers

- **The Haganah operated radio networks since 1937 until the establishment of the State of Israel in 1948.**
 - The radio networks operated at high frequencies, using Morse signaling.
- **The traffic on the radio networks was encrypted, using manual transposition methods.**
 - The Haganah commanders believed that the encryption was safe and reliable, but this was far from reality.
- **In July 1946, following a British 'White paper' after the 'Black Sabbath', it became clear that the British were intercepting the radio traffic and deciphering the Haganah codes.**
 - Following the incident, the Haganah's communications service changed the codes.
 - Since then, the British were in an 'Intelligence Blackout' regarding the Jewish Agency, the Haganah and the Palmach.
- **The British managed to decipher the code of the 'Gideon' radio network, in the service of the Mossad for Aliyah Bet, which enabled the British to intercept the illegal immigrant ships.**

British Activity

- **The British deciphered Haganah Signal Service ciphers since 1939. and intercepted the Haganah radio networks since 1942:**
 - The Haganah's radio traffic was for the British an 'open book'.
 - The British had no difficulties: the Haganah used simple ciphers, did not change keys frequently, and used to transmit many long messages.
- **In 1944, the Haganah networks were designated as a *"Priority Number 1"*, *"of prime importance"*, for the post-war period:**
 - The British established an effective mechanism for radio interception, transmitting the traffic to London for deciphering and translation to English, and delivering the information to Palestine.
- **The intercepted and decrypted traffic was transmitted by teleprinters on a dedicated network, encrypted using TypeX.**
- **The Haganah radio traffic, intercepted and deciphered, was the main and reliable British intelligence source.**

British Operations

- **Radio transmissions, intercepted in Sarafand (Palestine), Egypt and Cyprus, were transmitted to London for deciphering and translation.**
 - The process took four hours for urgent messages, 16 to 31 hours for all other traffic.
 - Special messages were distributed immediately; the rest of the messages were distributed in summaries of a thousand messages.
- **The British took unique security measures and decrypted messages had top security classification.**
 - Only a small number of specially indoctrinated staff (about 15 senior commanders in Palestine) received the information.
 - British code names: ISPAL, ISOATS, ISTRIA, FOG, GLINT, CREAM.

Practical Issues

- **Jewish employees of the British code breaking center in Bletchley Park did not hide their sympathy for Zionism.**
 - Bletchley Park Zionist cell operated openly.
- **Therefore, the decryption of Haganah ciphers was done at the GCHQ Diplomatic Department at 8 Berkeley street, London .**
 - In 1946, the operation moved to offices at 10 Chesterfield street, London.
- **Translating 'modern' Hebrew into English was a major challenge for the British.**
 - Especially since it was not possible to get help from Jews.



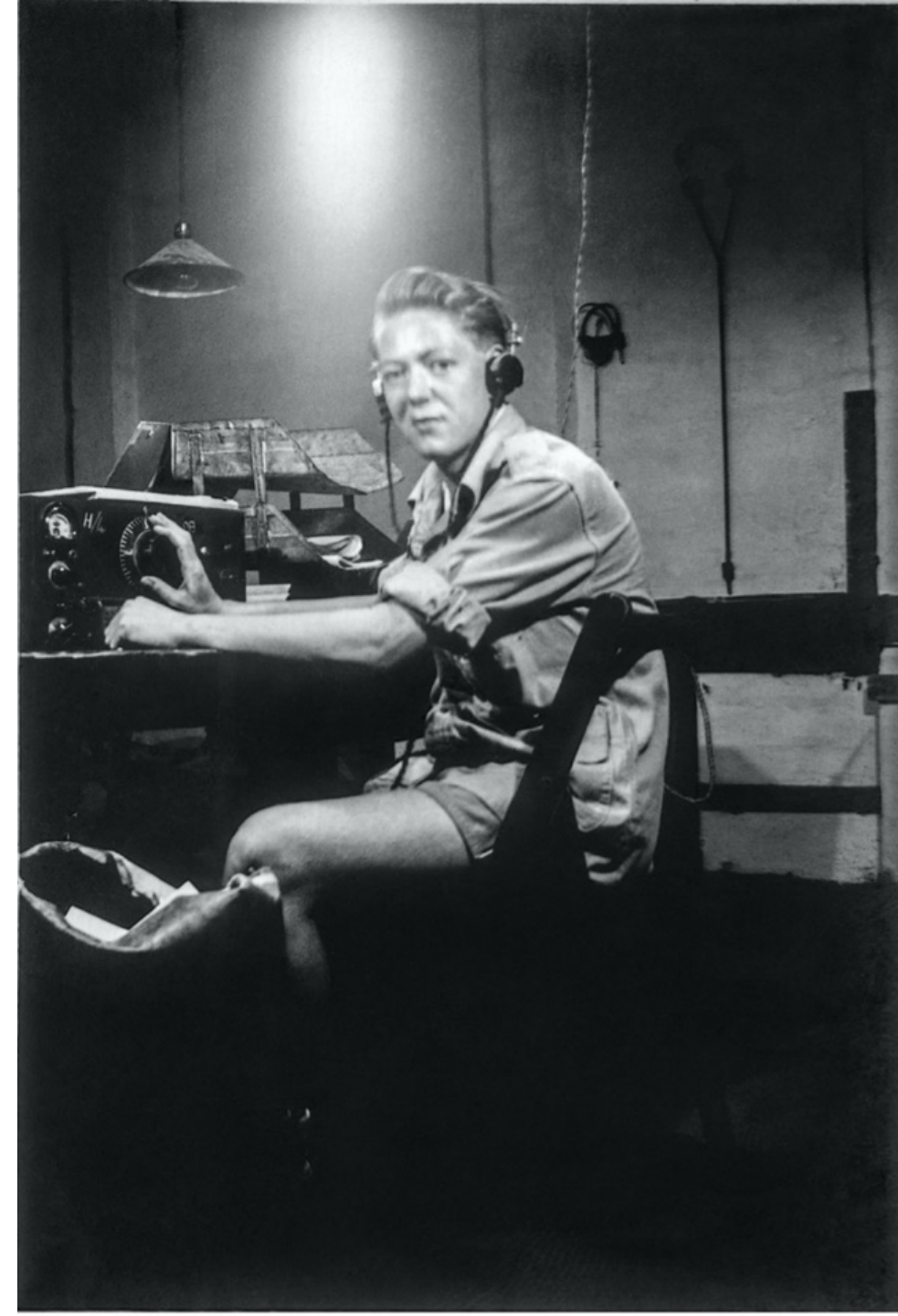
Clandestine HF Radio Station, Kibutz Dorot, 1940's

Courtesy of Government Press office,
National Photo Collection, D285-029

Radio Interception

- **MERS (Middle East Radio Security) unit operated from the Sidi Bishr camp near Alexandria - intercepting, among other, Haganah radio networks.**
- **This activity was carried out during the World War and until June 21, 1946, when the unit was closed and the activity was transferred to Cyprus**

MERS operator at the Sidi Bishr camp,
Courtesy Ray Wright



SIME in Cairo, DSO in Jerusalem

- **In 1939, MI5 established a counter-espionage center in Cairo, called SIME (Security Intelligence Middle East)**
 - The SIME branches, operating in Baghdad, Jerusalem, and Cyprus, were called DSO (Defence Security Officer).
- **The Jerusalem DSO was an officer in the rank of Lieutenant Colonel.**
 - An officer from the DSO brought the intelligence document to the indoctrinated partners and destroyed it after reading.
- **The DSO in Jerusalem had a unique intelligence function:**
 - Chief Comint and Humint analyst, including all material from CID and Military Intelligence, advising top political and military figures on intelligence, security and counter-terrorism.
 - Directing planes and warships to intercept illegal immigrant ships.
- **The DSO in Jerusalem operated from the King David Hotel.**
 - In the hotel explosion, 22 July 1946, six of its 13 members were killed, the rest were wounded and hospitalized, and the intelligence database was destroyed..

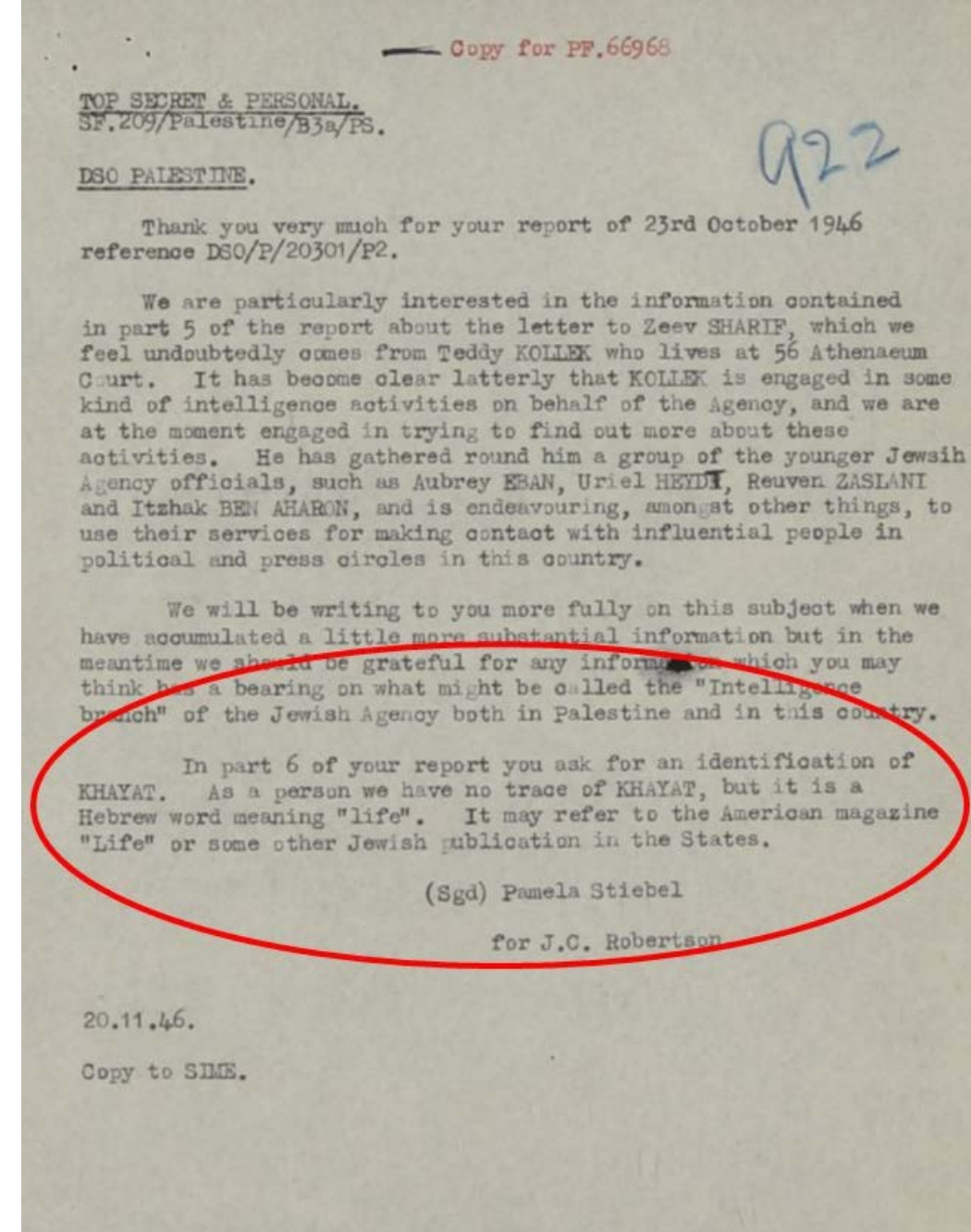
Major Owen Chadwick

- **On June 13, 1946, a British military court sentenced to death by hanging two Irgun fighters who had been captured in an attack on the Sarafand camp, on March 6.**
 - In response, on June 18, the Irgun kidnapped five British officers and threatened to hang them if the sentence was carried out.
 - One officer managed to escape after 36 hours; the rest were released after the High Commissioner commuted the death sentence to life imprisonment.
- **The fleeing officer, Major Chadwick, was a DSO officer who was kidnapped in Jerusalem on his way to General Barker, and in his pocket was a deciphered, 'top-secret' Haganah message.**
 - The Irgun fighters did not search him or locate the message.
- **After 36 hours, the officer escaped from his captors, boarded bus number 3 on Jaffa Street, got off at the King David Hotel and called the army.**
- **The British suspected that the Major was a double agent, flew him to London for interrogation, and 'calmed down' only when it became clear that the traffic continued to flow and that the Haganah continued to use the same cipher.**

The Tailor

- **George Francis Taylor was a senior staff member of the SOE, who was sympathetic to the Zionist movement.**
 - Taylor commanded the Special Operations Directorate's operations in the Balkans during WW2.
- **Members of the Jewish Agency political department maintained regular contact with him, calling him by the code name 'Khayat' (Tailor in Hebrew).**
- **The translator, apparently of Arab origin, translated the word 'Khayat' into the word 'life':**

...you ask for an identification of KHAYAT. As a person we have no trace of KHAYAT, but it is a Hebrew word meaning "life". It may refer to the American magazine "life" or some other Jewish publication in the States".



The King David Hotel Explosion

- **The Secretariat of the British Mandate Government and the British Military Headquarters.**
- **The Irgun blew up the hotel on July 22, 1946,**
 - Irgun fighters smuggled seven milk jugs into the kitchen on the lower floor of the southern wing, each containing 50 kilograms of explosives.
 - The explosion collapsed the entire southern wing, killing 91 people, including the Mandatory Postmaster General and DSO personnel, and injuring 45 people.
 - Among the dead were 15 Jews.
- **The violence shocked the Yishuv, and led to the splitting of the Jewish Resistance Movement, the operational cooperation between the Haganah, the Irgun and the Lehi, that existed since October 1945.**



IWM E.31975, photo by Sgt. Turner

Haganah Ciphers

The Haganah Ciphers – A Brief History

- **Established in 1937, the Haganah Signal Service initially utilized the cipher methods used by the British Mandate police.**
 - Over time, they shifted to techniques of the Yugoslav military, brought in by Eli Schwartz from Kibbutz Afikim, who had former experience as a Signals officer in the Yugoslav armed forces.
- **In July 1946, it became clear that the British decipher the messages, prompting a major change.**
 - This change created a period of British 'intelligence blackout'.
- **By August 1947, the Signal Service concluded that the British could once more decipher their communications and made further changes.**

Simple Cipher: 1939

- Secret cipher based on substitution of letters
- The list was changed every few days

X	א	י	ב	א	י
T	ב	U	ב	ב	J
I	ג	G	ג	ג	L
N	ד	P	ד	ד	E
D	ה	T	ה	ה	V
L	ו	A	ו	ו	H
V	ז	S	ז	ז	D
F	ח	B	ח	ח	C
B	ט	N	ט	ט	B
C	י	K	י	י	K
G	כ	R	כ	כ	N
E	ל	C	ל	ל	S
K	מ	H	מ	מ	G
Z	נ	X	נ	נ	X
A	ס	O	ס	ס	P
M	ע	J	ע	ע	F
P	פ	N	פ	פ	O
S	צ	M	צ	צ	R
R	ק	E	ק	ק	M
H	ר	V	ר	ר	A
O	ש	L	ש	ש	T
J	ת	F	ת	ת	Z
/11=15.6		.16/20=6.		21.25.6	

Yugoslav Transposition Cipher

- The encryption was based on an agreed password
- The password letters were replaced with numbers, with the numerical value – instead of the letters – given from low to high
- The message was written in a table, and transmitted in five letter groups composed in the numerical sequence.

Password →

11	7	1	4	2	6	3	12	9	5	8	10
מ	י	ד	ו	ה	י	ה	ת	מ	ח	ל	מ
ר	ח	מ	ה	פ	י	ח	ל	ע	י	ג	נ
נ	ל	ו	נ	י	כ	ה	ר	ק	ו	ב	ב
ז	ז	ה	פ	ו	ח	ד	ה	ר	ז	ע	ו
ז	ז	ר	ו	מ	ג	ל	מ	י	צ	ו	ר

The 'Black Sabbath' and the British 'White Paper'

'Black Sabbath' Events

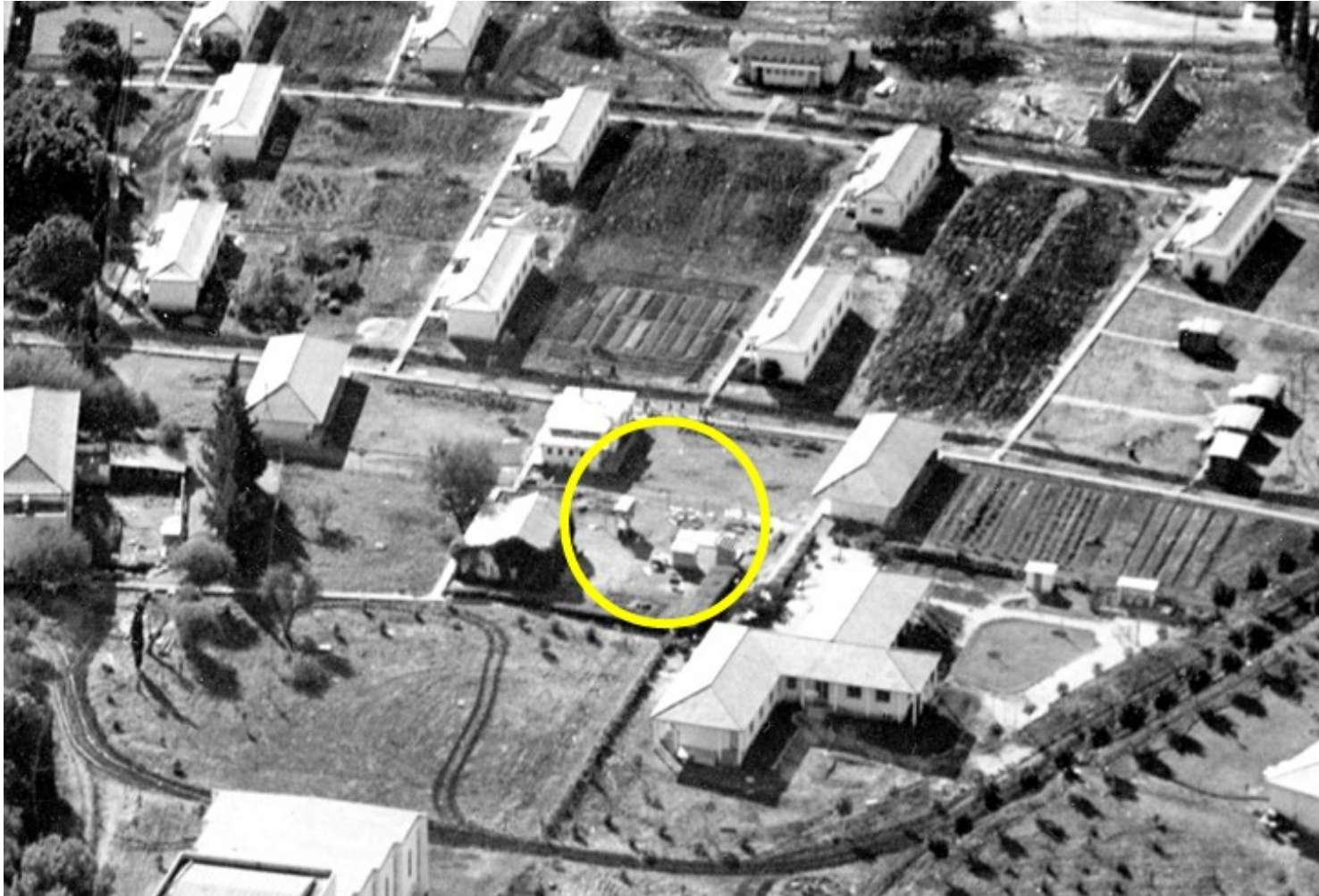
- **In October 1945, in an attempt to change the British policy on the Palestine question, the "Hebrew Resistance Movement" was established – Haganah activity, together with the Irgun and Lehi, against the British,,**
- **Extensive operations were carried out against the British.**
 - The most prominent of which was the 'Night of the Bridges', between June 16 and 17, 1946, blowing up 11 bridges on the Palestine borders, temporarily cutting off the British supply routes.
- **On Saturday, June 29, 1946, the British launched 'Operation Agatha' against the Jewish Agency and the Haganah, known as the 'Black Sabbath'.**
 - Curfews were imposed on Tel Aviv, Jerusalem, Haifa, Ramat Gan, Netanya and more, and house-to-house searches were conducted; 2,700 people, including many of the Yishuv's leaders, were arrested in detention camps in Rafah and Latrun.

'Black Sabbath' – Consequences

- **Hostile public opinion in the United States and a vocal pro-Zionist opposition in Britain 'pressured' the British Labour government, headed by Clement Attlee.**
- **In order to prove the claim that the Jewish Agency was a terrorist organization, the British government published a 'White Paper' on July 25, 1946, which included decrypts of eight encrypted telegrams between the Jewish Agency's offices in London and Jerusalem.**
 - The white paper included telegrams that were transmitted to London from the 'Dafna' radio station in Tel Aviv, 19 Kibbutz Galuyot St.. (today 19 Jabotinsky St.) and replies that were sent as 'Innocent' telegrams
 - The Signal Service operated a one-way radio link from Kibbutz Gevat ('Sarah' station) to London since 1939, and in 1943 the station was moved to Tel Aviv ('Dafna' station)
- **From the white paper, the Yishuv's leadership learned that the British had 'broken' the Haganah ciphers.**
- **Following this alarming revelation, the Signal Service swiftly altered the cipher system.**

'Sarah' Radio Station, Kibbutz Gevat

The secret station was used for a clandestine radio link to London, operating from a camouflaged underground bunker ('Slick') from 1939 to 1943



Hut and the dovecot above the secret bunker, 1946 aerial photograph

Photographer: Zoltan Kluger; Courtesy of the Central Zionist Archives, PHKH/1264710



The bunker ventilation pipes served as the base for the kindergarten's pigeon dovecote – 1943

'Dafna' Station, Tel Aviv

**Jabotinsky and Dizengoff
corner**

**The radio station served
the political department
of the Jewish Agency,
operating until 1947**

**Photograph from the early
1970s**

The British White Paper, July 1946



COLONIAL OFFICE

PALESTINE

STATEMENT OF INFORMATION RELATING TO ACTS OF VIOLENCE

*Presented to Parliament by the Secretary of State for the Colonies
by Command of His Majesty
July 1946*

LONDON

HIS MAJESTY'S STATIONERY OFFICE

TWOPENCE NET

Cmd. 6873

**The press detailed the
'White Paper' at length, and
dismissed it as 'Fake'**

"	"	"	1.	"Hasta Ularome + Caceres"	"	"	3.
"	"	"	2.	"H. S. Broad Castal Birya Trip"	"	"	4.
"	"	"	3.	"Funeral on St. John (P. 1200)"	"	"	2-3.
"	"	"	1.		"	"	

INDEPENDENCE
SINCE 1882

The Palestine Post, 25 July 1946:

**White Paper on Jewish
Resistance: Evidence
Seeks to Link Jewish
Agency with Violence**

4. Gunchala...
JERUSALEM
FRIDAY, JULY 26, 1946

THE PALESTINE POST

PRICE 25 MILS
VOL. XXI, No. 6161

ELECTRICAL DOMESTIC
APPLIANCES AND FIXTURES
of every description — all guaranteed.
Installations — Repairs given prompt
attention.
REASONABLE PRICES
Electric Bulbs — any quantity and wattage
JOHN LIESHITZ
Jaffa Rd., opp. G.P.O., Jerusalem, Tel. 349

Agency Denies White Paper

The following statement was issued by a spokesman of the Jewish Agency yesterday afternoon:

By adducing a jumble of alleged telegrams, stated to have been sent nine months ago, of extracts from broadcasts by the "Voice of Israel" Station and of passages culled from the publications of terrorist groups, the British Government claims to have obtained proof of co-operation between some members of the Jewish Agency and the Haganah and of co-ordination in some cases between the Haganah and terrorist bands.

Not a single one of the alleged telegrams emanated from the Jewish Agency in Jerusalem. The Jewish Agency, which cannot accept the authenticity of these alleged telegrams, challenges the British Government to prove that the Jewish Agency was responsible for their composition, authorization or despatch.

The Executive of the Jewish Agency is giving careful study to this curious collection of alleged telegrams, broadcasts and publications.

Column One By David Courtney

THE odd thing is that the Communists are so often right. On the overriding issue of the atom bomb, M. Gromyko has the disconcerting habit of taking sense; and on Wednesday, while Admiral Rಂದು was dashing about getting ready to turn the Pacific into a cauldron of up-to-date death, M. Gromyko was saying: there is no solution except the utter extinction of the monster; and if you refuse that, let it become a matter for the Security Council as that body is at present constituted. If the atom bomb is not a threat to world security, what is? Palestine? Persia? And being such a threat, why should the Security Council not get down to it? The suspicion grows that America, already in possession of an arsenal of atom bombs, and therefore with a good start even if someone else should tumble on the secret of manufacture, is unwilling to run the risk of submitting the problem to a body where a Soviet veto would be enough to hold up international sanction for the maintenance of America's lead. The Baruch Plan has a lot to be said for it; the trouble is that there is a point of departure for the saying of it, at which America is already in a position of special advantage.

THE bomb went off to schedule at Bikini on Wednesday night. One ship was towed and sink unless taken to shallow water. The battleship Arkansas has gone to the bottom. What has happened to the other ships it is too early to say; but there is no reason to doubt that the bomb was efficient. The fact that some days must elapse before the experts can examine the consequences of the explosion seems proof enough of the efficiency of the bomb. It may be easy to show that a battleship or an aircraft-carrier appropriately armoured will not necessarily break up and sink as the result of blast from an atom bomb; but if radio-activity is such that no one dare go near the wreckage of the ship until hours or even

JEWS INVITED "TO BE PRESENT" BRITAIN PLANS TALKS WITH ALL ARAB STATES ON PALESTINE

PALESTINE POST STAFF

The British Government yesterday invited the Arab States and Palestinian Arabs to take part in a conference on Palestine and European Jewry which is to be held in London some time before the United Nations General Assembly meets during September.

Jewish delegates are also being invited to be present. If the American cabinet committee on Palestine so desires, it will send observers to the conference. The Arab States are Egypt, Iraq, Syria, the Lebanon and Saudi Arabia. P.T.A. adds that Britain has agreed to the Arab League request for negotiations before deciding on the implementation of the Inquiry Report. Thus a Round-table will be held in London in the next three or four weeks it says.

The conference is likely to follow the pattern of the famous round table conference on India, Reuter adds. Mr. David Ben Gurion, Chairman of the Executive of the Jewish Agency, arrived by air in Paris from New York yesterday. He will confer with French Zionists and will attend the emergency meeting of the Executive due to open in Paris next Monday. The Anglo-U.S. talks are being carried on as before, unaffected by the new British White Paper, which the "Daily Telegraph" says editorially, adds little to the knowledge about the Palestine situation.

In Washington the U.S. State Department disclosed last night that the Secretary of State had received two alternative plans for a solution of the Palestine problem, drawn up by the Anglo-American Cabinet Committee.

A State Department spokesman said Mr. Byrnes will discuss the schemes with President Truman before he leaves on Saturday for the Peace conference in Paris. The spokesman added that details of the plans, which have not yet been thoroughly examined by Mr. Byrnes himself, will not be published — at any rate not until Mr. Byrnes and the President have thoroughly discussed them.

At midnight last night the official total of casualties from Monday's attack on the King David Hotel were:

Dead: 67
Injured: 47
Missing: 43

New names of dead given:

"Out of Bounds"

An order has been issued by H. Q. Palestine placing out of bounds to all ranks of the British Army all Jewish places of entertainment, restaurants, shops, private dwellings, said a P.I.O. press release last night.

Russia's Turn BIG "3" SPLIT ON PALESTINE

NEW YORK, Thursday. — It is reported that the Soviet Union delegation will bring up the Palestine issue before Uno, when the discussion on Trans-Jordan's application for membership comes up in the next few days before a committee. It is not yet known, however, what stand the Soviets will take.

The "New York Post" predicted a "Big Three" split over Palestine when the issue comes before the General Assembly at Egypt's request. United Nations informants today interpreted Egypt's request for a new regime in Palestine "in accordance with the provisions and aims expressed in the UNO Charter" meaning that Egypt and the Arab League wish to share in the negotiations for a UNO trusteeship over Palestine.

"Not Official"

Meanwhile Reuter reports from New York that the Secretary-General of Uno does not consider that the Egyptian communication constitutes an official request to put the question of Palestine on the provisional agenda of the forthcoming session of the General Assembly. Official notes calling on the General Assembly to meet in New York on September 29, were sent out to the 51 member States by the UNO Secretariat last night. (P.T.A. and Reuter)

Agency Denies White Paper

The following statement was issued by a spokesman of the Jewish Agency yesterday afternoon:

By adducing a jumble of alleged telegrams, stated to have been sent nine months ago, of extracts from broadcasts by the "Voice of Israel" Station and of passages culled from the publications of terrorist groups, the British Government claims to have obtained proof of co-operation between some members of the Jewish Agency and the Haganah and of co-ordination in some cases between the Haganah and terrorist bands.

Not a single one of the alleged telegrams emanated from the Jewish Agency in Jerusalem. The Jewish Agency, which cannot accept the authenticity of these alleged telegrams, challenges the British Government to prove that the Jewish Agency was responsible for their composition, authorization or despatch.

The Executive of the Jewish Agency is giving careful study to this curious collection of alleged telegrams, broadcasts and publications.

The Sappers

PALESTINE POST STAFF
For nearly four days now the red-beretted Sappers of the Sixth Airborne Division have laboured doggedly and courageously among the wreckage of the King David Hotel. They saved who could be saved. They have brought out the bodies of the dead.

K.D. SEARCH GOES ON

PALESTINE POST STAFF
Sixth Airborne Division sappers in shifts continued throughout Wednesday night and yesterday their arduous and painful task of clearing away the ruins at the corner of the King David Hotel dynamited by terrorists on Monday, and of bringing out the dead.

The rescue workers were furnished with deodorant gas masks. Disinfectants were being sprayed to prevent infection from bodies which had been in the wreckage over three days.

During the night it was an eerie scene under the illumination of arc lamps. The mechanical shovel was scooping up ton after ton of masonry, crumpled woodwork, pieces of concrete pillars, and plaster rubble, and loading them into waiting lorries. Sappers were working with oxy-acetylene

LATEST DEATH ROLL

At midnight last night the official total of casualties from Monday's attack on the King David Hotel were:

Dead: 67
Injured: 47
Missing: 43

New names of dead given:

The Palestine Post, 26 July 1946 Agency Denies White Paper

WHEN NO NEWS IS NEWS

PALESTINE POST STAFF
No news was news last night. Reuter's Jerusalem office reported a three-hour "black-out" on wireless communications between London and Palestine. The Reuter high-speed Hellschreiber system was completely disrupted by atmospheric and London had to be called to repeat news items missed. Nor was the interference confined to Reuter. The BBC's Army Radio Station were unable to relay the P.B.C.'s 8 o'clock news. Outgoing messages to London were also affected. A delay of one hour was reported by the Post Office. The reason: An ionospheric storm.

FLANDIN DEFENDS VICHY REGIM

PARIS Thursday (R). — Pierre Etienne Flandin, former Vichy Foreign Minister, defending himself before the High Court at Versailles on a charge of "national indignity" declared today that he was not pleading a case for himself but for certain of his Vichy colleagues whose election to the present Constituent Assembly had recently been contested on the grounds of their participation in the Vichy Government.

Referring indirectly to former Premiers Paul Reynaud and Edouard Daladier, an

RESISTANCE

The New York Times

26 July, 1946

***PALESTINE CHIEFS DENY
ACCUSATIONS; Challenge
Authenticity of White Paper's Sources-
-Confer on Bombing Crisis More
Detailed Statement Likely Recalls
Action Against Arabs Resignation
Demand Renewed***

Faced with the British Government's White Paper alleging that some officials of the Jewish Agency for Palestine themselves connived with the terrorist organizations responsible for these outrages, community leaders authorized a statement challenging the authenticity of some of the documents on which the British charges are based. A spokesman of the agency said that, *"by adducing a jumble of alleged telegrams stated to have been sent nine months ago, of extracts from broadcasts by the Voice of Israel station and of passages culled from the publications of terrorist groups, the British Government claims to have obtained proof of cooperation between some members of the Jewish Agency and Haganah and of coordination in some cases between Haganah and terrorist bands. Not a single one of the alleged telegrams emanated from the Jewish Agency in Jerusalem. The Jewish Agency, which cannot accept the authenticity of these alleged telegrams, challenges the British Government to prove that the Jewish Agency was responsible for their composition, authorization or dispatch."*

More Detailed Statement Likely

"The executive of the Jewish Agency is giving careful study to this curious collection of alleged telegrams, broadcasts and publications." as A more detailed statement may be issued as a result of the study. Meanwhile some of the questions raised in Zionist quarters are these: Would such astute men Moshe Shertok, Bernard Joseph and Moshe Sneh send incriminating telegrams knowing that they might be intercepted? Why did the British Government wait nine months to act on evidence that, if correct, points to a criminal conspiracy? Will this evidence stand the test of a court trial in which the accused would have the opportunity of defending themselves?

Arab opponents of Zionism accepted the evidence as authentic. In a statement issued today Dr. Hussein Khalidi, secretary of the Arab Higher Committee, said that the "Jewish Agency and all that it stands for must go. It is high time that it become an unlawful association."

Intelligence Blackout?

Following the event, the Signal Service changed its ciphers

- The British lost their ability to read the radio traffic of the Jewish Agency, the Haganah and the Palmach
- The British lost their Main Intelligence source at a crucial period
- The almost only British intelligence source at the time was the local press and the broadcasts of Kol Israel (the Voice of Israel), the Haganah underground broadcasting station
- The British jammed Kol Israel broadcasts from November 1945, but at the end of 1946 priority was given to listening to the broadcasts, and the jamming was stopped.
 - The cover story was that *"The venom of the Voice of Israel was weakened, and as a result the Jammers were instructed to lay-off"* (TNA WO 261/738).

Recovery of the Signal Service after the 'Black Sabbath'

TOP SECRET CREAM, 15 July 1946, 0615, From SLU Clover (Signal Liaison Unit Jerusalem)

TOP SECRET CREAM

To: L.S.I.C. &
SLU CAIRO.

TOO: 150615/7/46

From: SLU CLOVER.

TOR: 161015/7/46

IMMEDIATE

BRAN/YD 603. Personal for ROBERTS repeated.

KELLAR from BURBIDGE. SITREP 47.

12th July inclusive.

1. Political.

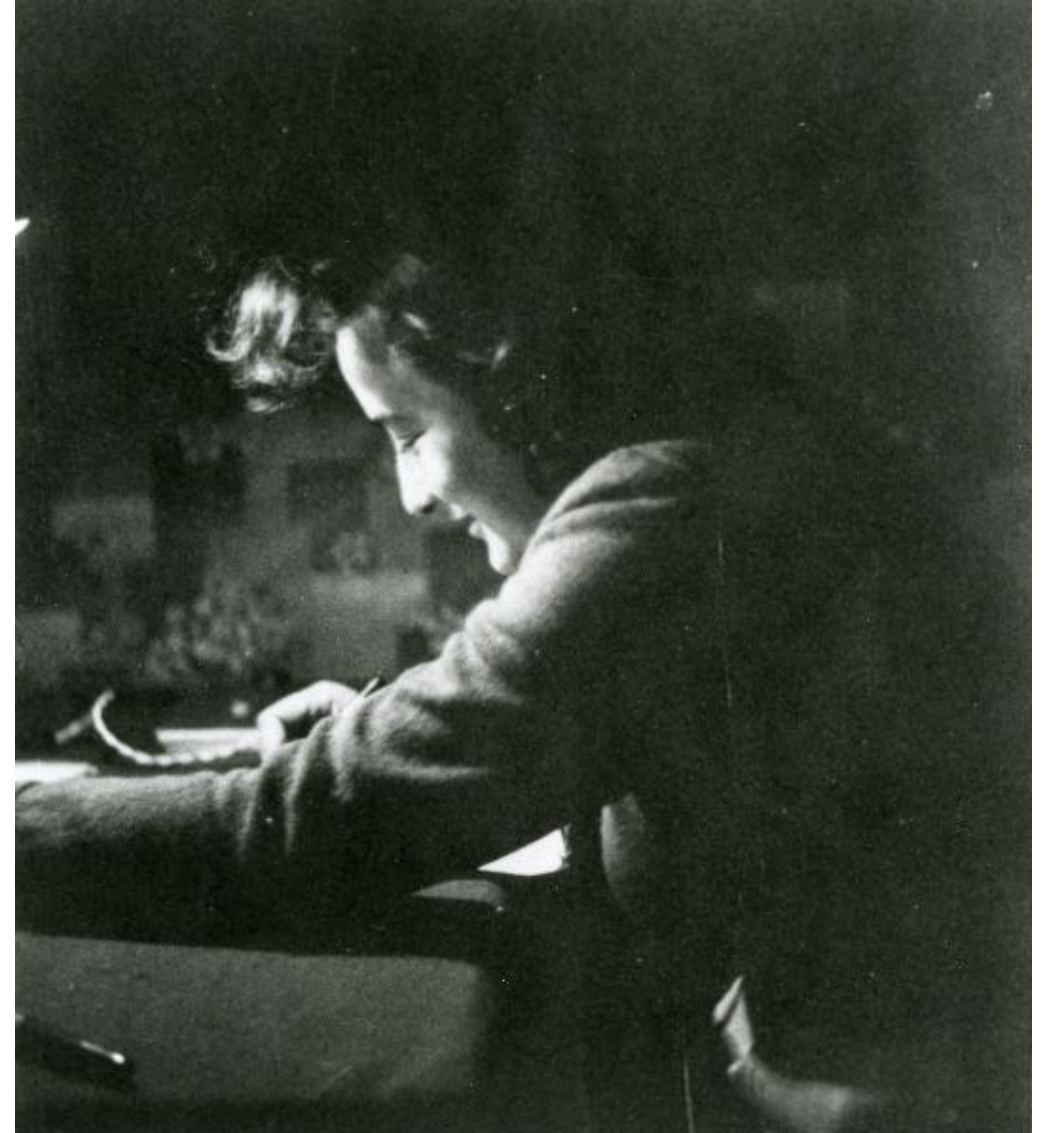
(A) Jewish political picture revealed by SNEH in signal to BEN C confusion. and possible discord between

2. W/T. HAGANA and PALMACH ciphers changed 0001 hours 9th July but illegal immigration network not affected. Changes of pseudonyms and cover terms also taking place in Palestinian system. Documents captured at YAGUR include HAGANA and PALMACH callsign lists, a code and 6 keys. PALMACH W/T course now reassembling.

Gideonim – Signal Service radio operators of the clandestine 'Gideon' radio network, serving the Mossad Le'aliya Bet, Haganah illegal immigration (Ha'apala) arm



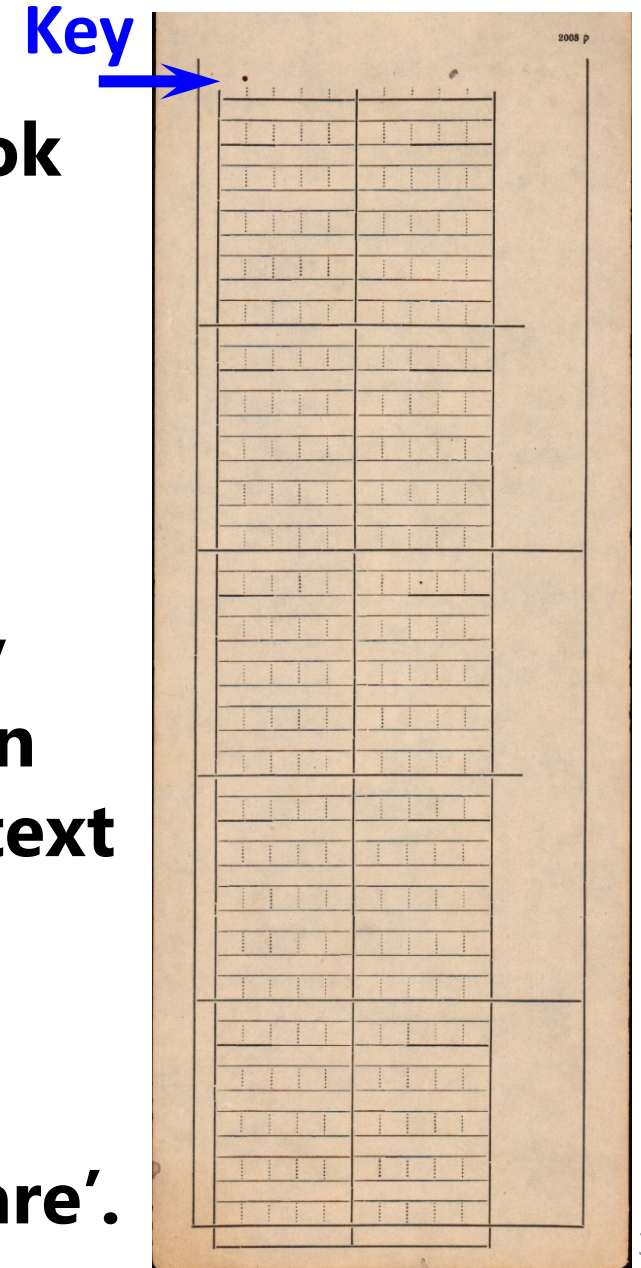
Radio operator aboard ship
Palmach Archive, 11522



Radio operator, Marseille, France, 1946
Palmach Archive, 17142

The Signal Service Changed to Advanced Substitution Cipher

- The key, 10 letters, was taken from an agreed book page or a line from a poem, and was frequently changed.
- The key was written as the top line of the encryption form.
- For transmission, the clear text was written every second line, and the encrypted text was written in the line underneath; in receiving, the encrypted text was written every second line, and the clear text was written underneath.
- Letter substitution was based on a manual calculation method, similar to the 'Vigenère square'.



20 × 20 'Vigenère Square'

Only 20 letters were coded, the letters
 ש, ת, פ, ו, ח & י were not coded.

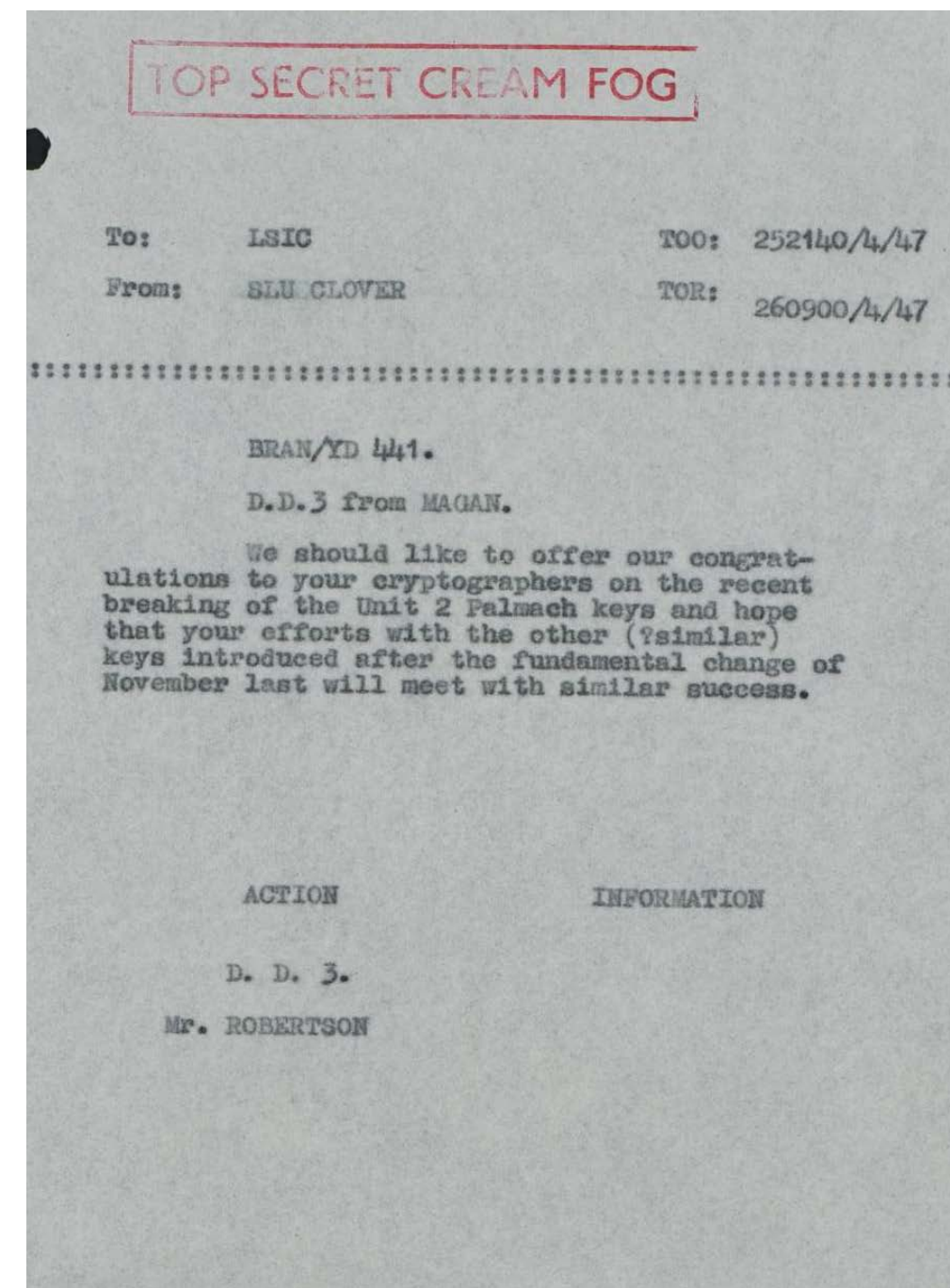
key

ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א	
א	י	ק	צ	פ	ע	ס	נ	מ	ל	כ	ר	ט	ח	ז	ו	ה	ד	ג	ב	א
ב	א	י	ק	צ	פ	ע	ס	נ	מ	ל	כ	ר	ט	ח	ז	ו	ה	ד	ג	ב
ג	ב	א	י	ק	צ	פ	ע	ס	נ	מ	ל	כ	ר	ט	ח	ז	ו	ה	ד	ג
ד	ג	ב	א	י	ק	צ	פ	ע	ס	נ	מ	ל	כ	ר	ט	ח	ז	ו	ה	ד
ה	ד	ג	ב	א	י	ק	צ	פ	ע	ס	נ	מ	ל	כ	ר	ט	ח	ז	ו	ה
ו	ה	ד	ג	ב	א	י	ק	צ	פ	ע	ס	נ	מ	ל	כ	ר	ט	ח	ז	ו
ז	ו	ה	ד	ג	ב	א	י	ק	צ	פ	ע	ס	נ	מ	ל	כ	ר	ט	ח	ז
ח	ז	ו	ה	ד	ג	ב	א	י	ק	צ	פ	ע	ס	נ	מ	ל	כ	ר	ט	ח
ט	ח	ז	ו	ה	ד	ג	ב	א	י	ק	צ	פ	ע	ס	נ	מ	ל	כ	ר	ט
י	ק	צ	פ	ע	ס	נ	מ	ל	כ	ר	ט	ח	ז	ו	ה	ד	ג	ב	א	י
כ	ר	ט	ח	ז	ו	ה	ד	ג	ב	א	י	ק	צ	פ	ע	ס	נ	מ	ל	כ
ל	כ	ר	ט	ח	ז	ו	ה	ד	ג	ב	א	י	ק	צ	פ	ע	ס	נ	מ	ל
מ	ל	כ	ר	ט	ח	ז	ו	ה	ד	ג	ב	א	י	ק	צ	פ	ע	ס	נ	מ
נ	מ	ל	כ	ר	ט	ח	ז	ו	ה	ד	ג	ב	א	י	ק	צ	פ	ע	ס	נ
ס	נ	מ	ל	כ	ר	ט	ח	ז	ו	ה	ד	ג	ב	א	י	ק	צ	פ	ע	ס
ע	ס	נ	מ	ל	כ	ר	ט	ח	ז	ו	ה	ד	ג	ב	א	י	ק	צ	פ	ע
פ	ע	ס	נ	מ	ל	כ	ר	ט	ח	ז	ו	ה	ד	ג	ב	א	י	ק	צ	פ
צ	פ	ע	ס	נ	מ	ל	כ	ר	ט	ח	ז	ו	ה	ד	ג	ב	א	י	ק	צ
ק	צ	פ	ע	ס	נ	מ	ל	כ	ר	ט	ח	ז	ו	ה	ד	ג	ב	א	י	ק
ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	ר	ט	ח	ז	ו	ה	ד	ג	ב	א	ר

Clear

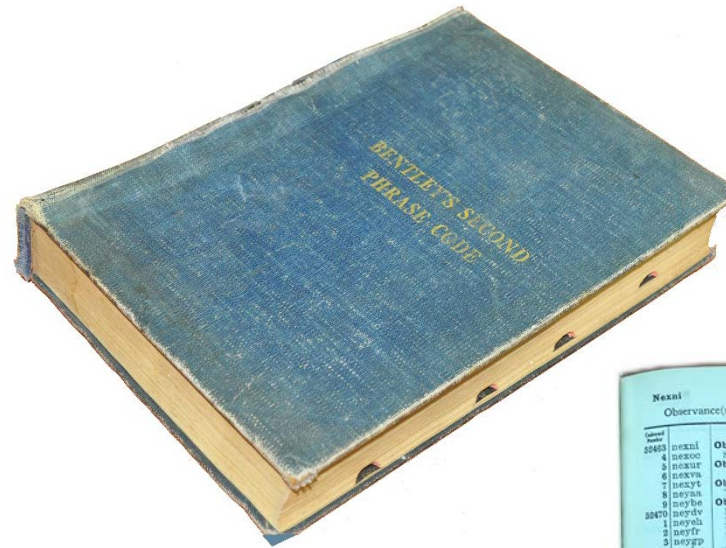
Congratulations to the cryptographers

- Operator errors allowed the British to crack a number of codes, but the intelligence achievement was insignificant.
- The telegram presented, dated April 25, 1947, congratulates the codebreakers for their achievements in deciphering the codes of the Palmach's Second Battalion (under the command of Yitzhak Rabin).



The Jewish Agency Political Department Used the Bentley's Code Book

- Commercial phrase book enabling transmission of five letter groups instead of full sentences, for saving on telegram costs, paid according to number of words.
- Used as a code book by the Government Department of the Jewish Agency for Palestine since late 1946.
 - A daily key number (for example: 41,945) was added to the code book number.



The image shows an open Bentley's Second Phrase Code book. The left page is titled 'Nexni' and the right page is titled 'Neyih'. Both pages contain a grid of code groups and their corresponding meanings. The code groups are listed in the left margin of each page, and the meanings are listed in the right margin. The book is open to a page showing code groups for 'Observance(s)' and 'Occurrence(s)'. The code groups are listed in the left margin, and the meanings are listed in the right margin. The book is open to a page showing code groups for 'Observance(s)' and 'Occurrence(s)'. The code groups are listed in the left margin, and the meanings are listed in the right margin.

Observance(s)	Occurrence(s)
00001 nexni	00001 nfon
00002 nexni	00002 nfon
00003 nexni	00003 nfon
00004 nexni	00004 nfon
00005 nexni	00005 nfon
00006 nexni	00006 nfon
00007 nexni	00007 nfon
00008 nexni	00008 nfon
00009 nexni	00009 nfon
00010 nexni	00010 nfon
00011 nexni	00011 nfon
00012 nexni	00012 nfon
00013 nexni	00013 nfon
00014 nexni	00014 nfon
00015 nexni	00015 nfon
00016 nexni	00016 nfon
00017 nexni	00017 nfon
00018 nexni	00018 nfon
00019 nexni	00019 nfon
00020 nexni	00020 nfon
00021 nexni	00021 nfon
00022 nexni	00022 nfon
00023 nexni	00023 nfon
00024 nexni	00024 nfon
00025 nexni	00025 nfon
00026 nexni	00026 nfon
00027 nexni	00027 nfon
00028 nexni	00028 nfon
00029 nexni	00029 nfon
00030 nexni	00030 nfon
00031 nexni	00031 nfon
00032 nexni	00032 nfon
00033 nexni	00033 nfon
00034 nexni	00034 nfon
00035 nexni	00035 nfon
00036 nexni	00036 nfon
00037 nexni	00037 nfon
00038 nexni	00038 nfon
00039 nexni	00039 nfon
00040 nexni	00040 nfon
00041 nexni	00041 nfon
00042 nexni	00042 nfon
00043 nexni	00043 nfon
00044 nexni	00044 nfon
00045 nexni	00045 nfon
00046 nexni	00046 nfon
00047 nexni	00047 nfon
00048 nexni	00048 nfon
00049 nexni	00049 nfon
00050 nexni	00050 nfon
00051 nexni	00051 nfon
00052 nexni	00052 nfon
00053 nexni	00053 nfon
00054 nexni	00054 nfon
00055 nexni	00055 nfon
00056 nexni	00056 nfon
00057 nexni	00057 nfon
00058 nexni	00058 nfon
00059 nexni	00059 nfon
00060 nexni	00060 nfon
00061 nexni	00061 nfon
00062 nexni	00062 nfon
00063 nexni	00063 nfon
00064 nexni	00064 nfon
00065 nexni	00065 nfon
00066 nexni	00066 nfon
00067 nexni	00067 nfon
00068 nexni	00068 nfon
00069 nexni	00069 nfon
00070 nexni	00070 nfon
00071 nexni	00071 nfon
00072 nexni	00072 nfon
00073 nexni	00073 nfon
00074 nexni	00074 nfon
00075 nexni	00075 nfon
00076 nexni	00076 nfon
00077 nexni	00077 nfon
00078 nexni	00078 nfon
00079 nexni	00079 nfon
00080 nexni	00080 nfon
00081 nexni	00081 nfon
00082 nexni	00082 nfon
00083 nexni	00083 nfon
00084 nexni	00084 nfon
00085 nexni	00085 nfon
00086 nexni	00086 nfon
00087 nexni	00087 nfon
00088 nexni	00088 nfon
00089 nexni	00089 nfon
00090 nexni	00090 nfon
00091 nexni	00091 nfon
00092 nexni	00092 nfon
00093 nexni	00093 nfon
00094 nexni	00094 nfon
00095 nexni	00095 nfon
00096 nexni	00096 nfon
00097 nexni	00097 nfon
00098 nexni	00098 nfon
00099 nexni	00099 nfon
00100 nexni	00100 nfon

**The British succeeded in
continuing to decipher
the messages of the
Mossad for Aliyah Bet**

XP Messages from 'Ha'apala' Vessels

- **Illegal immigrant ships transmitted an 'XP message' every several hours, in which they indicated their position, direction and speed of movement, in a fixed format.**
- **These messages were intercepted and deciphered by the British, and were the main source of intelligence for the 'Palestine Patrol'.**
- **These messages presented the British with a limited challenge: fixed format, numerals only content (no need for translation from Hebrew to English).**

XP Messages - Examples

אל: גליצות		מאת: דלת חללי גשר	
29.12.	האני	0680	לדב
39 39	פני	25 48	מסמ
184	קניס	100	מכיל
ב"ח		יב	

ע"י	שעה	יום	מ	
גליצות	1530	29.12.	א	נכתב
			א	נתקבל
				נמסר

2300

מסמ

19/2

א

19

1900

4004

1300

127

050

2

XP message sent from the ship 'Yod Dalet Halaley Gesher Haziv' in July 1946, as received in Tel Aviv.

Haganah Archive, 14/232

XP message sent from the ship 'Kibbutz Galuyot' in December 1947 and delivered to Tel Aviv via Italy, as received in Tel Aviv.

Haganah Archive, 14/275

British Lancaster GR111 observation plane follows the Ha'apala ship 'Lochamei Hagetatot'

- 'Lochamei Hagetatot' set sail from Italy on May 13, 1947 with 1,457 illegal immigrants.
- The British captured the ship in a fierce battle that lasted several hours, using water jets and tear gas.
- The ship was towed to Haifa and the immigrants were deported to Cyprus.
- Photo taken on May 23, 1947, from the deck of the British destroyer HMS Brissenden.



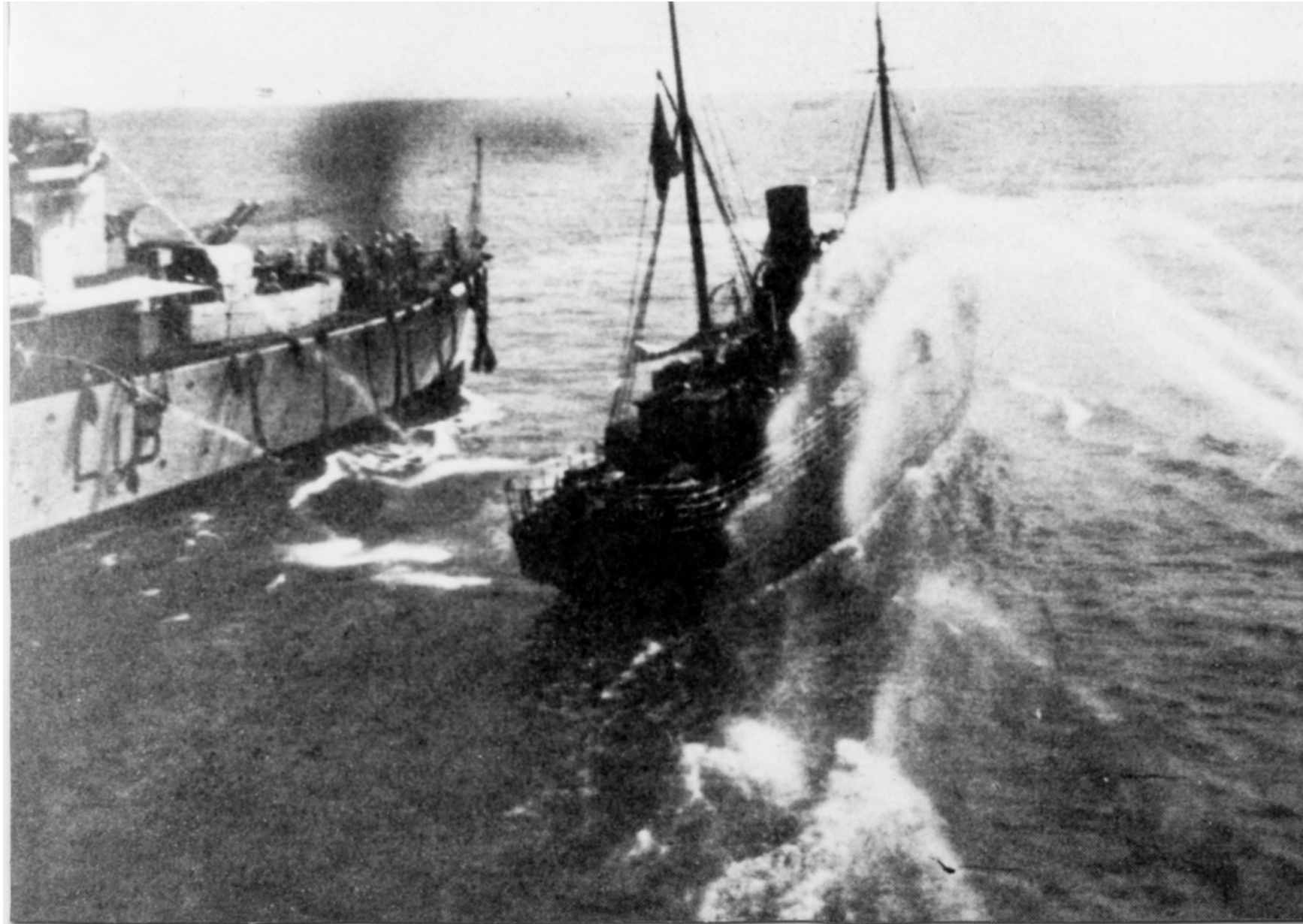
Capture of 'Hatikvah'

- British destroyer HMS Venus capturing the illegal immigrant ship 'Hatikva' on 17 May 1947, north of Rosh Hanikra.
- The ship, that sailed from Italy on May 8, 1947 with 1,414 illegal immigrants, surrendered after a fierce battle, in which the British used water cannons (pictured) and tear gas.



Capture of 'Yehuda Halevy'

- 'Yehuda Halevy' sailed from Algiers in May 1947, with 399 illegal immigrants
- On May 31, off the coast of Israel, British destroyers rammed the ship and took control of it, spraying jets of water and using tear gas
- The ship was towed to the port of Haifa and the immigrants were deported to Cyprus



The Drama of the 'Pans' (Pan York, Pan Crescent)

- **The 'Pan' ships, 'Kibbutz Galuyot' and 'Atzmaut', were the largest of the Ha'apala ships, carrying a total of 15,236 illegal immigrants, an impressive statement of the organization's capability**
 - At the same time, the struggle over the partition plan was being waged at the United Nations.
- **The ships set sail from Burgas, Bulgaria, on December 27, 1947.**
- **On the orders of the political leadership, the ships avoided a confrontation with the British and followed the British directly to Cyprus.**
 - The fear was that a confrontation with the British would sabotage the effort to implement the November 29 resolution.
- **Ben-Gurion's order was sent to the ships by a ciphered message.**

The Drama in the Messages

- **David Ben-Gurion sent a message to Yossi Harel, the Haganah commander, aboard the Pan York :**
"if the enemy proposes to the two great [Pan ships] to go straight to Cyprus, you must answer and do: 'We have turned to the Land of Israel, which was promised by God to Israel and reaffirmed by the United Nations, but if you intend to interfere with our journey, we will go to Cyprus, being sure that we will soon reach our liberated land. Give us the course to Cyprus and we'll follow you'.
- **The message was sent to the Mossad for Aliyah Bet HQ in Italy on December 29, 1520, resent on December 29, 1550**
- **The message was relayed through the Mossad station in Italy; the message reception by the Pan ships was delayed almost 24 hours due to communications difficulties.**

The British admiral knew about Ben-Gurion's message before Yossi Harel, the Haganah commander

- **On Monday, December 30, 1944, Rear-Admiral Simonds-Tayler, the British Squadron commander, aboard the light cruiser HMS Mauritius, received the following message from the British Military Commander in Palestine, classified as "Top Secret":**
"received from reliable high level source that the Jewish Agency have wirelessed instructions to the Pan. ships that requests or orders issued by Royal Navy including diversion to Cyprus are to be obeyed..."
- **Was the source of the British information the interception of the message sent from Tel Aviv to Italy, 23 hours earlier, and the deciphering its content?**
- **This information had a decisive impact on the conduct of the British Navy.**
- **The British believed that taking control of the ships by force, without material damage and many losses, was almost impossible, and therefore they gave the squadron commander freedom of action to avoid confrontation.**

Pan's Messages

[illegible]

The British and the Mossad for Aliyah Bet used Greenwich Mean Time (GMT).

151

DISTRIBUTION OF THIS MESSAGE IS TO BE LIMITED TO
THOSE OFFICERS WHO ARE CONCERNED WITH ITS CONTENTS

TOP SECRET

IN

WARNING : This is an unparaphrased version of a secret cypher or confidential code message, and the text must first be paraphrased* if it is essential to communicate it to persons outside British or Allied Government Services.

(*NOTE : Messages shown as having been sent in a One-Time Pad :
"O.T.P." are excepted from this rule.)

301430B/December

Date 30.12.47.

Rec'd 1424

From COMPAL

~~SECRET~~

To: C in C. Med., C.S.I.
Info: Admiralty

IMMEDIATE

Statement now received from reliable high level source that Jewish Agency have wirelessly instructions to Pan. ships that requests or orders issued by Royal Navy including diversion to Cyprus are to be obeyed. Agency have reiterated these instructions and are confident of compliance also of peaceful disembarkation in Cyprus.

2. Suggestion has been advanced that in view of high morale and hysteria of passengers propaganda matter should be very delicately handled and backed by a strong show of force. Matter could now be broached at C.S.I.'s inclination.

3. Army acting on info in para.1 are sending necessary reinforcements to arrive Famagusta a.m. 31st Dec. so that acceptance of situation by Cyprus Government is now to be taken for granted as this makes up the only deficiency complained of. Confirmation of their formal assent will however be communicated when known to authorities addressed.

301430B

1st Lord
1st S.L.(3)
V.C.N.S.
A.C.N.S.
U.S.S.
D.O.D.(4)
D.C.(2)
D.N.I.(4)
Ha. of I.(8)
D of P.(2)
D of P.(0) (2)
G.N.I.(2)

53
32
35

CC.
47.

TNA, ADM 1/20793

Summary

British intelligence superiority was based on deciphering the Haganah ciphers

- **The British decoded the Haganah's ciphers as early as 1939, and from 1942 onwards. The Haganah's radio traffic was the main source of British intelligence**
- **The British 1946 White Paper, whose purpose was to prove that the Jewish Agency was a terrorist organization, led to the changing of the Haganah ciphers, and the British found themselves in an "Intelligence Blackout"**
- **The main achievement of the British after that was to break the ciphers of the Mossad for Aliyah Bet (Gideon radio network), running illegal immigration activities**
 - The radio communication of the illegal immigrant ships was the British main information source; deciphering these transmissions led to seizing of most of the illegal immigrant ships.

Since activation of the Palestine Patrol in September 1945, only six of the 57 illegal immigrant ships managed to break the British naval blockade

● **Hannah Szenesh**

- Due to a malfunction, there was no radio traffic to the ship. Communication was renewed only prior to landing.

● **Shabtai Luzinsky**

- Sailed in 'wireless silence', radio communication was activated only prior to landing,
- The ship was intercepted by a British plane, but the immigrants landed on Nitzanim Beach before the British fleet arrived.

● **Aliyah**

- Due to a malfunction, there was no radio communication to the ship. Communication was renewed only prior to landing
- The ship was intercepted by a British plane, but a British destroyer 'confused' it with the ship Kadima, which sailed nearby and was seized.

● **Hachayal Haivri, Amiram Shochat, Haportzim**

- British destroyers intercepted the ships at sea, but they were not identified as illegal immigrant ships.

The ciphers underwent a fundamental transformation after the establishment of the State of Israel

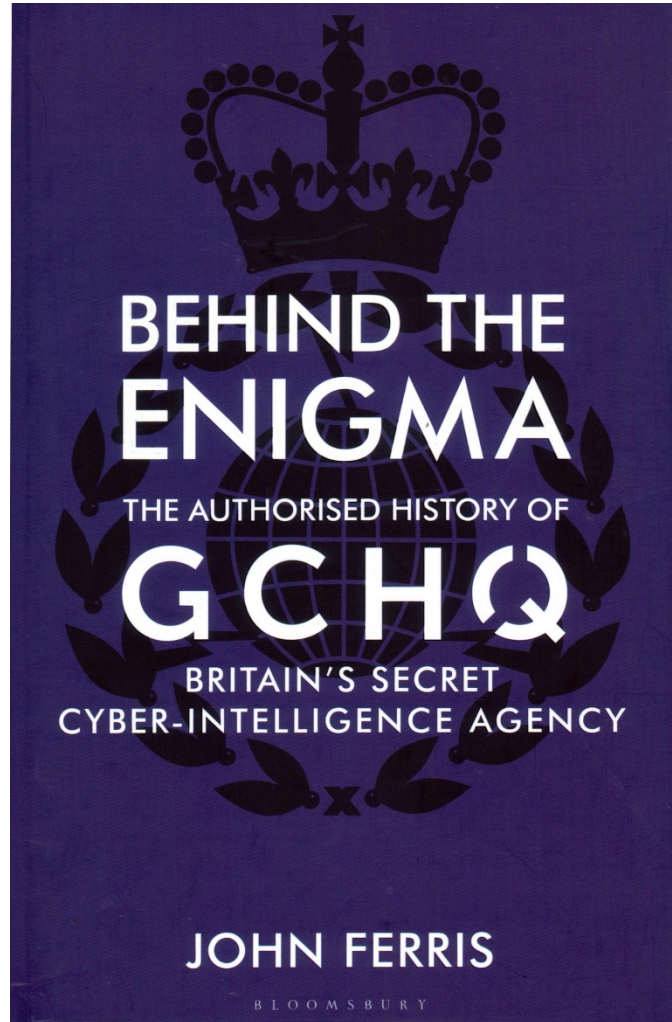
- **Jewish experts were recruited from South Africa, and laid the foundations of communication security in the IDF:**
 - Shaul Bar-Levav.
 - Meir Shapira.
- **In October 1948, the Haganah's ciphers were abolished, and new ciphers were put into use.**
- **A special unit was established for cipher and cipher keys production.**

The conclusions: once bitten, twice shy

- **Intelligence superiority is important, but it is not the be-all and end-all.**
- **One who trusts ciphers, puts his life in its hands.**
- **Trust in ciphers should be limited, in the sense of "respect him and suspect him".**

Additional Information

John Ferris, *Behind the Enigma: the Authorised History of GCHQ, Britain's Secret Cyber-Intelligence Agency*, Bloomsbury, 2020



Daniel Rosenne, *British Intelligence Superiority: Breaking Haganah Ciphers, The Association for the Commemoration of the Fallen Soldiers of the IDF Signal Corps*, 2024 (Hebrew)

https://www.amutakesher.org.il/Uploads/dbsAttachedFiles/British_Intel_Superiority_1.0.pdf



Thanks

© The Association for the Commemoration of the Fallen Soldiers
of the IDF Signal Corps, Yahud-Monoson, Israel, 2025

www.amutakesher.org.il