March 2026

British Intelligence Superiority in Palestine and Its Reliance on Breaking Haganah Ciphers, 1942-1948

Daniel Rosenne*

Abstract

In the final years of the British Mandate in Palestine, 1942 – 1948, British intelligence achieved clear superiority over the Jewish underground by intercepting the Jewish radio networks and breaking the Jewish ciphers. The British established a special mechanism for intercepting the transmissions, deciphering, then translating the contents into English, and distributing the high-quality intelligence to a limited number of confidants.

Political pressure from a vocal pro-Zionist opposition in the British Parliament and hostile public opinion in the United States led British Prime Minister Clement Attlee to order the publication of a "White Paper" denouncing the Jewish Agency — which had denied responsibility for the Jewish resistance movement — as a terrorist organization, based on intercepted and deciphered telegrams of the Agency's political department. The publication occurred despite opposition from the High Commissioner for Palestine, British military commanders, and the British Security Service MI5. The "White Paper" was published on 24 July 1946. The publication did not yield a political achievement for the British but stunned the Jewish resistance movements and the Political Department of the Jewish Agency, and made them instantly change their ciphers. The British intelligence source was "blown", cut off, and the British were "left in the dark".

The main British achievement after July 1946 was breaking the ciphers of the "Gideon" radio network, serving the Mossad LeAliyah Bet, responsible for Jewish illegal immigration, and tracking illegal immigrant vessels by intercepting the vessels' radio traffic. The intelligence obtained in this manner was essential for the success of the British efforts (the "Palestine Patrol") to intercept the illegal immigration vessels, and without it, most of the illegal immigration vessels would have reached their destination, thereby shaping the political constraints of the Palestine Mandate regime in a different way.

* Thanks to Prof. Yigal Shefi for his assistance with this research.
Translation of the original 2024 Hebrew paper. Language Editing: Zippi Rosenne. English Translation: Moshe Rubin.

© Copyright by the Association for the Commemoration of the Fallen Soldiers of the IDF Signal Corps, Yehud-Monoson, Israel, 2026
https://www.amutakesher.org.il

Woe unto them that seek deep to hide their counsel from the LORD, and their works are in the dark, and they say, Who seeth us? and who knoweth us?

Isaiah 29:15

Introduction

Documents in British archives, released for public access in recent years, present evidence of clear British intelligence superiority over the Jewish Yishuv in the final years of the British Mandate in Palestine, based on the interception of the Haganah, Palmach, Mossad LeAliyah Bet, and the Political Department of the Jewish Agency radio traffic,[1] and the success of the British GCHQ (Government Communications Headquarters) in breaking their ciphers. This radio traffic — encrypted messages transmitted in Morse code over high-frequency radio networks — was an "open book" to the British intelligence.

The complex political reality of the final years of the British Mandate in Palestine limited the British ability to leverage this intelligence superiority. The main British achievement based on this intelligence was the interception of illegal immigrant vessels. Without this intelligence, most of the illegal immigrant vessels would have reached their destination.

This article presents the British intelligence achievement, its exposure by the British in 1946, and its consequences.

The Haganah Signal Service

The outbreak of the Great Arab Revolt in the years 1936 – 1939 intensified the Haganah's communication needs and accelerated the necessity for an efficient communication system between the Jewish settlements. Radio communication, a new and developing technology of those days, was much more efficient than visual signaling methods (flags, signaling lamps, and heliographs). Therefore, the Haganah leadership decided to harness radio technology to defend the Yishuv. In late 1936, Haganah leadership — Eliyahu Golomb, Dov Hoz and Shaul Meirov (Avigur) — tasked Simcha Even-Zohar with establishing a Haganah communications unit, the "Signal Service", which was established in April 1937. The Signal Service began developing radio communications, and within a short time radio became the primary means of Haganah communication.

[1] Yishuv (in Hebrew – *settlement*) is the term used for the Jewish community in Mandatory Palestine before the establishment of the State of Israel; Haganah (in Hebrew – *defense*) was the main Jewish underground paramilitary organization during the British Mandate of Palestine (1920-1948), precursor to the Israel Defense Forces (IDF); Palmach was a permanently mobilized elite strike force of the Haganah, established in 1941; Mossad LeAliyah Bet, established in 1939, was the Haganah arm responsible for illegal immigration to Palestine during the British Mandate.

With great effort, despite significant difficulties, the Signal Service established clandestine high-frequency (HF) radio communications networks based on homemade CW (Continuous Wave) transmitters and receivers, radio operators training organization, and a cipher system. It maintained radio communication using Morse code. The radio network developed gradually. Initially, the focus was on creating reliable radio links between the main headquarters in Tel Aviv, Jerusalem and Haifa. Later, communication expanded to settlements across Palestine, forming the "Amnon" radio network, later renamed "Avinoam." In the "Homa u'migdal" operations,[2] beginning with the establishment of Kibbutz Hanita in March 1938, clandestine radio communication was established in all new settlements; visual signaling, intended for administrative communication, served as a cover for the radio communication, the very existence of which was secret (ZEX – "Top Secret" in the slang of the time). The network developed gradually: in 1937, 12 fixed radio stations operated; in 1939, 38 stations;[3] by the end of 1947, 184 stations were in operation.[4]

British censorship restrictions necessitated the establishment of an independent radio communication link between the Jewish Agency Headquarters in Palestine and the Agency's political department in London. The Signal Service built a powerful shortwave transmitter, concealed in an underground bunker at Kibbutz Gvat, and operated a secret receiving station in London, thus maintaining a continuous secret link from Palestine to London beginning in July 1939. The shortwave transmitter, named "Station Sarah", transmitted one-way Morse messages, each message was sent several times, and message reception was confirmed by a regular telegram via the post office.[5] Due to the expansion of British Royal Air Force activity at Ramat David and concern of the station's discovery, it was relocated in 1943 to Tel Aviv.

At the beginning of 1941, following the successful German offensive in Libya under the command of General Erwin Rommel, that brought German forces to the Egyptian border, the threat to the Jewish Yishuv in Palestine from Vichy forces (the puppet regime in France under Nazi German control) in Syria and Lebanon, and the anti-British revolt in Iraq, the Haganah reorganized and the "Shituf" (cooperation) was established — a collaboration between the Haganah and the British. Approximately thirty thousand men and women of the Yishuv enlisted in the British military services. The Palmach (Plugot Mahatz – Strike Companies), funded by the British, was established as a local underground organization that would carry out

---

[2] A Zionist settlement operation, setting 57 new settlements, based on the Ottoman law that buildings erected in one night didn't require a building permit and couldn't be demolished by the authorities.

[3] During this period, the stations were referred to as "libraries." A male radio operator was called "brother" and a female operator "sister."

[4] Daniel Rosenne, *The Haganah Signal Service*, The Association for the Commemoration of the Fallen Soldiers of the IDF Signal Corps, April 2022 (Hebrew).

[5] Daniel Rosenne, *Sara Station - Clandestine HF Wireless Station, 1939*, The Association for the Commemoration of the Fallen Soldiers of the IDF Signal Corps, October 2021.

sabotage operations behind enemy lines should the Germans occupy Palestine. A clandestine radio communications network was established for Palmach use, in cooperation with the British.[6] Haganah forces participated in intelligence and sabotage operations in preparation for the British invasion of Lebanon and Syria (Operation Exporter, June–July 1941).[7] By order of the Haganah General Staff, the Signal Service cooperated with the British. Its personnel established and operated a clandestine broadcasting station in Haifa — "Voice of Free France" (operating from September 1940 until June 1941, when it was relocated to Beirut). They also participated in preparatory activities for the British invasion of Syria and Lebanon and manufactured spy radio sets for use by the British Special Operations Executive (SOE). In late 1942, after the British succeeded in thwarting the German threat, the military cooperation with the British ceased, as the British viewed the Haganah as a factor threatening their interests.

Initially, the Palmach used the "Avinoam" radio network; however, the traffic load following its mobilization in June 1942 necessitated splitting into a separate network. "Tamar", the Palmach's radio network, began operating in the summer of 1942.



Radio operator Rachel Yaakobi operates a clandestine Haganah radio station at Kibbutz Dorot, 1948.
Courtesy of the Government Press Office, National Photo Collection, D285-029.

[6] The period from spring 1942 until 4 November 1942, during which the British under General (later Field Marshal) Montgomery defeated the Germans in the Second Battle of El Alamein, was called "The 200 Days of Dread."

[7] Reuven Shiloah files, *transmitters, 1941-1942*, Central Zionist Archives (hereinafter: CZA) S25\22463.

In addition to the "Avinoam", "Tamar", and "Sarah" radio networks, the Signal Service operated the "Gideon" radio network, serving the Mossad LeAliyah Bet in its clandestine illegal immigration operations. In 1945, the Signal Service assumed responsibility for operating this network, established 24 fixed stations in Europe and Arab countries, and maintained radio communication with the illegal immigration vessels.[8]

The fixed radio stations used equipment built in clandestine workshops, operated in Morse code in the high-frequency band (2 to 12 MHz) using three-letter callsigns and international communication procedures.[9] These stations transmitted at low power (usually about ten watts) with simple antennas (long wire), transmitted and received on different frequencies – unlike modern military radio networks, which typically transmit and receive on the same frequency – thus allowing the network manager station to operate efficiently with multiple stations. Communication was conducted during a predetermined schedule, several times throughout the day (during periods of security tension, the network manager stations operated 24 hours a day). The activity was clandestine and kept under strict security, and the covert radio stations were carefully concealed.

Radio traffic was carried out using messages ("memoranda", in the terminology of the time). Almost all messages transmitted over the radio networks were encrypted. Encryption and decryption were performed manually. Encrypted messages were transmitted in five letter groups. Initially, the Signal Service used the Mandate Police encryption methods, but at an early stage it transitioned to encryption methods used by the Yugoslav Army (see Appendix A), which were based on letter transposition.[10] The Haganah commanders regarded the encryption as secure and reliable.

The Political Department of the Jewish Agency used a civilian codebook, Bentley's Phrase Code. This was a "commercial code" based on transmitting five-letter codes instead of sentences, to reduce the financial cost of telegrams, as the tariff for sending telegrams was based on word count. It was enciphered by shifting each five-letter code according to a prearranged scheme that changed for each telegram. [11]

---

[8] Daniel Rosenne, *Gidonim: Wireless Operators in the Service of the Emerging State*, The Association for the Commemoration of the Fallen Soldiers of the IDF Signal Corps, 2nd ed., 2018 (Hebrew) (hereinafter: Rosenne, *Gidonim*).

[9] Daniel Rosenne, *Hebrew Morse*, The Association for the Commemoration of the Fallen Soldiers of the IDF Signal Corps, October 2018 (Hebrew).

[10] The Yugoslav cipher knowledge came from Eli Schwartz, a member of Kibbutz Afikim, who served as a Signal officer in the Yugoslav Army.

[11] Daniel Rosenne, *Bentley Code Book Cipher*, The Association for the Commemoration of the Fallen Soldiers of the IDF Signal Corps, January 2024 (Hebrew).

British Communications Intelligence (COMINT)

From recently declassified British archival material, it becomes clear that the British held absolute superiority over the Haganah in communications intelligence (COMINT).[12]

The British intercepted the radio networks operated by the Haganah Signal Service in order to address potential threats. The British Radio Security Service (RSS) monitored communications in Britain and across the Empire, searching for signs of subversion and espionage. Its branches in Palestine and Egypt, known as Middle East Radio Security (MERS), operated at the Sarafand camp (Wireless Hill, today's Gideonim Camp) and at the Sidi Bishr camp near Alexandria, and intercepted the radio networks of the Haganah, the Palmach, the Mossad LeAliyah Bet, and the Jewish Agency. The intercepted messages were sent to London for decryption and for translation of the content from Hebrew to English.

This signal interception activity was carried out during the war and up to 21 June 1946, when the unit was closed and the operation was transferred to Cyprus. The MERS unit numbered 35 personnel when it was consolidated in Cyprus.



MERS operator at the Sidi Bishr camp, near Alexandria.

Ray Wright collection, courtesy of GCHQ.

[12] John Ferris, *Behind the Enigma: The Authorised History of GCHQ, Britain's Secret Cyber-Intelligence Agency*, Bloomsbury Publishing, London, 2020, pp. 554–580 (hereinafter: Ferris, *GCHQ*).
Signals Intelligence (SIGINT) refers to intelligence derived from communications and electronic emissions. It includes Communications Intelligence (COMINT), obtained from intercepting adversary communications, and Electronic Intelligence (ELINT), derived from non-communication electromagnetic emissions.

Apparently, the British broke the Haganah ciphers as early as 1939, but during the period in which the Haganah cooperated with them, British use of this intelligence was limited. However, the situation changed in 1942. In an entry dated 23 September 1942 in the diary of Guy Liddell, then head of Counter Espionage in the British Security Service (known as MI5), who in 1945 was appointed Deputy Director General of the Security Service, it is noted that the information was of great assistance: "They [the intercepted Zionist telegrams] had been of considerable assistance to him [Alexander Kellar, a senior intelligence officer in MI5, the British Security Service, who, among other things, dealt with the Jewish Yishuv in Palestine and headed the Security Intelligence Middle East (SIME) in Cairo from December 1946 to 1948] on Zionist matters".[13] The diary entries from 1944 refer to intelligence obtained from deciphering Haganah ciphers, and to two ciphers designated ISPAL 1 and ISPAL 2 (ISPAL – Intelligence Service Palestine). In the diary entry of 26 September 1944, a meeting with the High Commissioner, Field Marshal John Vereker Lord Gort, is described, and a difficulty is noted in deciphering the cipher or in translating from Hebrew to English ("we had so much trouble about this project").[14]

In 1943, the British Foreign Office determined that "It will be of prime importance to obtain reliable secret intelligence about Zionist activities", particularly "the Jewish Agency's contacts with foreign governments and the Jewish Agency's efforts (if any) to establish good relations with the Arabs".[15] As a result, the Haganah networks were designated a preferred target. The Yishuv's cipher designation was changed from ISPAL to OATS and ISTRIA (OATS was the Haganah's cipher, ISTRIA was the Jewish Agency's cipher).[16] Another source was BUTTERCUP, the wiretapping of the telephone lines of Zionist institutions and of the Haganah.[17] Later, the designations CREAM, GLINT, and FOG were used.

The translated information was distributed to a few security indoctrinated confidants in London and transferred to Cairo and Jerusalem for intelligence processing and dissemination to indoctrinated confidants who had received special "clearance" to review the material. The work of deciphering the Jewish ciphers and translating into English was carried out by a unit under the command of Captain Hastings, Deputy Director for Diplomatic Intelligence (DD2, later DD3), that operated from offices on Berkeley Street, and in 1946 moved to Chesterfield Street in London, kept compartmentalized from other GCHQ bodies.[18]

---

[13] *Liddell Diaries*, Volume 6, The National Archives (hereinafter: TNA) KV 4/190, notes 23 September 1942.

[14] *Liddell Diaries*, Volume 9, TNA KV 4/193, notes 21 December 1943, 11 February 1944, 7 March 1944; *Liddell Diaries*, Volume 11, TNA KV 4/195, notes 26 September 1944, 9 December 1944.

[15] *Bland Committee Report – Future Organization of the S.I.S.*, October 1943, TNA CAB 301/48, p. 27.

[16] *Diary of Guy Liddell*, Deputy Director General of the Security Service, June to November 1945, TNA KV 4/466, notes 2 August 1945.

[17] *Robertson Report – Visit to S.I.M.E and its outstations in the Middle Ea*st, April – June 1947, TNA KV 4/438.

[18] The GCHQ codebreaking center at Bletchley Park employed many Jews, who openly expressed their Zionist sympathies and openly established a Zionist cell. Robert Hannigan, *The Secret Story of the Jewish Codebreakers Who Helped Win World War II*, the Jewish Chronicle, 26 January 2017.

British codebreakers did not find it difficult to deal with Haganah ciphers, as its radio networks used simple procedures and ciphers and encryption methods and keys that did not change frequently. Moreover, its personnel tended to send many messages, which facilitated the deciphering. Understanding the content of the messages proved more difficult than deciphering the messages. Apart from Jews, there were few British subjects who understood modern Hebrew; only those with Zionist affiliation understood the spoken language,[19] and this raised the question of loyalty. Until 1945, the British and the Zionists were allies, and GCHQ could rely on British Jews,[20] but the situation changed. From 1945, military and intelligence authorities refrained from employing Jews in London for work related to Palestine, as employing them against their own people raised questions of fairness and security, and apparently Arabs who knew Hebrew were employed in London for the purpose of translation from Hebrew to English.

In 1939, the British Security Service MI5, in cooperation with the British Intelligence Service MI6, established a counter-espionage body in Cairo, called Security Intelligence Middle East (SIME), with branches in Cyprus, Baghdad, and Jerusalem. The branch in Jerusalem was called DSO (Defence Security Officer). It was headed by Lieutenant Colonel Henry Hunloke,[21] followed by Lieutenant Colonel Sir Gyles Isham,[22] who in late 1946 was replaced by Lieutenant Colonel William Magan.[23] Intelligence dissemination in Palestine was carried out through the DSO in Jerusalem, who was also the main figure analyzing the information obtained from this interception and from other sources. The DSO had unique and exceptional powers compared to any other figure in British intelligence. He was the chief analyst of communications intelligence and human intelligence, including material from the Criminal Investigation Department (CID) and military intelligence. In addition, he advised political and military authorities on intelligence, security, and counterterrorism matters, and directed

[19] Ferris, GCHQ, p. 558.

[20] Before 1946, GCHQ was known as the Government Code & Cypher School.

[21] Henry Hunloke (1906–1978). Elected to Parliament in 1938 as a Conservative MP for West Derbyshire. Until March 1944, the DSO in Palestine was denied access to decrypted intelligence due to concerns about information security in Palestine. The final obstacle to sharing the information was suspicion that Hunloke had a romantic relationship with a Jewish woman. *Liddell Diaries*, Volume 9, TNA KV 4/193, notes 1943: 21 December; 1944: 11 February, 7 March.

[22] Giles Isham (1903–1976), 12th Baron of Lamport, graduate of Magdalen College, Oxford, known as a stage and film actor. Joined the British Army during WWII, commissioned in 1940, served as an infantry officer in the Western Desert campaign. Promoted to Lieutenant Colonel in 1943. After serving as DSO in Jerusalem, continued in MI6 in Britain and later held various public roles in Northamptonshire, England.

[23] Bill Magan (1908–2010), born in Ireland, graduate of Sandhurst Military Academy. Commissioned in 1928, served as a cavalry officer in India. Fluent in several languages, including Persian. Transferred to British intelligence in 1939, established a spy network in Persia in preparation for a possible Nazi invasion, later engaged in counterintelligence in Persia, India, and Afghanistan, and ran a double agent in the German embassy in Kabul. In 1948, after serving as DSO in Palestine, became head of SIME in Cairo and was promoted to Brigadier. In 1951, appointed head of a department in MI5, responsible for counterintelligence in Cyprus, Aden, Malaya, Kenya, and Nyasaland (now Malawi). Retired in 1968 and managed the family farm in Kent. Authored several books, including a memoir of his intelligence service from 1939 to 1948.

warships and aircraft intercepting illegal immigrant ships. The DSO maintained a card index of individuals, units, vessels, locations, and traffic.

In April 1947, the unit dealing with intelligence obtained from the deciphering of Haganah messages in the DSO office numbered nine people — four officers, a corporal, and four women. These individuals processed information and dealt with a broad category of communications intelligence, in intelligence production and in handling specific operations. The unit created an organized register of the traffic and a card index with real names of individuals, units, and locations.[24] In addition, two or three women dealt with the recording of communications intelligence traffic, less-classified COMINT, and other classified material.[25] The women were the wives of British military personnel serving in Palestine and were certified by the British Security Service, MI5.

Within the DSO, there was a separate and compartmentalized unit that dealt with FOG,[26] intelligence on illegal immigration matters obtained from the deciphering of the Mossad LeAliyah Bet radio traffic. Major James C. Robertson, head of the DD3 division in MI5, who visited Palestine in April 1947, noted: "The FOG unit is in a class apart from the rest of the office. Captain Burbidge, who is responsible for the organization, is a first-class intelligence officer whom Magan [Lieutenant Colonel Bill Magan, the DSO] has praised very highly. He receives useful assistance from Mrs. Sales and Miss Ann Clark (who however left for Singapore just before my return to the U.K.). The FOG records and situation maps are a model of precision and clarity. This assists materially in maintaining the prestige of the D.S.O. since the most important part of the service he provides is derived from CREAM [interception and deciphering of Haganah radio traffic]. It is in the FOG "cage" that the daily G.O.C.'s [Lt. Gen. Sir Hugh Evelyn Barker] meeting is held".[27]

Branches of GCHQ called SLU (Sigint Liaison Unit) operated in Cyprus, Fayid, Cairo, and Jerusalem. Their role was to transmit deciphered messages from London to SIME and the DSO. The branch in Jerusalem was called SLU CLOVER, comprised of nine radio operators and cipher clerks, operated from the DSO offices at the British headquarters in the King David Hotel, and used a dedicated communications network, separate from other networks used by

[24] *Signals from SLU Clover (Jerusalem)*, Feb – Nov 1947, TNA HW 92/2, BRAN/YD 375, 1 April 1947.
[25] *Signals from SLU Clover (Jerusalem)*, Feb – Nov 1947, TNA HW 92/2, BRAN/YD 804, 19 September 1947.
[26] Probably an acronym for *Flow of Gold*.
[27] *Robertson Report – Visit to S.I.M.E. and its outstations in the Middle Ea*st, April – June 1947, TNA KV 4/438, p. 23. Code names completed by John Ferris. Additional DSO units focused on intelligence regarding Arab activity and "leftist" (communist) activity.

British security forces. All information transmitted over this network was sent via teleprinters and encrypted using the TypeX electromechanical cipher machine.[28]

In the bombing of the King David Hotel in Jerusalem in July 1946, all DSO personnel were affected (except for Lieutenant Colonel Isham, who at the time was on a duty trip in Beirut) — eight members of the unit were killed, six were wounded and hospitalized, and the card index was destroyed.[29]

Passersby's flee for their lives after the bombing of the King David Hotel, July 1946

Photographer: Sergeant Turner, courtesy of the Imperial War Museum, E.31973



The Southern wing of the King David Hotel after the bombing, July 1946

Photographer: Sergeant Turner, courtesy of the Imperial War Museum, E.31975



[28] An electromechanical rotor-based encryption machine similar to the German Enigma, but more advanced. Unlike the Enigma, its rotor movement was non-regular, making it impossible to analyze rotor patterns from the encrypted data.

[29] *Signals from SLU Clover (Jerusalem)*, June – October 1946, TNA HW 92/1, BRAN/YD 627, 24 July 1946.

The intelligence from this activity was restricted and disseminated, cautiously and in a limited manner, to a small number of security indoctrinated confidants. In addition to the DSO and GCHQ personnel, in 1947 there were only 15 confidants in Palestine — the High Commissioner and his military secretary, the Chief Secretary of the Mandate Government and his assistant, five officers at Army Headquarters (two Generals, a Brigadier General, a Lieutenant Colonel and a Major), two officers at Royal Air Force Headquarters, one officer at Royal Navy Headquarters, the police commander and two senior police officials.[30] DSO officers distributed processed information to the confidants, including summaries for every thousand messages.[31] The intelligence was delivered by DSO officers, and the documents were destroyed immediately after reading. MI5 personnel in London would relay important messages to the Colonial Office by telephone.[32] The volume of information was very large, and as a result, the head of SIME in Cairo requested to reduce the information transmitted to him and to receive only important information in defined categories: the location of immigrant ships, changes in policy, information on planned operations, contacts between the Haganah and the Etzel and Lehi,[33] contacts between the Haganah and elements in neighboring countries, especially Lebanon and Egypt, and the Haganah connections in British security forces.[34]

In 1945, the process of intercepting the transmission, transferring it to London, deciphering the message, translating it into English, and transferring it to the DSO in Jerusalem took three to four days for regular traffic, and 8 to 24 hours for urgent traffic. The army believed that the operational value of intelligence would improve significantly if important messages were processed within eight hours, and regular messages within 24 hours.[35] Shortly thereafter, the process operated at lightning speed: special messages were processed within four hours, and regular messages within 16 to 31 hours.[36]

COMINT quickly became the primary source for operations and counter-espionage. A DSO officer reported that General Barker, commander of British forces in Palestine, said: "We are entirely dependent for our only absolutely reliable information".[37]

---

[30] *Signals from SLU Clover (Jerusalem)*, February – November 1947, TNA HW 92/2, BRAN/YD 375, 1 April 1947.
The practice of distributing a summary every thousand messages was discontinued in March 1947 due to the significant reduction in information volume since September 1946.

[31] *Signals from SLU Clover (Jerusalem)*, February – November 1947, TNA HW 92/2, BRAN/YD 362, 31 March 1947. As at the time of writing, Palestine intercepts files, TNA CO 968/1092, CO 968/1093, CO 968/1094, CO 968/1095, CO 968/1097, CO 968/1098, CO 968/1099, CO 968/1000, CO 968/1100, CO 968/1101, are "Retained by Department under Section 3.4", and not available to the general public.

[32] *Signals from SLU Clover (Jerusalem)*, October – November 1945, TNA HW 92/5, PROC 6150, 16 November 1945.

[33] Etzel was the revisionist Zionist underground paramilitary organization, called the Irgun by the British; Lehi was a militant group split from the Etzel in 1940, called Stern Group by the British. Etzel and Lehi rarely used electronic communication, and British intelligence on them was limited.

[34] *Signals from SLU Cairo*, October 1945 – August 1946, TNA HW 92/4, BRAN/CO 31, 28 November 1945.

[35] *Signals from SLU Cairo*, October 1945 – August 1946, TNA HW 92/4, BRAN/CO 18, 20 October 1945.

[36] TNA HW 14/133, *Time taken by Bays and Clover traffic*, Captain Barber to DD1, 5 August 1945.

[37] *Signals from SLU Clover (Jerusalem)*, June – Oct 1946, TNA HW 92/1, BRAN/YD 578, 5 July 1946.

The "*Tailor*" episode illustrates the British difficulties in translating Hebrew to English: George Francis Taylor, an Australian officer who during World War II commanded Special Operations Executive (SOE) operations in the Balkans (commanding several Jewish volunteers from Palestine) and later served in senior positions at SOE headquarters in London, maintained regular friendly relations with Reuven Zaslani (later Shiloah, a senior Foreign Ministry official and the first head of the Mossad), a member of the Jewish Agency Political Department in London. In these relations, he discussed, among other things, "current affairs," and Zaslani reported accordingly to his superiors. Members of the Political Department referred to him by the code name *Khayat* (in Hebrew – *Tailor*). Part of the correspondence between members of the Political Department was in English, and thus he appeared in the Political Department's messages, which the British intercepted and deciphered.[38] The British translator, apparently of Arab origin, translated the word *Khayat* as the word Life. In a letter from the DD3 division of the British Security Service MI5 (dated 20 November 1946) to the DSO in Jerusalem, we find the following sentence: "In part 6 of your report 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 to some other Jewish publication in the States".[39]

This intelligence was concealed from most analysts, including those who analyzed other sources on the same topics, and they received only "sanitized" intelligence, with the source concealed. Their activities and actions were monitored.

The Hebrew Resistance Movement and "Black Sabbath"

In October 1945, the Hebrew Resistance Movement was established — a joint operational cooperation between the Haganah, Etzel, and Lehi organizations. The nature of the struggle against the British changed, from a "close struggle" (targeted attacks on British targets directly linked to the prevention of illegal immigration) to a "continuous struggle" (comprehensive and ongoing attacks on British targets). The first step was the renewal of broadcasts by "Kol Yisrael – the broadcasting station of the Hebrew Resistance Movement" on 4th October. The first operation was the liberation of 200 illegal immigrants from the Athlit detention camp on the night of 9–10 October 1945. Additional attacks included the blowing up of railway tracks, raids on radar stations and police installations, and the destruction of ten bridges, on all the main roads connecting Palestine to the neighboring countries, on the "Night of the Bridges," 16–17 June 1946.

Contacts between the Haganah and Etzel and Lehi regarding cooperation had been ongoing since August 1945. However, the activity of the Hebrew Resistance Movement surprised the

[38] Moshe Sharett, *Months in the Ayalon Valley*, research and notes by Pinchas Ofer, The Moshe Sharett Heritage Association, 2011, p. 38 (Hebrew).

[39] *Security Service Personal Files: Theodore Kollek*, letter from J.C Robertson to DSO Palestine, dated 20 November 1946, TNA KV 2/2262.

British, as David Ben-Gurion had instructed the head of the Haganah High Command Council, Moshe Sneh, to initiate these actions in a letter written on 7 October and sent from Paris on 8 October 1945 by courier (by flight) and not by a radio message. Therefore, the order was not intercepted by the British.[40]

The Jewish Agency denied responsibility for the actions of the Hebrew Resistance Movement. The information obtained from the Haganah's radio networks accurately described the cooperation between the Haganah, Etzel, and Lehi. Nevertheless, senior British officials believed that the Jewish Agency should and could disassociate itself from the Haganah and suppress Etzel and Lehi. They overestimated Jewish leaders such as Chaim Weizmann, who preferred cooperation and compromise with Britain, and underestimated the hostility toward British policy.

A unique event during this period was the kidnapping of a British DSO officer: on 13 June 1946, a British military court sentenced two Etzel fighters, Yosef Simchon and Michael Ashbel, to death by hanging, after they were captured wounded following an Etzel attack on the Sarafand camp on 6 March 1946. In response, on 18 June 1946, Etzel fighters kidnapped four British officers in Tel Aviv and one British officer in Jerusalem, threatening to hang them if the sentence was carried out. The officers kidnapped in Tel Aviv were released on 3 July 1946, after the High Commissioner commuted the death sentence imposed on the Etzel fighters to life imprisonment. The officer kidnapped in Jerusalem was Major Owen Chadwick, a DSO officer, one of the confidants whose main role was to distribute the intercepted and deciphered Jewish messages to a small number of confidants in the senior British command, and to destroy them immediately after reading. He was kidnapped on his way to a meeting with General Barker, with such messages in his pocket, but his captors did not search him and did not discover them.

Liddell describes Major Chadwick's account of his experience: "He was walking down one of the main streets in Jerusalem when he passed a taxi drawn up at the side. There were two men standing outside and talking with a man and woman inside. As he approached the men drew their guns and bundled him into the taxi. The woman then took out a chloroform pad and stuck it over his face. When he recovered consciousness he was in a bakery, tied to a plank in a lying position. He was told he was among 26 other high-ranking officers who had been taken and would be executed if the Irgun men under sentence of death were shot or hanged. His guards wore masks and later an officer came to interview him. For this purpose his eyes were blindfolded, the officer told him more or less what the guards had told him and they chatted quite amiably. He was given food and allowed to sit on a low couch provided either his arms or

[40] *Ben-Gurion's diary*, 7 October 1945, Diaries Division – Complete Diary, 219480, Ben-Gurion Archives; Avi-Amos to Moshe Sneh, 7 October 1945; Sneh Collection, Labor Archive/Lavon Institute, File 66–2–812–104–IV (Hebrew).

his feet were tied. Later he was allowed to exercise and for this purpose got rid of his bonds. He then flopped down on the bed and pretended to be asleep. One guard remained inside the room and another was close at hand outside. While lying on his bed he noticed a piece of sacking over the roof, and also a ledge in the wall which would enable him to reach a beam. Noticing that his guard was apparently asleep (he could not see his eyes owing to the mask but he saw his head nodding), he got up on his bed, put his foot on the ledge and reached the beam. He looked around once more to see whether the guard was still asleep, tore away the sacking and went out through the hole. This of course made a certain amount of noise and the guard woke. He slid down from the roof and dropped into a courtyard with iron gates. Luckily the gates opened when he used a certain amount of pressure. He ran down the road, pursued at a certain distance by the guards. He could get no assistance but as luck would have it he was able to jump on a passing bus… He was never seriously interrogated or even searched. This was luck as he had several somewhat incriminating documents on him from the DSO office".[41]

Major Chadwick was held under close guard by Etzel fighters in a hiding place (an abandoned bakery) in the Bukharim Quarter of Jerusalem. After 36 hours, he took advantage of a moment of weakness among his guards and managed to escape, boarded a passing bus (line 3 of "Hamekasher"), and reached Army Headquarters at the King David Hotel. The British did not believe his escape story and suspected he was a double agent. He was arrested and flown for interrogation in London and was only cleared when it was confirmed that the Haganah continued to use ciphers that had been deciphered: "The proof is that OATS still goes on".[42]

The cooperation between the Haganah, Etzel, and Lehi ceased after the Jerusalem King David Hotel, which housed the British main headquarters, was bombed by Etzel several weeks later — on 22 July 1946.

In response to the activities of the Hebrew Resistance, the British launched a large-scale operation against the Jewish Agency and the Haganah, Operation Agatha, known as "Black Sabbath" (29 June 1946). Palestine's borders were sealed; telephone lines were cut; a curfew was imposed on the main cities; the Jewish Agency building in Jerusalem was seized by the British army and all its documents were confiscated; Yishuv leaders were arrested; in a raid on 27 settlements, about 2,700 people were arrested, including about 200 Palmach members; the Palmach headquarters card index at Kibbutz Mizra was seized; the large weapons cache at Kibbutz Yagur was discovered. The blow to the Yishuv was severe. The Signal Service was

[41] *Diary of Guy Liddell*, Deputy Director General of the Security Service, November 1945 to September 1946, KV 4/467, notes 25 June 1946.

[42] *Diary of Guy Liddell*, Deputy Director General of the Security Service, November 1945 to September 1946, KV 4/467, notes 28 June 1946. For a comprehensive account of the event, including the Irgun's perspective, see: Daniel Rosenne, *The Bird Has Flown: The Kidnapping of Major Chadwick*, The Association for the Commemoration of the Fallen Soldiers of the IDF Signal Corps, January 2022 (Hebrew).

'silenced', and activity was gradually resumed thereafter. Only in late February 1947 was the fixed radio network to the settlements, the "Avinoam" network, reactivated.[43]

The British intelligence assessment, as sent on 3 July by Captain Burbidge of the DSO in Jerusalem to the Security Service MI5 in London and to SIME in Cairo, under the security classification TOP SECRET CREAM, illustrates the British intelligence superiority, which was achieved through reading the encrypted traffic of the Haganah, the Palmach, the Political Department of the Agency, and the Mossad LeAliyah Bet:

"1. Effects of operation:

a. Army operation achieved element of surprise. Hagana intelligence, normally well informed in advance of authorities' intentions, learned of only one of the 25 searches and wrongly appreciated that it was local affair resulting from AZZIB bridge blow-up [the explosion occurred prematurely due to a bullet strike, and 13 Palmach fighters were killed in the blast]. As a result no changes in PALMACH dispositions made and no security precautions were taken with respect to documents, W/T [wireless Telegraphy] etc. This borne out by capture of PALMACH office plus card index at Mizra and W/T sets in Sharon.

b. Capture of PALMACH Headquarters serious [setback] but no fatal blow to PALMACH. Capture removed central control so necessary to scattered force such as PALMACH for rapid action. Similarly temporary closing down of all but one of PALMACH company [radio] sets will slow down communications. Routeing difficulties already noticeable. G.H.Q HAGANA TEL AVIV, the supreme authority now much subdued, greater part of organizing for both HAGANA and PALMACH being done via HAIFA station. Other HAGANA [radio] stations working normally and probably passing traffic for PALMACH when locations nearby.

c. HAGANA and PALMACH apparently not yet realised operation resulted from interception of their W/T traffic. Suspect however that HAGANA ciphers found at Mizra. This almost certainly means change in HAGANA cipher near future.

d. Not possible to measure effects of the arrests yet. We know Chief of Staff, HAGANA, Head of PALMACH and two unit commanders were not arrested. These will be able to do high level planning, but remains to be seen whether or not depleted Company staffs and men can carry out their instructions. Should be borne in mind that some 15 settlements containing PALMACH detachments without W/T were not entered. This represents total of 450 men.

2. HAGANA-PALMACH reaction:

[43] The Engineer (Haganah Chief of Staff, Yaakov Dori) to "Segel Beit", 27 February 1947, Haganah Historical Archives (hereinafter: HHA), 73/74 (Hebrew).

a. Primary concern evident is to save what remains of organization by instituting security measures as follows:

1) Courses and camps and personnel dispersed.

2) Office work and internal post to cease.

3) PALMACH units to destroy incriminating material but to keep W/T documents in ultra safe places.

4) Arrangements to be made for all males to evacuate settlements discreetly if [military] search believed imminent. No resistance to be offered by remaining.

5) No one above rank of N.C.O. permitted travel and rank and file only when in possession of valid identity documents.

6) No leave is granted in PALMACH.

7) HAGANA leaders in settlements to be changed.

8) Meeting places to be cleaned up.

b. Planning for recovery already evident:

1) London and Milan informed 2nd July that PALMACH forces are "organized".

2) Unit and Company commanders to return to Headquarters at once.

3) [The radio station in] Haifa reported 30th June all PALMACH and reserve (total 6,000 less detainees) had been issued with instructions. Suggests mobilisation of reserve.

4) Aviel [Yehoshua Globerman, head of the Training Department and commander of Tel Aviv], HAGANA field Army commander becoming prominent. Suggest eventual action possible by this force [the Ḥish - the main body of Haganah forces].

5) All formations instructed to listen to Kol Israel daily. Veiled general orders could be passed this way.

c. Morals: Impression from traffic is that organisations are stunned and PALMACH temporarily dislocated. Notable absence of panic often observed in earlier more located [British] operations. This impression supported by relatively accurate factual reporting of searches, unadorned by customary flights of imagination and general exaggeration. Exceptions to this are highly colored quite unfounded reports of tortures inflicted on detainees ATHLIT.

3. Possible courses [of action by the Haganah]: Too early and insufficient traffic yet to forecast with any accuracy. PALMACH occupied in safeguarding undamaged parts of organization but regrouping and mobilization hinted at. Suggest eventual violent retaliation against H.M. forces and/or an operation to release members in LATRUN and ATHLIT".[44]

[44] *Signals from SLU Clover (Jerusalem)*, June – Oct 1946, TNA HW 92/1, BRAN/YD 564, 3 July 1946.

On 15 July, an additional intelligence assessment was sent, also under the security classification TOP SECRET CREAM:

"1. Political:

a. Jewish political picture on 8th July as revealed by SNEH [head of the Haganah High Command] in signal to BEN GURION, was one of confusion, and possible discord between WEITZMAN [Weizmann] moderates and SNEH extremists. Conclusion resulting from apparent questioning of the authority of depleted J.A. Executive, with consequent independent attempts at a solution of situation. Possible discord may result from increase in WEITZMAN's moderating influence since imprisonment of other Jewish leaders, and from his ultimatum that HAGANA/PALMACH must cease [Anti British operations]. Tone of SNEH's signal suggests he is perturbed at increase of WEITZNAN's influence. Note – worthy that SNEH, now an outcast extremist, requested BEN GURION to issue him with clear and specific instructions.

b. As a move towards clarification of situation, BEN GURION has suggested early meeting of all available Executive members [of the Jewish Agency] in NEW YORK with purpose of defining Agency's political position on the PALESTINE situation. Conclusions of this meeting to be placed soon as possible before World Zionist Congress and members of NEW YORK Executive. It is held that a definition of Agency's political position by unanimous vote of representatives from all parties is vital if internal schism and independent activities are to be avoided. Further recommended that preparatory council should meet PARIS earliest. Full Executive of J.A. PALESTINE to be invited. Imprisoned members to send plenipotentiaries.

c. PALESTINE informed BEN GURION 18th July [this is likely an error, as the telegram was sent on 15 July] that literature and photographs presumably of result of Operation AGATHA had been sent to LONDON for CROSSMAN [codename] and would shortly be sent to AMERICA also.

d. HAGANA EGYPT reported on 7th July that Egyptian police had been asked to report on movements of a number of important American, English and Palestinian Jewish personalities who may arrive in Egypt by air. This information is accurate. Possible leak originated from RIAD BEY, coptic officer of Egyptian C.I.D., know to enjoy cordial relations with J.A. CAIRO.

e. Comments: Paras. a and b above substantiated by CIRCUS [codename, apparently surveillance via hidden microphone] and press reports respectively. BEN GURION now in AMERICA.

2. W/T: HAGANA and PALMACH ciphers changed 0001 hours 9th July but illegal immigration network [Gideon] not affected. Changes of pseudonyms and cover terms also taking place in

Palestinian system. Documents captured at YAGUR include HAGANA and PLAMACH callsign lists, a code and 6 keys. PALMACH W/T course now reassembling [the course had been disbanded following "Black Sabbath"].

3. Immigration: NORSID [the illegal vessel HAGANAH, which sailed from the port of Bakar, Yugoslavia, on 24 July 1946 with 2,678 immigrants and, due to engine failure, stopped on 28 July between Crete and Cyprus, transmitted a distress signal, was located by a British aircraft, and continued to Palestine escorted by a British destroyer] put into AEGEAN Island of Milos on 2nd July, where refueling and revictualling took place. Greek navy reported this. Actually sailed to Yugoslav port of SPLIT (SPALATO) arriving 10th July. Believed to have left SPLIT about noon 13th July ultimately for CRETE where 400 illegals are to be embarked. Not known if any have been taken on at Split. Will make for a second unidentified port where 2100 more will be embarked if available. Boat still in touch with ROUMANIA. Not possible to calculate E.T.A. PALESTINE at present.

4. Situation in HAGANA and PALMACH:

   a. Go ahead for operation to recover the YAGUR arms given from G.H.Q. on 6th July may have been nullified by WEITZNAN ultimatum. Overt reports state SNEH has agreed to operational truce providing WEITZMAN submits proposals J.M.G. on forthcoming visit to U.K. Same may apply to other hints at operations in OATS [intercepted and deciphered Haganah messages] viz: activity involving head of HAGANA medical services on 25th July, and activity SHARON area for which report on either transfer of detainees at ATHLIT or changing of guard at ATHLIT and TULKARM, was awaited on 8th July.

   b. Numerous reports of forthcoming searches have kept organizations in state of alert during past week. HAGANA report of 9th July from HAIFA mentioning possible searches links with similar report by ASO HAIFA of following day.

   c. HAGANA - PALMACH still perturbed at thought of betrayal from within. Now think that police informers in SHAAR HA AMAKIM (acting PALMACH H.Q.) have revealed increased activity there. Head of PALMACH reported from settlement next day that "exhibition" (PALMACH H.Q.?) moved to new place. Arms caches in settlements ACRE BAY area moved in anticipation more "YAGUR" searches by Army.

5. Kidnappings: After investigation into background of PAPANEK [Pfenek] and FREUND and revealing of general bad character of both, HAGANA H.Q. HAIFA stated on 6th July that the YAGUR colonists did not suspect PAPANEK. "PALESTINE POST" of 12th and 14th July states both now released bearing signs of ill-treatment. Neither have related full story of experience.

Kidnapping bear hall-marks of I.Z.L. work. FREUND was chloroformed when first taken and paid 1 Palestinian pound on release.[45]

6. Meeting of Unit 2 company commanders [the Palmach second battalion] took place at HASHOMER HATZAIR offices in Tel Aviv on 8th July. Of interest that PALMACH meeting took place in offices of this organization with whom relations were considerably strained in late 1945 owing to their disagreement with HAGANA policy of violence.

7. Interesting trend observed before ciphers changed. Several PALMACH members called to TEL AVIV to meet YAAL [codename]. Latter was organizer of PALMACH counter-terrorist squads [the "Saison", Haganah attempt to suppress Etzel insurgency against the British during World War II] in early 1945".[46]

The "White Paper" of July 1946

On 24 July 1946, following the international political storm caused by British actions on "Black Sabbath," the British government published a "White Paper" intended to portray the Jewish Agency as a terrorist organization,[47] to prove that it was a leading force in the violent actions against the British in Palestine, and to present its activity as illegitimate.

Political pressure from a vocal pro-Zionist opposition in the British Parliament and American pressure prompted British Prime Minister Clement Attlee to order, in July 1946, the preparation of a government document that would include conclusive evidence that the Jewish Agency was sponsoring a terrorist organization (the Haganah). The only evidence the British possessed were the deciphered messages, and Attlee ordered their publication.

The British Security Service MI5 strongly opposed the publication of the deciphered messages, fearing exposure of sources that would cause an "intelligence blackout" and harm the security of British forces in Palestine. The bombing of the King David Hotel by the Irgun on 22 July 1946 further heightened the importance of these sources, as it disrupted the activity of other British intelligence bodies.

The British Prime Minister rejected MI5's demand to omit the deciphered messages from the White Paper. In the diary of Guy Liddell, who was promoted to Deputy Director General of the Security Service, a series of meetings on the matter is described:[48]

---

[45] Otto Freund and Bernard Pfenek were immigrants from Czechoslovakia whose request to join Kibbutz Yagur was denied. They were suspected of aiding the British during the Yagur search and were arrested by the SHAI (Haganah intelligence) in Haifa on 3 July. Freund proved his innocence and was released. Pfenek was found guilty of treason, sentenced to death but managed to escape. Haifa police placed him in protective custody, after which he returned to Czechoslovakia. He immigrated again to Israel in 1964, at which point his innocence was confirmed.

[46] *Signals from SLU Clover (Jerusalem)*, June – Oct 1946, TNA HW 92/1, BRAN/YD 605, 16 July 1946.

[47] *Palestine: Statement of Information Relating to Acts of Violence*, H.M.S.O. Cmd 6873, July 1946.

[48] *Diary of Guy Liddell*, November 1945 to September 1946, TNA, KV 4/467, pp. 250–251, 254–259, 266–269, 277.

- On 5 July 1946, a meeting at the Colonial Office is described, where the pressure to issue the document was clarified. Liddell, for his part, proposed alternatives to prevent the publication of material that would reveal the ability to intercept and decipher messages, and immediately updated the head of MI5, who was also concerned about the risk of source exposure.
- On 8 July, the preparation of a memorandum for the Prime Minister and the Colonial Office is described, based on top-secret material and additional sources, stating that the Jewish Agency controls the Haganah and the Palmach, who are responsible for the violent and illegal activity, and that they cooperate with the Irgun and Lehi. The intention was to base this information on material seized in Palestine, thus avoiding source exposure.
- On 9 July, a meeting of the Prime Minister and the Colonial Secretary is described, with the participation of General Hastings Lionel Ismay[49] and the head of the Security Service MI5. The Prime Minister's conclusion from the discussion is redacted from the document (according to the diary entry on 11 July, it can be understood that the directive was to base the White Paper on top-secret sources unless alternative material was found in searches in Palestine), but it is written that the head of the Security Service claimed that if this were done, an intelligence blackout was expected: "C. pointed out that if we did this we might be in the dark, as far as future operations were concerned". Nevertheless, it was agreed to prepare a White Paper with "top-secret" material, while taking measures to cover the sources ("cover up").
- On 10 July, a discussion is described with Kellar and representatives of the Colonial Office on the draft document, and a meeting with the Director of Military Intelligence (DDMI) to persuade him that the Chiefs of Staff did not properly appreciate the implications of Palestine being in the dark if the sources were exposed, and that British forces would be dependent solely on HUMINT: "Palestine was going to be in the dark if [ISTRIA and OATS] were blown".
- On 11 July, a report is described from a military intelligence officer who spoke with the Director of Military Operations (DMO), to update the Chief of the Imperial General Staff (CIGS) on the matter. He received a report that the CIGS would speak with the Prime Minister about the issue. A meeting with the Colonial Office is described to finalize the draft document, and another meeting to persuade that there was no need to expose sources, since according to Kol Yisrael broadcasts, the Haganah and the Palmach had taken full responsibility for the military actions in Palestine. In a discussion at the Security Service with Kellar, the exposure of sources was discussed, and a telegram sent by the Commander-in-Chief in Palestine was read, expressing concern that he would find himself without

[49] Military Secretary to the Prime Minister.

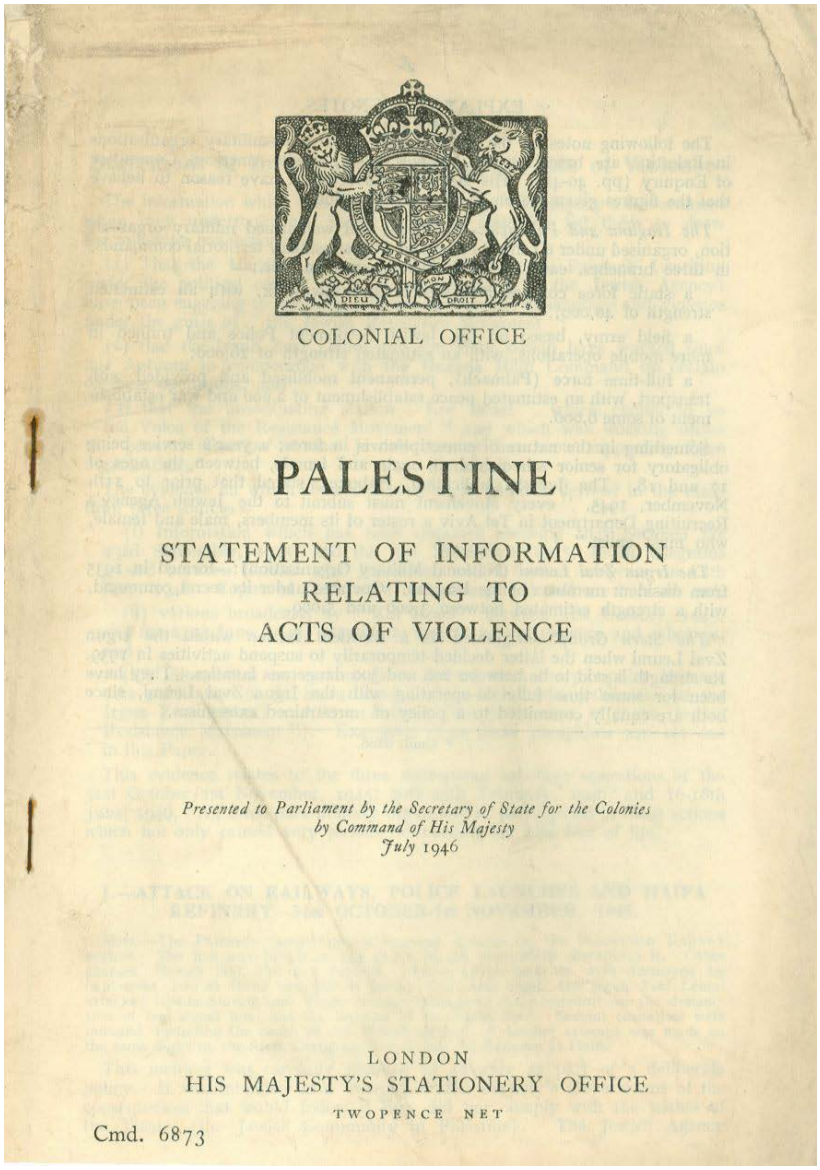
intelligence in a critical situation: "This telegram expressed the anxiety of the G.O.C. lest he should find himself entirely deprived of intelligence sources in what was obviously a critical situation". But all this was to no avail. The Prime Minister refused to discuss the matter despite the concern for the security of British forces, but granted them a one-week extension to bring alternative "incriminating information": "The Prime Minister seemed reluctant to discuss the aspect of the problem which affects the security of our troops… We were given a week to obtain evidence from Palestine, which if sufficiently convincing might prove a substitute for [ISTRIA and OATS]".

- On 12 July, a report was recorded of a meeting with the Lord Chancellor regarding the document's wording.[50] On 15 July, another meeting was reported, and a two-day extension was granted to bring alternative material. On 19 July, another meeting was reported in which a draft was presented without [erased word] at the beginning. It was agreed that additional material was needed to link the Jewish Agency to Kol Yisrael broadcasts. On 20 July, another meeting with the Lord Chancellor was held, in which wording of the draft of the document was completed.
- On 22 July, news arrived of the bombing of the British headquarters at the King David Hotel. On 23 July, it was reported that the draft document was submitted to the Prime Minister, who refused to remove the words about ISTRIA. The diary's recorded response was: "This is a pity, but I don't think it matters a great deal".

The matter did not end there. On 30 July, the diary reports dissatisfaction within the intelligence service MI6 (SIS – Secret Intelligence Service) with the claim that MI5 had mishandled the matter, and "it was really worse to have blown ISTRIA than OATS". On 9 August, a meeting with the head of the Security Service is reported, in which a rumor was recorded that had reached him from Kellar: "I also told 'C' that from certain remarks which had reached me from other offices and also from a conversation between Kellar and Travis [Sir Edward Wilfred Harry Travis, Head of Bletchley Park and later GCHQ director] that there was a certain amount of feeling that M.I.5. had let the party down over the White Paper" and therefore he proposed conducting a post-mortem review to demonstrate that the matter had been forced upon them by the Prime Minister.

[50] Lord Chancellor – A British cabinet minister who heads the judiciary and serves as Speaker of the House of Lords.

Cover page, 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 "Disaster"

The leadership of the Yishuv and the Signal Service believed that the encryption they used was secure and reliable, and the publication of the "White Paper" on 24 July 1946 was a profound shock to them — an actual "earthquake."

The "White Paper" included eight telegrams of the Jewish Agency, seven of which were sent from Palestine to London as encrypted telegrams, and one, which was an open telegram, was sent from London to Palestine. Below are some of the telegrams published in the "White Paper":

A. An encrypted telegram sent by Moshe Sneh (head of the Haganah High Command Counsel) to London on 23 September 1945: "It is suggested that we do not wait for the

official announcement but call upon all Jewry to warn the authorities and to raise the morale of the Yishuv. If you agree ask Zeev Sharif [Sherf] for statistical material about absorptive capacity and if you do not agree tell him that this material is not required. It has also been suggested that we cause one serious incident. We would then and publish a declaration to the effect that it is only a warning and an indication of much more serious incidents that would threaten the safety of all British interests in the country, should the government decide against us. Wire your views with the reference as before but referring to statistical material about immigration during the war years. The Stern Group have expressed their willingness to join us completely on the basis of our program of activity. This time the intention seems serious. If there is such a union we may assume that we can prevent independent action even by the IZL. Wire your views on the question of the union referring to statistical material about Jewish recruitment to the army. Sneh."

B. An encrypted telegram sent by Dov (Bernard) Yosef (Legal Advisor of the Jewish Agency) in Jerusalem to London on 10 October 1945: "Eliezer Kaplan [Head of the Finance Department of the Jewish Agency], basing himself on a word from Hayyim [Weizmann] via Nwbw [name redacted], says that we should undertake nothing before you give us instructions to do. He is opposed to any real action on our part until we hear from you. Other members, however, are of opinion that it is necessary to back your political effort with activities which do not bear the character of a general conflict. It is essential that we should know at once whether such actions are likely to be useful or detrimental to your struggle. Should you be opposed to any action whatever, wire that we should wait for the arrival of Wlsly [name redacted]. Should you agree to isolated actions, wire that you agree to sending a deputation to the dominions. If Hayyim [Weizmann] meant that us only to avoid general conflict not individual cases, send greetings to Chill for the birth of his daughter".

C. A telegram sent by Moshe Shertok (Sharett) in London to Dov Yosef in Jerusalem as a regular telegram via post office on 12 October 1945: "David [Ben-Gurion] will not leave before fortnight. Meanwhile probably visit Paris. Regarding [Eliyahu] Dobkin [Head of the Immigration, Organization, Youth, and Hechalutz Department in the Jewish Agency] written. David [Ben Gurion] himself favored delegate dominions. Please congratulate Chill on the birth of his daughter. Signed Shertok".

In the writings of Moshe Sharett, who was arrested on "Black Sabbath," concern is raised that the cipher of the Mossad LeAliyah Bet was also deciphered. These writings, which are a collection of notes smuggled from the Latrun detention camp, are written in an original style. In a note sent by Sharett from the detention camp to Ze'ev Sherf, Secretary of the Political

Department, on 24 July 1946, following the publication of the British "White Paper," it is written: "We had a ball [neshef – literally 'party'; here: our secrets are blown] with the participation of a trio: Avinoam [the Haganah's communications network], Efrat [the Agency's communications network], and Kellar [MI5]. The first either through listening or by reading the written notes [leak of plaintext material]. The second either through interpretation [cipher decryption] or by reading the lyrics [leak of the cipher key] (there is evidence for the first possibility). The third—one clause, the contribution of the undersigned. The first two will learn a lesson [draw conclusions and improve]".

The next day, on 25 July, he added in another note: "On second thought: perhaps only Avinoam (with a bit of Kellar), without Efrat?" On 3 August, Sharett sent Sherf this note:

> "The matter of the ball is now becoming clearer than before, though still not in all its details. Indeed, even from the first telegram I suspected something of the sort, but now it is clearer, though, as said, not entirely. So then — (a) If our people were involved — why did they not come to whisper in our ear? Hair-raising! (b) How did they move from algebra to arithmetic in identity [how did they decipher the cipher]? (c) In light of the experience — what is the fate of the connection to Lutecia [the branch in Paris]? (d) What is the meaning of 'also Bethlehem among the musicians' [Bethlehem is Efrat, the Agency's network — 'in the way of Efrat, which is Bethlehem' (Genesis 35:19)], surely they could not possibly have found the city map [cipher key], did it turn out that they identified the syllables without needing the map? (e) What is the meaning of 'the same applies to B [Mossad LeAliyah Bet]'?".

Ze'ev Sherf's response was: "The transition from algebra to arithmetic was not difficult when the numbers were few."[51]

Menachem Begin, the Etzel leader, also refers to the "White Paper":

> "An echo of the agreement [between the Etzel and the Haganah] is found in the secret telegrams sent by Moshe Sneh to his superiors in the Jewish Agency abroad. These telegrams were delivered by an unknown route to British intelligence or were captured and deciphered by its agents. They were published in a special White Paper by the British government. I regret to say that the "White Paper" is one of the rare British political documents in which I found only a few distortions".[52]

[51] Pinchas Ofer, *Months in the Ayalon Valley*, Tel Aviv: The Moshe Sharett Heritage Association, 2011, pp. 103–104, 108, 140, 145–146 (Hebrew).

[52] Menachem Begin, *The Revolt: Memoirs of the Commander of the Irgun*, Tel Aviv: Achiasaf, 1977, pp. 282–283 (Hebrew).

Senior officials of the Jewish Agency denied any connection to these telegrams. This was the response of the Agency's spokesman:

> "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 emanates 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."[53]

This was a formative event in the history of the Signal Service and was a true "wake-up call." Not only did it lead the Signal Service to change all cipher methods (see 20 × 20 Square Cipher, Appendix A), but it also caused it to recognize the need to institutionalize the matter of ciphering under the authority of experts in the field, with the allocation of necessary resources.[54]

The "Big Engineer" Misha Gordin (code name "Rahaf"), who headed the radio branch of the Signal Service until the beginning of 1946, recounts:

> "It is natural that I take upon myself responsibility in this matter… But in truth, the main leaders are not without blame, for they were not cautious despite repeated warnings. I told Eliyahu [Golomb] more than once, that the code must be changed, because these are not normal times, but times of war, and surely there is listening and it is possible that they have discovered our code and are deciphering our messages… But Eliyahu would dismiss my concerns — 'It is inconceivable that they would decipher a secret script, and in Hebrew no less.' I repeated my proposal to change the code, to strengthen it… Nothing was done, and in the end, what could have been foreseen in advance happened".[55]

---

[53] *Agency Denies White Paper*, The Palestine Post, 26 July 1946, p. 1.

[54] The new ciphers were based on letter substitution using a 20×20 Vigenère table. Initially, the keys were ten-letter passwords, and during the War of Independence, the use of one-time pads (OTP) was adopted.

[55] Testimony of Misha Gordin, HHA 13/1 (Hebrew). Under the command of Yerachmiel Belkin (February 1942 to November 1945), the Haganah's Signal Service operated in two "branches": "The Big Engineer" Misha Gordin ("Rachaf") headed radio operations, which were particularly clandestine at the time; Doctor of Agriculture Zvi (Charlie) Levin-Halevi ("Amos") led the "conventional" activities (visual signaling, carrier pigeons, wired communication, and training), focusing on developing signals activity within the Haganah units.

From Riches to Rags

The publication of the "White Paper" in July 1946 shook the Haganah's Signal Service, and its response decapitated the British communications intelligence apparatus in Palestine (with the exception of the immigration issue, as described below).

In 1917, the publication of the "Zimmermann Telegram" revealed Britain's ability to decipher German ciphers,[56] but it achieved a significant strategic goal — it was a decisive factor in the United States' entry into the war against Germany alongside the Allied Powers. Not so in 1946: the United States did not change its favorable policy toward the Jewish Yishuv, the attacks on British policy did not cease, but the British intelligence source dried up, and British intelligence superiority evaporated overnight.[57]

The heads of the British military and intelligence, who feared an intelligence blackout, failed in their efforts to persuade British Prime Minister Clement Attlee not to publish intercepted and deciphered messages. However, political pressure from a vocal pro-Zionist opposition in the British Parliament and hostile American public opinion led the Prime Minister to publish a government document that would present conclusive evidence of the Jewish Agency's involvement in organizing terrorist operations.

The publication of the "White Paper" led to a change in the ciphers of the Signal Service and the Political Department of the Jewish Agency. The Signal Service switched to cipher methods based on letter substitution combined with frequent changes of cipher keys starting on 15 September 1946. In August 1946, the Jewish Agency Political Department added a number to the Bentley code number (e.g. 41.945), which served as a key and was frequently changed. The transmitted text was the sum of the number in the codebook and the key number, using a special calculation method.[58] The British failed to break this code.[59]

---

[56] An encrypted telegram sent on 16 January 1917 by the German Foreign Minister to the German ambassador in Mexico authorized the ambassador to propose an alliance with Germany against the United States, offering broad economic support and an understanding that Mexico would reclaim Texas, New Mexico, and Arizona. The British handed the decrypted telegram to the Americans on 23 February. The U.S. entered the war on 4 April 1917. See:
Barbara Tuchman, *The Zimmermann Telegram*, Ballantine Books, New York, 1958.

[57] Israel acted similarly by releasing the recording of a conversation between Egyptian President Gamal Abdel Nasser and King Hussein of Jordan on the second day of the Six-Day War (6 June 1967), in which Nasser persuaded Hussein to open a "second front" against Israel. Defense Minister Moshe Dayan decided to release the recording despite opposition from Military Intelligence Chief, Major General Aharon Yariv.

[58] Internal memo (unsigned) to A.A., Nathanel and Raphael, 11 August 1946, CZA S25.10941 (Hebrew); corresponding English document titled *Instructions for Use*, 19 August 1946, CZA S25.8214.

[59] Request from Section B.3.a of the British Security Service MI5 for surveillance of the Jewish Agency office in Geneva, 18 July 1947, TNA KV 2/1435.

As a result, the British lost their ability to decipher the Haganah and Palmach's traffic — their best and most important intelligence source — at a critical moment for British security operations in Palestine.[60] Consequently, British intelligence superiority ceased to exist.

The British were concerned regarding the Palmach, "PALMACH are prime threat to security after terrorists", they did not know the location of the Zonal Haganah and Palmach headquarters, and were exposed to the danger of a general mobilization of the Haganah "in event unfavorable turn PALESTINE situation possible HAGANA field army would be mobilised" (i.e., if Britain acted decisively against the Yishuv), when the need to suppress these bodies "necessary contingency may well arise at any time in view present PALESTINE situation".[61] The Haganah and Palmach's traffic, which had expanded in volume, was intercepted, and direction-finding (D/F) devices were used to locate the Haganah's radio stations. These were installed in military ambulances without windows that had been converted into mobile direction-finding stations, without external antennas. The direction-finding was effective only in rural areas, and the British settled for locating at the level of the settlement.[62]

British intelligence analysts worked consistently and succeeded in reconstructing a database and code words.[63] In June 1947, communications intelligence provided an order of battle for the Haganah and the Palmach and operational information — rather speculative than certain. The broadcasts of Kol Yisrael, the Haganah's underground radio station, and the Palestine Post newspaper became the main intelligence sources for the British. From their perspective, the lack of intelligence harmed operational efficiency and the success of their activities.

As early as November 1945, the British had already deployed a system jamming Kol Yisrael broadcasts, after their attempts to locate the transmitters had failed. In January 1946, with two officers and 42 soldiers, they established a special secret electronic warfare unit to carry out the jamming — 634 Wireless Troop — and the effectiveness of the jamming gradually improved. The electronic jamming conflicted with British intelligence needs, and in late 1946 the British jamming unit was ordered to cease jamming Kol Yisrael broadcasts, under the cover story that "the venom of the Voice of Israel has weakened".[64]

---

[60] *Signals from SLU Clover (Jerusalem)*, June – October 1946, TNA HW 92/1, BRAN/YD 873, 23 September 1946.

[61] The British estimated that Haganah was capable of fielding 45,000 armed trained personnel and 1,500 Palmach personnel. CIGS report to the PM, *Jewish situation in Palestine*, April 1944, TNA HW 1/3789.

[62] *Signals from SLU Clover (Jerusalem)*, February – November 1947, TNA HW 92/2, BRAN/YD 181, 13 February 1947. It is unknown whether the medical ambulance markings were removed from the military ambulances used for D/F activities.

[63] *Signals from SLU Clover (Jerusalem)*, February – November 1947, TNA HW 92/2, BRAN/YD 566, 14 June 1947; BRAN/YD 598, 18 June 1947; BRAN/YD 870, 17 October 1947.

[64] *CSO's Branch HQ Palestine, Summary of Events*, July 1948, Part VI – Brief History of Skylark, TNA WO 261/738; Daniel Rosenne, *A Voice Was Heard in Ramah: The Broadcast War 1945–1948*, The Association for the Commemoration of the Fallen Soldiers of the IDF Signal Corps, December 2020 (Hebrew).



Haganah members operate a "Kol Yisrael" radio transmitter in a Tel Aviv safe house
From right to left: technician Yeshayahu (Ishi) Lavi (Lamberger), later a IDF Colonel and Chief Signal Officer, Director General of the Ministry of Communications and Director General of the Ministry of Defense, reading aloud; technician Ze'ev Ben-Yaakov (Hugo Zwiener), later an IDF Major, overseeing the transmitter; technician Naftali (Nafta) Raz, later an IDF Lieutenant Colonel, watching from the window to warn of a British military patrol.
Photograph: Zoltan Kluger, The National Photo Collection D814-066.

The contents of the messages transmitted over the Haganah and Palmach radio networks were not available to the British.[65] Operator errors allowed the British limited access to Haganah traffic in the North of Palestine,[66] and later to the traffic of the Palmach's Second Battalion (then under the command of Yitzhak Rabin),[67] but this achievement was of marginal significance. The British difficulty in overcoming simple improvements in encryption illustrates the breach between the unit dealing with the Haganah and Jewish Agency ciphers and the core operations of GCHQ. Had this traffic been a high priority, it would very likely have been deciphered.[68]

The most prominent and significant achievement of GCHQ during this period was the deciphering of the transmissions of the immigrant ships, under the codename FOG, which enabled the interception of the immigrant ships as they approached the shores of Palestine. The

[65] TNA HW 92/2, BRAN/YD 181, 13 February 1947
[66] TNA HW 92/2, BRAN/YD 165, 10 February 1947
[67] TNA HW 92/2, BRAN/YD 441, 15 April 1947
[68] Ferris, *GCHQ*, p. 577

interceptors were instructed to "intercept every ship no matter what size carrying illegal immigrants to PALESTINE", although SIME emphasized: "Need not be unduly disturbed however if small ship succeeds in running gauntlet as this provides degree of cover for OATS".[69]

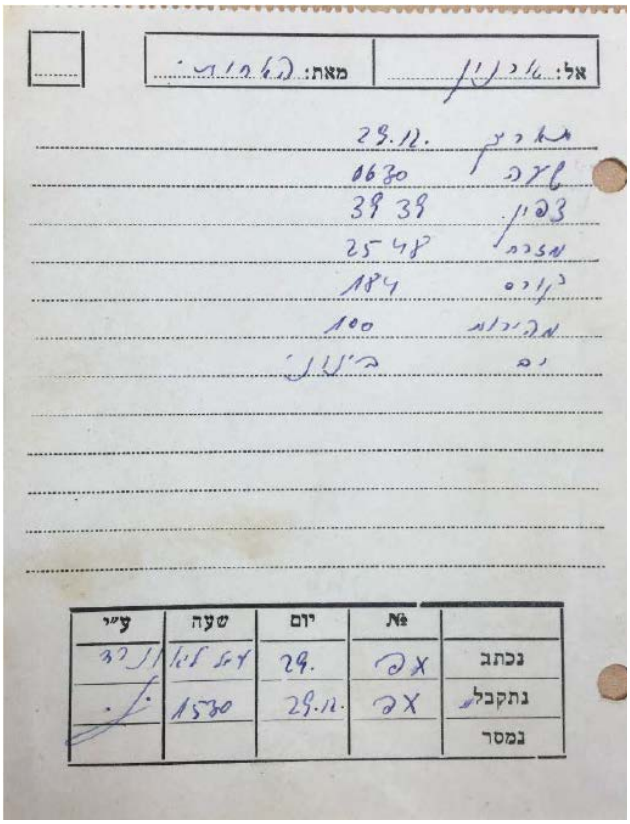
The British Achievement – Sealing Palestine Shores

After World War II, when the Haganah renewed the illegal immigration efforts, radio communication was used on all illegal immigration vessels, which transmitted daily two to three times a message called "XP" (when the longitude was west, they were called "XPM"), which included their location (coordinates), direction of movement, and speed. Streamlining the messaging process, these messages were sent in a uniform fixed format, in numerals only, and were, of course, encrypted. The encrypted "XP" message consisted of six five-letter groups, transmitted over high-frequency radio using Morse code (see Appendix B).

The fixed format, the simple encryption (with a fixed key that did not change during the voyage of the illegal immigration vessel), and the simple content (numerals only) simplified the message decryption.

The British intercepted the transmissions, deciphered the "XP" messages, and were able to track the movement of the illegal immigration vessels. When an illegal immigration vessel approached the Palestine shore, the DSO directed a Royal Air Force reconnaissance aircraft to locate it (these aerial patrols based on this information were codenamed "Sunburn", and later "Bobcat", "Doctor" and "Taffy"). Once the vessel was located, the reconnaissance aircraft guided a Royal Navy vessel to identify and seize it.

[69] *Signals from SLU Cairo*, October 1945 – August 1946, TNA HW 92/4, BRAN/YD 180, 17 August 1946

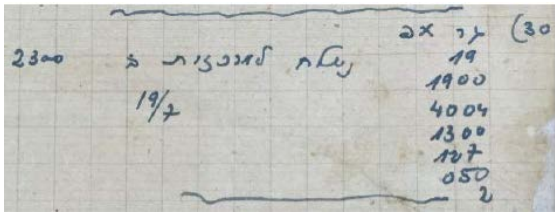


אל: מאת:

29.12.
0630
39 39
25 48
184
100

	יום	שעה	עיר
נכתב	29.		
נתקבל	29.12.	1530	
נמסר			

"XP" message sent from the vessel KIBBUTZ GALUYOT in December 1947 and transmitted to Tel Aviv via Italy
HHA 14/275

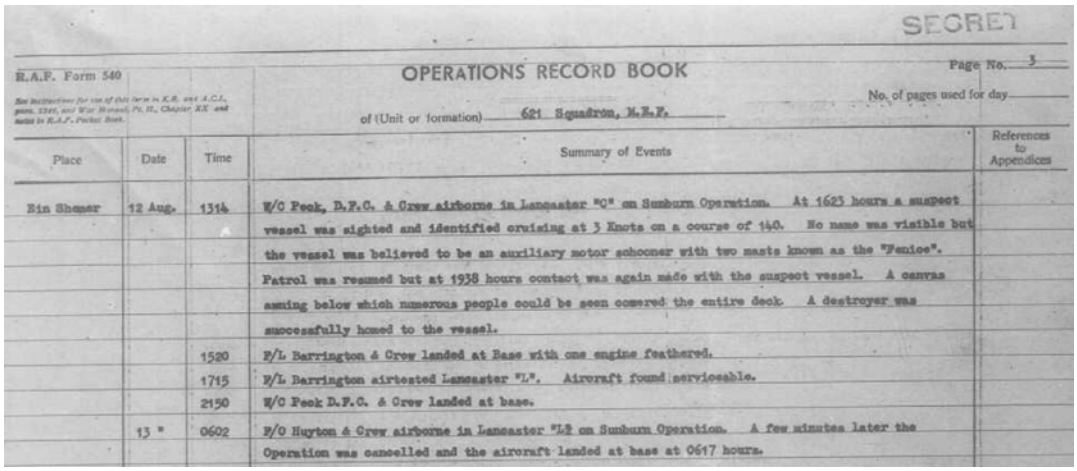


2300 נשלח לתנועת

19/7

19
1900
4004
1300
127
050

"XP" message sent from the vessel YOD DALET HALALEI GESHER HAZIV in July 1946
Tel Aviv radio station log, HHA 14/232



SECRET

R.A.F. Form 540

OPERATIONS RECORD BOOK

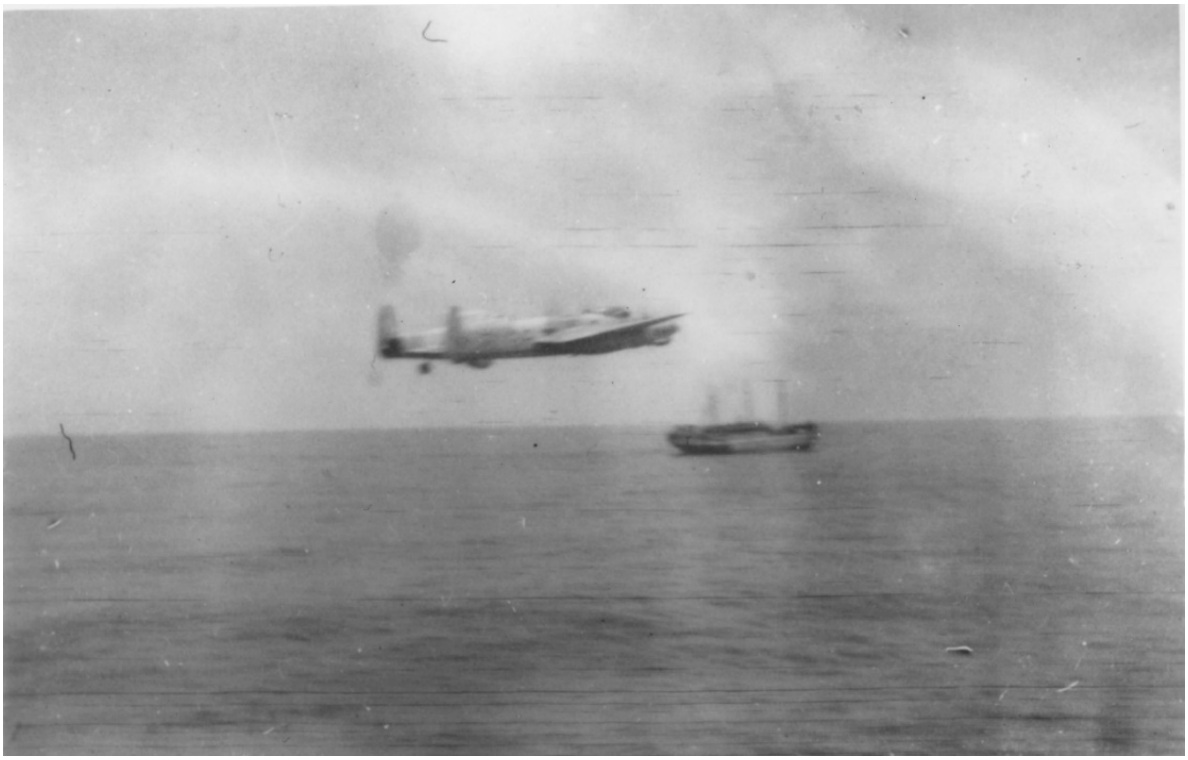
Page No. 3

of (Unit or formation) 621 Squadron, M.E.F.

No. of pages used for day

Place	Date	Time	Summary of Events	References to Appendices
Ein Shemer	12 Aug.	1314	W/C Peck, D.F.C. & Crew airborne in Lancaster "C" on Sunburn Operation. At 1625 hours a suspect vessel was sighted and identified cruising at 3 Knots on a course of 140. No name was visible but the vessel was believed to be an auxiliary motor schooner with two masts known as the "Venice". Patrol was resumed but at 1938 hours contact was again made with the suspect vessel. A canvas awning below which numerous people could be seen covered the entire deck. A destroyer was successfully homed to the vessel.	
		1520	F/L Barrington & Crew landed at Base with one engine feathered.	
		1715	F/L Barrington airtested Lancaster "L". Aircraft found serviceable.	
		2150	W/C Peck D.F.C. & Crew landed at base.	
	13 "	0602	F/O Huyton & Crew airborne in Lancaster "L2 on Sunburn Operation. A few minutes later the Operation was cancelled and the aircraft landed at base at 0617 hours.	

Interception of the illegal immigration vessel KATRIEL YAFFE
The vessel sailed on 31 July 1946 from the coast of Bocca di Magra, Italy, carrying 604 illegal immigrants. Operations record, 12 August 1946, Squadron 621 operating from Ein Shemer airfield. *Squadron 621 Operations Record*, TNA AIR 27/2135/39, p. 95.



A British reconnaissance aircraft, Lancaster GRIII, tracks the illegal immigrant ship LOCHAME-HAGETAOTH

On 13 May 1947, the ship departed from Italy carrying 1,457 illegal immigrants. The British seized it after a fierce battle lasting several hours, using water cannons and tear gas. The vessel was towed to Haifa, and the illegals were deported to Cyprus. The photo was taken on 23 May 1947 from the deck of the British destroyer HMS *Brissenden*.
Courtesy of the Palmach Archive, Freddy Liebrecht Collection 284.

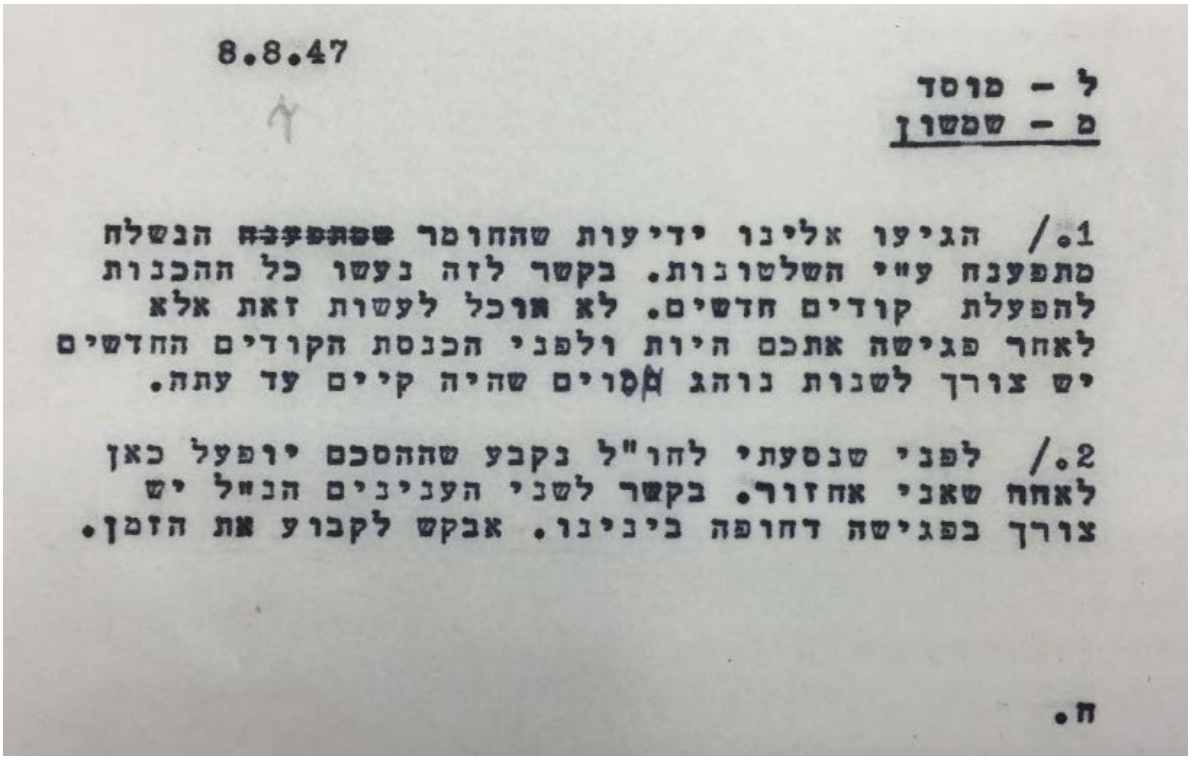
Despite the Haganah's cipher change in late 1946, the British ability to read the illegal immigration vessels messages was not impaired. In August 1947, the Signal Service received information "that the material [from the 'Gideon' network] being transmitted was being read by the authorities",[70] and an additional change was made to the encryption method. This change did not withstand the British.

The interception of the illegal immigration vessels off the Palestine shores was the British most significant success in exploiting their intelligence superiority, and the "XP" messages transmitted by the illegal immigration vessels were the primary British intelligence source for this.

British intelligence had a direct impact on operational decisions. A notable incident in which an order from the Yishuv leadership reached the commander of a British warship before it reached the commander of the illegal immigrant vessel was David Ben-Gurion's instructions

[70] Shimshon Memo, 8 Aug 1947, HHA 534/14 (Hebrew).

to Yossi Harel, emissary of the Mossad LeAliyah Bet and commander of the "Pans" voyage,[71] aboard the illegal immigrants vessel KIBBUTZ GALUYOT, to surrender to the British at sea and sail with the illegal immigrants directly to Cyprus without resistance. This order was sent from Tel Aviv via the Mossad LeAliyah Bet headquarters in Italy on 29 December 1947 at 1520, and its transmission to the "Pans" was delayed. Within 23 hours, on 30 December at 1430, concurrently with Ben-Gurion's order reaching Yossi Harel, the Commander of the British Cruiser Squadron 1, Rear Admiral Richard Symonds-Tayler, aboard the light cruiser HMS Mauritius, received the following telegram from the British military commander in Palestine, classified Top Secret: "Statement now received from reliable high level source that Jewish Agency have wirelessed instructions to Pan. ships that requests or orders issued by Royal Navy including diversion to Cyprus are to be obeyed". This intelligence had a decisive impact on the conduct of the British Navy, as the British believed that seizing the Pan ships by force without heavy casualties was nearly impossible, and therefore granted operational discretion to the British admiral.[72]



8.8.47

ל – מוסד
מ – שמשון

1./ הגיעו אלינו ידיעות שהחומר ~~ששפשפכה~~ הנשלח מתפענח ע"י השלטונות. בקשר לזה נעשו כל ההכנות להפעלת קודים חדשים. לא אוכל לעשות זאת אלא לאחר פגישה אתכם היות ולפני הכנסת הקודים החדשים יש צורך לשנות נוהג ~~מסוים~~ שהיה קיים עד עתה.

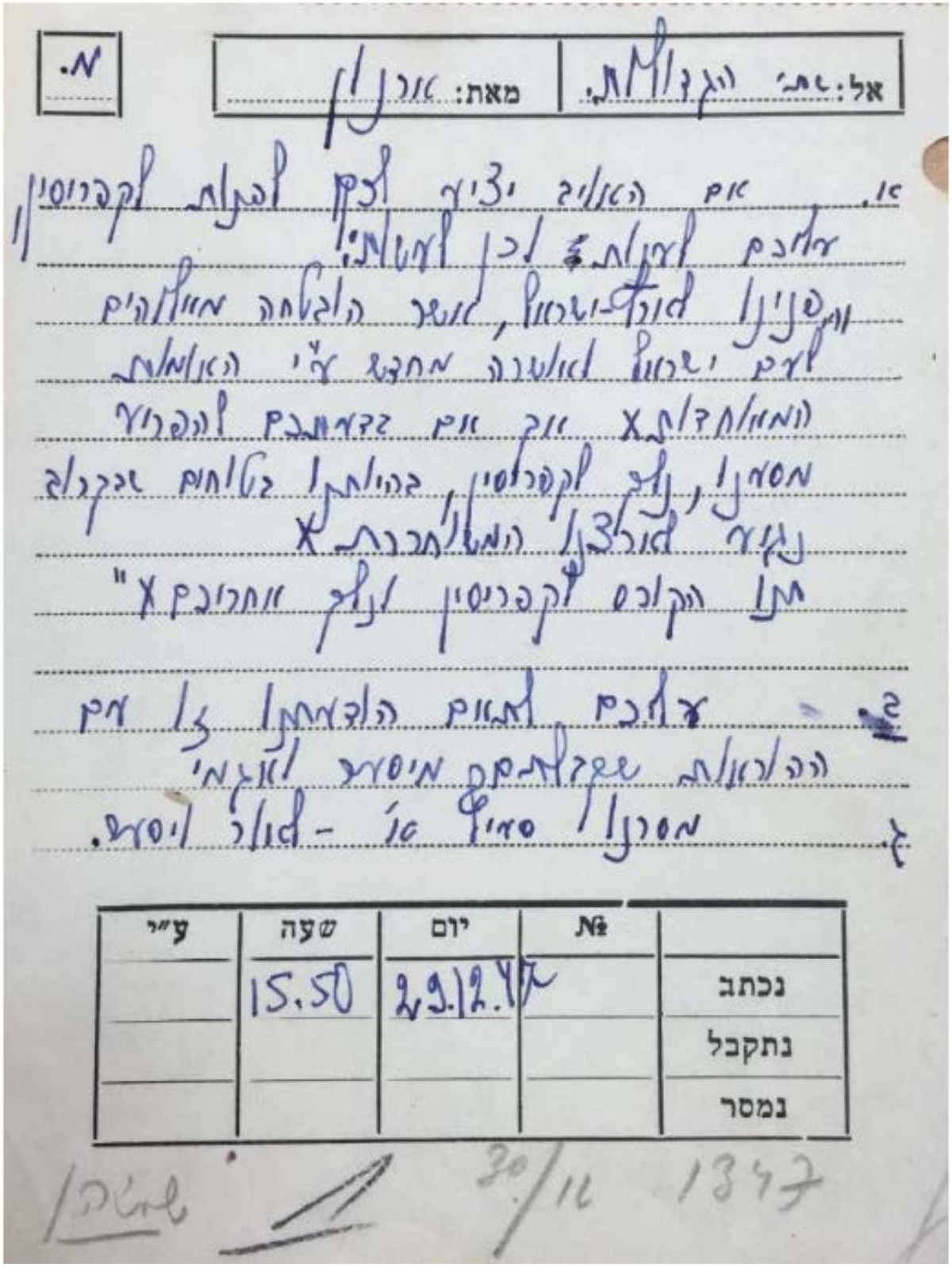
2./ לפני שנסעתי לחו"ל נקבע שההסכם יופעל כאן לאחה שאני אחזור. בקשר לשני העניינים הנ"ל יש צורך בפגישה דחופה ביניינו. אבקש לקבוע את הזמן.

ח.

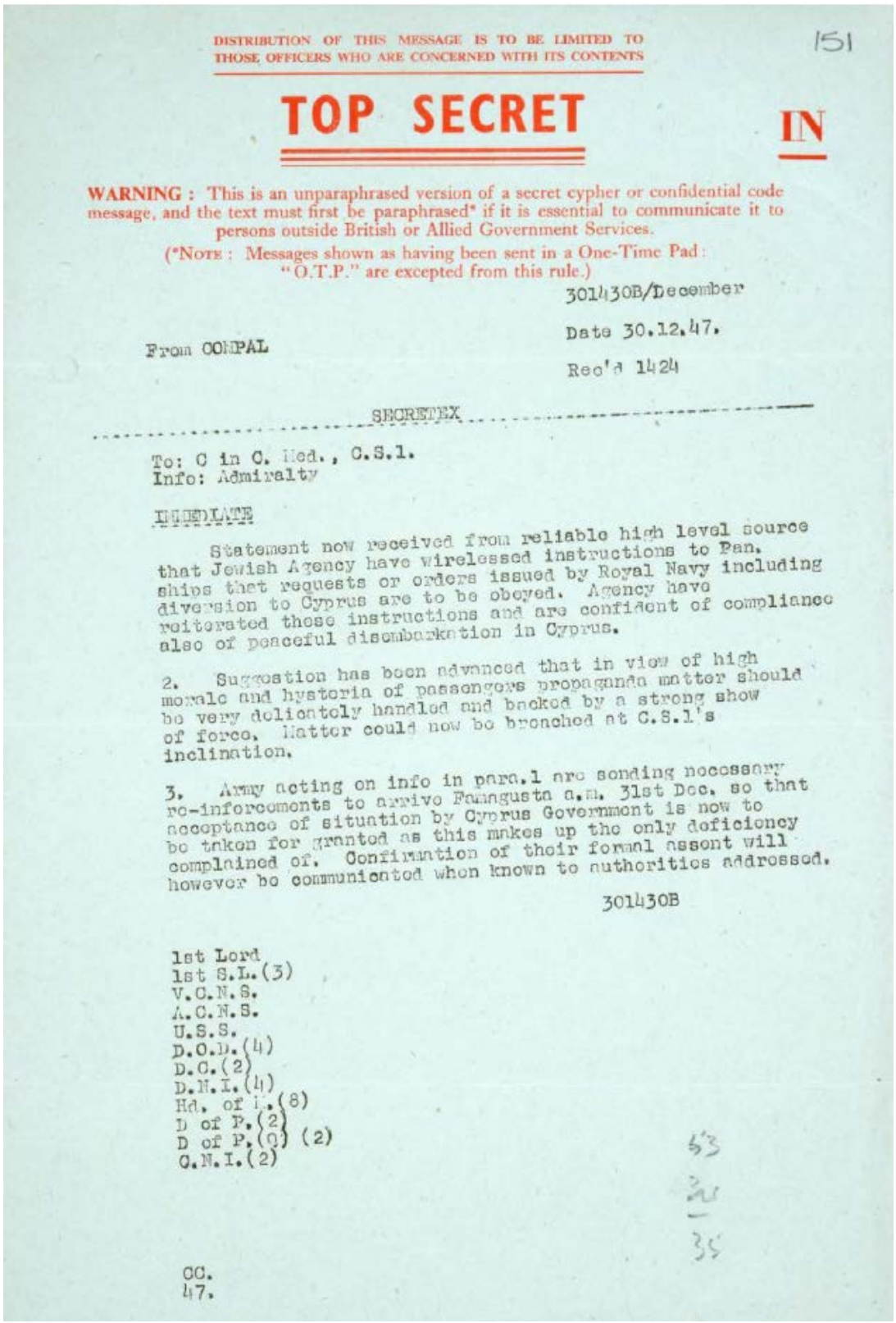
"The [Gideon] messages are deciphered by the authorities. We are ready to implement new codes"
A memo from "Shimson" (Head of Hagana Signal Services) to the Mossad
(Mossad LeAliyah Bet), 8 August 1947, HHA 534/14.

[71] On 27 December 1947, the illegal immigration vessels *Pan York* (KIBBUTZ GALUYOT) and *Pan Crescent* (ATZMAUTH) sailed from Bulgaria, carrying 15,236 illegal immigrants. Known as the "Pans," this was the largest Aliyah Bet operation during the critical period before Israel's establishment.

[72] Daniel Rosenne, *Like a Blind Man in a Chimney: Cipher in the Haganah's Signal Service*, in: Nir Mann (ed.), *The Imperial Turn: Issues in the Study of the Yishuv on the Eve of the British Mandate*, *Olive and Sword*, Vol. 19, Ben Shemen: Modan Publishing; Ramat Efal: The Magen Research Center founded by Israel Galili; Tel Aviv: Ministry of Defense, 2019, pp. 142–145 (Hebrew).



David Ben-Gurion's Order to the "Pans"
An urgent message sent from Tel Aviv (*Arnon*) to the "Pans" (the large immigrant ships) on 29 December 1947 at 1550. The "Received" line was not filled in, and in the margin of the message a pencil note reads: "1347 30/12 both". HHA 14/275.



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

151

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.

From COMPAL

Rec'd 1424

SECRETEX

To: C in C. Med., C.S.1.
Info: Admiralty

IMMEDIATE

Statement now received from reliable high level source that Jewish Agency have wirelessed 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.1's inclination.

3. Army acting on info in para.1 are sending necessary re-inforcements 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)
Hd. of I.(8)
D of P.(2)
D of P.(Q) (2)
C.N.I.(2)

53
2
35

CC.
47.

The British Message

A Top Secret telegram sent by General Sir Alan Gordon Cunningham, Commander of the British Army in Palestine (COMPAL), to the Commander-in-Chief of the British Mediterranean Fleet (C in C Med) and to the Commander of the British Cruiser Squadron 1, on 30 December 1947 at 1430. Both the British and the Mossad LeAliyah Bet used Greenwich Mean Time (GMT). *TNA ADM 1/20793*

To illustrate British intelligence superiority, we present a British report discussing operations against illegal immigration during the four months from September 1947 to the beginning of 1948. During these months, 13 immigrant ships reached Palestine, three of which — ALIYAH, HAPORZIM, and HAUMOT HAMEUCHADOT — broke through the British blockade and landed illegal immigrants on Palestine shores. The British were frustrated by this, and as a result, Major Wright, deputy to the DSO Magan, prepared a debriefing report describing the operations against the illegal immigration vessels under his responsibility.[73] Below is the British document, classified TOP SECRET GLINT FOG, as sent from the DSO in Jerusalem to the Security Service in London and to SIME in Cairo on 12 January 1948:

"1. High percentage of unsuccessful operations to intercept illegal ships during last four months may have caused misgivings in some quarters. Comparative analysis of operations against 11 ships (FARIDA [AF-AL-PI-CHEN] through the Pans [KIBBUTZ GALUYOT and ATZMAUT]), with particular stress on FOG [British codename for interception and decryption of Haganah radio traffic], may therefore be of interest. Am taking FARIDA [AF-AL-PI-CHEN] as the first significant operation because she was the first ship for which FOG had to render usual assistance after period May–August, during which this unnecessary owing to Royal Navy's shadowing tactics [EXODUS 1947 and YUD-DALED HALALEI GESHER HAZIV were shadowed from the start of their voyage by British destroyers].

2. FADUCAH [GEULAH], NORTHLANDS [MEDINAT HAJEHUDIM], GIOVANI MARIA [KAF-TET BENOVEMBER], and the PANS [Pan York (KIBBUTZ GALUYOT) and Pan Crescent (ATZMAUTH)] can be excluded from analysis, because intercepted as result of Naval shadow. Remaining six ships taken in chronological order below.

3. FARIDA [AF-AL-PI-CHEN] (FOG ship 33) [when the British identified radio transmissions from a "new" vessel, they assigned it a serial number, in this case FOG 33. Over time, they analyzed the ship's radio transmissions and constructed a comprehensive picture of the ship's activity, crew, and passengers]:
    a. Overt Aspect: No indication, description, or identity.
    b. FOG Aspect [radio traffic interception and cipher decryption]: Abundant nautical and D/F fixes throughout operation, though little traffic and no indication description or identity.[74]

[73] The report discusses only 11 immigrant ships. It does not address the ships YEHUDA HALEVI and SHIVAT TZION, which sailed from Algeria, were intercepted by the British in the western Mediterranean, and were escorted to Palestine by British destroyers.

[74] Several messages sent from AF-AL-PI-CHEN described it as an LCT, but this important detail was lost during traffic interception or in translation into English.

c. Comment: Despite (a), above available FOG material enabled search to be started at correct time and indicated generally most dangerous area. Also later served to counteract ship's confusing tactics (wearing Egyptian flag and name among Egyptian coastal traffic) by directing suspicion toward her, which confirmed by subsequent R.N. search.

[Note: AF-AL-PI-CHEN was a 300-ton diesel-powered tank landing craft (LCT) launched in Canada in 1941 and sailed under the Italian flag.

AF-AL-PI-CHEN sailed from an open sea coast near the town of Formia, in the Gulf of Gaeta, Italy, on 15 September 1947 with 434 illegal immigrants. The vessel was located by a British reconnaissance aircraft on 26 September, northeast of Port Said. On 27 September, as it approached the Nitzanim coast, it was intercepted by the destroyers HMS Chequers and HMS Talybont, rammed, boarded, and seized after a battle in which live fire was used. The ship was towed to Haifa port, and the illegal immigrants were deported to detention camps in Cyprus. During the resistance to transferring the immigrants to the deportation ships, one immigrant was killed.

AF-AL-PI-CHEN minimized radio communication and maintained no contact at all on the final night.][75]

4. RAFAEL LUCIA **[KADIMA]** (FOG ship 63):
   a. Overt Aspect: Reports of embarkation near VENICE and sailing of suspect ship with few identifiable particulars.
   b. FOG Aspect: Normal amount of nautical and D/F fixes and traffic throughout operation.
   c. Comment: Combination overt and FOG material gave reasonably straightforward operation once FOG confusion with ALIYAH cleared up.

   [Note: KADIMA was a wooden two-masted sailing vessel with a diesel engine, 200 tons in capacity, launched in 1921, sailing under the Italian flag. Captain and crew were Italians, reinforced by an American Jewish mechanic.

   KADIMA was prepared for its voyage in a bay near Venice, Italy. It sailed on 5 November 1947 from the island of Pellestrina, south of Venice, with 794 illegal immigrants, including over 100 infants and toddlers under the age of three.

   A British reconnaissance aircraft located the ship on 15 November, and within a few hours the destroyer HMS Venus approached it, and the following day boarded and seized the ship and led it to Haifa port. Due to the ship's poor condition and the large

[75] Information regarding the illegal immigration vessels and their communications is from the vessels' messages and the original operational reports, preserved in HHA (Rosenne, *Gidonim*).

number of infants and children, there was no resistance to the seizure. The immigrants were sent to detention in Cyprus.

KADIMA maintained proper radio contact throughout the voyage.]

5. ALIYAH (FOG ship 64):
   a. Covert Aspect: Complete absence information.
   b. FOG Aspect: FOG alone revealed ship, but only when initial confusion with RAFAEL LUCIA [KADIMA] finally cleared up. This only two and a half days before arrival. During last stages, bearing only receives and, once inside search area, ship kept W/T silence for over 48 hours. No useful ship's traffic received before conclusion operation.
   c. Comment: Complete lack overt information and ship's W/T tactics created difficulties. Hence, although reported by R.A.F. of BEIRUT, hugging coast among similar craft at that time, no reason to consider her suspect.

   [Note: ALIYAH was a 109-ton cargo vessel, launched in 1945 and sailing under the Italian flag. Captain and crew were Italians.

   ALIYAH sailed on 5 November 1947 from a coast in the Bay of Bandol, France, with 184 illegal immigrants.

   ALIYAH's radio was not functioning, and it was repaired only on 15 November, when ALIYAH approached the Lebanese coast. Only at this stage, ALIYAH reported its location. At that time, only a few dozen miles separated KADIMA from ALIYAH. At this point, the ship was given the operational name ALIYAH and the order to attempt to break the blockade at the Nahariya coast. British reconnaissance aircraft and destroyers inspected the ship but did not identify it as an illegal vessel. At dawn on 16 November, it landed on the shore at Nahariya, the illegal immigrants disembarked quickly, boarded buses, and were dispersed among settlements in the Western Galilee.]

6. BLOCKADE RUNNER [HAPORZIM] (FOG ship 65):
   a. Overt Aspect: Complete absence information.
   b. FOG Aspect: Abundant nautical and D/F fixes and traffic (though latter afforded no descriptive particulars) through operation.[76]
   c. Comment: FOG enabled start of search at correct time and indicated generally most dangerous area. Also served to direct suspicion toward the right ship, which sighted by R.A.F. and later inspected by R.N. despite employment tactics similar to FARIDA

[76] A description of the ship was detailed in a message sent from "Sidney" (the Mossad LeAliyah Bet headquarters in France) to "Arnon" (the Mossad LeAliyah Bet headquarters in Tel Aviv) on 23 November, but it appears the British did not intercept this message. HHA 14/219.

[AF AL PI CHEN]. Was however declared innocent. Failure due entirely to absence descriptive particulars and any reaction from ship when inspected by R.N.

[Note: HAPORZIM was a wooden cargo vessel with a diesel engine and sails, 200 tons in capacity, launched in 1927 and sailing under an Italian flag. Captain and crew were French.

HAPORZIM sailed from Bandol, France, on 22 November 1947 (a week before the UN Palestine Partition Plan vote), with 123 illegal immigrants. The ship sailed to Corsica, where it met the ship HECHALUTZ, which transferred to it 44 youths it had gathered during a failed illegal immigration attempt from the Algiers area. After the rendezvous, it continued toward Palestine.

HAPORZIM was painted red and disguised as a Turkish vessel. Near Port Said, HAPORZIM was inspected by a British destroyer, which did not identify its purpose and withdrew. It continued northward and arrived on 4 December before dawn at the landing point near the Yarkon estuary in Tel Aviv, disembarked the illegals, and departed.

HAPORZIM radio operated properly throughout the voyage.]

7. UNAFRAID [LO TAFCHIDUNU] (FOG ship 67):
   a. Covert Aspect: No useful overt information available, apart from general reports of several suspect ships in PORTO VENERE area at crucial time, which gave certain indication of possible identity.
   b. FOG Aspect: Normal amount nautical and D/F fixes and traffic, though latter of no great help to operation.
   c. Comment: Generally, as in case of FARIDA [AF-AL-PI-CHEN], MUTATIS MUTANDIS.

   [Note: LO TAFHCHIDUNU was a wooden ship with a diesel engine, 500 tons in capacity, launched in 1946 and sailing under the Italian flag. Captain and crew were Italians.

   LO TAFHCHIDUNU was prepared for its voyage at the port of La Spezia, Italy. It sailed on 11 December 1947 from the area of Civitavecchia, Italy, with 850 illegal immigrants. The boarding was done at sea by boats at night under the disguise of filming a movie.

   Reconnaissance aircraft located LO TAFHCHIDUNU on 22 December, and within a few hours the destroyer HMS Chequers arrived, reinforced by the destroyer HMS Volage and the auxiliary ship HMS Mermaid. The following morning, LO TAFHCHIDUNU was boarded and seized. There was no resistance; the ship was

towed by the auxiliary ship HMS Mermaid to Haifa port, and the illegals were deported to Cyprus.

LO TAFHCHIDUNU's radio operated properly throughout the voyage.]

8. ARCHIMEDES [HAUMOT HAMEUCHADOT] (FOG ship 68):
   a. Overt Aspect: Complete absence information.
   b. FOG Aspect: Reasonable number nautical and D/F fixes during second half voyage, but negligible traffic of no assistance. No position report received for last 48 hours.
   c. Comment: Very scanty information from all sources. Sole grounds for search at right time obtained from FOG. One cause of failure was organizers' immediate switching of totally unsuspect ship from legal to illegal run, which beat reporting agencies and rendered descriptive particulars of all known suspects valueless to Navy and R.A.F. Second was failure of R.A.F. to sight and report ship on first day of search.

   [Note: HAUMOT HAMEUCHADOT was a wooden vessel with sails and a diesel engine, 350 tons in capacity, launched in 1920 and sailing under the Italian flag. Captain and crew were Italians.

   HAUMOT HAMEUCHADOT was prepared for its voyage in Porto Venere. On 24 December 1947, while anchored near the coast, north of Civitavecchia, Italy, 537 immigrants boarded via an improvised gangway: two rubber boats and a cable stretched between the pier and the ship. The illegal immigrants — members of youth movements from Hungary, Rumania, and Poland — were young, with an average age of about 35.

   The voyage lasted eight days without notable events. In the final two days, special preparations were made to prevent the ship from being identified as an illegal immigrant vessel: the kitchen and bathing facilities built on deck were thrown overboard. The illegal immigrants ate only canned food, were ordered to remain below deck, and were allowed to use the toilets only at night.

   Near its arrival at the shores of Palestine, on 1 January 1948, HAUMOT HAMEUCHADOT was located by aircraft, which summoned the destroyer HMS Chevron. HAUMOT HAMEUCHADOT's commander quickly changed course and brought the ship ashore near Nahariya. The illegals disembarked using boats and by sliding down a cable, were received on shore by Palyam members and local residents, and quickly dispersed from the beach.

   HAUMOT HAMEUCHADOT's radio malfunctioned as it neared Palestine, and it had only a single radio contact, on 31 December.]

9. SUMMING UP: Above analysis shows:

a. That in cases of three intercepted ships, available FOG material ample for operational purposes. In one case well supported and in another supported by overt information.
b. Complete absence of overt information in cases of three ships not intercepted.
c. That FOG alone revealed each of the three ships, being solely responsible for institution of search, and at correct time.
d. That beyond this FOG assistance was slight in one of the three cases (ALIYAH), abundant in one case (BLOCKADE RUNNER [HAPORZIM]), and normal in third case (ARCHIMEDES [HAUMOT HAMEUCHADOT]).
e. That in one of these three cases (BLOCKADE RUNNER [HAPORZIM]), ship was actually inspected at close quarters by Navy and in another (ARCHIMEDES [HAUMOT HAMEUCHADOT]) should have been sighted by R.A.F.

10. GENERAL CONCLUSIONS:

a. No significant points emerge from these three successful operations which followed usual course.
b. Absence of overt information (Paragraph 9.b above) invariably hampers successful interception but is not in itself adequate reason for failure.
c. Appears that recent ships have maintained consistently better W/T security within search area.
d. Nevertheless, despite sometimes scanty material, FOG played its part entirely satisfactorily in each of three unsuccessful operations by instituting search at right time and (with possible exception of ALIYAH and the later stages ARCHIMEDES [HAUMOT HAMEUCHADOT]) by giving accurate picture of ship's probable movements.
e. Whereas R.N. ships and R.A.F. did very good work on sometimes unsatisfactory material in three successful operations, failure in at least two of other three operations is attributed to incomplete reporting by R.A.F. (ARCHIMEDES [HAUMOT HAMEUCHADOT]) and failure to elicit any guilty reaction by R.N. inspection of BLOCKADE RUNNER [HAPORZIM].

11. This has been written in consultation with, and agreement of NLO".[77]

[77] *Signals from SLU Clover (Jerusalem)*, January 1948, TNA HW 92/3, BRAN/YD 152, 12 January 1948.



The Gideonit Yochi (Yocheved) Yahel (Sverovich) operates a clandestine radio station in the Gideon network, Monte Mario, Rome, 1947.
Courtesy of the Palmach Archive, 17096.

Epilogue

The achievement of British COMINT in intercepting the Haganah and the Jewish Agency Political Department radio networks, and breaking the ciphers, created British intelligence superiority, which served British policymakers and security forces from 1942, when cooperation between the Yishuv and the British ceased. The Haganah and Jewish Agency messages were "an open book" to the British, and this intelligence was an important tool for shaping British policy and operations toward the Yishuv.

The British maintained strict "source security" and developed an efficient system for collecting, processing, analyzing, and distributing information to a limited number of indoctrinated trusted partners, in cooperation between GCHQ and the Security Service (MI5). For this purpose, a dedicated intelligence unit was established in Jerusalem, headed by a DSO (Defence Security Officer).

The exposure of the Haganah and the Jewish Agency to the British cipher superiority, following the publication of the "White Paper" in July 1946 — through which the British attempted to prove that the Jewish Agency was a terrorist organization — prompted an immediate response, and from September 1946 the ciphers of the Haganah and the Jewish Agency Political Department were replaced. The British intelligence source dried up. From intelligence superiority, the British transitioned to an intelligence blackout — at a critical time for shaping their policy on the question of Palestine.

After the publication of the "White Paper" in July 1946, the primary and most significant (and nearly sole) British intelligence achievement derived from intercepting the Mossad LeAliyah Bet radio network and decrypting its messages was the sealing of the Palestine shores against illegal immigration ships (see Appendix C). Without this achievement, most illegal ships would have reached Palestine, thereby reshaping the political constraints of the Mandate.

The campaign against illegal immigration was a public relations disaster for Britain, a highly unpleasant duty for the Royal Navy, the Royal Air Force and the British Army, but in their view, it was necessary for implementing British policy on the question of Palestine. The British command assessed that successful illegal immigration would lead to unrest in Palestine[78] and that the Mandate police would be unable to handle the arrest of illegal immigrants arriving on Palestine shores.[79]

The intelligence obtained from intercepting immigrant ship transmissions and decrypting ciphers, codenamed FOG, was disguised as "reliable intelligence" to conceal from British personnel the use of COMINT (using "source security" methods similar to those used to conceal the decryption of Nazi Germany's ciphers during the war).[80] It was used to dispatch reconnaissance aircraft and warships to appropriate locations to intercept illegal immigration ships and enabled the British to succeed in their mission. Most ships were intercepted, and the illegal immigrants were sent to detention in Cyprus. This was a significant contribution of British COMINT to the implementation of British policy objectives in Palestine.

The "disaster" — finding that the Signal Service cipher was read by the British — was a formative event in the history of the Signal Service.[81] The 1946 "disaster" caused senior Signal Service officials to become conservative and cautious and led to a substantial investment of resources and means in cipher systems. The ciphers and the supporting system for their operation were institutionalized in the IDF from early years.

The cipher used prior to the establishment of the State of Israel, during the period when the Signal Service operated as a clandestine organization, was characterized by "short" encryption

---

[78] *Signals from SLU Cairo*, October 1945 – August 1946, TNA HW 92/4, BRAN/CO 15, 9 October 1945.
[79] *Signals from SLU Cairo*, October 1945 – August 1946, TNA HW 92/4, BRAN/CO 99, 17 May 1946.
[80] *Signals from SLU Clover (Jerusalem)*, January 1948, TNA HW 92/3, BRAN/YD 221, 27 January 1948.
[81] Daniel Rosenne, Mordechai Popper, *The Sealed Book – The Origins of Cryptography in the IDF*, Association for the Commemoration of the Fallen of the IDF Signal and Cyber Corps, December 2021 (Hebrew).

keys that were infrequently changed. With the establishment of the state, it became possible to use one-time cipher keys, resulting in a significant improvement in quality and security. Information security in the early years of the IDF was entirely different from that of today: in its early years, the primary classified communication was the transmission of letters via military mail or transmission through physical lines, and only urgent messages were sent by radio, most of which were encrypted.

In the modern era, communications equipment and information systems are widely used; the IDF operates and fights in cyberspace, and protecting the cyber domain involves not only communication encryption but a broad array of measures. The cipher systems used by the IDF have evolved over the years and are no longer similar to those used before the establishment of the State of Israel and in its early years, but the importance of ciphers remains unchanged, and the question of how much one can trust a cipher remains unresolved.

Appendices

To complete the picture, the following appendices are attached:

- Appendix A: Encryption methods in the Haganah Signal Service.
- Appendix B: “XP” Message.
- Appendix C: Interception of Illegal Immigrant Vessels.

Appendix A: Encryption Methods in the Haganah Signal Service

Hebrew Aspects

In this appendix, two encryption methods used by the Haganah Signal Service are presented: (a) a transposition cipher; and (b) a keyed polyalphabetic cipher.

To simplify the examples, which were performed originally in Hebrew, the Hebrew processes are converted into equivalent English ones.

There are some facts the reader should know about Hebrew:

- The Hebrew alphabet consists of 22 basic letters (see the table below) and is written from right to left.
- Five Hebrew letters have different terminal forms used as the final character of a word. These are not used in morse code or in the encryption process, where they are always substituted in the plaintext and ciphertext by the corresponding non-terminal letter.
- Every one of the basic 22 Hebrew letters has a corresponding Morse Code equivalent (see the following table).
- The Haganah Signal Service made operational use of the Latin Morse symbols F, V, X, and Y for punctuation and spacing (F for period, V for comma, X for emphasis, Y for space). These symbols do not correspond to Hebrew alphabetic characters and may alternatively be treated as nulls in plaintext.
- The Hebrew letters and Morse code equivalents are presented in the following table.

Hebrew			English Morse Equivalent
Letter	**Transliteration**	**Alphabetical order**	
א	Aleph	1	A
ב	Beit	2	B
ג	Gimel	3	G
ד	Daleth	4	D
ה	Hei	5	O
ו	Vav	6	E
ז	Zayin	7	Z
ח	Het	8	H
ט	Tet	9	U
י	Yod	10	I
כ	Kaf	11	K
ל	Lamed	12	L
מ	Mem	13	M
נ	Nun	14	N
ס	Samekh	15	C
ע	Ayin	16	J
פ	Pei	17	P
צ	Tzadei	18	W
ק	Qof	19	Q
ר	Reish	20	R
ש	Shin	21	S
ת	Tav	22	T

The Yugoslav Transposition Cipher

Prior to World War II, the Yugoslav military employed several forms of columnar transposition. One such method was later adopted by the Haganah Signal Service through a member who had previously served as a Yugoslav Signal officer.

A transposition cipher writes plaintext letters into an encryption grid — often determined by a keyword — and then extracts the letters in a prescribed order to form the ciphertext.[82] The letters themselves are unchanged; only their positions are permuted.

The Yugoslav Transposition Cipher is a distinctive variant that may be described as a columnar transposition with keyword-determined row truncation.

The method begins with an agreed-upon keyword of length *N*. The letters of the keyword are converted into a numerical key consisting of the numbers *1* through *N*, assigned in alphabetical

[82] The numerical key's permutation is defined by the alphabetical order of the letters in the keyword. For example, see Gaines, Helen Fouché. *Cryptanalysis: A Study of Ciphers and Their Solution,* Dover Publications, 1956, page 17.

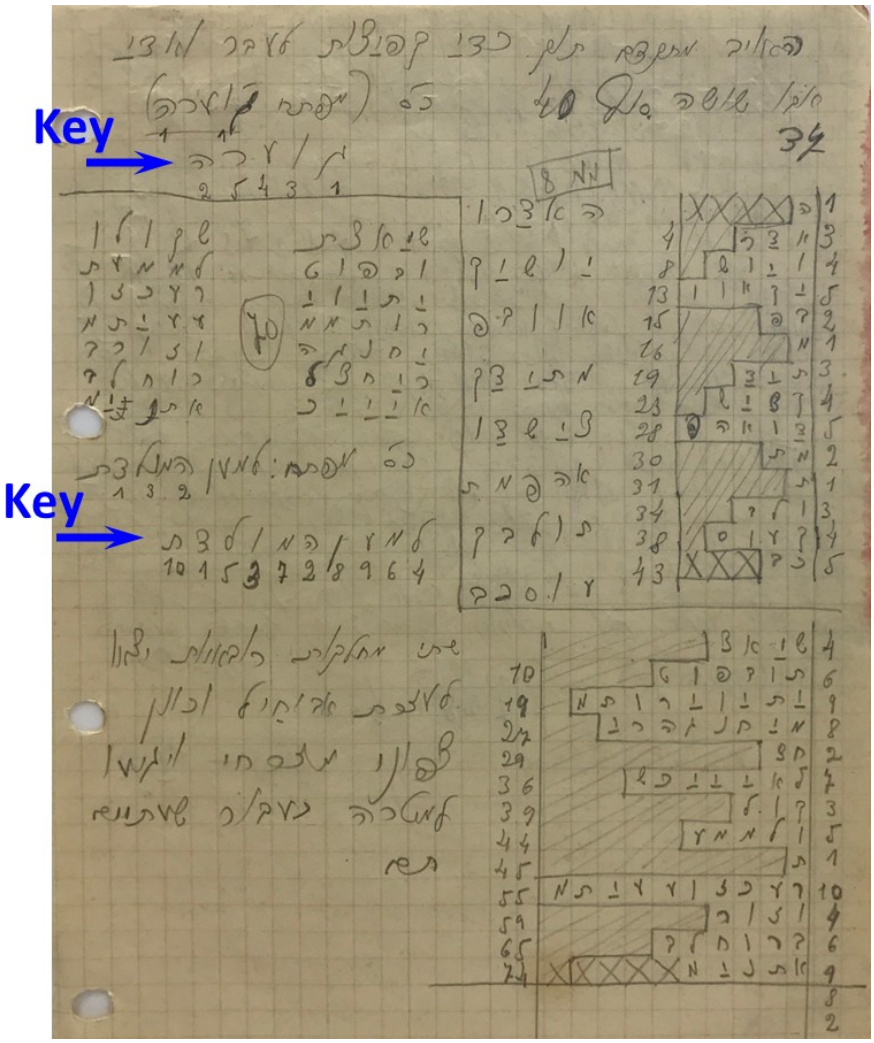
order of the keyword's letters. This numerical key determines the number of active cells in each row of the encryption grid.

The grid is arranged in rows whose maximum length is *N*. For each row, the number of active cells is given by the next value of the numerical key; inactive cells are left blank or blackened out. The numerical key is repeated cyclically until enough rows exist to accommodate the entire plaintext.

As Hebrew is written right-to-left, the following paragraphs describe the inscribing and extracting of the text from right to left.

- The plaintext is then written vertically, column by column, from right to left, into the active cells of the grid. When a column is filled, writing continues at the top of the next column.
- The ciphertext is obtained by reading the active cells row by row, from right to left, and grouping the output into five-letter groups.

Two original examples (in Hebrew) appear in the following worksheet.



Transposition Cipher Example
Source: HHA 80/1

For the non-Hebrew reader, the cipher method is demonstrated by converting the two examples from right-to-left Hebrew to left-to-right Latin characters.

The first example above is as follows:

a. Plain Text (40 characters):
OAEIB MTQDM TEK KDI QPIWET LJBR EADI ABE SESO SEP
[Translation: Enemy advancing by bounds towards Wadi Abu Shusa End]

b. Keyword:

Keyword	G	E	J	R	O
Numerical value	1	3	4	5	2

c. Grid:

Key Value	Plaintext					Count
1	O					1
3	A	D	R			4
4	E	I	E	S		8
5	I	Q	A	E	E	13
2	B	P				15
1	M					16
3	T	I	D			19
4	Q	W	I	S		23
5	D	E	A	O	P	28
2	M	T				30
1	T					31
3	E	L	B			34
4	K	J	E	S		38
5	K	B	X	X	X	43

d. Encrypted message:

OADRE UESIQ AEEBP MTIDQ WISDE AOPMT TELBK JESKB XXX

The Second example above is as follows:

a. Plain Text (70 characters):
STI MHLQET REBAIET IWAE LJZRT ABIHIL EKEEN WPENI MZRHI EIGIJE LMTRO KJBER SJTIIM TM
[Translation: Two rifle platoons went to aid Avihail towards NE will reach destination in two hours End]

b. Keyword:

Keyword	L	M	J	N	O	M	E	L	D	T
Numerical value	4	6	9	8	2	7	3	5	1	10

c. Grid:

Key Value	Plaintext										Count
4	S	I	A	W							4
6	T	E	B	P	E	T					10
9	I	T	I	E	I	R	E	T	M		19
8	M	I	H	N	G	O	R	I			27
2	H	W									29
7	L	A	I	I	I	K	S				36
3	Q	E	L								39
5	E	L	E	M	J						44
1	T										45
10	R	J	K	Z	E	J	J	I	T	M	55
4	E	Z	E	R							59
6	B	R	E	H	L	B					65
9	A	T	N	I	M	X	X	X	X		74

d. Encrypted message:

```
SIAWT EBPET ITIEI RETMM IHNGO RIHWL AIIIK SQELE LEMJT RJKZE
JJITM EXERB REHLB ATNIM XXXX
```

The Polyalphabetic Cipher (20 × 20 Square)

Following the 1946 "White Paper", the Signal Service switched to a polyalphabetic substitution cipher, memorizing the Vigenère-like cipher by using a 20-letter alphabet and arithmetic operations modulo 100. A 10-letter encryption keyword was used, taken from an agreed page in a novel or a line from a poem, and was frequently changed.

To avoid being found with incriminating enciphering material, no physical table was used; Signal Service operators memorized "Arithmetic Rules" for encryption and decryption,[83] based on the "Numerical Value" of each letter.

Key characteristics of the system:

- Only 20 letters were encrypted: 'Shin' (S) was replaced by 'Tav' (T); 'Tav' (T) was replaced by 'Shin' (S); The letters 'F', 'V','X' and 'Y' were not encrypted.
- Notation: K = key letter; P = plaintext letter, C = ciphertext.
- Arithmetic Rules:
  - Encryption: C = (K + P) (mod 100);
  - Decryption: P = (C – K) (mod 100).[84]

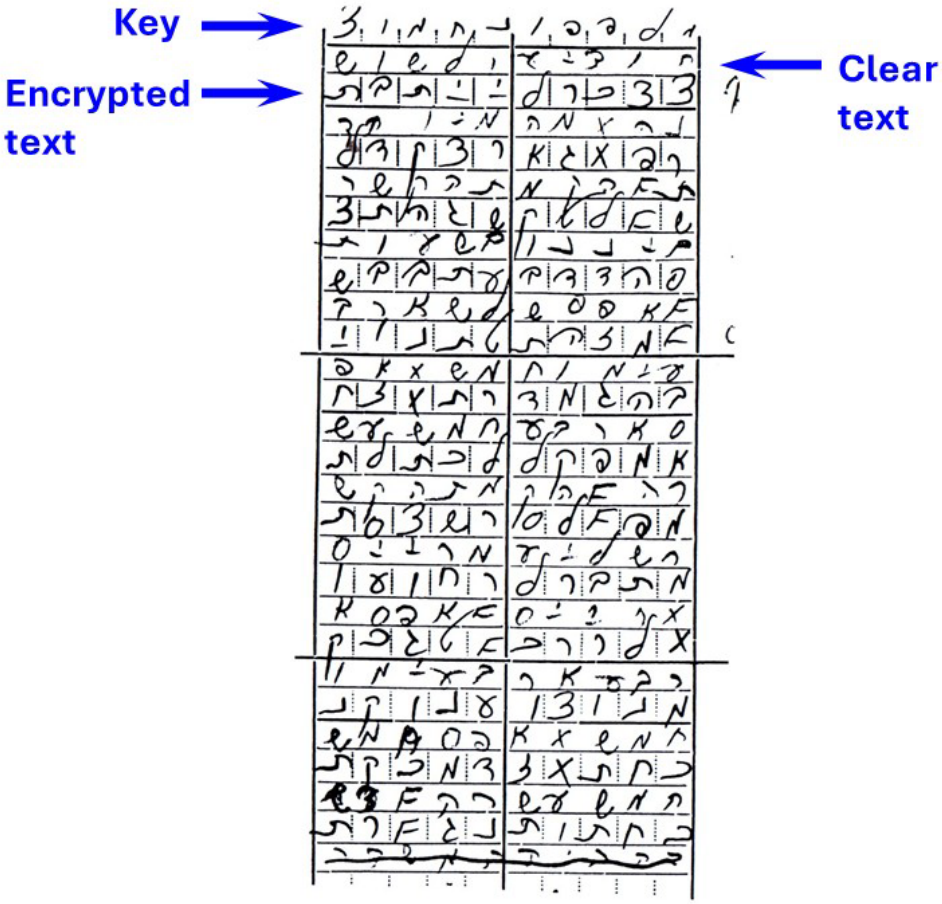
[83] When interviewed years later, Haganah Signal Service personnel reported they did not use a Vigenère table, instead having memorized enciphering rules consisting of addition and subtraction. None of them remembered what those rules were, and no references to these rules were ever located in archives. These rules were reconstructed by the author.

[84] (mod 100) is a mathematical way of saying "take a number and keep only its last two digits".

The “Numerical Value” of each letter, used for this calculation, was assigned according to the following table:

Hebrew		English Morse Equivalent	Numerical Value
Letter	**Transliteration**		
א	Aleph	A	10
ב	Beit	B	20
ג	Gimel	G	30
ד	Daleth	D	40
ה	Hei	O	50
ו	Vav	E	60
ז	Zayin	Z	70
ח	Het	H	80
ט	Tet	U	90
י	Yod	I	15
כ	Kaf	K	25
ל	Lamed	L	35
מ	Mem	M	45
נ	Nun	N	55
ס	Samekh	C	65
ע	Ayin	J	75
פ	Pei	P	85
צ	Tzadei	W	95
ק	Qof	Q	5
ר	Reish	R	100

Encryption and decryption used a special enciphering form (see the following figure). The keyword was written on the top line of the form. For encryption (transmitting), the clear text was written horizontally along every second line, and the encrypted text was written in the lines underneath; for decryption (receiving), the encrypted text was written every second line, and the clear text was written underneath.



Message Encryption Form Example (in Hebrew, right to left))
Courtesy of Reuven Oren.[85]

The example above, in Latin letters (Left to right):

a. Plain text:

`OEDIJE LSESNO X MOMIEHDT F OQMT OQSR BINNE BSJET F APC SLS ARBJIM EHMS X APC ARBJ HMS JSRO F OQMT OQSR SLI JM RIIC RIIC F APC ARBJ ARBJIM EHMS X APC HMS HMS JSRO F DS`

[Translation: Inform SHOSHANA [Haifa] from the special [the vessel KARISH]. Establish contact between us at 0345, 0415. My contact with REIS [Cyprus] at 0445, 0515. Regards]

b. Keyword: `MLPPENHMEW`

[85] Reuven Oren (1927–2017). Born in Argentina. (Oren's father, a medical doctor from Vienna, Austria, worked in the Baron Maurice de Hirsch Jewish agricultural settlements in Argentina. In order to raise the sum of 1,000 British pounds required by the British authorities to receive an immigration certificate to Palestine, he worked there until the family immigrated to Palestine in 1935.) Volunteered for the Palmach in 1945. Served as a 'Gideoni' (radio operator) on the illegal immigration vessels HAMAAPIL HAALMONI, KIBBUTZ GALUYOT, LANITZAHON, HAPORTZIM M 17 (arms-smuggling vessel), and KARISH (a vessel smuggling illegal immigrants from Cyprus to Palestine). Served during the War of Independence in the Israeli Navy and the Jerusalem Brigade. Studied electrical engineering and worked as an electronics engineer.

c. Form:

Keyword	M	L	P	P	E	N	H	M	E	W
Clear	O	E	D	I	J	E	L	S	E	S
Cipher	W	W	K	R	L	I	I	T	B	T
Clear	N	O	X	M	O	M	I	E	H	D
Cipher	R	P	X	G	A	R	W	Q	D	L
Clear	T	F	O	Q	M	T	O	Q	S	R
Cipher	S	F	L	U	Q	S	G	O	T	W
Clear	B	I	N	N	E	B	S	J	E	T
Cipher	C	O	D	D	B	J	T	B	B	S
Clear	F	A	P	C	S	L	S	A	R	B
Cipher	F	M	Z	O	T	U	T	N	E	I
Clear	J	I	M	E	H	M	S	X	A	P
Cipher	B	O	G	M	D	R	T	X	Z	H
Clear	C	A	R	B	J	H	M	S	J	S
Cipher	A	M	P	Q	L	L	K	T	L	T
Clear	R	O	F	O	Q	M	T	O	Q	S
Cipher	M	P	F	L	C	R	S	W	C	T
Clear	R	S	L	I	J	M	R	I	I	C
Cipher	M	T	B	R	L	R	H	E	J	E
Clear	X	R	I	I	C	F	A	P	C	A
Cipher	X	L	R	R	K	F	U	G	K	Q
Clear	R	B	J	A	R	B	J	I	M	E
Cipher	M	N	E	W	E	J	N	E	Q	N
Clear	H	M	S	X	A	P	C	H	M	S
Cipher	K	H	T	X	Z	D	M	K	Q	T
Clear	H	M	S	J	S	R	O	F	D	S
Cipher	K	H	T	E	T	N	G	F	R	T

d. Encrypted message:

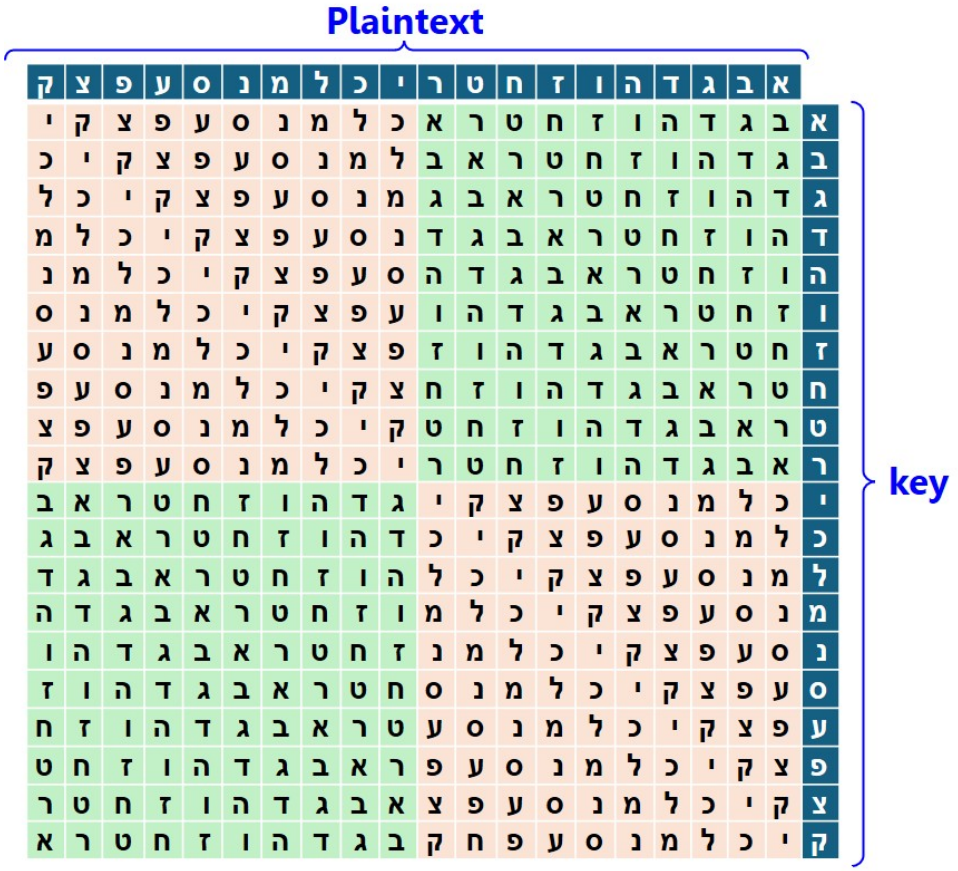
```
WWKRL  IITBT  RPXGA  RWQDL  SFLUQ
SGOTW  CODDB  JTBBS  FMZOT  UTNEI
BOGMD  RTXZH  AMPQL  LKTLT  MPFLC
RSWCT  MTBRL  RHEJE  XLRRK  FUGKQ
MNEWE  JNEQN  KHTXZ  DMKQT  KHTET
NGFRT
```

The polyalphabetic substitution employed a 20-letter square with a mixed cipher alphabet, as shown on the following page.[86]

As this cipher was not based on a truly random one-time key, it was vulnerable to classic polyalphabetic cryptanalytic methods.

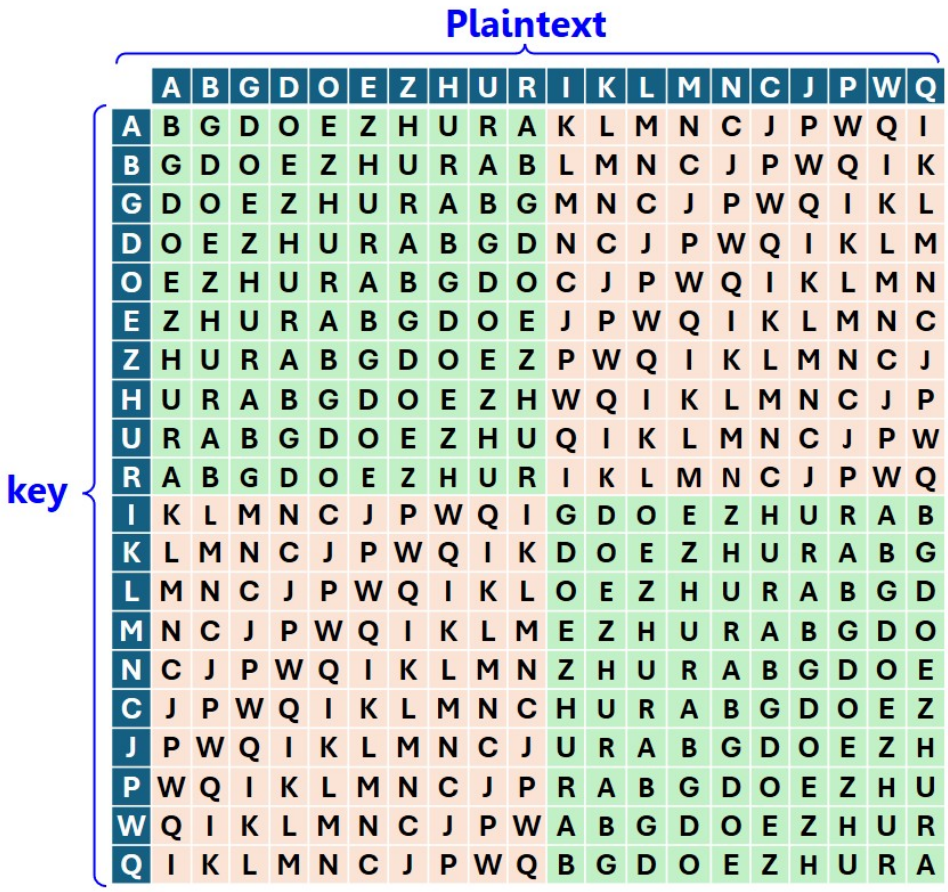
[86] The 20 × 20 square was reconstructed by Moshe Rubin.

20 × 20 square Hebrew version



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

20 × 20 square English translation



	A	B	G	D	O	E	Z	H	U	R	I	K	L	M	N	C	J	P	W	Q
A	B	G	D	O	E	Z	H	U	R	A	K	L	M	N	C	J	P	W	Q	I
B	G	D	O	E	Z	H	U	R	A	B	L	M	N	C	J	P	W	Q	I	K
G	D	O	E	Z	H	U	R	A	B	G	M	N	C	J	P	W	Q	I	K	L
D	O	E	Z	H	U	R	A	B	G	D	N	C	J	P	W	Q	I	K	L	M
O	E	Z	H	U	R	A	B	G	D	O	C	J	P	W	Q	I	K	L	M	N
E	Z	H	U	R	A	B	G	D	O	E	J	P	W	Q	I	K	L	M	N	C
Z	H	U	R	A	B	G	D	O	E	Z	P	W	Q	I	K	L	M	N	C	J
H	U	R	A	B	G	D	O	E	Z	H	W	Q	I	K	L	M	N	C	J	P
U	R	A	B	G	D	O	E	Z	H	U	Q	I	K	L	M	N	C	J	P	W
R	A	B	G	D	O	E	Z	H	U	R	I	K	L	M	N	C	J	P	W	Q
I	K	L	M	N	C	J	P	W	Q	I	G	D	O	E	Z	H	U	R	A	B
K	L	M	N	C	J	P	W	Q	I	K	D	O	E	Z	H	U	R	A	B	G
L	M	N	C	J	P	W	Q	I	K	L	O	E	Z	H	U	R	A	B	G	D
M	N	C	J	P	W	Q	I	K	L	M	E	Z	H	U	R	A	B	G	D	O
N	C	J	P	W	Q	I	K	L	M	N	Z	H	U	R	A	B	G	D	O	E
C	J	P	W	Q	I	K	L	M	N	C	H	U	R	A	B	G	D	O	E	Z
J	P	W	Q	I	K	L	M	N	C	J	U	R	A	B	G	D	O	E	Z	H
P	W	Q	I	K	L	M	N	C	J	P	R	A	B	G	D	O	E	Z	H	U
W	Q	I	K	L	M	N	C	J	P	W	A	B	G	D	O	E	Z	H	U	R
Q	I	K	L	M	N	C	J	P	W	Q	B	G	D	O	E	Z	H	U	R	A

Appendix B: "XP" Message

After World War II, when the Haganah renewed the illegal immigration efforts, radio communication was used on all illegal immigration vessels, which transmitted two to three times each day a message called "XP" (when the longitude was west, they were called "XPM"), which included their location (coordinates), direction of movement and speed. Streamlining the messaging process, these messages were sent in a uniform fixed format, in numerals only, and were, of course, encrypted. The encrypted "XP" message consists of six five-letter groups, transmitted over a high frequency radio using Morse code.

An example from an instruction sheet from late 1946 "XP" message guide, translated to English for illustration (see table on page **Error! Bookmark not defined.**):[87]

- Date in two digits, e.g., 21, recorded as: BA
- Time of composition in four digits, e.g., 1300, recorded as: AGII
- North coordinates in four digits, e.g., 42°17', recorded as: DBAZ
- East coordinates in four digits, e.g., 14°06', recorded as: ADIE
- Course in three digits, e.g., 180°, recorded as: AHI
- Speed in three digits, e.g., 7.5 knots, 075, recorded as: IZO
- Sea state in one digit (1 – calm sea, 2 – moderate, 3 – rough), e.g., 2 (moderate), recorded as: B

The plaintext is first written into rows whose length matches the 10-letter keyword; each column is then enciphered with the 20×20 Vigenère-style table in the previous section, using the corresponding keyword letter, producing a table of substituted characters. Once all rows are enciphered, the columns are reordered according to the numerical order of the keyword's letters (i.e., the columnar transposition step), and the ciphertext is obtained by reading out the columns in that order. Here is the above message prepared for transmission:

Keyword	L	M	R	K	O	T	E	R	J	I
Numerical Key	5	6	9	4	1	10	2	8	7	3
Plain text	B	A	V	A	G	I	I	F	D	B
Encrypted Characters	N	N	V	L	H	I	J	F	I	L
Plain text	A	Z	V	A	D	I	E	Y	A	H
Encrypted Characters	M	I	V	L	U	I	B	Y	P	W
Plain text	I	X	I	Z	O	V	B	Y	F	X
Encrypted Characters	O	X	I	W	R	V	H	Y	F	X

In this example, the encrypted "XP" message, as sent, is:

GR6 XP $\overline{\text{BT}}$ HURJB HLWXL LWNMO NIXIP FFYYV VIIIV $\overline{\text{AR}}$

[87] *Geographical Definition Key*, HHA 114/74 (Hebrew).

Appendix C: Interception of Illegal Immigrant Vessels

The first illegal immigration vessel to sail to Palestine after World War II was DALIN (August 1945), which arrived undetected by the British. It was followed by five more vessels that also went undetected (NATAN A, GABRIELLA, PETER A, NATAN B, PETER B). The seventh vessel, BERL KATZNELSON, was detected by a Royal Air Force aircraft on 22 November 1945. Since then, all illegal immigrant vessels were intercepted, except for those that did not transmit during their voyage — thus preventing British tracking (HANNAH SZENES, SHABTAI LOZINSKI) — and a few ships that were located and inspected by the British but not identified as illegal immigration vessels (ALIYAH, HAPORZIM).[88]

The British used two techniques to track illegal immigration vessels:

1. **"Warship shadow"** – Following the illegal immigrant ship from the port of departure (or from a strait, such as the Dardanelles). This method also relied on intercepting and decrypting vessel radio messages to determine when and where to wait for the vessel.
2. **Radio interception and message decryption** – When the illegal vessel approached Palestine, it was initially located and identified by a reconnaissance aircraft, which then directed a warship to complete the identification and interception and board the vessel. One known case (KNESSET ISRAEL) involved the aircraft establishing visual signaling contact with the illegal immigrant vessel to verify its identity.[89]

Reconnaissance aircrafts were not "searching blindly." They were given precise missions: to locate a suspicious ship (often with a description) in a defined sea sector, at a defined time.[90]

The following table presents the record of illegal immigration vessel interceptions by the British from the launch of the 'Palestine Patrol' on 27 September 1945 until the establishment of the State of Israel in May 1948:[91]

Serial No.	Vessel Name	Interception Method	Notes
1	BERL KATZENELSON	Aircraft + Warship	Captured on Palestine coast, after most illegals landed.
2	HANNAH SZENESH	Not intercepted	• No radio communication with the vessel. Communication was renewed shortly before landing. • Royal Navy, on Christmas leave, was slow to respond,
3	ENZO SERENI	Aircraft + Warship	

[88] For additional information: Ninian Stewart, *The Royal Navy and the Palestine Patrol*, Frank Cass Publishers, London 2002.

[89] Rosenne, *Gideonim*, pp. 197–198

[90] With the technology of the time, aircraft or ship position reports at sea had an accuracy of approximately ±10 nautical miles.

[91] Source: Reports of ship commanders and Gideonim (Rosenne, *Gidonim*).

Appendix C: Interception of Illegal Immigrant Vessels

Serial No.	Vessel Name	Interception Method	Notes
4	WINGATE	Aircraft + Warship	
5	TEL HAI	Aircraft + Warship	
6	MAX NORDAU	Aircraft + Warship	
7	ELIYAHU GOLOMB	Warship shadow	Detained in La Spezia, Italy. Shadow by agreement.
8	DOV HOZ	Warship shadow	Detained in La Spezia, Italy. Shadow by agreement.
9	HAVIVA REIK	Aircraft + Warship	
10	JOSIAH WEDGWOOD	Aircraft + Warship	
11	BIRIA	Aircraft + Warship	
12	HAGANAH	Aircraft + Warship	Sent a distress call.
13	HACHAJAL-HAIVRI	Not intercepted	• Destroyer inspection did not identify the vessel as illegal. • Sailed to the port of Haifa.
14	YAGUR	Aircraft + Warship	
15	HENRIETTA SZOLD	Aircraft + Warship	
16	KATRIEL YAFFE	Aircraft + Warship	
17	KAF GIMEL YORDEI HASIRA	Aircraft + Warship	
18	AMIRAM SHOCHAT	Not intercepted	Aircraft located the ship; destroyer inspection it did not identify the vessel as illegal, and illegals landed at Sdot Yam.
19	ARBA HERUYOT	Aircraft + Warship	
20	PALMACH	Aircraft + Warship	
21	BRACHA FULD	Aircraft + Warship	
22	LATRUN	Aircraft + Warship	
23	KNESSET ISRAEL	Aircraft + Warship	The only vessel that established visual signaling contact with a reconnaissance aircraft.
24	RAFIAH		RAFIAH sunk in the island of Sirina, sent a distress signals and the Jewish Agency summoned British assistance.
25	LANEGEV	Warship	• The vessel radio was out of order for most of the voyage and was repaired shortly before landing. • Reached Tel Aviv without being detected but was sent to land the next day at Caesarea, where it was captured.
26	HAMAAPIL HAALMONI	Aircraft + Warship	
27	HAIM ARLOSOROFF	Aircraft + Warship	
28	BEN HECHT	Aircraft + Warship	

Serial No.	Vessel Name	Interception Method	Notes
29	SHABTAI LUZINSKI	Not detected	• Sailed under radio silence. • Located by Aircraft after landing.
30	MOLEDET	Aircraft + Warship	
31	THEODOR HERZL	Aircraft + Warship	
32	SHEAR YASHUV	Aircraft + Warship	
33	HATIKVAH	Aircraft + Warship	
34	LOCHAME-HAGETAOTH	Aircraft + Warship	
35	YEHUDA HALEVI	Warship	
36	EXODUS 1947	Warship shadow	From Sète, France.
37	YUD DALET HALALEI GESHER HAZIV	Warship shadow	From Messina Strait.
38	SHIVAT ZION	Ship	
39	AF-AL-PI-CHEN	Aircraft + Warship	
40	GEULAH	Warship shadow	From the Dardanelles.
41	MEDINAT HAJEHUDIM	Warship shadow	From the Dardanelles.
42	KADIMA	Aircraft + Warship	
43	ALIYAH	Not intercepted	• ALIYAH's radio was out of order and repaired a day before landing, when the vessel was near KADIMA. • Aircraft located the ship, a destroyer 'confused' ALIYAH with KADIMA, which was captured. • Illegals landed in Nahariya.
44	HAPORZIM	Not intercepted	• Destroyer inspection did not identify the vessel as illegal, and the illegals landed at Tel Aviv.
45	LO TAPHCHIDUNU	Aircraft + Warship	
46	KAF-TET BENOVEMBER	Warship shadow	From South of Crete.
47	HAUMOT HAMEUCHADOT	Aircraft + Warship	
48	ATZMAUTH	Warship shadow	From the Dardanelles.
49	KIBBUTZ GALUYOT	Warship shadow	From the Dardanelles.
50	LAMED-HEH GIBOREI KFAR ETZION	Aircraft + Warship	
51	YERUSHALAIM HANETZURA	Aircraft + Warship	
52	KOMEMIUT	Aircraft + Warship	

Appendix C: Interception of Illegal Immigrant Vessels

Serial No.	Vessel Name	Interception Method	Notes
53	BONIM VELOCHAMIM	Aircraft + Warship	
54	YEHIAM	Aircraft + Warship	
55	TIRAT ZVI	Aircraft + Warship	
56	MISHMAR HAEMEK	Aircraft + Warship	
57	NACHSHON–HACASTEL	Warship	