דניאל רוזן

כְּסוּמָא בְּאַרְבְּה: הצופן בשירות הקשר של 'ההגנה'

ארגון 'ההגנה' החל לפתח מערכות קשר רדיו בשלהי שנות ה־20 של המאה העשרים. אמצעי קשר רדיו, פרי הטכנולוגיה החדישה והמתפתחת באותם הימים, היו יעילים פי כמה מאמצעי איתות הראייה (דגלים, פנסים והליוגרף) שקדמו להם. התלקחות המרד הערבי הגדול, בשנים 1936–1939, העצימה את צורכי התקשורת ב'הגנה', האיצה את הצורך במערכת קשר יעילה בין היישובים היהודיים, ומפקדי 'ההגנה' החליטו לרתום את טכנולוגית הרדיו להגנת היישוב.[1] הדבר הביא להקמת שירות הקשר הארצי, כאחת היחידות המקצועיות הראשונות של 'ההגנה'. כדי להבטיח את חשאיות המידע שהועבר ברשתות הרדיו, הוצפנה התעבורה ששודרה בהן.

במאמר זה מוצגים שלבי פרשת שבירת צופני ארגון 'ההגנה' בידי הבריטים ותגובת 'ההגנה' לכך. במאמר מועלית ההשערה כי הצלחת הסגר הימי הבריטי על חופי הארץ בשנים 1945–1948 נבעה, בין היתר, משבירת צופני הדיווח בתקשורת הרדיו עם ספינות המעפילים, והוא מבוסס על חומר ארכיוני בריטי שנחשף לעיון מחקרי בשנים האחרונות ועל מסמכים מתיקי ארכיונים מוסדיים בישראל.

הקמת שירות הקשר ב'הגנה'

שירות הקשר הארצי ב'הגנה' הוקם באפריל 1937 בראשות שמחה אבן־זהר, מזכיר הוועד הפועל בהסתדרות הכללית, שמונה לתפקיד בידי המפקדה ארצית של 'ההגנה'. שירות הקשר הקים ארבע רשתות רדיו: **רשת אבינועם** – רשת ארצית לקשר בין המטכ"ל

---

1 תחנת השידור הראשונה בארץ ישראל הופעלה כאטרקציה ב'תערוכה הארץ־ישראלית' בתל־אביב בשנת 1929. תחנת השידור הממשלתית הראשונה לציבור, 'קול ירושלים', שהופעלה בידי שלטונות המנדט הבריטי, הופעלה ב־30 במארס 1936, ורק אז נפתחו בארץ ישראל סוכנויות למכירת מַקלטי רדיו לציבור. בשנת 1936 היו בארץ ישראל 20,400 מקלטי רדיו פרטיים, ובשנת 1939 הוכפל מספרם ל־42,600 מַקלטים (כ־80% מהם בידי יהודים). באותה התקופה נדרש רישיון מטעם שלטונות המנדט להחזקת מקלט רדיו. בשנת 1947 נאמד מספר מקלטי הרדיו בארץ ב־116,000 מכשירים. דניאל רוזן, **התקשורת בארץ ישראל בתקופת המנדט הבריטי: דואר, מברקה, טלפון ורדיו**, יהוד: העמותה להנצחת חללי חיל הקשר והתקשוב, 2019, עמ' 292.

ליישובים, שפעלה מראשית הקמתו של שירות הקשר; **רשת גדעון** - לקשר עם אנשי המוסד לעלייה ב׳ בחו״ל וספינות המעפילים, שהחלה לפעול באפריל 1939;[2] **רשת שרה** - שהחלה לפעול ביוני 1940 וקישרה בין משרדי הסוכנות היהודית בירושלים למשרדי הסוכנות בלונדון ובניו־יורק; **רשת תמר** - רשת ארצית לקשר בין מטה הפלמ״ח ליחידות הפלמ״ח, שהחלה לפעול כרשת נפרדת בקיץ 1942.

רשתות אלו היו רשתות רדיו בתדר גבוה (ת״ג). רוב תעבורת הקשר הייתה באיתות מורס.[3] בקשר אלחוטי (דיבור) נעשה שימוש מועט יחסית. שירות הקשר פיתח מנגנון להכשרת אלחוטנים, לייצור מכשירי קשר (שנקראו ׳מזוודה׳, שכן הם הורכבו במזוודת עץ קטנה),[4] להכנת צפנים ולהכנת הוראות קשר (בלשון הימים ההם: ׳הסכם קשר׳).

שבירת צופני תעבורת הרדיו

החשיבות המבצעית של קשר רדיו הועלתה על מדוכת המִפקדה הארצית של ׳ההגנה׳ בפרוץ המרד הערבי באפריל 1936 ובשנות מאורעות הדמים. הביטוי המיידי לנחיצותם היה בעיקר בדיווח בין יישובי ה׳גושים׳ (לימים, הנפות) באזורים הכפריים. עם השקת פעילות ההעפלה בידי המוסד לעלייה ב׳ בשנת 1938, קיבל נושא הקשר האלחוטי משנה תוקף, וחידוש ההעפלה לאחר מלחמת העולם השנייה באירופה החרבה, שבה מערכות התקשורת האזרחיות לא תפקדו, אף הגדיל את חשיבות קשר זה. באוקטובר 1945 החלה הפעילות המבצעית של תנועת המרי העברית, ולראשונה התחוורה למפקדי השדה מלוא חשיבותם המבצעית של אמצעי הקשר בקרב כ׳זרוע המפקד לשליטה׳. בקורס מפקדי מחלקות של ׳ההגנה׳ באוקטובר 1945 הופעלו חמישה מכשירי קשר (מ״ק) אלחוטיים

---

2 המוסד לעלייה ב׳ בראשות שאול אביגור הוקם בשנת 1938 על־ידי חברי ׳הקיבוץ המאוחד׳ בתמיכת ההסתדרות הכללית, והוכפף ב־3.7.1939 לארגון ׳ההגנה׳. אריה אבנרי, **מוֹלוֹס עד טאורוס: עשור ראשון להעפלה 1934–1944**, אפעל: יד טבנקין, 1985, עמ׳ 110.

3 המורס שבו נעשה שימוש אז בארץ היה מורס בא״ב עברי, המבוסס על הא״ב הלטיני. תרגום כתב המורס לעברית נעשה בשנת 1922 בתנועת הצופים היהודים בווילנה בידי זלמן כהן, לימים מבכירי שירות הקשר ב׳הגנה׳. המורס בשירות הקשר התבסס על תרגום זה, בשינויים אלה: הוחלפו האותיות טי״ת בתי״ו, כ״ף בקו״ף, סמ״ך בשי״ן. כתב המורס לאותיות וי״ו, טי״ת, עי״ן וצד״י שונה. מאחר שבעברית 22 אותיות ובאנגלית 26, נוספו בטקסט הגלוי - לפני הצפנה - האותיות F, V, X ו־Y, במטרה ששדר מוצפן לא יזוהה כשדר בעברית. האות F שימשה כנקודה, האות V שימשה כפסיק, האות X שימשה כרווח והאות Y שימשה כמקף (בהמשך שונה הדבר: האות X שימשה להדגשה וכדי לשדר מילים קשות פעמיים, והאות Y שימשה כרווח). גבי שריג, **לקסיקון למונחי קשר**, קיבוץ דליה: מערכת, 1988, עמ׳ 328 (להלן: שריג, **לקסיקון למונחי קשר**).

4 עד קום המדינה בנו טכנאי שירות הקשר בהסתר כ־500 מכשירי קשר מסוגים שונים, כמחציתם ׳מזוודות׳. שם, עמ׳ 170, 356 ו־424.

מדגם מ"ק־20 לטווח יעיל של כשני קילומטרים,[5] וברשות הפלמ"ח היו כמה מכשירי ווקי־טוקי פרימיטיביים.[6] אבל כבר במבצע הראשון – שחרור כלואֵי מחנה המעצר בעתלית בליל 9–10 באוקטובר 1945, התוודעו המפקדים להשלכות המבצעיות החמורות שנבעו מהיעדר מכשירי קשר. בסיכום ההתקפה על מחנה שׂרונה הבריטי ב'ליל המשטרות', ב־22 בפברואר 1946, הצביע יגאל אלון, מפקד הפלמ"ח, על כשל הקשר הקריטי בכתבו: "אלמלא המחסור החמור במכשירי־קשר־של־שדה היתה התוכנית מתגשמת, ודאי, במלואה. [...] ראוי היה לבטל את הפעולה בשׂרונה, אולם לא היו מכשירי קשר".[7] כעבור חודש צוינה ב'ליל וינגייט', ב־25 במארס, אבן דרך בהגברת המודעות לחיוניות האופרטיבית של מערכת הקשר כאמצעי שליטה, אולם המימוש הטכנולוגי והתקציבי של תובנה זו יושם רק בפרוץ מלחמת העצמאות.[8] במהלך תקופה זו הסלימה 'תנועת המרי העברי' את מבצעי התקיפה, וב'ליל הגשרים', ב־16 ביוני 1946, פוצצו יחידות פלמ"ח 11 גשרים בגבולות ארץ ישראל. המבצע גרם לניתוק זמני של נתיבי האספקה בשימוש הבריטים. במהלך תשעת חודשי קיומה של תנועת המרי העברי, התבצע גל השחרור הנרחב של מגויסי היישוב מהצבא הבריטי. משוחררי הצבא הבריטי, שמרביתם היו חברי ארגון 'ההגנה', נחשפו בקרבות מלחמת העולם השנייה לחשיבות המכרעת של הקשר בשדה המערכה.

עד יולי 1946 הוצפנה תעבורת הרדיו של שירות הקשר בצפנים פרימיטיביים. רוב ההודעות שהועברו ברשתות הרדיו היו מוצפנות, וההצפנה והפיענוח בוצעו באופן ידני. הודעות מורס מוצפנות שודרו בקבוצות בנות חמש אותיות, שנקראו 'חמישיות'. מדידת מהירות השידור והקליטה צוינה על פי מהירות השידור והקליטה של קבוצות חמישיות לדקה (קל"ד). ברשתות מורס של 'ההגנה' מקובל היה לשדר ולקלוט במהירות של 18 עד 22 קל"ד (אלחוטנים מנוסים נהגו לשדר ולקלוט במהירויות של 28 ו־30 קל"ד).

ההצפנה הייתה מבוססת על שיטה של שינוי מיקום אותיות (transposition). אבן־זהר, ראש שירות הקשר הראשון של 'ההגנה', העיד כי "מבעוד מועד עלה בידינו לרכוש, תודות לש"י [שירות הידיעות של 'ההגנה'], את הצופן [הקוד] ושיטת האלחוט שהייתה נהוגה במשטרת המנדט – שיטה שנראתה טובה בתחילה, עד שנפלו לידינו שיטות הצופן

5 עדות יגאל ידין, 'קורס לקציני מפקדי מחלקות 1945', תיק 198.20, (ללא תאריך), הארכיון לתולדות ההגנה (להלן: את"ה). מ"ק־20 היה מכשיר קשר SCR־300 מתוצרת ארה"ב, שכונה בצה"ל מ"ק־300.

6 עדות מיכאל (מייק) הררי, פלמ"חאי שהפעיל אז מכשיר ווקי־טוקי, מראיין: ניר מן, 2011, אוסף המראיין.

7 יגאל אלון, **מערכות פלמ"ח: מגמות ומעש**, תל־אביב: הקיבוץ המאוחד, 1965, עמ' 558–559.

8 ניר מן, "'ליל וינגייט': הישגי המבצע שלא בוצע", בתוך: הנ"ל (עורך), **עלי זית וחרב: עמוד האש**, יב, ירושלים: כרמל והמרכז לחקר כוח המגן מייסודו של ישראל גלילי, 2012, עמ' 87.

והפענוח הנהוגות בצבא היוגוסלבי ועל פיהן פעלנו אחר־כך".[9] אלי שוורץ, חבר קיבוץ אפיקים ואיש שירות הקשר, הוא שהביא ארצה את שיטות הצופן של הצבא היוגוסלבי.[10] מיומנו של משה שרת, ראש המחלקה המדינית בהנהלת הסוכנות היהודית ומי שהופקד על נושא הביטחון ו'ההגנה', עולה כי המחלקה המדינית (רשת שרה) עשתה שימוש בשיטת הצפנה אחרת.[11] לפי היומן, מפתח הצופן של הסוכנות היה מבוסס על עמוד משתנה בספר עברי, שעותקיו היו מצויים בידי השולח ובידי המקבל.

להערכת אנשי שירות הקשר, שיטת ההצפנה הייתה מאובטחת ואמינה, אך פרסום 'הספר הלבן', ב־24 ביולי 1946, העמיד אותם על טעותם המרה. בעקבות 'ליל הגשרים' יצאו הבריטים, ב־29 ביוני 1946, למבצע 'אגתה' ('השבת השחורה') שנועד להנחית מהלומה קשה על 'ההגנה' ולהוכיח לדעת הקהל העולמית כי הארגון המתקומם נגד השלטון המנדטורי כפוף להנהלת הסוכנות היהודית. במבצע השתתפו 17 אלף חיילים בריטים, ובמהלכו נערכו חיפושים בבנייני המוסדות הלאומיים אחר מסמכי הנהלת הסוכנות, נערכו חיפושים נמרצים ב־27 קיבוצים בניסיון לאתר את מחסני הנשק הארציים ('הסליקים'), הוטל עוצר על ערים ומועצות מקומיות (תל־אביב, ירושלים, חיפה, רמת־גן, נתניה ועוד) ונערכו חיפושים מבית לבית. 2,700 איש, מרביתם חברי קיבוצים ולוחמי פלמ"ח וכמה ממנהיגי היישוב, נעצרו והועברו למחנות מעצר (רפיח, לטרון ועתלית). בתוך כחודש, ב־24 ביולי 1946, פרסמה ממשלת בריטניה 'ספר לבן', שנועד להציג את הסוכנות היהודית כגורם חתרני, המנהיג את מעשי האלימות נגד הכוחות הבריטיים בארץ.[12] במסמך זה פורסמו שמונה ממברקי הסוכנות היהודית, ששבעה מהם נשלחו מהארץ ללונדון כמברקים מוצפנים, ואחד, שהיה מברק גלוי, נשלח מלונדון לארץ. להלן שני קטעים מהמברקים שפורסמו ב'ספר הלבן' בתרגום לעברית (ההתכתבות המקורית הייתה כנראה באנגלית):

---

9 שמחה אבן־זהר, "בראש הקשר של 'ההגנה'", בתוך: אברהם גרנית (עורך), **קשר אלקטרוניקה ומחשבים** (גיליון מיוחד), צה"ל: מפקדת קצין קשר ואלקטרוניקה ראשי, י"ח/2 (204), אוגוסט 1987, עמ' 22 (להלן: גרנית (עורך), **גיליון מיוחד של קשר אלקטרוניקה ומחשבים**).

10 עדות איש שירות הקשר חיים פרידלנדר, תיק 114/17, את"ה.

11 במכתבו של שרת צוין המונח 'ספרות עברית', דהיינו, ספר עברי ששימש כמפתח. פנחס עופר, **ירחים בעמק איילון**, תל־אביב: העמותה למורשת משה שרת, 2011, עמ' 28 (להלן: עופר, **ירחים בעמק איילון**). אנשי שירות הקשר, מפעילי רשת שרה, השתמשו בצופן שונה מזה של בכירי המחלקה המדינית. המפעילים של רשת שרה, שהחלה לפעול ביוני 1940, העידו כי הצפינו ופִענחו רק חלק מהמברקים, שכן היו מברקים שהוצפנו ופוענחו רק בידי הנמענים. מנחם יצחקי, "שליחות עלומה בלונדון", בתוך: י' בעל־שם (עורך), **קשר אלקטרוניקה ומחשבים**, צה"ל: מפקדת קצין קשר ואלקטרוניקה ראשי, מס' 88/2, י"ח/4 (207), אפריל 1988, עמ' 36–39.

12 *Palestine: Statement of Information Relating to Acts of Violence*, July 1946, ראו: עופר, **ירחים בעמק איילון**, עמ' 533–542.

א. מברק מוצפן שנשלח מדב יוסף (היועץ המשפטי של הסוכנות) בירושלים ללונדון ב־10 באוקטובר 1945:

אליעזר קפלן [ראש מחלקת הכספים של הסוכנות], המתבסס על ידיעה מחיים [וייצמן] דרך Nwbw [הבריטים הסתירו את השם], אומר כי אין אנו צריכים לעשות כלום בטרם תתנו לנו הוראות לעשות. הוא מתנגד לכל פעולה ממשית מצדנו עד שנקבל ידיעות מכם. אולם לדעת חברים אחרים מן הכרח לתמוך במאמצינו הפוליטיים על־ידי פעולות שאין בהם משום אופי של סכסוך כללי. הטוב ביותר שנדע מייד אם פעולות כאלו עשויות להועיל או להזיק למאבקנו. אם תהיו נגד כל פעולה שהיא, טלגרפו שעלינו לחכות לבואו של Wlsly [הבריטים הסתירו את השם]. אם תסכימו לפעולות בודדות, טלגרפו כי אתם מסכימים לשיגור משלחת אל הדומיניונים. אם חיים [וייצמן] יתכוון לומר שנמנע רק מסכסוך כללי, ולא לפעולות בודדות, שִׁלחו ברכות לחייל להולדת בתו.

ב. מברק תשובה גלוי שנשלח בדואר כ'טלגרמה' רגילה ממשה שרת בלונדון לדב יוסף בירושלים ב־12 באוקטובר 1945:

דוד [בן־גוריון] לא יצא לפני עבור שבועיים. בינתיים שוב יבקר קרוב לוודאי בפאריס. בעניין דובקין [אליהו דובקין, ראש מחלקות העלייה, הארגון, הנוער והחלוץ בסוכנות] נכתוב. דוד עצמו הוא בעד משלחת לדומיניונים. בבקשה ברך את החייל להולדת הבת.

בכתבי משה שרת מאוזכר נושא זה ומועלה החשש כי נשבר גם הצופן של המוסד לעלייה ב'.[13] כְּתבים אלה, שהם אסופת פתקים שהובריחו ממחנה המעצר בלטרון, כתובים בצורה מקורית. בפתק ששלח שרת ממחנה המעצר לזאב שרף, מזכיר המחלקה המדינית, ב־24 ביולי 1946, בעקבות פרסום 'הספר הלבן' הבריטי, נכתב:

היה לנו נשף [נשיפה: דליפת מידע סודי] בהשתתפות שלישיה: אבינועם [רשת הקשר של 'ההגנה'], אפרת [רשת הקשר של הסוכנות] וקֶלֶר [Kellar, קצין מודיעין בכיר ב־MI5, שירות הביטחון הבריטי[14]. הראשון או בסכיתה [האזנה] או בקריאת התוים הכתובים [דליפת החומר הגלוי]. השני או באינטרפרטציה [שבירת הצופן] או בקריאת מילות השיר [דליפת מפתח הצופן] (יש הוכחות לאפשרות הראשונה). השלישי – סעיף אחד, תרומת הח"מ. שני הראשונים ילמדו לקח [יסיקו מסקנות וישפרו].

13 עופר, **ירחים בעמק איילון**, עמ' 103–104, 108, 140, 145–146.

14 קלר היה מומחה לענייני המושבות הבריטיות, שעמד בראש שלוחת המודיעין למזרח התיכון SIME (Security Intelligence Middle East) מדצמבר 1946 עד 1948.

למחרת, ב־25 ביולי, הוא הוסיף בפתק נוסף: "בשיקול שני: שמא רק אבינועם (עם קצת קֶלֶר), בלי אפרת?" ב־3 באוגוסט שלח שרת לשרף פתק נוסף:

> ענין הנשף מסתמן עכשיו יותר מקודם, אך עדיין לא בכל פרטיו. אמנם גם מהשדר הראשון שיערתי משהו מעין זה, אך כעת יותר ברור, אם כי, כאמור, לא לגמרי. ובכן – (א) אם טיפלו אנ"ש [אנשי שלומנו] – מדוע לא באו לגלות אוזן? מסַמר שערות! (ב) איך עברו מאלגברה לאריתמטיקה בזהות [איך שברו את הצופן]? (ג) לאור הניסיון – מה גורל הזיקה ללוטציה [השלוחה בפריז]? (ד) מה פירוש 'גם בית לחם במנגנים' [בית לחם היא אפרת, הרשת של הסוכנות – בדרך אפרתה היא בית לחם], הלא את מפת העיר [מפתח הצופן] לא יכלו בשום פנים למצוא, כלום התברר כי עמדו על המְעָנים מבלי היזקק למפה? (ה) מה פירוש 'הוא הדין בב' [המוסד לעלייה ב']'?

תשובת שרף הייתה: "המעבר מאלגברה לאריתמטיקה לא היה קשה כשהמספרים מעטים". בכירי הסוכנות היהודית הכחישו כל קשר למברקים אלה. זו הייתה תגובת דובר הסוכנות:[15]

> הממשלה הבריטית טוענת, על סמך תערובת של מברקים, כביכול, שלדבריה נשלחו לפני תשעה חודשים, על סמך קטעים מתוך שידורים של תחנת 'קול ישראל' ועל סמך משפטים שונים שהוצאו מתוך עלונים של קבוצות טרוריסטיות, כי השיגה הוכחות לשיתוף פעולה בין כמה מחברי הסוכנות היהודית לבין ההגנה וכן לתיאום פעולה במקרים אחדים בין ההגנה לבין הכנופיות הטרוריסטיות. אף אחד מבין המברקים שעליהם מסתמכת הממשלה לא יצא מהסוכנות היהודית בירושלים. הסוכנות היהודית, שאין בידה לאשר את מקוריותן של הטלגרמות האלה, דורשת מאת הממשלה הבריטית להוכיח שהסוכנות היהודית היא האחראית לתכנן, מקוריותן ומשלוחן. הנהלת הסוכנות היהודית מעיינת בתשומת לב באוסף מוזר זה של מברקים, כביכול, של שידורים ושל פרסומים.

חשיפה זו הייתה אירוע מכונן בתולדות שירות הקשר והיא שימשה 'קריאת יקיצה' של ממש. בעקבותיה שינה שירות הקשר את שיטות הצופן, ונוסף לכך הטמיע את התובנה בצורך למיסוד נושא הצופן בידי מומחים לדבר תוך הקצאת המשאבים הנדרשים.

יעקב ינאי (יאן ינובסקי), ראש שירות הקשר באותה עת, העיד:[16]

> אומנם עבדנו בקודים, אבל הבריטים פרסמו "ספר לבן" שבו הופיע תוכנם של הרבה

15 "המברקים שפורסמו בספר הלבן לא נשלחו מירושלים ולא נתקבלו בלונדון", **דבר**, 26.7.1946, עמ' 1.

16 גדעון רדין, "משירות הקשר לחיל הקשר", בתוך: גרנית (עורך), **גיליון מיוחד של קשר אלקטרוניקה ומחשבים**, עמ' 17.

מברקים שמקורם בקשר בין הארץ לבין לונדון - כלומר שהם פענחו את מברקינו. ראש יחידת הפענוח בבריטניה היה יהודי, ואנחנו הצלחנו לחקור אותו בארץ ולאמת את עניין הפענוח. כתוצאה מכך החלפנו את כל הקודים ויסדנו יחידה מיוחדת שעסקה בכתבי סתר, ואשר נעזרה במומחים בתחום זה שהבאנו מדרום אפריקה.[17]

בעיצומו של המשבר החמור בין הנהלת הסוכנות לשלטונות המנדטוריים, באוגוסט 1946, הונהג השימוש בצופן שהיה מבוסס על ספר הקוד של Bentley למסמכי המחלקה המדינית של הסוכנות היהודית.[18] ספר זה היה קוד מסחרי שהתבסס על שידור מספרים בני חמש ספרות במקום משפטים שלמים, כדי לחסוך בהוצאות כספיות על מברקים, שכן התשלום עבור משלוח מברקים היה לפי מילים. מצפיני המחלקה המדינית הוסיפו למספר של קוד Bentley מספר נוסף, ששימש כמפתח (לדוגמה: 41.945) ושונה מדי יום. הטקסט ששודר היה הסכום של המספר בספר הקוד ומספר המפתח.[19] שירות הקשר לא השתמש בשיטה הצפנה זו.

שבירת צופני שירות הקשר

עם פתיחת תיקי שירות הביטחון הבריטי (MI5) בארכיונים הבריטיים לעיון הציבור בפברואר 2006, החל להיחשף מידע על שבירת צופני 'ההגנה' ונסיבות פרסום 'הספר הלבן' מיולי 1946. מהחומר עולה כי הבריטים הקימו תחנת האזנה במחנה סרפנד (צריפין) כבר בשנת 1923,[20] וההאזנה המודיעינית (סיגינט) שימשה אותם כמקור מודיעין עיקרי. קומנדר (רב־סרן) אלסטיר דניסטון (Denniston), ראש ה־Government Code and Cypher School, יחידת ההאזנה הבריטית (שקדמה ל־GCHQ, כדוגמת ה־NSA בארצות הברית), ציין בשנת 1944 את הקשר ההדוק עם סרפנד במשך 20 שנה.[21] הבריטים שברו את הצפנים שבשימוש 'ההגנה' משנת 1942 או אף קודם לכן.

17 המומחים מדרום אפריקה שהניחו את היסוד לביטחון הקשר בצה"ל היו שאול בר־לבב ומאיר שפירא.

18 יעקב שרת, בנו של משה שרת, העיד כי בימי נערותו בירושלים, בתחילת שנות ה־40, אביו השתמש בספר אנגלי עב כרס לצורכי הצפנה. עדות יעקב שרת, מראיין: דניאל רוזן, אוקטובר 2015, אוסף המראיין.

19 מזכר פנימי (ללא חתימה) לא"א, 'נתנאל ורפאל', 11.8.1946, תיק S25.10941; מסמך לועזי תואם בשם: Instructions for Use, מ־19.8.1946, תיק S25.8214, הארכיון הציוני המרכזי.

20 תחנת ההאזנה, שנקראה 'גבעת האלחוט' (Radio Hill) הייתה באזור 'מחנה גדעונים', מצפון לכביש 44 (דרך יפו־רמלה). תחנת ההאזנה שימשה בעיקר למעקב אחרי פעילויות רוסיות וגרמניות. שריג, **לקסיקון למונחי קשר**, עמ' 86.

21 Christopher Andrew, *The Defence of The Realm: The Authorized History of MI5*, London: Penguin Books, 2010, p. 353.

ברישום מ־23 בספטמבר 1942 ביומנו של הגנרל הבריטי גאיי לידל (Liddell), ראש הריגול הנגדי (Counter-Espionage) ב־MI5 באותה עת, מצוין כי המידע היה להם לעזר רב: "הם [המברקים הציוניים שיורטו] היו לו [לקלר, שהיה אחראי על ארץ ישראל] לעזר רב בעניינים ציוניים".[22] הרישומים ביומן משנת 1944 מתייחסים למודיעין שהושג משבירת צופני 'ההגנה', ומתייחסים לשני צפנים שכונו: ISPAL1, ISPAL2 (ISPAL – Intelligence Service Palestine). ברישום מ־26 בספטמבר 1944 ביומן מתוארת פגישה עם הנציב העליון, הפילדמרשל ג'ון ורקר הלורד גורט (Gort), ומצוין קושי בשבירה או בתרגום ("היו לנו קשיים רבים בפרויקט [הפיענוח]").[23] היה גם מקור שכונה ISPAL3. הכינויים ISPAL1 ו־ISPAL2 שונו במהלך שנת 1944 ל־OATS ו־ISTRIA (OATS היה הצופן של 'ההגנה', ISTRIA היה הצופן של הסוכנות). מקור נוסף היה Buttercup,[24] ההאזנה לקווי הטלפון של המוסדות הציוניים ו'ההגנה'.

פיצוח השדרים של 'ההגנה' בידי הבריטים באותה העת נמשך כשבועיים מקליטת השדר ועד להפצתו כשהוא מפוענח ומתורגם.[25] הסיבה למשך הזמן הארוך הייתה נעוצה כנראה במורכבות התהליך – התשדורת שנקלטה במתקן האזנה בארץ או במצרים הועברה לאנגליה לפיענוח ולתרגום, והוחזרה לארץ.[26] המחסור של הבריטים בדוברי עברית מהימנים תרם אף הוא להאטת קצב הפיענוח. חשיפת המקורות הבריטיים, ביולי 1946, גרמה ל'הגנה' לשנות מהיסוד את שיטת הצופן. החוקר סטיבן וגנר (Wagner) טען בשנת 2013 כי שינוי שיטת ההצפנה גרם ל'עלטה מודיעינית', ובמשך שנה שלמה, רבת תהפוכות מדיניות, המודיעין הבריטי לא הצליח לשבור את הצופן. רק ביולי 1947 הצליחו הבריטים לפענח

22 The National Archives (TNA), KV 4/190, *Diary of Guy Liddel*, vol. 6, May 1942 to November 1942, Part 2, pp. 791-792.

23 TNA, KV, 4/195, *Diary of Guy Liddel*, vol. 11, September 1944 to December 1944, pp. 35, 42, 54 & 108.

24 TNA, KV 4/438, *Report on Visit to S.I.M.E and its outstations in the Middle East*, Maj. J.C. Robertson (B.3.A), April–June 1947, 26 June 1947, p. 27 (hereinafter: Robertson Report).

25 Steven Wagner, *British Intelligence and the 'Fifth' Occupying Power: The Secret Struggle to Prevent Jewish Illegal immigration to Palestine*, London: Intelligence and National Security, 2014, vol. 29, no. 5, pp. 698-726 (see p. 706).

26 ההאזנה הבריטית לשירות הקשר של 'ההגנה' התבצעה כנראה בארץ, ולכן המברקים שפורסמו ב'ספר הלבן' של יולי 1946 היו כאלה שנשלחו מהארץ לחו"ל (המרחק האווירי מתל־אביב, משם בוצעו השידורים ללונדון עבור המחלקה המדינית משנת 1943, לבסיס ההאזנה הבריטי בסרפנד הוא כ־15 ק"מ בלבד, וזה אִפשר קליטה בבהירות וללא שיבושים).

מברקים של המחלקה המדינית בצופן החדש.[27] המבצע הבריטי כונה FOG.[28] מאוחר יותר שברו הבריטים צופן נוסף, שכונה CREAM.[29]

המענה לשאלה - מה הצליחו הבריטים לפענח (מברקים של הסוכנות? מברקים של שירות הקשר? רשת מסוימת, עורק מסוים או את כל החומר?), וכיצד עשו זאת? - היא עדיין בגדר תעלומה. האם הם הצליחו לשים יד על ספרי מפתחות? האם ביצעו שבירה סטטיסטית מתוחכמת? האם בוגד העביר להם תוכן מברקים? כך לדוגמה, אחד המסמכים הבריטיים מצביע על כך שהם פעלו לשים יד על ספר מפתח של המחלקה המדינית בז'נבה,[30] וייתכן שהשיגו אותו, ופענחו רק מברקים שהוצפנו באותו מפתח. במסמך בריטי אחר מתועד מבצע בשם Goulash, שלפיו הצליחו הבריטים, בעזרת מודיע, לשים יד על ספר מפתח, לרבות הוראות השימוש, ששימש בכירים בהנהגת היישוב.[31]

המברקים המפוענחים, שפורסמו בידי הבריטים ב'ספר הלבן' ביולי 1946, היו מברקי ISTRIA סוכנותיים. האם הבריטים לא חששו לחשוף מקורות מודיעין כאשר פרסמו מברקים מפוענחים, שהעידו על יכולתם ליירט תשדורות של שירות הקשר ולפענח את הצופן של שירות הקשר?

נראה כי לחציה הפוליטיים של אופוזיציה פרו־ציונית קולנית בפרלמנט הבריטי ולחץ אמריקני הם שהניעו את ראש הממשלה הבריטי, הרוזן קלמנט אטלי (Attlee), להורות על הכנת מסמך ממשלתי שיכלול ראיות חותכות לכך שהסוכנות היהודית מעניקה חסות לארגון טרוריסטי ('ההגנה'), למרות התנגדות ה־MI5 לפרסום המברקים המפוענחים, מחשש לחשיפת מקורות שתגרום ל'עלטה מודיעינית' שתפגע בביטחון הכוחות הבריטיים בארץ ישראל. פיצוץ מלון המלך דוד בידי האצ"ל ב־22 ביולי 1946 הגביר את חשיבות המקורות הללו ביתר שאת, שכן הוא שיבש פעילות גורמי מודיעין בריטיים אחרים. ראש ממשלת בריטניה דחה את תביעת MI5 להשמיט את המברקים המפוענחים מ'הספר הלבן'. ביומנו של לידל, שקודם לתפקיד המשנה לראש ה־MI5, מתוארת סדרת פגישות בעניין 'הספר הלבן':[32]

27 Steven Wagner, *'Blowing the Source': Britain's use of SIGINT in Palestine, 1933–47*, Center for cryptologic History – 2013 Cryptologic History Symposium, 18 Oct 2013, Johns Hopkins Applied Physics Lab.

28 *Robertson Report*, p. 6 .

29 לא הובהר האם CREAM היה מודיעין שהושג משבירת צופן או בדרך אחרת.

30 TNA, KV 2/1435, minute 521, P. Steibel, 18 July 1947, Part 2 of file named "JEWISH AGENCY FOR PALESINE", p. 10.

31 TNA, KV 4/469, *Diary of Guy Liddel*, May to December 1947, pp. 61-62

32 TNA, KV 4/467, *Diary of Guy Liddel*, November 1945 to September 1946, pp. 250-251, 254-259, 266-269, 277.

- ב־5 ביולי 1946 נערכה פגישה במשרד המושבות שבה הוברר הלחץ על הוצאת המסמך. הוא מצדו הציע חלופות למנוע פרסום חומר שיעיד על היכולת ליירט מברקים ולפענחם, ועדכן מייד את ראש ה־MI5, שהיה אף הוא מודאג מהסיכון בחשיפת מקורות.
- ב־8 ביולי מתוארת הכנת תזכיר לראש הממשלה ולמשרד המושבות, בהתבסס על חומר סודי ביותר ומקורות נוספים, על כך שהסוכנות היהודית שולטת על 'ההגנה' והפלמ"ח, האחראים לפעילות האלימה והבלתי חוקית, וכי הם משתפים פעולה עם האצ"ל והלח"י, כאשר הכוונה הייתה לבסס מידע זה על חומר שנתפס בארץ ישראל, וכך להימנע מחשיפת מקורות.
- ב־9 ביולי מתוארת פגישת ראש הממשלה ושר המושבות בהשתתפות גנרל הייסטינגס ליונל איסמאי (Ismay)[33] וראש ה־MI5. מסקנת ראש הממשלה מהדיון מחוקה מן המסמך (על פי הרישום ביומן ב־11 ביולי, ניתן להבין כי ההנחיה הייתה לבסס את 'הספר הלבן' על מקורות סודיים ביותר, אלא אם יאתרו בחיפושים בארץ ישראל חומר חלופי), אך נכתב שם כי ראש ה־MI5 טען שאם כך ייעשה, צפויה עלטה מודיעינית: "היה ונעשה זאת אנו עלולים להיות בעלטה (we might be in the dark), בכל הנוגע למבצעים בעתיד". למרות זאת סוכם להכין 'ספר לבן' עם חומר סודי ביותר, תוך פעילות לכיסוי המקורות ("cover up").
- ב־10 ביולי התקיים דיון בהשתתפות קלר ונציגי משרד המושבות על המסמך, ומפגש עם ראש המודיעין הצבאי (DDMI) כדי לשכנעו שראשי המטה הכללי לא מעריכים כראוי את המשמעות שארץ ישראל תהיה שרויה בעלטה אם ייחשפו המקורות, והכוחות הבריטיים יהיו תלויים רק ביומינט: "פלסטיין צפויה להיות בעלטה".
- ב־11 ביולי דיווח איש המודיעין הצבאי שהוא שוחח עם ראש אגף המבצעים (DMO), כדי שהלה יעדכן את ראש המטה הכללי (CIGS) בנדון. הוא קיבל דיווח כי ראש המטה הכללי ישוחח עם ראש הממשלה על העניין. התקיים מפגש עם משרד המושבות כדי לסיים את הכנת טיוטת המסמך, ומפגש נוסף כדי לשכנע שאין צורך בחשיפת מקורות, שהרי לפי שידורי קול ישראל, 'ההגנה' והפלמ"ח לקחו אחריות מלאה על הפעולות הצבאיות בארץ ישראל. בדיון אצל ראש ה־MI5 בהשתתפות קלר, נדונה חשיפת המקורות והוקרא מברק שנשלח מהמפקד העליון בארץ ישראל, שבו הובע חשש שהוא יימצא ללא מודיעין

33 מזכיר צבאי לראש הממשלה.

בסיטואציה קריטית: "המברק ביטא את חשש המפקד העליון מכך שימצא את עצמו במצב קריטי ללא מקורות מודיעין". אך כל זה היה ללא הועיל. ראש הממשלה מיאן לדון בנושא למרות החשש לביטחון הכוחות הבריטיים, אך נתן להם ארכה של שבוע להביא 'מידע מרשיע' חלופי: "ראש הממשלה הסתייג מדיון בנושא של ההשפעה על ביטחון כוחותינו. [...] ניתנה לנו ארכה של שבוע להשיג מפלסטיין עדויות שאם הן יהיו משכנעות, ייתכן שיוכלו לשמש תחליף ל[כמה מילים מחוקות]".

- ב־12 ביולי נרשם דיווח על מפגש עם הלורד צ'נסלור (Lord Chancellor) בעניין ניסוח המסמך.[34] ב־15 ביולי דווח על מפגש נוסף, ועל כך שניתנה ארכה של יומיים להבאת חומר חליפי. ב־19 ביולי דווח על מפגש נוסף שבו הוצגה טיוטה ללא [מילה מחוקה] בתחילתה. סוכם כי נדרש חומר נוסף שיקשר בין הסוכנות היהודית לבין שידורי קול ישראל. ב־20 ביולי התקיים עוד מפגש עם ה־Lord Chancellor, שבו הושלם ניסוח טיוטת המסמך.
- ב־22 ביולי הגיעה הידיעה על פיצוץ המפקדה הבריטית במלון המלך דוד. ב־23 ביולי דווח כי טיוטת המסמך נמסרה לראש הממשלה, שסירב להוציא את המילים על ISTRIA. התגובה הרשומה ביומן היא "שזה חבל, אך לא משנה" ("This is a pity, but I don't think it matters a great deal").
- בזה לא נגמר העיסוק בנושא. ב־30 ביולי מדווח ביומן על אי נחת בשירות המודיעין החשאי (SIS – Secret Intelligence Service/MI6) בטענה כי ה־MI5 לא טיפל נכון בעניין. ב־9 באוגוסט מדווח על פגישה עם ראש ה־MI5, שבו הוא מדווח על שמועה שהגיעה אליו מקלר כי: "קיימת הרגשה כי בטיפול בספר הלבן ה־MI5 אִכזב את החבורה [המודיעינית] (let the party down)", ולכן הוא מציע לבצע בדיקה בדיעבד (post mortem), כדי לשכנע שהעניין נכפה עליהם על־ידי ראש הממשלה.

הנזק המודיעיני לכוחות הבריטיים היה רציני והם סבלו מ'עלטה' במשך שנה קריטית, שבה הם התקשו להפיק מודיעין מתשדורות של שירות הקשר ושל המחלקה המדינית.[35] בשנה זו נקבע עתיד המנדט הבריטי בארץ ישראל, וממשלת בריטניה החליטה להעביר את הנושא להכרעת האומות המאוחדות. על הנזק המודיעיני יעיד הרישום ביומנו של

34 Lord Chancellor – שר בקבינט הבריטי, העומד בראש מערכת המשפט ומכהן כיושב ראש בית הלורדים.

35 שירות הקשר סיפק למחלקה המדינית קשר רדיו מוצפן בין משרדיה הראשיים בלונדון ובארץ (ובין פברואר לספטמבר 1947 – גם לניו־יורק), אך הקשר ליתר משרדי המחלקה המדינית נעשה בשירות מברקים מסחרי, בצופן של המחלקה המדינית.

לידל מ־5 בדצמבר 1946.[36] בדיווח זה מודגש היעדר המודיעין עקב פרסום 'הספר הלבן' ומפורטות ההאשמות ההדדיות בין ראשי המודיעין הבריטי בשאלה מי אשם במחדל: "ג'יימס רוברטסון שוחח עמי על התזכיר שראש המודיעין הצבאי שלח לראש המטה הכללי על העובדות של הפגיעה (blowing of) ב[מילים מחוקות] ב'ספר הלבן'. מאז אין אנו יכולים לטפל ב[מילים מחוקות], ועברנו ל[מילים מחוקות]. הייסטינגס, בדרכו האופיינית, אומר שאין לזה קשר אלינו ושהוא אישית יסביר זאת לראש המודיעין הצבאי. אמרתי שאין לי התנגדות, בתנאי שהוא לא יציע בהערתו, כפי שעשה בעבר, כי ה־MI5 אִכזב את החבורה (let the party down). הנחתי שגישתו היא שאין כל ביטחון שמצב העניינים הנוכחי הוא תוצאה של הפגיעה (blowing) ב[מילים מחוקות], והוא סבור שמדובר באמצעי זהירות שגרתיים (?). אמרתי לראש המודיעין הצבאי שהוא יקבל תזכיר מה־MI6. הוא אמר שהייסטינגס שוחח עמו והוא סבור שיש מידה של קנאה בין הארגונים, וכי כל העניין הוא טיפשי". השיקולים המדיניים של הקברניטים הבריטים גברו אפוא על שיקולי ביטחון הגייסות הבריטיים ועל השלכות אובדן מקור מודיעיני חשוב. זו לא הפעם הראשונה ולא האחרונה ששיקולים פוליטיים, שהם ודאי פרוגטיבה של הקברניטים, גוברים על שיקולים מודיעיניים.

מפקד ספינת המעפילים 'נירית', ראובן יתיר (משמאל) והגדעוני אהרן מיכאלי ומפתח מורס בידו, ארכיון בית הפלמ"ח

הגדעונית פנינה נורקין בתחנת האלחוט במרסיי, צרפת, 1948, ארכיון בית הפלמ"ח

36 TNA, KV 4/468, Diary of Guy Liddel, September 1946 to March 1947, pp. 95-96.

הגדעוני יהודה לימוני בתא האלחוט בספינת רכש, 1948, עיזבון מייק הררי

המשחתת הבריטית HMS Child, בראש התורן מתנוססת אנטנת מְאַפֵּן HFDF,
אוסף מוזאון המלחמה האימפריאלי, בריטניה

השלכות 'האסון'

המהנדס הבכיר בשירות הקשר הארצי, מיכאל גורדין ('המהנדס הגדול'), העיד לימים כי 'האסון' – כך נקרא האירוע בשירות הקשר – זעזע את שירות הקשר. מקור 'האסון' נבע מכך "שאליהו גולומב ['המפקד הבלתי מוכתר של ההגנה' וחבר המפקדה הארצית] לא רצה לשמוע מהחלפת מפתחות – הקודים שהיו יותר מדי זמן בשימוש; גולומב סבר שזה לא הגיוני שהבריטים גם יתפסו וגם יפענחו קודים שלנו ועוד בעברית".[37] הוסיף על כך פרץ

37 **שריג, לקסיקון למונחי קשר**, עמ' 372.

רוזנברג, הצנחן הארץ־ישראלי הראשון ששימש אלחוטן בצבא הבריטי:[38]

אנחנו יצרנו מערכת ודאגנו לכסות אותה מבחינה מקצועית שגם כתבי הסתר וגם שיטת הקשר והכל יהיו מכוסים. לא יכלו לגלות אותנו. לא פענחו את הדברים שאנחנו שידרנו. אבל לגבי קשר ללונדון, כמובן שמה יש בסוכנות תמיד אנשים עם ידע יותר גדול. נמצא שם מישהו שלמד כנראה פעם כתבי סתר שהיה בישיבה, עם איזה מפתח מאיזה פסוק מהתנ"ך או משהו כזה. [...] מאחר וזה לא היה מתפקידנו, אלא תפקידנו היה לדאוג שהמכשיר יהיה בסדר שהעברה תהיה בסדר ושהקליטה תהיה טובה. לא רצינו להתערב בעניין הזה. אבל הזהרנו את מישה גורדין פעם, פעמיים, שלוש פעמים שירד מהכתב הזה. [...] לא עזר שום דבר המשיכו לשלוח מברקים ואני הייתי עסוק בדברים שלי והם בשלהם. עד שביוגוסלביה כשהייתי, התיידדתי עם כמה אלחוטאים אנגלים [...] אחד מהם מספר לי: תשמע, אני הייתי בארץ ישראל, בפלסטיין, ואני הייתי בעקיר [עקרון – תל־נוף], שם הייתה לנו תחנה לעשות ג'וניק [לוחמה אלקטרונית – הפרעות מכוונות] מהמרגלים הגרמנים [...] שהם לא יוכלו להעביר מברקים מהארץ לגרמניה. אבל הייתה תחנה אחת שקיבלנו הוראה לא להפריע לאנשים האלה. וזה אתם. עשיתי כל המאמצים לצאת מיד מיוגוסלביה. ולא קל היה לצאת משם. צריך היה לעבור קווי גרמנים. [...] והייתה לי סיבה גם אחרת לצאת [...] באתי לארץ. דבר ראשון נכנסתי לחברה שבמחסן למעלה, שם מוישל'ה [משה סנה] יושב עם לוינסקי, אליהו גולומב ישראל ג'מילי. והסתגרנו שמה [...] ואנצו סרני. מקבלים את כל הדו"ח שלי וכל העסק הזה, ואני על תחנת האלחוט אומר למוישל'ה באוזן אחת. הוא אומר: רוץ לבן־גוריון. בן־גוריון היה עסוק באותה תקופה. [...] ובעזרת פולה נכנסתי אליו. ישבתי. אני מדבר, הוא שואל אותי על טיטו. אני מספר לו את זה, אבל נכנס לו מכאן ויוצא משם. חקר אותי שעתיים על טיטו. בסוף הוא אומר לי: תראה, בקשר לעניין הזה שאמרת שמה בכתב הזה, אז אני אדבר בירושלים עם ראובן [שילוח] והוא כבר. הוא לא דיבר הוא לא סידר שום דבר. עד שיום בהיר אחד יאן [יעקב ינאי] הופיע בנהלל. [...] זה היה בערך ב־12:00 בלילה. איפה פרץ? תעיר אותו מהר. האם זה יכול להיות שהאנגלים כל הזמן פענחו את המברקים שיצאו בתחנה הזו שם? אמרתי לו: שלום. מה לעשות עם כל העסק הזה? למה סיפרתי לכם את הסיפור הזה?

38 פרץ רוזנברג התנדב לקבוצת צנחני היישוב וצנח בהרי דורמיטור שבמונטנגרו במאי 1943 כאלחוטן ביחידת קישור צבאית בריטית שחברה לקבוצת הפרטיזנים בפיקוד טיטו היוגוסלבי. עדות פרץ רוזנברג, 10.1.1982, תיק 13/96, עמ' 23–26, את"ה.

מוניה אדם, מבכירי הטכנאים בשירות הקשר ב'הגנה' ('המהנדס הקטן'), כתב בזיכרונותיו:[39]

> השידורים ללונדון ולניו־יורק היו בכתב סתרים, אך אלה לא הגיעו לרמת בטיחות שאינה ניתנת לפיצוח על־ידי גורם עוין, ולימים אכן נתברר כי הבריטים פענחו כמה מברקים משידוריה של תחנת שרה. [...] לאחר 'השבת השחורה' פרסמו הבריטים ספר־לבן שהכיל תוכנם של עשרות מברקים ששודרו מירושלים ללונדון על־ידי הסוכנות היהודית. התברר שהבריטים פענחו את המברקים האלה במשך שנים. יותר מאוחר נודע לנו, מפי איש מן המחלקה לעיקוב אחרי תחנות זרות ופענוח מברקים בממשלה הבריטית, כי הקודים של תחנת הסוכנות היו להערכתם פרימיטיביים ביותר.

האירוע גרם להחלפת הצפנים שבשימוש שירות הקשר, אך השינוי לא עמד בפני הבריטים. במברקי המוסד לעלייה ב' מפברואר 1947 צוינו "חששות מבוססים שידידינו [הבריטים] מבינים את שפת נוגה [הצפנים בשימוש ה'גדעונים' בשירות המוסד לעלייה ב']".[40] באוגוסט 1947 הגיע שירות הקשר למסקנה כי הבריטים החלו לקרוא מחדש את הצפנים של 'ההגנה', והניע שוב מהלך להחלפת הצפנים, שנמשך שבועות אחדים. ינאי, ראש שירות הקשר, הוציא למוסד לעלייה ב' ב־8 באוגוסט 1947 את המברק (תזכיר, בלשון הימים ההם) הבא: "הגיעו אלינו ידיעות שהחומר הנשלח מתפענח על ידי 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".[41]

יצוין כי שירות הביון האיטלקי (SIM – Servizio Informazioni Militari) ידע לקרוא את שיטת הצופן של הצבא היוגוסלבי, ששימש את שירות הקשר של 'ההגנה', ועשה שימוש נרחב ביכולת זו בעת הלחימה עם הצבא היוגוסלבי באלבניה באפריל 1941.[42] אורי גורן, מוותיקי ה'גדעונים' ולימים מבכירי חיל הקשר בצה"ל, העיד:[43]

> בעקבות קשרים מצוינים שהיו למודיעין הישראלי עם שירותי המודיעין האיטלקי,

---

39 מוניה אדם, **קשר אמיץ**, תל־אביב: משרד הביטחון, 1986, עמ' 207 ו־256.

40 מברקים שנשלחו מהארץ לצרפת ואיטליה ב־18.2.1947, תיק 524/14, את"ה.

41 תיק 534/14, את"ה.

42 במסמכי המודיעין האמריקאי לאחר כיבוש איטליה מצוינת יכולת גבוהה של האיטלקים בפיענוח צפנים המבוססים על שינוי מיקום אותיות (transposition), כמו הצופן של שירות הקשר. http://chris-intel-corner.blogspot.co.il/2012/08/italian-codebreakers-of-wwii.html; וכן:
https://www.nsa.gov/public_info/_files/history_today_articles/21_March_2011.pdf

43 אורי גורן, **משני צידי הקריפטו**, הוצאת המחבר, 2008, עמ' 55. ראו: http://www.uri-goren.com/files/final_version_web.pdf

התארחה [בראשית שנות ה־60] משלחת שלהם אצלנו. בסיום הביקור הוזמנתי כחבר במשלחת של המודיעין הישראלי לביקור גומלין באיטליה. המארחים האיטלקים לקחו אותנו לסיור ברומא ובמסגרתו הגענו לאזור מונטה מריו, שם הפעלנו ב־1947 תחנת אלחוט מחתרתית כזו של המוסד לעלייה ב׳. כיון שעברו שנים רבות, העזתי וסיפרתי למארחים על שירותי במקום. הם לא הגיבו, אך למחרת הביא לי אחד המלווים תיק ובו מברקים מפוענחים של השידורים ה׳סודיים׳ שלנו. המלווה הסביר לי שהם ידעו על פעולותינו, האזינו לשידורים שלנו, פענחו אותם ללא קושי רב, וכל זאת על מנת לוודא שאין זו תחנה של המחתרת הקומוניסטית או של גורם אחר המהווה סכנה לשלטון האיטלקי.

גופי ההאזנה בשירות הביון הבריטי – GC&S (Government Code & Cypher School) וה־RSS (Radio Security Service), שקדמו לסוכנות הביון GCHQ (Government Communications Headquarters) הנוכחית, יירטו ופענחו את שידורי שירות הקשר בשמות הקוד BUTTERCUP, FOG ו־CREAM.[44] החוקר חיים שנהב טען כי הבריטים קלטו ופענחו את רוב השדרים שהוחלפו בין ספינות המעפילים למטה ההעפלה בארץ, בהתבססו על עדותו של קצין הצי היהודי, אלן טיילר (Tyler), ששירת על המשחתת הבריטית HMS Chevron משלהי שנת 1946 ובמשך רוב שנת 1947.[45] ואכן, קרוב לוודאי כי יירוט ופיענוח התקשורת עם ספינות מעפילים היו גורמים מכריעים בהצלחת הסגר הימי הבריטי. שכן מאליהן מתעוררות השאלות כיצד הצליח הצי הבריטי להפעיל סגר יעיל על חופי הארץ, ולמנוע בצורה כמעט מוחלטת הגעת ספינות מעפילים לחופי הארץ? כיצד איתרו בצורה כה יעילה מטוסי סיור בריטיים את ספינות המעפילים משלהי שנת 1945 ועד להקמת המדינה במאי 1948, וכיוונו אליהם את ספינות הסיור (ספינות ה־Palestine Patrol)?

נתוני ההעפלה מחזקים את ההשערה בדבר מרכזיות הפיענוח של תעבורת התקשורת במצור הימי. מתוך 19 ספינות מעפילים שהגיעו בחשאי לחופי הארץ בשנת 1946 רק ספינה אחת, ׳עמירם שוחט׳, הצליחה לפרוץ את הסגר, ואף היא יורטה סמוך לחופי הארץ בידי מטוס סיור בריטי ומשחתת בריטית, אך לא זוהתה כספינת מעפילים. מתוך 22 ספינות מעפילים שהגיעו בחשאי לחופי הארץ בשנת 1947, רק שלוש

44 Matthew Grant, *British Way in Cold Warfare: Intelligence, Diplomacy and the Bomb 1945–1975*, London: Bloomsbury, 2009, p. 143; Calder Walton, *Empire of Secrets*, London: Harper Press, 2013.

45 חיים שנהב, ״פִּענוח צפני שרת״, בתוך: ניר מן (עורך), **עלי זית וחרב: עמוד האש**, יב, ירושלים: כרמל והעמותה לחקר כוח המגן מייסודו של ישראל גלילי, 2012, עמ׳ 278–284.

הצליחו לפרוץ את הסגר: 'שבתאי לוז'ינסקי', ששמרה בהפלגתה על דממת אלחוט, 'עלייה', שיורטה סמוך לחופי הארץ בידי מטוס סיור בריטי ומשחתת בריטית, אך לא זוהתה כספינת מעפילים (וסמוך אליה יורטה ונתפסה בידי הבריטים ספינת המעפילים 'קדימה'), ו'הפורצים', ספינת המעפילים היחידה בשנים 1946–1947 שקיימה במהלך הפלגתה קשר אלחוט סדיר ולא יורטה בידי הבריטים.

חיל האוויר המלכותי הבריטי הפעיל כמה טייסות סיור וצילום במשימה זאת.[46] עיון ביומני המבצעים של טייסות מטוסי הסיור הבריטיים ממחיש כי טיסות הסיור ליירוט ספינות המעפילים נעשו על פי מידע מודיעיני מדויק. מבצעים אלה כונו בשם הקוד Sunburn (ראו נספח ג').[47] ספינות מעפילים שידרו פעמיים־שלוש ביום 'תזכירי הגדרה' שכונו 'Xפ', שבהם צוינו נתוני מיקומן הגאוגרפי, כיוון תנועתן ומהירותן. מברקים אלה נכתבו במתכונת אחידה וקבועה. 'תזכיר ההגדרה' המוצפן היה הודעה של שש חמישיות, ששודרה לפי הדוגמה הבאה (ראו פירוט בנספח ב'):

גר 6 Xפ בת

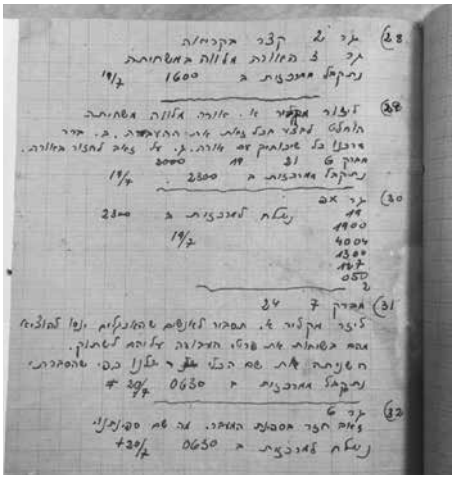
חטרעב חלצXל לצנמה ניXיפV VYYFF Vייי

הייתכן כי הבריטים קלטו ופענחו את מברקי ה'Xפ', ואלה היו מקור המודיעין העיקרי לטייסות מטוסי הסיור, שיירטו את ספינות המעפילים? יצוין כי מברקים אלה הציגו לבריטים אתגר מוגבל: מתכונת קבועה, תוכן שהוא ספרות בלבד (ללא צורך בתרגום מעברית לאנגלית). לא נמצאה עדות ישירה בנושא זה, אך קיים מידע עקיף. לדוגמה: דו"ח 'סודי ביותר' הדן בפעילות נגד ההעפלה, שמשרד הביטחון הבריטי הגיש לקבינט הבריטי ב־8 ביולי 1947, מזהיר כי:[48] "הונאה באלחוט [בקשר לספינות מעפילים] תגרום בוודאות לכך שהארגונים היהודיים ישנו תדרים וקודים, ואנו נאבד את המודיעין המתקבל מההאזנה. סביר כי הונאה [מהסוג המוצע] לא תהיה יעילה, אך אובדן המודיעין יפגע ביכולתנו ליירט ולעצור מהגרים בלתי לגליים. התייעצנו בעניין עם חברי ועדת ה־SIGINT בלונדון והם הביעו אי־נכונות לחשוף את שירותי ההאזנה שלהם [services "Y"], אלא אם יקבלו הוראה מפורשת מדרג בכיר".

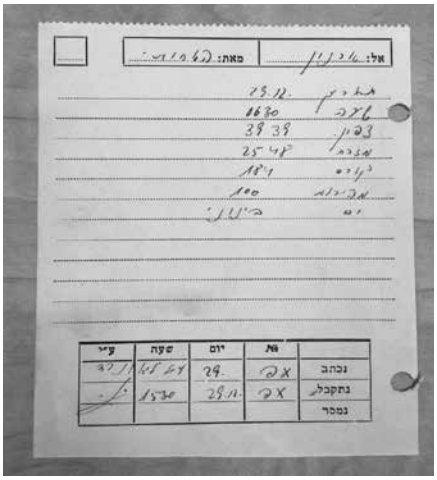
46 דניאל רוזן, **גדעונים: מפעילי הקשר האלחוטי בשירות המדינה שבדרך**, יהוד: העמותה להנצחת חללי חיל הקשר והתקשוב, 2018, עמ' 8–9.

47 בנספח ג' מוצגת דוגמה מיומן המבצעים של טייסת 621, שמטוסיה הופעלו משדות התעופה בעין־שמר ובעקיר (תל־נוף). TNA, AIR 27/2135/39.

48 TNA, CAB 81/80, p. 2.



מימין: תזכיר Xפ שנשלח מהספינה ׳י״ד חללי גשר א־זיב׳ ביולי 1946, כפי שנרשם (לאחר שפוענח) ביומן תחנת האלחוט בתל־אביב, תיק 14/232, את״ה



משמאל: תזכיר Xפ שנשלח מהספינה ׳קיבוץ גלויות׳ בדצמבר 1947 והועבר לתל־אביב דרך איטליה, כפי שנרשם בתחנת האלחוט לאחר הפיענוח, תיק 14/275, את״ה

ה׳פאנים׳: הוכחה נוספת לשבירת הצופן

ספינות ההעפלה ׳פאן יורק׳ ו׳פאן קרסנט׳, שנקראו ה׳פאנים׳, הפליגו מבולגריה ב־27 בדצמבר 1947 עם 15,236 מעפילים על סיפונן. היה זה גדול מבצעי ההעפלה בתקופה המכרעת ערב הקמת המדינה.

ב־30 בנובמבר, יום לאחר החלטת החלוקה, התכנסה הנהלת הסוכנות בירושלים, ואחרי התלבטות קשה החליטה לעכב את הפלגת ה׳פאנים׳, מחשש שהפלגתן תשבש את המאמצים המדיניים ליישום החלטת האו״ם. אנשי המוסד לעלייה ב׳ באירופה, בהנהגת ד״ר משה סנה, ראש המחלקה המדינית באירופה וראש המחלקה לעלייה ב׳ בהנהלת הסוכנות,[49] לא קיבלו זאת וקבעו תאריך הפלגה. ההנהגה הציונית הבינה שהפור נפל, אך דרשה לסיים את הפרשה בפשרה: הספינות ייכנעו לבריטים בלב ים וישוטו עם המעפילים ישירות לקפריסין ללא מאבק. בן־גוריון שלח מברק ליוסי הראל, שליח המוסד לעלייה ב׳, שמונה למפקד המסע, על סיפון ה׳פאן יורק׳, דרך מפקדת המוסד באיטליה:[50]

> באם האויב יציע לשתי הגדולות [ה׳פאנים׳] ללכת ישר לקפריסין עליכם לענות וכן לעשות: ׳פנינו לארץ ישראל שהובטחה מאלוהים לישראל ואושרה מחדש על ידי

49 משה סנה, ״שאלות לדוקטור משה סנה״, בתוך: יאיר צבן (עורך), **אחרית כראשית: מבחר דברים 1972–1967**, תל־אביב: הקיבוץ המאוחד, 1981, עמ׳ 102.

50 תיק 14/275, את״ה.

האומות המאוחדות אולם אם בדעתכם להפריע למסענו, נלך לקפריסין, בהיותנו בטוחים שבקרוב נגיע לארצנו המשוחררת. תנו לנו את הקורס לקפריסין ונלך אחריכם'.

המברק נשלח למפקדת המוסד לעלייה ב' באיטליה ב־29 בדצמבר בשעה 15:20, אך קליטתו בספינות התעכבה עקב קשיי קשר עם ה'פאנים'. המברק נשלח שוב מהארץ ל'פאנים', ב־29 דצמבר בשעה 15:50, באמצעות תחנת המוסד לעלייה ב' באיטליה, שכן באותה עת טרם הוקם הקשר מהספינות לארץ.[51] על פי הרישום על המברק במפקדת המוסד לעלייה ב' בתל־אביב, קיים ספק אם המברק הגיע לתעודתו. בתחקירי המלווים שלאחר האירוע ובדוח ה'גדעוני' מברק זה לא מוזכר כלל. הספינות חצו את מצרי הבוספורוס לים האגאי, שם פגשו שייטת ספינות מלחמה בריטיות. ב־31 בדצמבר 1946 התקיים האירוע שאותו תיאר ה'גדעוני' ראובן (פופכן) אורן:[52]

> ביציאה מהדרדנלים ממתין לנו heavy cruiser ועוד חמש משחתות. האדמירל של השייטת מבקש (איתות דגלים) שנעבור לקשר רדיו/דיבור. הוא פותח במילים: 'כאן אדמירל XX, מפקד השייטת הבריטית. אני מבין שאתם קיבלתם מסר להפליג עמי לקפריסין ואני מבקש מכם לעשות זאת'. בחדר האלחוט – נוכחים: יוסי הראל, גד הילב (הקפטן), ניסן לויתן (המלווה), גדע שוחט ואנוכי. בפאן קרסנט מקשיבים במקביל ברצ'יק (המלווה והמפקד שלה), אייק (יצחק ארן־אהרונוביץ) הקפטיין והגדעונים גד ליפשיץ וחיים גולדיס. כולנו, חוץ מיוסי הראל, מוכי תדהמה. הערה חשובה: לפני כשנתיים, עם צאת הספר 'אקסודוס – אודיסיה של מפקד' (יורם קניוק) בדקתי נקודה זו עם ניסן, גד, ברצ'יק ואייק. כולם אשרו את נכונות גרסתי.

והנה, מתברר כי ביום ב', 30 בדצמבר 1947, בשעה 14:24, קיבל מפקד השייטת הבריטית, אדמירל ריצ'רד סימונדס־טיילר (Rear Admiral Symonds-Tayler), על סיפון הסיירת הקלה HMS Mauritius, את המברק הבא מהמפקד הצבאי הבריטי בארץ ישראל, בסיווג 'סודי ביותר': "קיבלנו הודעה ממקור בכיר ואמין שהסוכנות היהודית העבירה ברדיו הוראות לספינות הפאנים כי הן יצייתו לבקשות או הוראות של הצי המלכותי, כולל הפלגה לקפריסין".[53]

מפקדי הספינות ומלוויהן אכן קיבלו את ההחלטה בלב כבד. הספינות הגיעו לנמל פמגוסטה ב־1 בינואר 1948, והמעפילים הועברו למחנות מעצר בקפריסין.

מתברר אפוא כי האדמירל הבריטי ידע על דבר ההוראה ששוגרה ברדיו לספינות בעוד יוסי הראל, מפקד המסע, לא קיבל אותה כלל. מה היה מקור המידע של הבריטים? האם ראשי הסוכנות קיימו מגעים חשאיים עם הבריטים, או שמקור המידע היה האזנה לשיחות טלפון

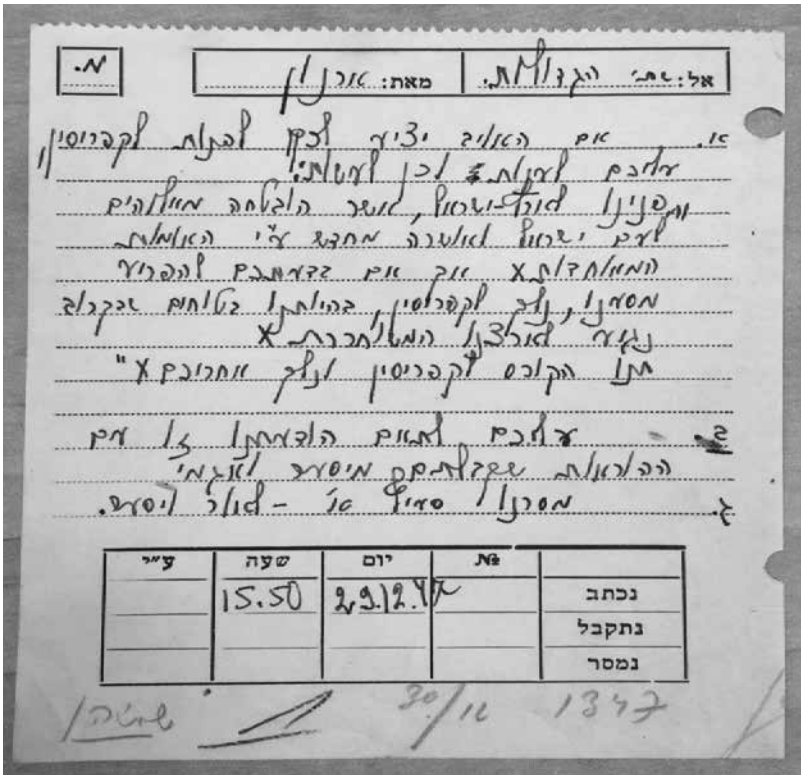
---

51 בעיות הקליטה ב'פאנים' מפורטות בהרחבה בדוח ה'גדעוני' ראובן אורן, שנכתב כשחזר מקפריסין לארץ, כחודש לאחר האירוע. תיק 14/275, את"ה.

52 "זיכרונות ראובן אורן (פופכן)", 2001, תל־אביב: הוצאת המחבר (להלן: **זיכרונות ראובן אורן**).

53 TNA, ADM 1/20793

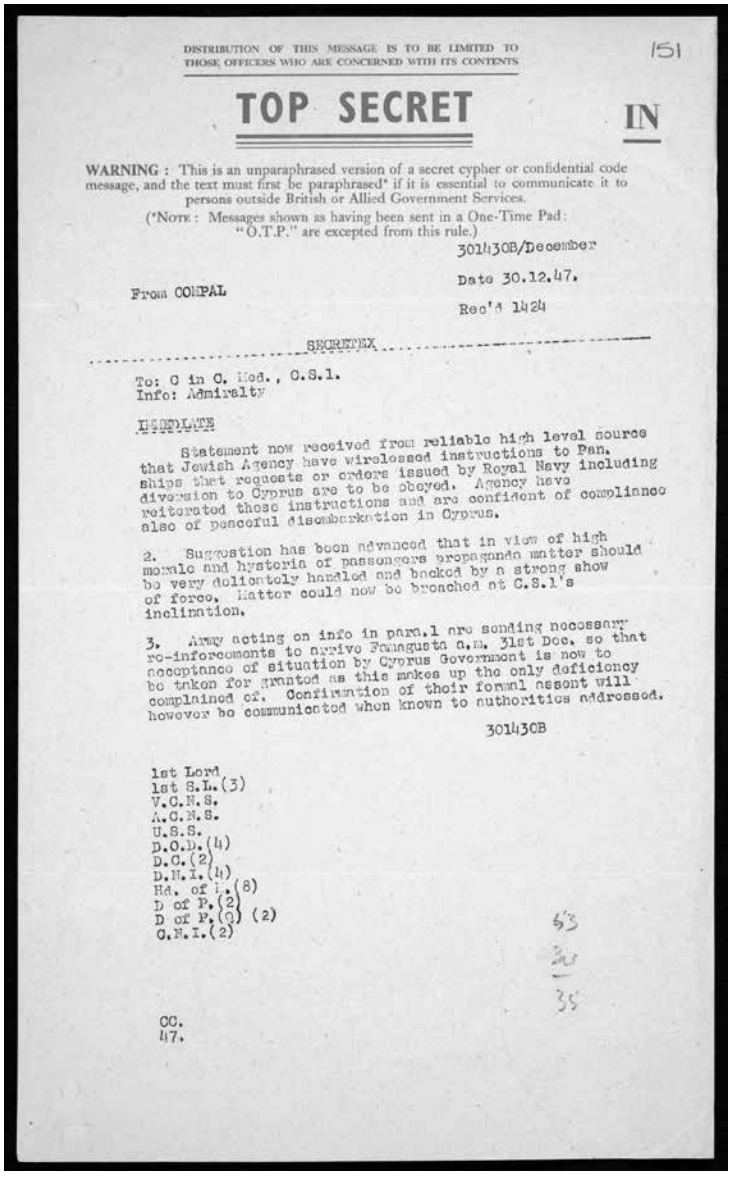
בין מנהיגי הסוכנות? או שמא המידע הושג הודות לשבירת הצופן ופענוח המברק שנשלח מהארץ לאיטליה, 23 שעות קודם לכן? למידע זה הייתה השפעה מכרעת על התנהגות הצי הבריטי, שכן הבריטים סברו כי השתלטות בכוח על הספינות, ללא נזקים מהותיים ואבידות רבות, היא כמעט בלתי אפשרית, ולכן נתנו חופש פעולה לאדמירל הבריטי.[54]



המברק שנשלח מהארץ (ארנון) ל'פאנים' (הגדולות) ב־29 בדצמבר 1947, שעה 15:50

ארנון: מזכירות המוסד לעלייה ב' בארץ; אור: שאול אביגור, ראש המוסד לעלייה ב'; יסער: זאב (וָניה) הדרי, קצין המבצעים של המוסד לעלייה ב'; אגמי: משה אוורבוך, ראש שלוחת המוסד לעלייה ב' ברומניה. בניגוד למברקים אחרים בתיק, שורת 'נתקבל' לא מולאה, ובשולי המברק נרשם בעיפרון "30/12 1347 [13:47] שתיהן". בתחקירים שלאחר המבצע המברק לא הוזכר כלל. האם ייתכן שמברק זה לא הגיע מעולם לתעודתו? תיק 14/275, הארכיון לתולדות ההגנה

54 **לטענת פריץ ליבריך (Liebreich), היסטוריון שחקר את פעילות הצי הבריטי, אילו המשיכו הספינות להפליג לחופי הארץ, ניתן להניח כי האדמירל הבריטי לא היה מחליט לנסות להשתלט על הספינות.**
Fritz Liebreich, *Britain's Naval and Political Reaction to the Illegal Immigration of Jews to Palestine*, London: Routledge, 2005, p. 251.



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 wireless 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)

CC.
47.

המברק המיידי שנשלח בידי גנרל סר אלן גורדון קנינגהם, הנציב העליון ומפקד הצבא הבריטי בארץ ישראל (COMPAL), למפקד הצי הבריטי בים התיכון (C in C Med) ולמפקד השייטת הבריטית (Cruiser Squadron 1) ב־30 בדצמבר 1947, והתקבל באדמירליות בלונדון בשעה 14:24. הבריטים והמוסד לעלייה ב׳ השתמשו בשעון גריניץ (גמת – GMT). תיק ADM 1/20793, הארכיון הלאומי הבריטי

אחרית דבר

הדיון במאמר הנוכחי נסוב על חשיפת הפיענוח של צופני שירות הקשר בידי הכוחות הבריטיים בשנות המערכה לעצמאות. התוצאות האופרטיביות הבולטות ביותר שנגזרו מהישגם המודיעיני של הכוחות הבריטיים היו יירוט ספינות המעפילים שפילסו דרכן מנמלי אירופה לחופי ארץ ישראל. בניתוח נושא זה אין להתעלם מן המערך המודיעיני של אנשי קשר, סוכנים ומרגלים שפרסו הבריטים בנמלי הים התיכון והים השחור. הם ידעו על תנועתן של מרבית ספינות המעפילים: מי הצוות, מה שם הספינה, מי קנה אותה והיכן, מספר נוסעיה ועוד,[55] אך מערך זה לא מסביר כיצד מטוסי הסיור הבריטיים יירטו באופן כה יעיל את ספינות המעפילים שהתקרבו לחופי הארץ, גם כשהן הפליגו בנתיבים בלתי צפויים.[56]

שבירת הצופן של 'ההגנה' סיפקה מקור מודיעין חשוב לבריטים במאבקם למניעת ההעפלה ולעצירת ספינות המעפילים. למרות זאת, דרג הקברניטים בבריטניה החליט בשלב מסוים במאבק, בתהליך עבודת מטה מסודר, לחשוף מקורות מודיעין ולהסתכן בעלטה מודיעינית לשם השגת תוצאות פוליטיות־מדיניות, הגם שהעלטה המודיעינית הסבה להם נזק ממשי. הייתה זו החלטה יוצאת דופן במיוחד על רקע הפעילות הבריטית המתמדת להגנה מפני חשיפת מקורות, שהתבטאה, בין היתר, בסיכום בין ה־MI5 לנציב העליון גורט, כי ה־CID לא יהיה שותף סוד למידע על שבירת הצפנים ולמודיעין המופק מפעילות זו.[57]

ראשי היישוב ומפקדי 'ההגנה' והמוסד לעלייה ב' היו זהירים וחשדנים ונקטו אמצעי ביטחון קפדניים. עיקר התקשורת בין הבכירים הייתה תקשורת פנים־אל־פנים, במפגשים חשאיים ולא שגרתיים, במקומות שונים. מסמכים מסווגים מאוד הועברו בידי שליחים, ולא ברדיו. למרות הזהירות והחשדנות הם בטחו, להוותם, בצפנים. אירועי יולי־אוגוסט

---

55 יואב גלבר, **שורשי החבצלת: המודיעין ביישוב, 1918–1947**, ב, תל־אביב: משרד הביטחון, 1992, עמודים 568–572 (להלן: גלבר, **שורשי החבצלת**); אלדד חרובי, **הבולשת חוקרת: מסמכי ה־C.I.D. בארץ ישראל 1920–1948**, צור־יגאל: פורת, 2011, עמודים 323–324.

56 גלבר ציין כי "שיטת פעולתם של הבריטים בחסימת החוף לגישת ספינות המעפילים לא הייתה ידועה ומובנת, ואילו עמדו עליה, אולי היה ניתן למצוא בה נקודות תורפה ופרצות ולהחדיר לחופי הארץ ספינות רבות יותר". הוא טען כי המטוסים הבריטיים איכנו את שידורי ספינות המעפילים. גלבר, **שורשי החבצלת**, עמ' 571–572. ספינות המלחמה הבריטיות ב־Palestine Patrol (1945–1948) בשנים 1945–1948 היו מצוידות במערכות לאיכון שידורים (HFDF). מערך איכון השידורים הנייח בחופי הים התיכון פורק בתום מלחמת העולם. TNA HW 41/356, DF Site at Nahariya, Palestine. ספינות המלחמה הבריטיות ב־Palestine Patrol (1945–1948) היו מצוידות במערכות לאיכון שידורים (HFDF). מערך איכון השידורים הנייח בחופי הים התיכון פורק בתום מלחמת העולם. TNA HW 41/356, DF Site at Nahariya, Palestine.

57 TNA, KV 4/466, *Diary of Guy Liddel*, June to November 1945, pp. 32-33

1947, שבהם התברר כי הבריטים פיצחו את הצופן של שירות הקשר, היו אירועים מכוננים בתולדות שירות הקשר הצעיר, והביאו למיסוד מערך הצופן בשירות הקשר.

עם הקמת חיל הקשר חל שדרוג מהותי במערך הצפנים הישראלי ובמיסוד נושאי ביטחון קשר בחיל הקשר. הלקח העיקרי מהפרשה ההיסטורית הינו בר־תוקף ביתר שאת בעידן תעבורת המחשבים ולוחמת הסייבר, ולפיו מי שנכווה ברותחין, ראוי שייזהר עשרת מונים בצוננים. מי שבוטח בצופן, שם נפשו בכפו, והאמון בצופן ראוי שיהיה מוגבל, בבחינת כבדהו וחשדהו.

מטוס סיור בריטי מיירט את ספינת המעפילים 'נחשון הקסטל',
24.4.1948, ארכיון בית הפלמ"ח

נספח א': שיטות הצפנה בשירות הקשר ב'הגנה'

<u>השיטה היוגוסלבית</u>

שיטת הצפנה שהייתה מקובלת ב'הגנה' עד שנת 1946 התבססה על שִׁחלוף (שינוי מיקום אותיות - transposition).[58] ההצפנה התבססה על סיסמה מוסכמת. אותיות הסיסמה הוחלפו למספרים, כאשר הערך המספרי - במקום האותיות - ניתן מן הנמוך אל הגבוה. לדוגמה: הסיסמה 'מלחמת היהודים' הפכה ל:[59]

מ	י	ד	ו	ה	י	ה	ת	מ	ח	ל	מ
11	7	1	4	2	6	3	12	9	5	8	10

ידיעה לשידור, "נגיע לחיפה מחר בבוקר הכינו לנו עזרה דחופה רוצים לגמור", נרשמה כך:

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

והחמישיות שודרו לפי הסדר הבא: דמוהר הפיום החהדל...

<u>הצפנה עם מפתח עשר אותיות, בשיטת ויז'נר בטבלה 20X20</u>

מעדויות 'גדעונים' עולה כי בשלהי שנת 1946, אחרי אירועי 'השבת השחורה', כאשר התברר כי הבריטים שברו את הצופן של 'ההגנה', עבר שירות הקשר להשתמש בצופן אחר, בהצפנה בעורקים וברשתות.[60] הצופן החדש היה בשיטה של החלפה (Substitution),

58 בספרות בנושא הצפנה מכונה שיטה זו בשם Columnar Transposition Cipher.

59 שריג, **לקסיקון למונחי קשר**, עמ' 371.

60 'גדעונים' היו אלחוטנים של שירות הקשר בשירות המוסד לעלייה ב', רובם היו לוחמי פלמ"ח. הגדעונים פתחיה פייג ומרגה גורן (גוטהלף) העידו כי בקורס ה'גדעונים' זבולון במרסיי, בשלהי שנת 1946, הם למדו להשתמש בהצפנה זו. עדויות פתחיה פייג ומרגה גורן, מראיין: דניאל רוזן, סתיו 2015, אוסף המראיין.

שלפיה אות הוחלפה באות אחרת לפי כללי ההצפנה. הצופן היה מבוסס על מפתח בן עשר אותיות, כאשר בדרך כלל השתמשו בסיסמאות פשוטות (כמו: 'מלפפון חמוץ', 'מדינה עברית'), ולתשדורת 'רצינית' השתמשו במפתח על בסיס מילים מתוך דף מוסכם מספר קריאה באנגלית.[61] המרת האותיות התבססה על שיטת ריבוע ויז'נר (Vigenère),[62] והשיטה שבה זכרו את הטבלה הייתה הפיכת האות לערכה המספרי, ו'חיבור' ערך האות הגלויה (בהצפנה) או האות המוצפנת (בפיענוח) לערך אות המפתח, במערכת כללים שנלמדה בעל־פה.[63]

הגדעוני יואש צידון העיד על שיטת ההצפנה בשלוחת המוסד לעלייה ב' בצרפת:[64] "את המברק סידרנו בטור של שתי חמישיות, או עשר אותיות. מעל המסר, בראש הטור, כתבנו את המפתח לכתב הסתר, גם הוא בן עשר אותיות. במקרה שלנו, זה היה יכול להיות, למשל, בימפלסודרכ - 'בים פלסו דרך'. לכל אות ניתן ערך מספרי. על ידי חיבור או חיסור ערך האות הנשלחת או המתקבלת במברק מוצפן לערך אותיות הסיסמה, הוא המפתח, התקבלו ההצפנה או הפענוח".

הגדעוני שמשון לוטן תיאר את שיטת ההצפנה בצפון איטליה:[65] "תוכן ההודעות היה מוצפן, כשהמפתח הוא סיסמה כמו: מלפפון חמוץ, מיץ עגבניות, חומה ומגדל וכדומה. כל סיסמה כללה 10 אותיות, והייתה טובה להצפנה (או פענוח) של שתי 'חמישיות' עוקבות של אותיות. הסיסמה גם הייתה מוחלפת כל יום על פי טבלה מוסכמת מראש".

הגדעוני נחום מנור סיפר על פעילותו במרסיי בשנת 1947:[66] "חלה התקדמות בשטח כתבי הסתר. לצורך הצפנת מברקים השתמשנו בכמה ספרי־כיס אנגליים אשר היו אז להיטים, והטבלאות היו מסודרות וברורות. כדי לזרז את הפעולה, נהגנו לבצע את ההצפנות בזוגות: אחד מקריא מן הספר ושני מחפש בטבלה".

---

61 ספרים "פופולריים" למטרה זו היו *Lust for Life* (ספר מאת אירווינג סטון על חיי ואן־גוך), *Three Men in a Boat* (ספר הומוריסטי של ג'רום ק' ג'רום), *How Green Was My Valley* (רומן מאת ריצ'רד לוולין על משפחת כורים בוולס) ו־*Frenchman's Creek* (ספר היסטורי מאת דפנה די מורייה).

62 כללי חיבור האותיות שבהם השתמשו היו למעשה סימולציה של ריבוע ויז'נר לא רגולרי של 20 אותיות. ארבע אותיות לא הוצפנו (שי"ן, תי"ו, X, V, F), שי"ן הומרה בתי"ו והאות תי"ו הומרה בשי"ן, האות רי"ש הומרה ביו"ד והאות יו"ד הומרה ברי"ש. מאוחר יותר, כאשר מפתח כתב הסתר הפסיק להיות דף מספר ועבר להיות דף חמישיות שהודפס במיוחד, עבר חיל הקשר להשתמש בריבוע ויז'נר סימטרי, עם 25 אותיות (ללא האות V), כדי להקל על זכירת הטבלה בעל־פה.

63 צופן זה לא היה מבוסס על מפתח חד־פעמי אקראי, ולכן היה חשוף להתקפה המבוססת על חוסר איזון סטטיסטי בטקסט הצופן, כפי שבמלחמת העולם השנייה פוענח הצופן היפני Purple בידי האמריקנים.

64 יואש צידון (צ'אטו), **ביום בליל בערפל**, תל־אביב: ספרית מעריב, 1995, עמ' 56.

65 גדעון רדין, "שמשון לוטן מספר על רשת הבריחה באירופה", בתוך: גרנית (עורך), **גיליון מיוחד של קשר אלקטרוניקה ומחשבים**, עמ' 54–55.

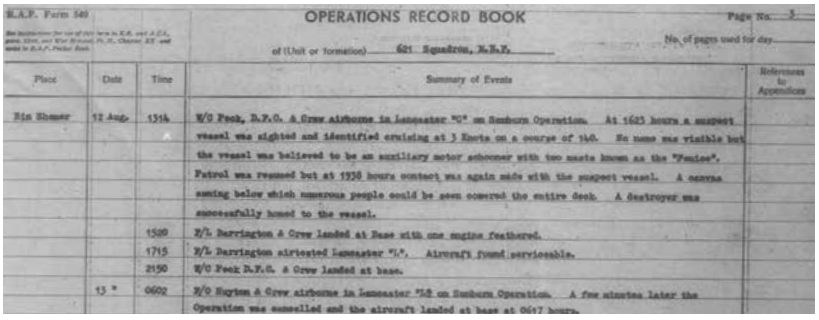
66 עדות, **השערים פתוחים**, הוצאת קרן הפלי"ם, 2001, עמ' 341–348.

הגדעוני ראובן אורן מספר על פעילותו במרסיי באפריל־אוגוסט 1947:[67] "עבדנו בקשר, עברנו לכתבי סתר טובים יותר. הדרכתי גם השתלמות ושיפור יכולת עבודה (מהירות) של החברה מ'קורס מרסיי".

דו"ח מיוחד של 'מפקח האלחוט' בפלמ"ח, אברהם תנחלסון, שנכתב לראש שירות הקשר ב־17 בספטמבר 1947, לאחר סיור בתחנות ה'גדעונים' באירופה, התייחס, בין היתר, להפעלת כתבי סתר נפרדים לפעילות ארגון 'הבריחה', וציין:[68] "בהזדמנות זו הכנסנו לעבודה גם את הכתב החדש עם ספר מיוחד (כתבי סתר) ובנינו את הרשת הזו כעורק קשר מיוחד, המכיל שני מרכזים מחוץ לליאונרד [מילנו] ויסעור [פריז], הקשורים לענייני הבריחה, והקשר דופק.[69] העבודה מתנהלת כבר לפי הכתבים החדשים ובהיפגשי עם מפקדי הבריחה הובעה מצידם שביעות רצונם על ששירתנו אותם באופן היעיל ביותר ועבודתנו הייתה חוליה חשובה בהצלחת העבודה שלהם".

מרדכי בן־פורת, שליח המוסד לעלייה ב' בעיראק, כתב כי בשלהי שנת 1949 הוא הביא ל'גדעונים' בעיראק "צופן חדש שהוכן בארץ", וכי "השידורים החלו אז להתנהל על־פי הצופן החדש".[70]

רשומה מיומן המבצעים של טייסת 621, חיל האוויר המלכותי[71]



R.A.F. Form 540

OPERATIONS RECORD BOOK

Page No. 3

No. of pages used for day

of (Unit or formation) 621 Squadron, R.A.F.

Place	Date	Time	Summary of Events	References to Appendices
Sin Homer	12 Aug.	1314	W/O Peck, R.F.C. & Crew airborne in Lancaster "Q" 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 1930 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	P/L Barrington & Crew landed at Base with one engine feathered.	
		1715	P/L Barrington airtested Lancaster "L". Aircraft found serviceable.	
		2150	W/O Peck R.F.C. & Crew landed at base.	
	13 "	0602	P/O Hayton & Crew airborne in Lancaster "S2 on Sunburn Operation. A few minutes later the Operation was cancelled and the aircraft landed at base at 0617 hours.	

יירוט ספינת המעפילים 'כתריאל יפה', שהפליגה ב־31 ביולי 1946 מנמל בוקה די־מגרה שבאיטליה ובה 604 מעפילים. ביומן המבצעים מצוינים פרטי המעקב אחר הספינה, ב־12 באוגוסט, שערכו מטוסי טייסת 621 משדה התעופה בעין־שמר.

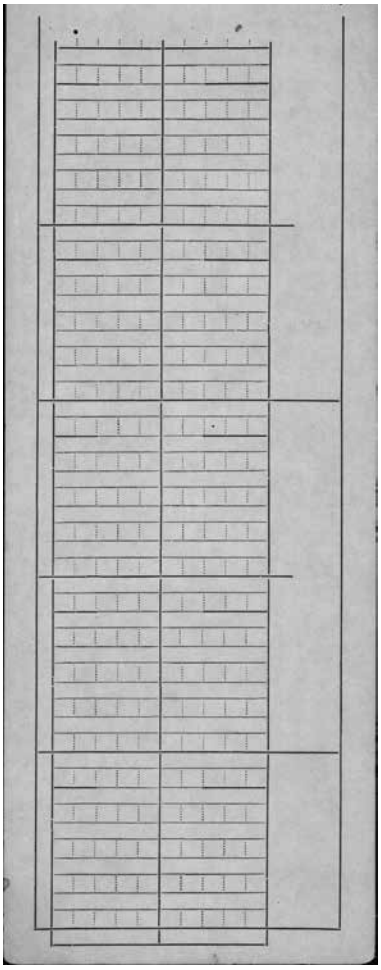
67 **זיכרונות ראובן אורן**.

68 גבי שריג, **הגדעונים באניות העפלה**, אפעל: המרכז לחקר תולדות כוח המגן 'ההגנה' ע"ש ישראל גלילי, 1988, עמ' 130–131.

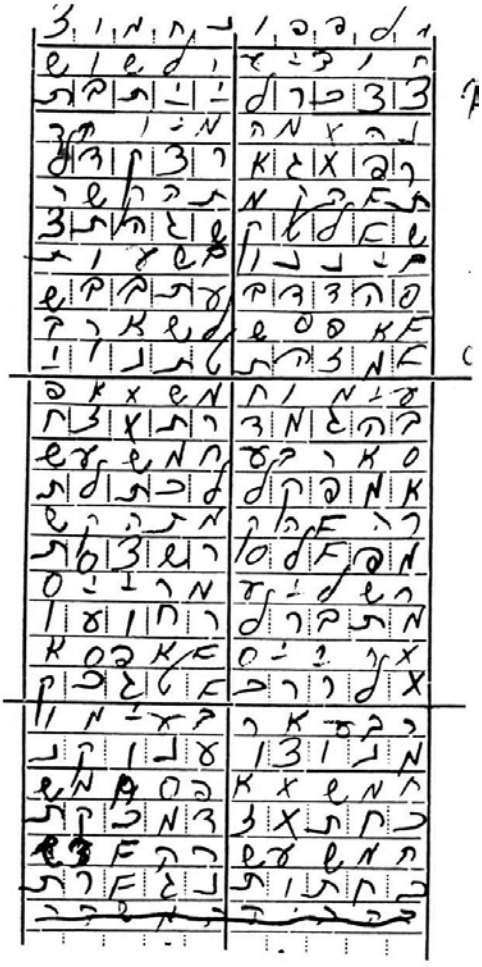
69 שימוש בכתב סתר (הצפנה) נעשה בעורק או ברשת, וההתייחסות היא לעורק כתב סתר בין אינסברוק באוסטריה ומארנו בצפון איטליה, ציר התנועה המרכזי של המעפילים ממזרח אירופה.

70 מרדכי בן־פורת, **לבגדאד וחזרה**, תל־אביב: ספרית מעריב, 1996, עמ' 189.

71 TNA, AIR, Squadron 621 Operations Record, 27/2135/39, p. 95



טופס הצפנה משנת 1947
באדיבות אברהם (מיקו) בכר



דוגמה להצפנת מברק
התוכן: "הודיעו לשושנה [חיפה] מהמיוחדת [הספינה 'כריש']. הקמת הקשר בינינו בשעות 0345, 0415. הקמת הקשר שלי עם רייס [קפריסין] 0445, 0515. דש". באדיבות ראובן אורן

נספח ב': תזכיר הגדרה (Xפ)

האלחוטנים בספינות מעפילים שידרו כמה פעמים ביום 'תזכירי הגדרה' שכונו 'Xפ' (כאשר קו האורך היה מערבי הם כונו 'Xפמ'), שבו ציינו את מיקומם הגאוגרפי, כיוון תנועתם ומהירותם. מברקים אלה נכתבו במתכונת קבועה. כך לדוגמה, מתוך דף הנחיות משלהי שנת 1946, המנחה כיצד יש לרשום 'תזכיר הגדרה':[72]

תאריך בשתי ספרות, לדוגמה: 21, שנרשמו: א ב

זמן החיבור בארבע ספרות, לדוגמה: 1300, שנרשמו: י י ג א

קואורדינטות צפון בארבע ספרות, לדוגמה 17′ 42°, שנרשמו: ז א ב ד

קואורדינטות מזרח בארבע ספרות, לדוגמה 06′ 14°, שנרשמו: ו י ד א

קורס בשלוש ספרות, לדוגמה 180°, שנרשמו: י ח א

מהירות בשלוש ספרות, לדוגמה 7.5 קשר, 075, שנרשמו: ה ז י

ים בספרה אחת (1 – ים שקט, 2 – בינוני, 3 – סוער), לדוגמה 2 (בינוני), שנרשם: ב

המידע הוצפן טרם שיגורו, בהצפנה שהתבססה על שילוב של החלפת אותיות לפי טבלת ויז'נר 20x20 בשינוי מיקום עמודות לפי אותיות המפתח (בדומה לשיטה 'היוגוסלבית'). בדוגמה של שימוש במפתח 'יערות הכרמל', ההצפנה נראית כך:

5	6	9	4	1	10	2	8	7	3
ל	מ	ר	כ	ה	ת	ו	ר	ע	י
ב	א	V	א	ג	י	י	F	ד	ב
נ	נ	V	ל	ח	י	ע	F	י	ל
א	ז	V	א	ד	י	ו	Y	א	ח
מ	י	V	ל	ט	י	ב	Y	פ	צ
י	X	י	ז	ה	V	ב	Y	F	X
ה	X	י	צ	ר	V	ח	Y	F	X

'תזכיר ההגדרה' שודר כך:

גר 6 Xפ בת [בנוהל איתות מורס – הודעה על שידור מברק Xפ הכולל שש 'חמישית']

חטרעב חלצXל לצנמה ניXיפV YYFF Vייי [שש ה'חמישיות' של המברק]

72 תיק 114/74, את"ה.