


# מקור ראשון

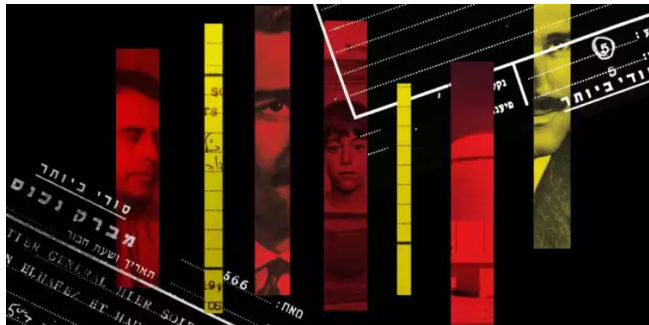
חדשות > דעות > יהדות > תרבות > בעולם > מגזין > ראשונות > חדש > עוד קטגוריות

ראשי > מגזין > דעות

## מסע בעקבות שיטות הסתרה והצפנה שפיתחו מרגלים, פושעים ופרסומאים

זה יכול להיות מצמוץ תכוף של מרואיין בטלוויזיה, ניסוח מוזר בדיווח על דוגמנית שנחקרה במשטרה, או קובץ תמים שנשלח אלינו בדואר אלקטרוני: ד"ר גיל דוד, מומחה סייבר ואיש המוסד לשעבר, יצא למסע בעקבות שיטות הסתרה והצפנה שפיתחו מרגלים, פושעים ופרסומאים, מההיסטוריה הרחוקה ועד היום. אם לא נלמד לשים לב למסרים הסמויים שרוחשים סביבנו, הוא אומר, אנחנו עלולים להיות הקורבן הבא שלהם

מאת  אריאל שנבל — כ"ז בכסלו ה'תשפ"ג (21/12/2022 11:39)



צילום: היסטוריה

WhatsApp שתיק ב- 

שתיק בטוויטר 

שתיק בפייסבוק 

שתיק בדוא"ל 

# בסיום

שיחתנו מצביע ד"ר גיל דוד על קיר בית הקפה שאנחנו יושבים בו: מאחורי לוח זכוכית גדול מסודרים שם פלפלים אדומים לרוב. הוא מבקש ממני להביט היטב. "נו, אחרי שדברנו, אתה רואה כאן סתם פלפלים שהונחו אקראית, או אולי מסר מוסתר שמישהו שתל?"

האמת היא שבשלב הזה לא רק הפלפלים נראים לי כמו שדר סמוי, אלא בערך כל דבר שהעין קולטת. מהי נקודת הדיו השחורה הקטנה בקצה החשבון שקיבלנו מהמלצר? למה החץ שמורה ימינה ביציאה מהחניון גדול יותר מהיציאים בשלטים שלפניו? זה בדיוק הרעיון שמנסה דוד להעביר בספרו החדש "אמנות ההסתרה": משחר ימי האנושות ועד היום, בני אדם מעבירים מידע ללא הרף – וגם מסתירים אותו. הם עושים זאת במגוון דרכים ולמגוון מטרות, וההסתרות הללו משפיעות על כל אחד מאיתנו, ולעיתים גם עלולות להזיק לנו.

נושא ההסתרה, התחתית הכפולה שבתוכה סוד כמוס, מלווה את דוד לאורך הקריירה שלו – גם בחלקה הגלוי יותר, וגם בשנים שאי אפשר להרחיב עליהן את הדיבור. הוא בן 49, נשוי ואב לארבעה, תושב זיכרון יעקב, ירושלמי במקור. את התואר הראשון במדעי המחשב עשה באוניברסיטה העברית, וכבר אז חלם על שירות במוסד. הצעד הראשון שלו בכיוון היה תפקיד הקשור לאבטחה במשרד ראש הממשלה, אבל אחר כך עבר להיִי־טק ועבד כמה שנים בחברת אינטל. גם אז חיידק המוסד לא עזב אותו, והוא רקם קשרים שסייעו לו להיכנס לגוף הביון הממלכתי החשאי. בשלב מסוים אכן הוזמן דוד לריאיון בדירה בתל־אביב, והתקבל. "זה היה צעד מוזר", הוא משחזר. "אנחנו מדברים על תחילת שנות האלפיים. ההיִי־טק בשיאו, לפני התפוצצות הבועה. כולם רוצים לעבוד בענף הזה, ואני דווקא הולך מההיִי־טק למשרד ממשלתי".

"יש לנו צנזורה פנימית חזקה מאוד, והיא מונעת מתכנים שירדו לתת־מודע לצוף בחזרה למעלה. בלילה השמירה קפדנית פחות, והמידע יוצא מהתת־מודע דרך החלום. ברגע שאתה מתעורר, צנזורת היום נכנסת לפעולה וחוסמת שוב את היציאה. אני חושב שמכאן מגיע החיבור שלנו לסיפורים על הסתרה, כי בעצם זה משהו שקורה לכולנו"

במשך שבע שנים עבד דוד במוסד, כראש ענף וכמנהל של צוותי מחקר ופיתוח. בשלב מסוים החליט להרחיב את הידע המחקרי הטהור שלו, ולשם כך למד לתואר שני במדעי המחשב. משם המשיך לדוקטורט, וכתב את אחת העבודות הראשונות בעולם בנושא השימוש בלמידת מכונה ובנייה מלאכותית לזיהוי תקיפות ברשת. השלב הבא היה פוסט־דוקטורט באוניברסיטת ייל בארה"ב, שם המשיך לחקור בינה מלאכותית בתקשורים של סייבר, רפואה ופיננסים.

"כשחזרתי ארצה התחלתי לתת ייעוץ בתחומי הסייבר לסטארט־אפים ולחברות גדולות כמו התעשייה האווירית", הוא מספר. "במקביל לימדתי באוניברסיטה בפינלנד כפרופסור חוקר. מדי חודש הייתי נוסע לשם לשבוע". אחרי חמש שנים הרגיש שהנסיעות התכופות לסקנדינביה מתישות אותו, והחליט להתמקד בייעוץ לחברות בישראל. בכך הוא עוסק עד היום. העבודה הגמישה מאפשרת לו להקדיש זמן לתחביביו המגוונים – שחייה, שיט, טיפוס על צוקים ונגינה בסקסופון.

### **כמי שעוסק בהצפנות ובהסתרות מהסוג העכשווי ביותר, מה גרם לך לכתוב ספר שלוקח את הנושא הזה עשרות ומאות שנים אחורה?**

"המטרה הייתה לכתוב משהו שקשור לריגול, ושאבא שלי יתחבר אליו. הוא תמיד היה שומע ממני קרעי פרטים על העבודה שלי, ואומר – זה מדהים, אבל לא הבנתי כלום. החלטתי לכתוב סיפור אמיתי שקשור לנושא, ושיהיה מובן לכולם. כתבתי פרק על שבוי אמריקני בווייטנאם ששובי קיימו איתו ריאיון טלוויזיוני, ותוך כדי השיחה הוא הצליח להעביר מסר בשפת מורס באמצעות מצמוצים בלבד. זו דוגמה פנטסטית לצופן די פשוט שהוסתר באופן גאוני, והגיע ליעדו. שלחתי את הפרק לקבוצה מצומצמת של חברים ובני משפחה, והם אהבו אותו מאוד. כך המשכתי לכתוב עוד פרק ועוד פרק, עד שנוצר ספר".



כדי לבנות את הפרקים לקח דוד בכל פעם שיטת הסתרה אחרת, ואז חיפש סיפורים שקשורים אליה. "הפרק שהכי התקשיתי לכתוב הוא זה שמדבר על הסתרות בתקופה השואה. חקרתי את הנושא במשך שמונה חודשים, והגעתי לסיפורים מדהימים שלא רבים מכירים. היה למשל מקרה של אסירות יהודיות שהורשו לשלוח גלויות מהמחנה שהחזקו בו. כדי להעביר מסר סמוי בגלויות הללו, שעברו כמוזר צנזורה קפדנית, הן כתבו במקלון שטבלו בשתן של עצמן, כמעין דיו סתרים מאולתרים".

## קריאת מצוקה קטלנית

פרק אחר בספרו של ד"ר דוד עוסק באלי כהן, המרגל הישראלי שהפך מקורב לצמרת השלטון בדמשק. הפרק הזה גם מספק הזדמנות לעמוד על ההבדל בין הצפנה להסתרה – חלוקה שנודעת לה משמעות רבה בעולמות הצללים.

"אלי כהן הצליח בהצפנה אבל נכשל בהסתרה, וזה מה שהביא לסיום המר של חייו", אומר דוד. "גם בספר אני כותב שהוא נכשל. זו מילה קשה, נאבקתי עם עצמי הרבה בשאלה אם להשאיר אותה, ובסוף החלטתי שחשוב להבין מה קרה שם, כלקח לעתיד. אלי כהן שלח מתוככי דמשק מאות שדרים ובהם תוכן מודיעיני שלא יסולא בפז, חומר שבין השאר סייע לישראל רבות במלחמת ששת הימים. המידע היה מוצפן, כלומר – המרגל לקח את הטקסט והשתמש במערכת הצפנה בסיסית אבל חזקה, שהופכת את האותיות לחסרות משמעות, אם אתה לא מחזיק בידוך את המפתח לפענוח. המפתח היה חד-פעמי ושונה בכל מברק, ורק אלי כהן ומפעיליו בתל-אביב ידעו מהו. בשיטה כזו ההצפנה אינה ניתנת לפיצוח, גם לא בעזרת מחשבי-על שקיימים היום. אבל המסרים הועברו בשידור רדיו שלא הוסתר, והסורים קלטו אותו. הם הבינו שיש מרגל שמעביר מידע מתוך דמשק, והניחו שזה מרגל ישראלי."

"מה שהיה נכון לאלי כהן נכון גם לעולם הסייבר. כלומר, גם כשאתה מחדיר סוס טרויאני למחשבים בכור גרעיני או במערכת ביוב, הוא צריך לדבר עם המפעיל שלו ולהפך. זה אומנם מרגל וירטואלי, אבל הוא עדיין שולח ומקבל מסרים, וצריך להסתיר את העובדה הזו"

"יש כל מיני השערות לגבי ניטור מקור השידור – אולי נעזרו בצידור רוסי מתקדם שהובא לבירת סוריה במיוחד, או שהורו על דממת אלחוט כללית וכך השידור של אלי כהן נותר

בודד וקל לגילוי. ההנחיות שהוא קיבל ממפעיליו במוסד דווקא היו יעילות למניעת חשיפה: להקפיד על מסרים קצרים, ולא לשדר בשעות קבועות. אלא שלקראת הסוף זה השתנה. הוא עבר למתכונת קבועה, שידר בכל בוקר וערב באותה השעה, ואורך השדרים הגיע לפעמים ליותר מ־15 דקות".

### **נשמע כמעט התאבדותי.**

"היה מאבק בין המפעילים שלו, שתפסו את הראש בייאוש, ל'צרכני' המודיעין שאמרו: יופי, תביאו עוד ועוד מהחומר הזה. איך אף אחד לא עצר בזמן? שאלה טובה, אבל זה מה שקרה".

### **אחד השדרים של אלי כהן עסק בהפסד של קבוצת כדורגל, לא בדיוק חומר מודיעיני חיוני.**

"נכון, ומכאן עולה הסברה שאולי הוא נזקק לקשר אנושי. אנחנו מדברים על מרגל שפועל בזהות בדויה, מנהל חיים כפולים, לבד, תחת סכנה מתמדת. הפרשנות שלי אומרת שהשדרים הללו צעקו, אולי מתוך תת־מודע, 'אני קיים, אני במצוקה, איך אתם לא רואים את זה. כשהוא חזר לדמשק בפעם האחרונה, כבר התנהגו אליו שם אחרת. היה ברור שחושדים בו, ובכל זאת הוא המשיך ואף הגביר את תדירות השידורים. קשה לפרש את זה באופן אחר מקריאת מצוקה.

"הוא היה יכול להשתמש בשיטות אחרות להעברת מידע – למשל דיו סתרים, או הטמנת פילם ברגליים של שולחנות שש־בש שהוא ייצא מסוריה בכסות שלו כאיש עסקים לגיטימי. זו הייתה יכולה להיות הסתרה טובה. את השידורים שלו איש לא ניסה להסתיר, רק להצפין".



רייזר רז, צילום: אביאל רוזן

**רובם המוחלט של המקרים שאתה מתייחס אליהם שייכים לעולם הריגול ה"ממשי" של פעם. בספר אין כמעט סיפורים של הסתרות ממוחשבות ושימוש**

## באמצעי סייבר.

"אנחנו נמשכים לסיפורי ההסתרות בסגנון של פעם, כי קל יותר לספר ולהסביר אותם, ובעיקר כי יש בהם ממד אנושי. אבל צריך לזכור שמה שהיה נכון לאלי כהן נכון גם לעולם הסייבר. כלומר, גם כשאתה מחדיר סוס טרויאני למחשבים בכור גרעיני או במערכת ביוב, הוא צריך לדבר עם המפעיל שלו ולהפך. זה אומנם מרגל וירטואלי, אבל הוא עדיין שולח ומקבל מסרים, וצריך להסתיר את העובדה הזו. נוסף על כך, גם בעידן הסייבר יש סוכנים אנושיים; מישהו צריך להכניס את הדיסק־און־קי למחשב בכור. אבל אנחנו נחשפים לסיפורים רק כשהם מתפוצצים, ולפעמים זה לוקח שנים, כך שאין עדיין הרבה דוגמאות שאפשר להביא מעידן הסייבר".

## אולי השיטות עצמן מרתקות פחות כשהכול נמצא על המחשב או בענן, ואפשר להסתיר מידע אינסופי בפיסקל אחד.

"זו תובנה שאני כל הזמן חושב עליה. מטבענו אנחנו נמשכים לרמז שמושגל במודעת דרושים, או למרגל שיושב על הספסל ומחזיק עיתון שבאמצעו חור. אבל בסופו של דבר גם את ההסתרות של עולם המחשבים עושים אנשים".



סמס קטנה לטורים מבוגרים היצורים נמוכים. סמס וסמסם והסמס ד"ר צילום סמס מתוך מרעון הקמפיון של רוביט Grey

Spain

טכניקות ההסתרה של ימי הדפוס, אומר דוד, יכולות להופיע שוב בעידן האינטרנט. "בעיצומה של מלחמת העולם השנייה הפליגה מרומניה ספינת המעפילים 'סטרומה', ועל סיפונה מאות בני אדם. הספינה טובעה בידי צוללת, והבריטים אסרו לפרסם זאת בעיתוני הארץ, כדי למנוע תסיסה ביישוב העברי (בשל סירובם של שלטונות המנדט להכניס את המעפילים ארצה, שהתה האונייה בלב ים, ושם פגע בה טורפדו - א"ש). מה עשה העיתון 'דבר'? פרסם בעמוד הראשי שישה פסוקים מהתנ"ך שעוסקים במוות ובמים, וצירף אותיות הראשונות שלהם ויצר את המילה סטרומה. כך הוא עקף את הצנזורה, והביא את הידיעה לקוראים. שנים רבות אחר כך, בהקשר אחר לגמרי, האתר ביזפורטל השתמש בשיטת הסתרה דומה כדי לעקוף צו איסור פרסום על שמה של בר פפאלי".

"גם בעידן הסייבר יש שיטות מגניבות. יצרתי פעם חידת הסתרה שהשתמשה בקואורדינטות של מסלול אופניים בזיכרון יעקב. כתבתי סיפור מסגרת על מרגל איראני שרוצה להעביר מידע דרך מפה תמימה כביכול, והזמנתי את העוקבים אחריי ברשתות לגלות מהי שיטת ההסתרה. מה שעשיתי היה להכניס שינויים קלים מאוד בקואורדינטות של המסלול, שבע ספרות אחרי הנקודה. גם כשהשינויים הללו בלתי נראים על המפה, אפשר להעביר באמצעותם מידע מודיעיני רב. זה אומנם נעשה ברשת, כלומר בעולם הסייבר, אבל החשיבה הייתה אנושית, וגולשים רבים התחברו וניסו לפתור את החידה".

## להרוס כדי לתקן

מעבר למגוון שיטות ההסתרה, השאלה שעולה מספרו של ד"ר גיל דוד היא אם כל זה רלוונטי לחיים שלנו, האנשים הרגילים שאינם עוסקים בביון. "נושא ההסתרות אמור להטריד את כולנו, בהחלט", אומר דוד. "הדוגמה המובהקת היא גנבת זהויות וסיסמאות, אבל גם מלחמות סייבר בין מדינות משפיעות על חיינו. כשמדינה חווה תקיפה מהסוג הזה, תנועת הרכבות משתבשת ותחנות דלק מפסיקות לעבוד, וזה בהחלט משפיע על האדם הפשוט.

"עמותה ספרדית למען ילדים שסובלים  
מאלימות רצתה לפרסם את קו הטלפון  
האנונימי שלה, אבל הבינה שיש בעיה: הילדים,  
שהם קהל היעד, הולכים ברחוב יחד עם ההורה  
שלהם, שאולי הוא הגורם האלים. לכן הם יצאו  
בקמפיין שילוט שבו רק הילד, מהזווית הנמוכה  
שלו, רואה את המסר 'אם מישהו פוגע בך,  
אתה לא לבד', ומספר טלפון"

"בכל מתקפת סייבר יש רכיב של הסתרת מידע, אחרת מערכת ההגנה תזהה את

האיום ותנטרל אותו. בקמפיין תקיפה ארוך טווח, השלב הראשון הוא הדבקה. זו תקיעת היתד, פעולה חד-פעמית שמתבצעת בעזרת זיהוי נקודת חולשה. לאחר מכן יש צורך בהסתרה כדי להישאר במחשב המותקף כמה שיותר זמן – או כי מחכים לרגע הנכון לפעולה, למשל אם המטרה היא להשבית את הכר באיראן, או משום שרוצים להשתמש במחשב הזה. עברייני קריפטו, למשל, מתלבשים על מחשבים של אחרים ומנצלים אותם לכריית מטבעות. פתחת מייל ספאם או קובץ קול שנראה תמים לגמרי, ופתאום המחשב שלך נהיה קצת יותר איטי, ומשתמש ביותר חשמל. אז כן, זה קשור לכולנו ולכיס שלנו".

## יש מה לעשות נגד פעולה מהסוג הזה?

"כן, אבל צריך לדעת שברמת המשתמש הפשוט, חברות האנטי-וירוס לא מתמודדות עם זה. מבחינתן זה לא איום גדול וחשוב מספיק כדי להשקיע בו. לכן תוכנות ההגנה במחשבים שלנו יודעות לזהות נזקות, אבל קשה להן מאוד לזהות כל מיני הסתרות אחרות. בארגונים גדולים, כמו למשל חברות ביטחוניות, הדרך להתמודד עם האיום הזה נקראת הלבנה, כשלמעשה מדובר בהריסה ובנייה מחדש. אם יש למשל תמונה שצריכה להיכנס למאגר הממוחשב שלי, אני יודע שייתכן שהסתירו מידע בפיסקלים שלה, אבל אני לא יודע לזהות אותו וגם אין לי זמן לחפש. מה עושים? מקטינים את התמונה, או מגדילים אותה, או משנים את הפורמט שלה – במקרים רבים הפעולה תהרוס את מה שניסו להשתיל שם, אבל לא תפגע במה שהמשתמש צריך. זה נכון גם למסמכים, קובצי קול, אימיילים וכן הלאה".

ההסתרות המתוחכמות ביותר הן אלה שלא טורחות להסתתר. הן יהיו גלויות לחלוטין עבור קהל מסוים, אף ללא שימוש במפתח מחוכם, בעוד אחרים לא יבחינו בדבר יוצא דופן. "יש לכך דוגמה מאלפת שלא נכנסה לספר. עמותה ספרדית למען ילדים שסובלים מאלימות בבית פתחה קו אנונימי. הם רצו לפרסם את מספר הטלפון ואת המסר, אבל הבינו שיש בעיה: רוב הילדים, שהם קהל היעד, הולכים ברחוב יחד עם ההורה שלהם, שאולי הוא הגורם האלים. לכן הם יצאו בקמפיין שילוט חוצות מדיהים, שבו אתה רואה שני דברים שונים, בהתאם לזווית המבט. מגובה של מבוגר אפשר לראות בשלט תמונה של ילד קצת עצוב, ואמירה כללית על כך שיש ילדים שחווים אלימות. הילד שהולך ברחוב רואה מהזווית הנמוכה שלו חלקים נוספים בתמונה: מסר שאומר 'אם מישהו פוגע בך, אתה לא לבד', ומספר טלפון. הם חשפו את השיטה בסרטון יוטיוב שהפך ללהיט".

Donald J. Trump   
@realDonaldTrump

 Follow 

Despite the constant negative press covfefe

RETWEETS	LIKES
36,741	44,759

6:06 PM - 30 May 2017

מזה זמן קובצות הרצף והסמליות של טראמפ. צילום מסך



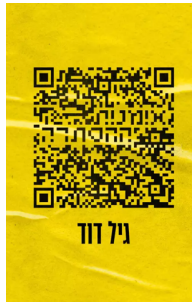
## הספר שלך לא עלול לטעת פראנויה בקרב הקוראים?

"זו התגובה שאני מקבל מהרבה אנשים אחרי שסיימו את הספר – 'אני מסתכל עכשיו היצירה כל הזמן'. אני מבין את התחושה, אבל לי אישית הסיפורים האלה הם כף, כי אני רואה בהם אתגר מחשבתי. בעולם של דיגיטל והצפת מידע, הכול נראה לנו כמו שטף אחד גדול של מילים ותווים, אבל כדאי שנעצור רגע ונחשוב מה המסר.

"בכלל, אנשים נמשכים להסתרות, למסתורין. דוגמה טובה לכך ראינו כשדונלד טראמפ, בעת שכיהן כנשיא ארה"ב, צייץ פתאום בטוויטר 'covfefe' – מילה שלא קיימת באנגלית. ככל הנראה הכוונה הייתה למילה coverage, כיסוי. הציוץ נמחק אומנם אחרי כמה שעות, אבל בינתיים צצו אלפי דיונים סביב השאלה למה התכוון הנשיא. החיפוש הזה טבוע בנו וקשור לעולם הנפש".

### כלומר?

"אם תשאל את פרויד, הוא יגיד לך שיש קשר הדוק בין הסתרה בעולם הרגיל למה שמתחולל אצלנו בתוך הנפש. חלומות, למשל, הם דוגמה מצוינת להסתרה. בחלום יש לך תמונה ברורה של אירוע שאתה מרגיש שאתה חייב לזכור, אבל אז אתה מתעורר ולא זוכר. פרויד אומר שיש מאבק של צנזורה פנימית בין התת־מודע ובין הסמוך־למודע. במהלך היום הצנזורה חזקה מאוד, והיא מונעת מתכנים שירדו לתת־מודע לצוף חזרה למעלה, בגלל טראומות שונות. בלילה השמירה קפדנית פחות, והמידע יוצא מהתת־מודע דרך החלום. ברגע שאתה מתעורר, צנזורת היום נכנסת מיד לפעולה וחוסמת שוב את היציאה. אני חושב שמכאן מגיע החיבור שלנו לסיפורים על הסתרה, כי בעצם זה משהו שקורה לכולנו.



"כתבתי פרק שלם על הקשר בין הסתרות לעולם הנפש, עבדתי עליו הרבה זמן ואהבתי אותו במיוחד, אבל הוא הוסר מהטקסט הסופי. אנשי 'בית העורכים', שאליהם פניתי לצורך עריכת הספר, חשבו שהוא לא מתאים. הם עשו אגב עבודה מצוינת. את החיבור בין הפרקים, שיצא בסופו של דבר לשביעות רצוני המלאה – מי שמכיר אותי יודע כמה זה נדיר – צריך לזקוף לזכותם, גם אם בדרך היו הרבה דיונים ואפילו מריבות. בסופו של דבר, המבחן הוא שאבא שלי קרא את הספר והיה מרוצה ממנו".

לצורך הוצאת ספרו נעזר דוד במימון המונים. "עשיתי את זה אחרי שלמעשה כבר הוצאתי את כל הכסף שהיה דרוש. זו הייתה הרפתקה, התנסות במשהו שלא הכרת, וגם סוג של שיווק שהצלח מעבר לציפיות. גייסתי 170 אחוז מהסכום שביקשתי, ונרכשו יותר מ־500 ספרים. הקמתי בפייסבוק ובלינקד אין קבוצות שעוסקות בהסתרה, והצטרפו אליהן הרבה אנשים שנחשפו לספר דרך הפרויקט".

**בסופו של דבר, ספר כזה גורם לי להבין אנשים כמו בנימין נתניהו, שבמשך שנים התעקש לא להחזיק טלפון סלולרי או מחשב נייד.**

"יש משפט שאומר שהדרך הכי טובה להגן על מחשב היא לסגור אותו, לשבור אותו לרסיסים, ואז לקבור אותו באדמה ולהציב מעליו כמה שכבות של בטון. אחרת, אם אתה מטרה – אפשר להגיע אליך. כל אחד מאיתנו צריך לקחת את העובדה הזו בחשבון".

**לתגובות: [dyokan@makorishon.co.il](mailto:dyokan@makorishon.co.il)**

**תגיות:** היסטוריה המוסד הצפנה כתב סתרים ספרים