מבט על
INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
אוניברסיטת תל אביב
TEL AVIV UNIVERSITY

עין אחת לציון והשנייה לבייג'ינג: מצלמות סיניות בישראל

יובל לס | גיליון 2143 | 20 במאי 2026

מערכי מצלמות בישראל חשופים לניסיונות חדירה מצד גורמים עוינים, בהם איראן. ראש מערך הסייבר הלאומי ציין כי מתחילת המלחמה איראן וחיזבאללה פועלים במשותף לפרוץ למצלמות אבטחה בישראל לצורך איסוף מודיעין, המשמש בין היתר, לדיוק תקיפות טילים ולניסיונות פגיעה באישים. כך מתחדד אופיין הדו-שימושי (Dual-use) של מצלמות מתקדמות, ובפרט מצלמות סיניות שנועדו במקור לצרכים אזרחיים, אך הן נושאות גם פוטנציאל אסטרטגי עבור גורמי מודיעין וביטחון זרים.

בראשית המלחמה עם איראן ב-28 בפברואר 2026, ביצעה ישראל את אחד החיסולים המרשימים בתולדות הלוחמה המודרנית, כאשר התנקשה בחיי המנהיג העליון של איראן, עלי ח'מינאהי. אחד האמצעים המרכזיים שסייעו למודיעין הישראלי היה מערך מצלמות התנועה בטהרן, אשר נפרץ ושימש לאיסוף שיטתי של מידע על אודות פעילות צמרת המשטר ומעגלי האבטחה סביבה. מערך זה, שנועד לפקח על הציבור ולדכא מחאות, הפך למקור מודיעיני משמעותי שאפשר בניית תמונת מצב מדויקת. המידע נותח באמצעות אלגוריתמים שזיהו "דפוסי חיים" של בכירים, לצד מצלמות שסיפקו זוויות קריטיות למעקב אחר תנועתם. ביום המבצע, יכולות אלו אפשרו זיהוי מדויק בזמן אמת של היעד וסביבתו, ותרמו להצלחת החיסול.

ניצול מערך המצלמות באיראן על ידי ישראל אינו תופעה חדשה, וגורמים בממשל בטהראן אף הזהירו בעבר כי מערכות אלו עלולות לסכן את הביטחון הלאומי וקראו להחמיר את בקרות האבטחה על מצלמות מתוצרת חוץ. בד בבד, פגיעות זו אינה ייחודית לאיראן אלא משקפת תופעה רחבה יותר. מערכות מצלמות, ובייחוד כאלה המחוברות לרשת, אמנם נועדו להגביר ביטחון ולאפשר פיקוח ושליטה, אך הן עלולות להיות נקודת תורפה בידי גורם עוין לצורכי איסוף מודיעין ומעקב. בהקשר הישראלי, השימוש הנרחב במצלמות, ובכלל זה בטכנולוגיות מתוצרת חוץ, מחדד את פוטנציאל החשיפה והסיכון הביטחוני.

מצלמות סיניות בישראל

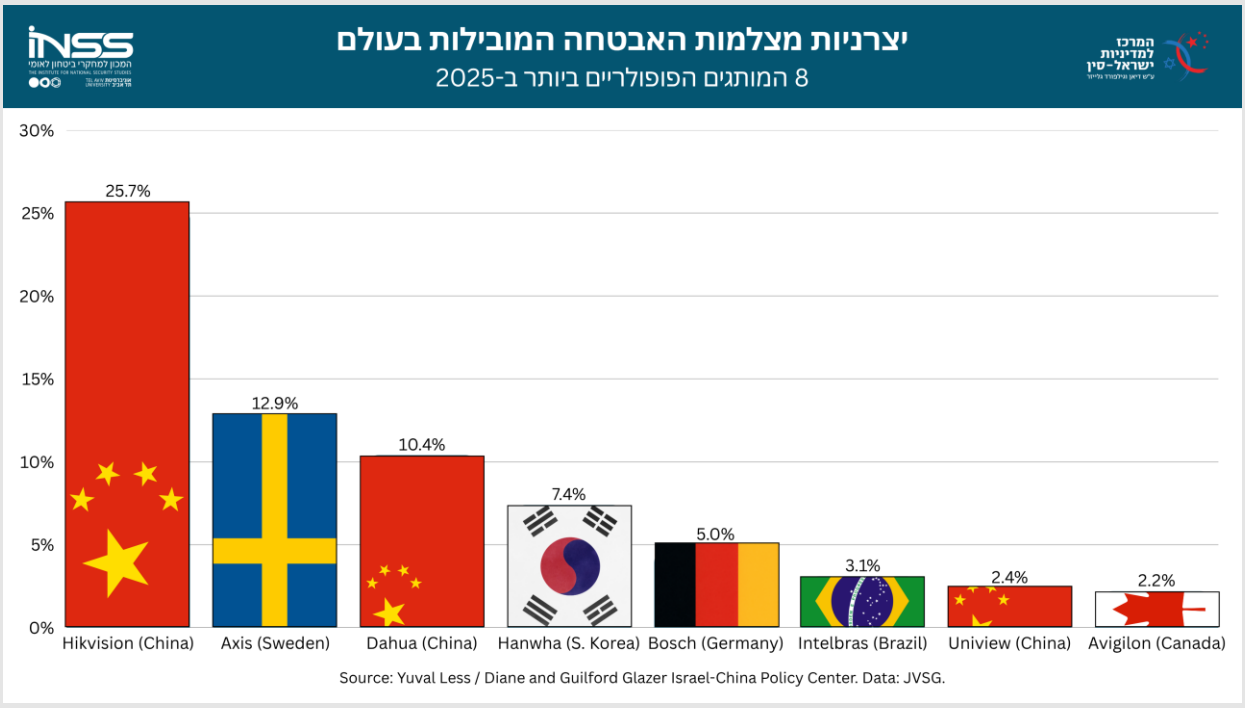
מצלמות הן כלי מרכזי בניהול ובקרה של המרחב הציבורי, ונודע להן תפקיד משמעותי בתחומי הביטחון, התחבורה ואכיפת החוק. דור המצלמות החדש, המבוסס על בינה מלאכותית ומערכות IoT, לא רק מתעד באופן פסיבי, אלא גם מנתח ומזהה בזמן אמת וכך מאפשר איתור דפוסים וחריגות ותומך בקבלת החלטות מהירה. לצד היתרונות, מערכות אלו חשופות לחולשות אבטחה, השתלטות מרחוק, דליפת מידע ופגיעה בפרטיות. חיבורן של המצלמות לענן והאפשרות לגישה מרחוק מגבירים את הסיכון לניצול המידע על ידי גורמים עוינים. בהשוואה למכשירי IoT אחרים – חיישנים בסיסיים (למשל חיישני טמפרטורה, תנועה ואור) ומכשירי "בית חכם" ובכלל זאת מנורות ומנעולים חכמים – מצלמות מתקדמות אוספות מידע בהיקף רחב יותר, וכך עלולות לשמש "עיניים ואוזניים" עבור גורם עוין, ולאפשר איסוף מודיעין, מעקב וסיוע בתכנון פעולות.

בישראל, סיכוני החשיפה הנובעים משימוש במצלמות מתחדדים לנוכח ההקשר הביטחוני והיותה יעד בולט למתקפות סייבר מצד גורמים זרים. בשנים האחרונות הזהירו גורמי ביטחון מפני ניסיונות לנצל מצלמות לאיסוף מודיעין על מוקדים ותנועות רגישות. בעוד שסיכוני אבטחה קיימים בכל סוגי המצלמות, ללא קשר ליצרן או למדינת המקור, האתגר הסיני

מוסיף שכבת מורכבות נוספת ומציב סוגיות ייחודיות, טכניות וגאופוליטיות, המחייבות בחינה מחודשת של הסיכונים הכרוכים בשימוש בטכנולוגיות מתוצרת סין.

סין הפכה למעצמה בייצור ובפרישת מצלמות אבטחה. היקף הפעילות וההשקעה הממשלתית, לצד מחירים תחרותיים וביצועים גבוהים, אפשרו לסין לבסס יתרון ולהצמיח חברות מובילות, בהן Hikvision ו-Dahua, המחזיקות יחדיו למעלה מ-30% מנתח הייצור העולמי. (ראו גרף A).

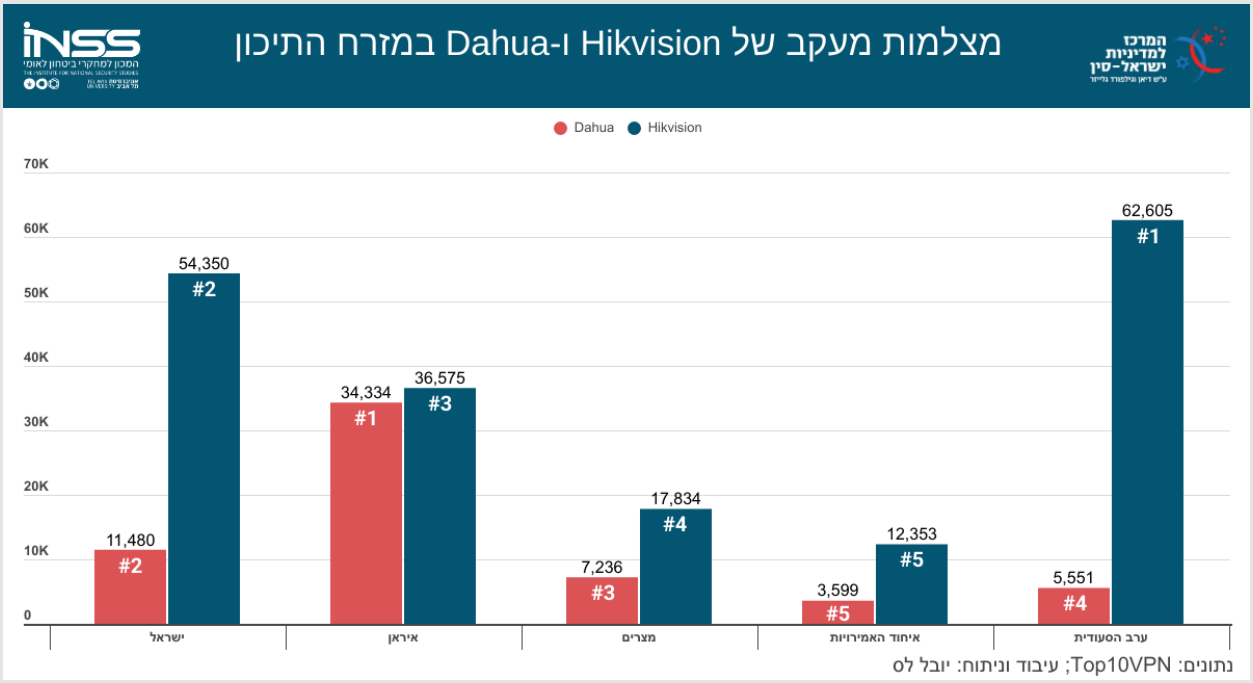
גרף A:



לפי נתוני JVSG (פלטפורמה לתכנון מערכות וידאו ואבטחה המבוססת על נתוני שימוש בפועל) לשנת 2025, חברת Hikvision הסינית חולשת על כ-25.7% מהשוק העולמי. אחריה Axis משוודיה (12.9%), Dahua מסין (10.4%), Hanwha מדרום קוריאה (7.4%), Bosch מגרמניה (5.0%), Intelbras מברזיל (3.1%), Uniview מסין (2.4%) ו-Avigilon מקנדה (2.2%). קידום מעמדה של סין כיצרנית מובילה בתחום מצלמות האבטחה משתלב כנדבך טכנולוגי באסטרטגיה רחבה יותר לייצוא טכנולוגיות ולקידום סטנדרטים סיניים, כחלק ממאמץ להרחיב את השפעתה הגלובלית של בייג'ינג.

נוכחותן של מצלמות סיניות מורגשת במרחב הציבורי והפרטי בישראל, לרבות בתחבורה הציבורית, במוסדות חינוך ובריאות, בבנייני מגורים ואף באתרים רגישים ביניהם משרדי ממשלה ומעברי גבול. במסגרת פרויקט "עין הנץ", משטרת ישראל עושה שימוש במצלמות מתקדמות לזיהוי לוחיות רישוי, בכללן מצלמות של Dahua ומערכות של Hikvision. בשנת 2021 פרסמה חברת Top10VPN – גוף מחקר בריטי המתמחה במעקב דיגיטלי, פרטיות וטכנולוגיות ניטור – דוח מחקר שהציג מיפוי של פריסת מצלמות אבטחה מתוצרת החברות הסיניות Hikvision ו-Dahua מחוץ לגבולות סין, לרבות במזרח התיכון. על פי הממצאים, בישראל מותקנות כ-65,830 מצלמות של חברות אלו, מהן כ-54,350 מצלמות מתוצרת Hikvisionוכ-11,480 מצלמות מתוצרת Dahua (ראו גרף B).

גרף B:



עבור ישראל, השימוש במצלמות סיניות מציב שורת אתגרים פוליטיים, טכנולוגיים וגאופוליטיים, ומחדד את ההשלכות של הסתמכות על טכנולוגיה זרה באופן המחייב תשומת לב גוברת מצד גורמי הממשל והביטחון.

האתגר הראשון מתקשר להיבט הפוליטי, ונובע מהקשר ההדוק בין הממשל הסיני לחברות הטכנולוגיה. בסין, חברות ממשלתיות ופרטיות כאחת פועלות בזיקה למנגנוני המדינה, כך שאינטרסים עסקיים משתלבים ביעדים אסטרטגיים. חברת Hikvision, למשל נמצאת בשליטת התאגיד הממשלתי הסיני China Electronics Technology Group (CETC), הפועל גם עבור התעשייה הביטחונית, כאשר בכירים בחברה ממלאים במקביל תפקידים במפלגה הקומוניסטית ובגופים ממשלתיים. חברת Dahua, על אף שאינה בבעלות ממשלתית מלאה, גם היא בעלת זיקות לממשל ולמערכת הביטחונית. שתי החברות הללו פועלות בסביבה שבה הזיקה למפלגה ולמדינה היא חלק מובנה, באופן המטשטש את הגבול בין פעילות מסחרית לבין אינטרסים לאומיים. קשר זה מעוגן גם במסגרת חוקית המחייבת חברות בסין לשתף פעולה עם רשויות המדינה ולהעביר אליהן כל מידע לפי דרישה. חוקים וביניהם Counter Espionage Law (2014) ו-National Intelligence Law (2017) ממסדים חובה זו ומגבירים את החשש כי מידע הנאסף באמצעות טכנולוגיות סיניות עלול להיות נגיש לגורמי שלטון בסין.

שנית, האתגר הטכנולוגי שסין מציבה מתבטא בעיקר בחולשות אבטחה. אף שפגיעות קיימת בכל סוגי המצלמות, מחקרים מצביעים על כי במצלמות סיניות, ובהן Hikvision ו-Dahua, הפגיעות היא לעיתים חמורה יותר ומורכבת לטיפול. מחקר שפורסם ב-Journal of Cybersecurity מצא כשלים במנגנוני אימות והרשאות, שימוש בסיסמאות ברירת מחדל וחולשות המאפשרות גישה לא מורשית, הרצת קוד ודליפת מידע. חלק מהבעייתיות נובעת מתהליכי עדכון מורכבים והיעדר מנגנוני אבטחה מתקדמים כברירת מחדל. בנוסף, במצלמות אלו יש פחות שכבות הגנה ובה בעת ריבוי שירותים פתוחים, מה שמגדיל את שטח התקיפה בכך שהוא מרחיב את מספר נקודות הכניסה האפשריות למערכת ומקל על תוקף לזהות ולנצל חולשות קיימות.

חולשות אלו מעוררות חשש ביטחוני נוכח העמקת הקשרים האסטרטגיים בין סין לאיראן והחשש שגורמים איראניים ינצלו חולשות אלו נגד ישראל. בשנים האחרונות הזהירה ארצות הברית מפני השימוש בטכנולוגיות סיניות, כאשר מחלקת ביטחון המולדת האמריקאית (DHS) התריעה כי מצלמות מתוצרת סין עלולות לשמש אמצעי ריגול נגד תשתיות קריטיות.

אתגר שלישי הוא גאופוליטי, הנגזר מהתחרות הטכנולוגית הגוברת בין סין לארצות הברית. Hikvision ו-Dahua נכללות ברשימת ה-Covered List של ה-FCC בארצות הברית, המגדירה יצרני ציוד תקשורת וטכנולוגיה הנחשבים בעלי סיכון לביטחון הלאומי בשל זיקותיהם לממשל הסיני ולתעשייה הביטחונית. הכללתן ברשימה מובילה להגבלות משמעותיות ובהן איסור על אישור ושיווק ציוד חדש, הגבלת השימוש במערכות ממשלתיות והסרת ציוד ממתקנים רגישים. במקביל, ארצות

הברית הטילה סנקציות על חברות סיניות, ובהן Hikvision, Dahua, Uniview ו-Tiandy, על רקע מעורבותן בפרויקטים של פיקוח ודיכוי אזרחי בסין.

לארצות הברית מצטרפות מדינות נוספות מרחבי העולם הפועלות להסיר ציוד סיני מאתרים רגישים ותשתיות קריטיות. כך למשל, בריטניה הנחתה להסיר ציוד של Hikvision ו-Dahua ממבני ממשל רגישים ואסרה התקנתם באתרים ביטחוניים; אוסטרליה הובילה מהלך להסרת מצלמות סיניות ממשרדי ממשלה ותשתיות קריטיות; קנדה הגבילה שימוש בציוד סיני בגופים פדרליים ובחנה מחדש התקשרויות קיימות; והודו אסרה השתתפות של ספקים סיניים בפרויקטים ממשלתיים מסוימים והעדיפה ספקים חלופיים ומקומיים מטעמי ביטחון לאומי. בישראל, לעומת זאת, טרם גובשה מדיניות כוללת ביחס לשימוש במצלמות סיניות. על רקע צעדים אלו, ישראל צריכה להיערך לאפשרות של לחץ אמריקאי לצמצום השימוש בטכנולוגיות סיניות ולבחון את התאמת מדיניותה למסגרות שיתוף פעולה טכנולוגי עם ארצות הברית ומדינות המערב, לרבות יוזמות כמו Pax Silica.

מסקנות והמלצות:

סין אוחזת בנקודות קריטיות בשרשרת הייצור והאספקה הגלובלית של מצלמות ולכן ניתוק טכנולוגי מלא ממנה אינו מעשי, גם משום שרכיבים סיניים משולבים גם במוצרים מערביים. מורכבות זו מתחדדת לנוכח תופעת ה-White labeling, המטשטשת את מקור הטכנולוגיה ומקשה על הערכת רמת האבטחה. בנוסף, בשוק פתוח יכולת הפיקוח של המדינה על טכנולוגיות במרחב הפרטי מוגבלת מטבעה. לפיכך, נדרש לאמץ גישה של ניהול סיכונים מושכל, הכוללת קידום צעדים פרקטיים לצמצום החשיפה לסיכונים הנובעים מהישענות על טכנולוגיה סינית.

- **מעבר לחלופות מערביות:** באתרים ביטחוניים ותשתיות קריטיות יש לקדם מעבר הדרגתי לחלופות שאינן סיניות, במטרה לצמצם סיכוני אבטחה במוקדים אסטרטגיים בישראל. בנוסף, נדרש מעבר מוסדר לחלופות שאינן סיניות במערכי הביטחון בישראל, גם במחיר כלכלי. בפרט, פרויקטים דוגמת "עין הנץ" של משטרת ישראל, הנשענים בין השאר על מערכות מתוצרת סינית, ממחישים את היקף השימוש בטכנולוגיות אלו ואת הצורך בבחינה מחודשת של מידת ההסתמכות עליהן. חלופות אלו יכולות להישען על ספקים מקומיים או על ספקים מערביים.
- **חיזוק התעשייה המקומית:** יש לעודד פיתוח וייצור של תשתיות אבטחה, מצלמות, תוכנה ושירותים ישראליים בתחום הווידאו והמעקב. מהלך זה עשוי לסייע בצמצום התלות ביבוא ובשיפור השליטה בשרשרת האספקה, לצד חיזוק היכולות הטכנולוגיות של ישראל. בתוך כך, יש לשאוף לקידום אקוסיסטם הנשען על פתרונות ישראליים ומערביים, תוך שילוב רכיבים ממקורות אמינים.

עורכי הסדרה: ענת קורץ, רינת חרש ואלדד שביט.