08

ישראל כמובילת סייבר עולמית - הדרך, ההובלה וחיוניות הביקורת להמשך ההצלחה

יגאל אונא

מר יגאל אונא שירת במשך 33 שנה בשירות הציבורי-ביטחוני במגוון תפקידים, בין היתר כיהן כראש אגף הסייבר-סיגינט בשב"כ וכראש מערך הסייבר הלאומי (2018 - 2022). לאורך כל שנות שירותו עסק בתחום לוחמת המידע והסייבר ההתקפי וההגנתי והיה מופקד על הנחיית האמונים על התשתיות הלאומיות הקריטיות של ישראל להתגוננות מפני איומי הסייבר ועל תפיסות הביטחון הלאומיות בתחום. מייעץ בנושא לממשלות ולדירקטוריונים בארץ ובעולם ומקדם את תעשיית הסייבר הישראלית כמובילה בעולם.

המאמר בקצרה

- במאמר נבחנות התפתחות תחום הסייבר ולוחמת המידע והשלכותיה על הביטחון הלאומי, הכלכלה והממשל בישראל בעידן הדיגיטלי, בדגש על מאפייני האיום, מגמות ההתעצמות של תקיפות סייבר ומשמעותן האסטרטגית עבור מדינות וארגונים.
- עלייתה של מדינת ישראל למעמד של מעצמת סייבר עולמית נובעת משילוב בין תפיסה לאומית, הון אנושי איכותי, אקו-סיסטם מתקדם ושיתוף פעולה בין גופי ממשל, מערכת הביטחון והתעשייה.
- לצד היכולות הטכנולוגיות והמבצעיות, למערך הביקורת - הפנימית והחיצונית - תפקיד מרכזי בהבטחת ניהול סיכונים אפקטיבי, בשיפור מתמיד של מערכי ההגנה ובחיזוק החוסן הארגוני והלאומי.
- שילוב הדוק בין הגנת סייבר מקצועית לביקורת עצמאית ושיטתית הוא תנאי הכרחי לשימור יתרונה היחסי של ישראל בתחום הסייבר ולהבטחת עמידותה מול איומים מתפתחים במרחב הדיגיטלי.

מבוא | הסייבר ולוחמת המידע - קווים לדמותם | כיצד מדינת ישראל מתמודדת עם איום הסייבר | כיצד הפכה ישראל למעצמת סייבר? | מה בין סייבר לביקורת? | סיכום

מבוא

במסגרת תפקידיי הממלכתיים הוריתי לספק לתשתיות הלאומיות הקריטיות בישראל הגנה מאיומי סייבר, משימה שדרשה ביקורים בשטח ופגישות עם הגורמים השונים בחברות. באחד מביקוריי בתשתית קריטית כזו, עלתה שאלה שמעסיקה רבות את כל העוסקים בתחום: למי כפוף האחראי על הגנת הסייבר בארגון? לא ארחיב כאן על הדילמות והשאלות המקצועיות הרבות (המצדיקות מאמר בפני עצמו), אולם מקובלים שני מודלים - כפיפות למנהל מערכות המידע (CIO, מנמ"ר) וכפיפות לאחראי הביטחון (קב"ט) - אף שיש יותר ויותר מקרים של כפיפות ישירה למנכ"ל עצמו.

בעת התלהטות הדיון המקצועי, בקע מקצה השולחן קול שקרא: "מדוע לא תחת מבקר הפנים?" - דממה השתררה. אני עטתי על ההערה כמוצא שלל רב ופיתחתי את הדיון והרעיון, שכן יש קווי דמיון רבים מאוד, שלא לומר התאמה, בין המשימות של שני בעלי התפקידים - ביקורת שוטפת, ניהול סיכונים, ציות ודיווח. גם מאפייני התפקיד הנדרשים - עצמאות, יושרה, סמכויות וכשירות מקצועית - חופפים.

האם התהליכים הגלובליים עוד יביאו אותנו לשינוי כאמור - העברת הכפיפות למבקר הפנים? מה נדרש לשם כך? ובכלל, מה בין הגנת סייבר לביקורת?

הסייבר ולוחמת המידע - קווים לדמותם

כדי לרדת לשורש המונחים "סייבר" ו"תקיפות סייבר" יש להרחיק עד לשחר ההיסטוריה. לאורך כל הקיום האנושי, כל טכנולוגיה שהמציאו בני האנוש לשיפור רווחתם ואיכות חייהם נוצלה במהירות רבה גם לרעה, כדי לפגוע בבני אנוש אחרים. ככל שטכנולוגיה כזו מלווה בהטעיה ובהונאה גדולות יותר, כך היא יעילה יותר. פרשת הסוס של טרויה תופסת מקום מיוחד בפולקלור הסייבר, שכן הרעיון להחדיר בעורמה מרכיב עוין ומסוכן בתוך אריזה תמימה של פסל עץ מהודר ומושקע לעורף החשוף של אויב, רעיון שהביא להכרעה במאבק צבאי, משמש עד היום כאנלוגיה נפוצה בעולם הסייבר, ו"סוס טרויאני" הוא כינוי רווח לפוגען סייבר המורכב מקוד זדוני המוחדר במעטפת תמימה למערכות הקורבן וכך מאפשר לתוקפים לבצע את זממם.

טכנולוגיות המידע - שם כולל לעולם הדיגיטלי ההולך ומשתלט על כל היבט ותחום חיים מודרני - פרצו לעולמנו אחרי מלחמת העולם השנייה, וככל שהתפתחו בקצב הולך ומואץ, כך התפתח גם הצד האפל והזדוני שלהן. למעשה, זהו הסייבר, בהגדרתו העממית המופשטת ביותר - ניצול לרעה של כל אותן טכנולוגיות.

בכמעט ארבעת העשורים שבהם אני פעיל בתחום חוויתי כניסה של כמה טכנולוגיות מידע: המודם ההיסטורי ששימש להעברת מידע בין מחשבים, הפקסימיליה (מהפכה של ממש בסוף שנות השמונים של המאה העשרים), המרשתת (האינטרנט), הטלפונים הסלולריים, הטלפונים "החכמים" (שהם למעשה "מיני מחשב" יותר מאשר טלפון), לווייני ה-GPS, הדרכון הביומטרי, מטבעות הקריפטו, הענן, מערכות בקרה ממוחשבות (סקאדה), מרשתת הדברים (IoT), ה-Wi-Fi והתשלום דרך המובייל (NFC). בימים אלה אנו מתרגלים לשימוש בבינה המלאכותית (AI), והמחשוב הקוואנטי כבר נוקש על דלתנו.

בכל הטכנולוגיות הללו, גם "העתיקות" יותר, אנו משתמשים בדרך זו או אחרת; קשה לאנושות להיפרד מהמצאותיה המוצלחות. כך, גם תקציב התא המשפחתי שלנו לתקשורת ולדיגיטל רק הולך וגדל הדרגתית לאורך השנים עקב צריכה מוגברת ומגוונת.

קצב השינוי וההתפתחות הטכנולוגית משתנה במהירות. הקצב שבו טכנולוגיות חדשות מפציעות רק הולך וגובר, ואיתו עולה גם הסיכון.

בעולם הסייבר, כל טכנולוגיה כזו מספקת משטח תקיפה - כינוי למרחב המעניק לתוקף סייבר הזדמנות לבצע את זממו. משטחי התקיפה האלה רק הולכים ומתרחבים וחושפים את כולנו באופן חסר תקדים לסיכונים אינדיבידואליים וארגוניים מיידיים ברמות שונות של חומרה.

מהי תקיפת סייבר?

תקיפת סייבר משמעותה השגת שליטה ללא רשות במערכת מידע, או להפך, מניעת שליטה במערכת המידע. כאשר תוקף סייבר משיג שליטה, ביכולתו לבצע במערכת כל מה שירצה, לרבות העתקת מידע (ריגול), פגיעה במידע תקיפות כופרה (Ransomware), פגיעה במערכות עצמן עד כדי השמדתן, גנֵבת כסף או גרימת נזק בעולם הפיזי (למשל השבתת חשמל, הפלת מטוס או התכת כור גרעיני).

מערכת מידע היא כל דבר שיש בו מעבד נתונים. כיום מדובר בפריטים רבים המקיפים אותנו, בהם השעון, הטלפון ואפילו משקפיים ופריטי לבוש. הקישוריות של כמעט כל חפץ וכלי למרשתת מאפשרת לתוקף סייבר שנמצא עשרות אלפי קילומטרים מהקורבן לבצע את התקיפה כאילו היה בחדר הסמוך.

הפורום הכלכלי העולמי (The World Economic Forum; WEF), ששיא פעילותו הוא בכנס הנערך בדאבוס מדי שנה בשנה, מפרסם בכל שנה דוח סיכונים גלובלי. סיכון הסייבר "מככב" שם בעשרת המקומות הגבוהים ביותר (מתוך יותר מ-30), ובשנים מסוימות הוא אף משובץ במקום השני או השלישי.

מטרת התקיפות

לתוקפי סייבר מניעים שונים ומטרות שונות. רוב רובן של התקיפות נועדו ל**מטרות כלכליות**: סחיטת כסף באמצעות הצפנת המידע של הקורבן ומניעת יכולתו להפעיל את

מערכותיו, אלא אם ישלם סכום במטבע קריפטו עבור מסירת סיסמת הפיענוח. תחום זה התפתח בקצב אדיר מאז פרוץ טכנולוגית הבלוקצ'יין ויצירת עולם מטבעות הקריפטו האנונימיים, דבר המאפשר לעבריינים לסחוט דמי כופר באופן בטוח ויעיל.

חלק מרכזי נוסף של התקיפות תכליתו **דלף מידע** (Data Leakage), כלומר החצנה בפומבי של מידע - בעיקר פרטי ורגיש - של לקוחות, של מטופלים ועוד כדי לגרום למבוכה. גם כאן נכנס פעמים רבות מרכיב כלכלי בדמות סחיטת כסף מהקורבן, שעשוי להעדיף לשלם כדי להימנע מפרסום שעלול לחשוף אותו לתביעות משפטיות מצד לקוחותיו.

יש תקיפות שמטרתן **גרימת נזק** גרידא, בעיקר מצד מדינות וארגוני פרוקסי של מדינות. הן מכוונות לרוב נגד תשתיות קריטיות או גופים חיוניים (מערכות ותשתיות של חשמל, מים וכד').

זן ספציפי נפוץ של תקיפות הוא **תקיפות מניעת שירות**. תקיפות אלה מתמשכות בדרך כלל שעות בודדות או ימים בודדים, ותכליתן "סתימת" התקשורת במרשתת של הקורבן שיכול להיות יעד ספציפי או אפילו מדינה שלמה.

זהות התוקפים

מקובל לחלק את התוקפים לקטגוריות: מדינות, ארגוני טרור וקבוצות פשיעת סייבר, ולכל אחת מהן שם ידוע או כינוי שהצמידו לה חברות סייבר גדולות. יש גם בודדים שתוקפים, אבל אלה נדירים וזניחים. בעבר התוקפים היו גם אקטיביסטים והתארגנויות "אידיאולוגיות", אך אלה כמעט אינם קיימים עוד, והאינטרס הכלכלי או הלאומני גבר על כולם. עד היום, ללא יוצא מן הכלל, נטלו קבוצות פשיעת סייבר את האחריות לתקיפות משמעותיות, גם אם היה ברור לחלוטין שמאחורי התקיפה עומדת מדינה. כך למשל מוכרות הקבוצות "חנדלה" המזוהה עם איראן ו"הדרור הטורף" המזוהה עם האופוזיציה האיראנית. עד כה לא מוכרת נטילת אחריות של מדינה על תקיפת סייבר, והדבר נובע ממגוון סיבות, לרבות אימת הדין הבין-לאומי. מקרה בולט הוא תקיפת הסייבר נגד הממשל המקומי באלבניה ביולי 2022, שיוחס לממשלת איראן והביא לניתוק היחסים הדיפלומטיים בין המדינות ואף לפנייה לנאט"ו (שאלבניה חברה בה) בדרישה להפעיל את סעיף 5 לאמנה ולרתום את כלל המדינות החברות כנגד התוקפן - איראן. הפנייה הזו נדחתה בטענה שאין לאלבניה הוכחה מוצקה לכך שאיראן היא העומדת מאחורי התקיפה. אכן, תקיפות סייבר הן עדיין הפשע המושלם. בפועל, ניתן גם לזהות שילוב בין אינטרסים ומטרות. איראן למשל מגייסת לשירותיה קבוצות פשיעת סייבר פרו-איראניות ומסמנת להן מטרות ישראליות. התכלית היא גרימת נזק ומבוכה, אבל כל סכום כסף שהעבריינים מצליחים לסחוט מהקורבן נשאר בידיהם. מעין מודל Revenue Share.

האבולוציה של הסייבר

עולם הסייבר החל להתפתח עם כניסת המחשב הראשון, והתפתחותו הואצה כשהתאפשרה תקשורת בין מחשבים. השימוש המקובל במונח "סייבר" עצמו החל בסוף העשור הראשון של שנות האלפיים. בראשית התפתחותו הייתה התכלית המרכזית של הסייבר ריגול, קרי חדירה למחשב בחשאי ואיסוף מידע בלי שהקורבן מרגיש בכך. לאחר מכן החלו תקיפות למטרת גרימת נזק. הידועה שבהן היא Stuxnet שפגעה בצנטריפוגות העשרת האוראניום באיראן בשנים 2009 - 2010. לאחר מכן החלו תקיפות הכופר - פגיעה מותנית (ההופכת לקבועה רק אם לא משלמים כופר). השלב ההתפתחותי הבא הוא תקיפות למטרות השפעה, ואנו אכן חווים זאת בעוצמה מאז מערכת הבחירות בארצות הברית ב-2016. סוג עדכני של תקיפות הוא תקיפות שמטרתן גנבת מטבעות קריפטו שהיקפן הולך ועולה. ההערכה המקובלת היא ש-80% מכלכלת צפון קוריאה מתבססים על ערוץ הכנסה זה.

תקיפות מוכרות

יש לציין כי עד כה לא אירע "11 בספטמבר סייברי". כלומר, לא אירעו אסונות בהיקף נרחב כתוצאה מאירוע יחיד. אולם יש מספר אירועים אשר ראויים לציון, שכן התעשייה העולמית כולה מתייחסת אליהם כאל "קו פרשת מים" בהתפתחות ההתייחסות לסייבר ולצורך להתגונן מפני איומיו. להלן נתייחס לשני אירועים כאלה.

יגואר-לנד רובר (JLR) - ענקית תעשיית רכב בריטית שספגה באוגוסט 2025 תקיפה ששיתקה אותה למשך שישה שבועות. הנזקים שהסב האירוע נחשבו לקטסטרופליים במונחים עסקיים:

1. **השבתה ארוכה** - שישה שבועות ללא ייצור של אף רכב חדש, במקום 1,000 רכבים חדשים בשבוע. כלומר אובדן הכנסה של 50 מיליון פאונד בשבוע.
2. **השפעה לאומית** - ממשלת בריטניה הקצתה ערבויות של 1.9 מיליארד פאונד, הכרה בכך שתקיפת סייבר על שחקן תעשייה מרכזי משמעה איום על הביטחון הלאומי.
3. **השפעה כלכלית מיידית** - הפסד מוערך בכ-2 מיליארד פאונד שהם יותר מכל הרווח הנקי של החברה בשנת 2024.
4. **היעדר ביטוח** - האירוע התרחש כאשר החברה הייתה לקראת אישור של פוליסה, ומשכך הוטל הנזק כולו על כתפי החברה.
5. **פגיעה חמורה בכל שרשרת האספקה** - החברה פרנסה עוד כ-100,000 נושאי משרות מחוצה לה רק בבריטניה. נוצר אפקט דומינו שפגע לאורכה ולרוחבה של השרשרת והביא עסקים רבים לחדלות פירעון.

כך נחשפה הפגיעות של מודל Just-in-time בייצור תעשייתי לכשל דיגיטלי מערכתי.

Colonial pipeline - ענקית אנרגיה אמריקאית שמשנעת תוצרי דלק מזוקק ממפרץ אמריקה וטקסס, בעיקר לחוף המזרחי של ארצות הברית. החברה מעבירה את הדלק "עד המייל האחרון", כלומר משנעת את מכליות הדלק עד לתחנות הדלק. במאי 2021 שיתקה קבוצת תקיפה רוסית את המערכת המינהלתית של החברה (המערכת התפעולית שמשנעת דלקים יכלה להמשיך לעבוד ללא הפרעה, אבל לא היה ניתן לגבות תשלום). שיתוק החברה (שסירבה לשלם כופר של 2 - 4 מיליון דולר, הכנסתה הממוצעת בכמה שעות עבודה) הביא למחסור חמור בדלק, לרבות בדלק סילוני, לשיתוק כלכלי ותחבורתי ולהכרזת מצב חירום בידי הנשיא ביידן.

חומרת איום הסייבר

כיום היקף הנזק שמסיבות תקיפות סייבר זכה להגדרה "הכלכלה השלישית בגודלה בעולם", אחרי ארצות הברית וסין (ולפני הודו). הנזק מוערך בסכום דו-ספרתי של טריליוני דולר ארצות הברית. קצב הגידול עצמו גבוה - כ-15% - 20% בשנה. היקפן העצום של התקיפות נובע מכמה סיבות:

1. **היעדר אכיפה יעילה** - מעטים מאוד האסירים שנשפטו ונכלאו, כמעט בכל מדינה, על עבירות סייבר בלבד. היכולת לשבת במדינת הבית ולתקוף במדינות אחרות, חלקן גם ללא הסכמי הסגרה, ייחודית לתחום הסייבר. גופי האכיפה מאוגדים תחת ארגון האינטרפול, שרמת הבנת הסייבר אצלו נמוכה מאוד. גופי הגנת הסייבר ההולכים וצומחים בעולם מאוגדים גם הם ומשתפים מידע, אך הם אינם עוסקים כלל באכיפה ובהעמדה לדין, כך שמדובר בשני עולמות מקבילים שאינם נפגשים. במרווח בין העולמות הללו חוגגות כנופיות הסייבר.
2. **אנונימיות** - המרשתת והטכנולוגיה מאפשרות לתוקפים רמת הסתוות ואנונימיות גבוהה למדי (יכולת זו אינה עומדת בפני מדינות מתקדמות, אך אלה מתעדפות יכולות מול איומים לאומיים).
3. **פער משפטי** - הטכנולוגיה תמיד הקדימה את המשפט והאסדרה (רגולציה), והדבר מורגש היטב גם בפשיעת סייבר. קשה להוכיח עבירות סייבר גם כשהעבריין מזוהה ונתפס, וכאמור הזיהוי והתפיסה מורכבים דיים. גם כשכבר מצליחים לספק הוכחות, בתי המשפט אינם מבינים את הנושא לעומק והעונשים בדרך כלל קלים יחסית.
4. **התנהלות כלכלית ועסקית של התוקפים** - לתוקף שמטרתו כלכלית יש כלים המאפשרים לו ללמוד את הקורבן מבעוד מועד. הוא מכיר את יכולותיו הכלכליות (תזרים, יתרה, מדיניות עסקית וכו'), יודע אם בבעלותו פוליסת ביטוח סייבר ומנוסה בהצבת דרישות שאינן גבוהות מידי עבור הקורבן כדי שיעדיף לשלם. האמינות והמוניטין של קבוצות פשיעת הסייבר מזכירות עולמות עסקיים אחרים. הקורבן יודע שאם ישלם יקבל את התמורה, כי אחרת "שמו הטוב" של התוקף ייפגע אנושות. גם בתהליך המשא והמתן בין התוקף לקורבן שוררת התנהלות עסקית לכל דבר, ועסקים רבים בכל העולם מתייחסים לנזק כתוצאה מתקיפה כאל חלק בלתי נמנע כמעט של עולם העסקים.
5. **תקיפות ריסוס גנריות** - קבוצות הפשיעה פועלות, בדומה לארגוני מודיעין, גם בשיטות של "ריסוס", כלומר חיפוש רחב של יעדים אשר "תלויים נמוך מהעץ" וקלים יותר להשגה, גם אם הכיס שלהם אינו עמוק, בעיקר באזורי ה(Server Message Block; SMB), שם גם תקציבי הגנת הסייבר ויכולות ההגנה נמוכים במיוחד.
6. **ניצול פרצות וחולשות מפורסמות** - ברוב רובן של תקיפות הסייבר התוקפים משתמשים בשני סוגי כלים (והרבה פעמים בשילוב ביניהם): הגורם האנושי (שעליו יורחב בהמשך) וניצול חולשות. חולשה היא טעות אנוש בכתיבת קוד תוכנה של יצרנים, לרבות של חומרה (חברות סיסקו ואנבידיה למשל). מרבית הטעויות האלה אינן מזיקות בהיבט הסייבר, אולם מיעוטן בהחלט כן, ואלה עלולות להותיר פרצה חמורה. בדרך כלל החולשות הללו מתגלות בידי היצרנים עצמם או על ידי חברות הגנת סייבר שמוכרות את הגילוי ליצרנים באופן אחראי. במקרה כזה היצרן מפתח "חיסון" - טלאי (Patch) - תוכנה קטנה שמתקנת את החולשה. אולם, כדי להפיץ את החיסון לכלל הלקוחות שכבר שילמו נדרש פרסום פומבי רחב. מרגע שהדבר מתפרסם מתחיל מרוץ בין התוקפים שמייצרים כלי נשק סייברי שמנצל את החולשה לביצוע זממם ובין המגינים שנדרשים להתקין את החיסון. המונח Zero day מתייחס לכך: מתחילים לספור ימים מרגע שהחולשה מתפרסמת ברבים, ועד אז זו חולשה שרק התוקפים נהנים ממנה, ועל כן יוקרתה ומחירה גבוהים מאוד. משך הזמן בין פרסום חולשה להשמשתה כנשק בידי התוקפים ירד מחודשיים ליום אחד. במרוץ הזה הצד המרושע כמעט תמיד מנצח, אלא אם יש למגן פתרון הולם.
7. **קריפטו** - מטבעות הקריפטו וארנקי הקריפטו הפכו למשטח תקיפה ויעד מבוקש לתקיפות סייבר. מדובר ביקום דיגיטלי שלם עם הון עתק. קבוצות פשיעה רבות מכוונות את מאמציהן לתחום זה. הוא אנונימי, בלתי מדווח ונטול אסדרה, גן עדן גם למדינות כמו צפון קוריאה ולמדינות סוררות דומות.

8. **ניצול הגורם האנושי** - כאמור, הגורם האנושי הוא אחד משני הגורמים המרכזיים לתקיפות סייבר. קצרה היריעה, אולם המשתמשים האנושיים הם משטח התקיפה האולטימטיבי. כך ניתן לנצל את הטעויות שאנחנו עושים, את ההטעיות שעובדות על כולנו, בחירת סיסמאות גרועה (כי קשה לזכור, כי מתעצלים להחליף וכו') או מצגי שווא יצירתיים (פישינג). כמעט שאין בן אנוש שחסין למניפולציות או סתם לביצוע טעויות שמשמעותן פתיחת דלת לתוקף והורדת ההגנות אם הן קיימות.

כיצד מדינת ישראל מתמודדת עם איום הסייבר

כיום מדינת ישראל היא מעצמת סייבר במגוון פרמטרים, שנייה אולי רק לארצות הברית, ובפרמטרים מסוימים, כשמחשבים פר-גולגולת, אף קודמת לה.

בטרם אפרט את האינדיקציות והסיבות לכך, חשוב להבין כיצד הגענו עד הלום.

מדינת ישראל הייתה החלוצה העולמית של התייחסות ממשלתית מסודרת לאתגר ההגנה מפני איומי סייבר, שנים לפני שהמונח נכנס לשימוש רווח. כבר ב-1997, במסגרת פרויקט תהי"ה (תשתית הממשלה לעידן האינטרנט), שולב מרכיב ההגנה על חיבור משרדי הממשלה למרשתת כחלק אינטגרלי מהאחריות ומהפעילות. ב-2002 החליטה הממשלה בהחלטה ב/84, באמצעות ועדת השרים לביטחון לאומי ("הקבינט"), להסדיר את הגנת המערכות הממוחשבות החיוניות במדינה והטילה על השב"כ את האחריות לנושא. כך הוקמה רשות אבטחת המידע - רא"ם - יחידה אינטגרלית בשב"כ, באגף אבטחה דאז, שעליה הוטל הביצוע הלכה למעשה, וישראל טבעה לראשונה את המונח תשתיות מידע לאומיות קריטיות (תמ"ק), תשתיות שעליהן מוחלות הנחיות של קצין מוסמך מטעם הממשלה, הן במגזר הפרטי הן במגזר הציבורי.

ראש הממשלה בנימין נתניהו נחשף בשנת 2010 להתפתחות תחום הסייבר ההתקפי ביחידה 8200 ובכלל מערכת הביטחון הישראלית. אחרי שגם קרא את ספרו הבדיוני של פיליפ גי גולדסטיין "בבל שעת אפס", המתאר תרחיש של מלחמת עולם בין ארצות הברית לסין המשלב סייבר עם נשק קונבנציונלי, הטיל ראש הממשלה על פרופסור יצחק בן ישראל להקים מיזם לאומי בתחום הסייבר - המיזם הקיברנטי הלאומי - שהקיף את כלל הארגונים והיבטי העשייה השונים בתחום, אזרחיים וביטחוניים, הגנתיים והתקפיים. עבודת המטה המקיפה ארכה כשנה, ובסיומה הוגשו המלצות לממשלה, והיא קיבלה אותן בהחלטה 3611 באוגוסט 2011, תחת הכותרת "קידום היכולת הלאומית במרחב הקיברנטי". התוצאה המיידית הייתה הקמת מטה הסייבר הלאומי בכפיפות לראש הממשלה. המטה החל מייד בפעולות שונות למימוש המלצות אלה.

אחת ההמלצות המרכזיות הייתה הקמת גוף חדש, מבצעי, שיבצע בעצמו פעולות שונות להגנה על כלל המרחב הקיברנטי הלאומי והקמה של גופי הגנה מגזריים בקרב כלל משרדי הממשלה וגופי ממשל נוספים כבנק ישראל (החלטות הממשלה 2443 ו-2444 בפברואר 2015). הרשות הלאומית להגנה בסייבר קמה בפועל באפריל 2016, וזמן קצר לאחר מכן קיבלה לידיה את רוב תחום האחריות מרא"ם בשב"כ. אולם ריבוי הגופים וחפיפת תחומי האחריות בין המטה הלאומי, רשות ההגנה, שב"כ והממונה על הביטחון במערכת הביטחון (מלמ"ב) לא אפשר התנהלות תקינה. באורח פלא הממשלה הבינה זאת בתוך פרק זמן קצר יחסית, כשנה וחצי, והמטה והרשות מוזגו לגוף אחוד - מערך הסייבר הלאומי. גוף זה פועל החל בינואר 2018 ועד היום, בכפיפות ישירה לראש הממשלה, אך עדיין ללא חוק שמסדיר את פעילותו. הצעת החוק הראשונה פורסמה ביוני 2018, ולאחרונה, ביוני 2026, פורסמה הצעת חוק מתוקנת, כך שרוב הבסיס החוקי לפעילות המערך נובע מתיקונים ותוספות לחוק הסדרת הביטחון ולחוקים אחרים.

אולם בד בבד עם התהליכים הממשלתיים והבירוקרטיים החשובים הללו, קרה תהליך משמעותי לא פחות - עלייתה של תעשיית הסייבר הישראלית. את חוזקה של התעשייה הזו בקנה מידה עולמי ניתן להמחיש בעזרת היקף ההשקעות הגלובליות בישראל והיקף ההנפקים (אקזיטים) של חברות בישראל.

יותר מ-40% מההשקעות הגלובליות בתחום הסייבר מגיעים לחברות ישראליות. נתון זה מרשים עוד יותר בהשוואה לשנת 2019, אז "רק" 20% מההשקעות הגיעו לישראל, שכזכור, כוללת רק 0.1% מאוכלוסיית העולם.

הֶנפֵּק (אקזיט) הוא מימוש ההשקעות בחברה (בדרך כלל בתחום ההיי-טק), כלומר הנפקה או רכישה בידי שחקן גדול יותר. בשנת 2025 לבדה חצה היקף ההנפקים של חברות ישראליות הפועלות בתחום את רף ה-66 מיליארד דולר, לאחר שבשנת 2024 הגיע "רק" ל-5.8 מיליארד. עסקאות ענק של 32 מיליארד דולר ו-25 מיליארד דולר הפכו לחזון נפוץ.

כיצד הפכה ישראל למעצמת סייבר?

ישראל הפכה למובילה עולמית בסייבר לא רק בשל החלוציות בהתייחסות הממשלתית והלאומית המסודרת להגנה, אלא גם הודות למאפיינים רבים, שאנסה לסכם את העיקריים שבהם בקצרה.

1. **חוק שירות ביטחון** - בישראל קיים גיוס חובה של בני ובנות 18 לצה"ל. עד שנות האלפיים העדיפות הראשונה בניתוב המתגייסים האיכותיים לצה"ל הייתה הפנייתם לקורס טיס וליחידות עילית לוחמות. עם עליית הסייבר חל שינוי דרמטי בכך, וזכות הבחירה הראשונה עברה ליחידות הסייבר השונות, בראשן 8200. כך, בני נוער שחלקם צברו כבר יותר מ-10 או אף 12 שנות ניסיון בפעילות בתחום המחשוב, לפעמים על סף החוקית (ולא אציין מאיזה צד של הסף), שולבו עם גיוסם ביחידות הסייבר, שאליהן נבנו מסלולי הכשרה רבים ומגוונים שהשכילו גם לפלח בפילוחי משנה את הכישורים ואת היכולות של המתגייסים הצעירים. כך השכיל צה"ל לאתר את הטובים שבטובים בסייבר באוכלוסייה, ואז לתת להם "רישיון" והכשרה לבצע פעילויות שנחשבות עד היום פורצות דרך וכמעט דמיוניות, כולל בהחתמה לשירות קבע. לאחר ארבע או חמש שנות התנסות מבצעית השתחררו מרבית הצעירים משירות, ובשונה מרוב חבריהם לשירות הצבאי, גילו שניתן לרתום את הניסיון הרב והידע שצברו לכדי הצלחה בעולם העסקי. מימוש החזון התנ"כי "וכיתתו חרבותם לאתים" מעולם לא קיבל משמעות כה מוחשית. ניתן להסב את יכולות תקיפת הסייבר ולפתח בעזרתן "חיסונים ותרופות" - יכולות הגנה שיגנו מפני האיומים בתחום - ועוד תמורת תשלום מכובד. כך קמה בתחילת שנות התשעים של המאה העשרים חברת צ'קפוינט, שהקימו קבוצת יוצאי 8200 שלא עסקו כלל בהגנה בעת שירותם הצבאי, אבל השכילו לבנות פתרונות הגנה מתקדמים אל מול האיומים שהם עצמם היו שותפים לבנייתם. בעקבותיהם באו עוד ועוד, בכל מחזור שהשתחרר מצה"ל. יודגש כי אליהם הצטרפו גם בוגרי שירות צבאי שאינו בתחום הסייבר ואף אינו טכנולוגי, מפקדים ולוחמים מכלל הזרועות שחלקם למדו טכנולוגיה באקדמיה. אלה הוסיפו ממדים וכישורים עסקיים חשובים לתמהיל האמור לעיל.

2. **תרבות ההיי-טק הישראלית** - היעדר משאבי טבע, תחושת מחסור ומצור, מערכת חינוך טובה יחסית (גם אם מושמצת) וחשוב מכול - תרבות המעודדת יזמות, חדשנות, יצירתיות ואלתור וכן סלחנות כלפי כישלונות לצד נשיאה על כפיים של המצליחים וההישגיים - כל אלה דחפו ליצירת "אומת הסטארט-אפ". סף הכניסה להקמה של חברת היי-טק בכלל וחברת סייבר בפרט נמוך עד כדי הסתפקות בידע ובכמה מחשבים. ניתן אפילו להמיר משרדים בבתי קפה.

3. **הלכידות הישראלית** - בסייבר לא ניתן להצליח לבד. לא סוכנות בודדת ואף לא מדינה בודדת. זהו משחק קבוצתי מאין כמוהו בשל טבעו של מגרש המשחקים - המרשתת וטכנולוגיות המידע חובקות העולם. בודדים או גופים מנותקים לעולם לא יצליחו להתמיד בהתמודדות מוצלחת עם הקצב והמגוון של האיומים בתחום. שיתוף ידע, שיתוף מידע קונקרטי ואף שילוב יכולות שונות ומשלימות (שילוב האצבעות השונות לאגרוף) - כל אלה חיוניים להצלחת ההגנה מסייבר. לחברה הישראלית, על אף הביקורת העצמית המפותחת שלנו (וביקורת היא דבר חשוב, זו בדיוק הבמה לציין...) היא בעלת לכידות והדדיות מהגבוהות בעולם, בוודאי כשהדבר נוגע להתמודדות מול איומים. בשנת 2021 הוענק פרס ביטחון ישראל על ידי נשיא המדינה ל"אורגן" - מנגנון המשלב שישה גופי ביטחון במאמץ מרוכז להגנת הסייבר על המדינה: מערך הסייבר הלאומי, צה"ל (יחידה 8200 באמ"ן וחטיבת ההגנה בסייבר באגף תקשוב), שב"כ, המוסד ומלמ"ב במשרד הביטחון. האורגן פעיל מבצעית כבר משנת 2013, והפרס הוענק לו לא רק על היכולות הטכנולוגיות שפיתחו הגופים במשותף, אלא בעיקר כהערכה על היכולת לפעול באופן משולב על אף ניגודי עניינים וקונפליקטים מובנים בין הגופים. לדוגמה, גופי המודיעין חרדים לשמירת ביטחון מקורות המידע ואינם מעוניינים לחשוף מודיעין המתקבל ממקורות רגישים, ואילו גופי הגנת סייבר משתמשים באופן גלוי ולעיתים "רועש" במידע כדי לייצר את ההגנה הנדרשת, ובכך מסכנים במודע את ביטחון המקורות. נוסף על כך, גופי סיכול פועלים להגעה ל"ראש הנחש" ואוספים מידע בסבלנות עד שהתמונה השלמה והמדויקת מתקבלת וניתן לפעול על פיה, ואילו גופי הגנה מנהלים את הסיכון באופן הדוק יותר ואינם דוגלים במתן הזדמנות לתוקף לבצע את זממו, אלא בסיכול פעילותו ברגע שבו היא מתגלה. מדוע האורגן כה מצליח על אף נתוני פתיחה מורכבים אלה? התשובה היא בתרבות המקומית של ה"ביחד" וההבנה שאף אחד משאת הגופים, גדול, חזק וסמכותי ככל שיהיה, אינו מסוגל לנצח לבדו. אציין כי עד היום מערכות ביטחוניות ברחבי העולם עומדות משתאות אל מול הצלחת האורגן הישראלי, ללא כל שכפול או חיקוי מוצלח של המודל.

4. **האקו-סיסטם** - מדינת ישראל השכילה לייצר מערכת יעילה למדי של אקו-סיסטם בסייבר, המורכבת מפעילות הממשלה, האקדמיה והתעשייה האזרחית. מדוע אקו-סיסטם? כי בדומה למערכות דומות בטבע, המערכת מזינה את עצמה ודואגת להמשכיות עצמית ואף לצמיחה. הממשלה פתחה שבעה מרכזי מצוינות בסייבר במימון ממשלתי נכבד, בכל אוניברסיטה שהביעה עניין בכך. האקדמיה דואגת להכשרה ולליטוש של כוח אדם איכותי שנמשך לתחום בשל הפוטנציאל העסקי הגבוה והעניין המקצועי, התעשייה נהנית מכוח האדם הזה שמעשיר אותה ומעצים את יכולתה לייצר עסקים, ההון חוזר לממשלה במיסים, וגם האקדמיה נהנית מהתשומות במישרין ובעקיפין בדמות יוקרה ורלוונטיות. במילים אחרות, זהו מעגל קסמים חיובי ומתעצם שבו הממשלה מעודדת באמצעות גופים כמו מערך הסייבר הלאומי, משרד הכלכלה ומשרד הביטחון את התעשייה והאקדמיה לבנות ולשפר יכולות ואף למכור אותן לגופי ממשל ולקוחות בחו"ל.

5. **"עם כלביא יקום"** - הנסיבות האזוריות וההיסטוריה המדממת יצרו במדינת ישראל חברה אסרטיבית ולוחמנית באופייה, הבנויה למאבק מתמשך, שנלחמה לאורך כל שנות המדינה ואף לפני הקמתה על קיומה ועצמאותה. הנוער הישראלי גדל וצומח לאווירה ביטחונית והתמודדות מתמדת מול איומים (אפילו בעת נסיעות לחופשה בחו"ל, הצנעת סממנים ישראלים היא "צמצום משטח תקיפה" מסוג מסוים). הצעירים חווים זאת גם באופן אקטיבי, "ציד" של האיומים בעיקר במסגרת השירות הצבאי. לוחמת סייבר, הגם שעיקרה בעולם האזרחי-פלילי, היא עדיין לוחמה שדורשת "ציד של הרעים", תחכום, תחבולה ובעיקר היעדר נאיביות ומצב נפשי של תחרות שאינה ספורטיבית. ברוב המדינות האחרות, שלשמחתן אינן חוות את האיום ברמה היומית, התמימות המבורכת היא גורם מעכב המונע התפתחות כישורים החיוניים לתחום הסייבר. בישראל זהו יתרון תחרותי במלוא מובן המונח.

מה בין סייבר לביקורת?

כפי שציינתי באנקדוטה בפתיחה, יש קווי דמיון רבים מאוד בין ביקורת להגנת סייבר.

תפקיד הביקורת בארגון הוא לספק הערכה של תהליכים פנימיים, להצביע על פערים וכשלים, לוודא ניהול סיכונים וציות לרגולציות, לזהות פערים ובעיות ממשליות ולדחוף לשיפור תהליכים ולהתייעלות. כל אלה מופיעים גם בכתב האחריות של מגן הסייבר בארגון.

הגנת הסייבר של ארגון מתחילה מסקר סיכונים כולל וממיפוי כלל הסיכונים לארגון שיכולים להיגרם כתוצאה מתקיפת סייבר: פגיעה ברציפות התפקודית, פגיעה ונזק של ממש, נזק כלכלי, נזק למוניטין, זליגת מידע רגיש של לקוחות, חטיפת המידע למטרות כופר ועוד ועוד. על בסיס הסקר נבנית תוכנית פעולה שוטפת המתבססת על פי רוב על סוג של אסדרה מקובלת - מסגרות כמו NIS2, NIST, ISO 27001 ועוד, הכוללות סדרה ארוכה ומפורטת של בקרות (Controls) ועמידה בדרישותיהן מגבירה מאוד את הסיכוי שהארגון ינהל את הסיכונים באופן טוב ולא ייפגע מתרחישי סייבר.

הבקרה על עמידות הארגון בפני סייבר מתבצעת הן באופן שוטף ורציף באמצעות טכנולוגיות שונות, סנסורים הממוקמים בכל רחבי הארגון מדווחים על ניסיונות תקיפה ולפעמים גם מונעים אותם, הן במסגרת מבחני חדירה (Penetration tests) המבוצעים מפעם לפעם על ידי גורמי מקצוע מחוץ לארגון, כסוג של ביקורת חיצונית, ומדמים פעילות של תוקף סייבר אותנטי, אך ללא כוונות זדון וללא גרימת נזק בפועל.

מבדקי החדירה בתצורותיהם השונות הם המרכיב האיכותי ואולי החשוב ביותר במערך ההגנה של ארגון. עמידה בנהלים ובבקרות, הגדרה נכונה של טכנולוגיות ופתרונות ההגנה, אימון והכשרת העובדים - כולם מכוונים למטרה אחת: למנוע בפועל תקיפה מוצלחת. מבדק החדירה, אם הוא נעשה בצורה מקצועית וטובה, הוא "היהלום שבכתר" שבודק במבחן אמת את כלל המרכיבים השונים, בלי "עיגולי פינות" או הנחות. דומה הדבר לבניית צוללת והכנסתה למים כדי לוודא שאין בה שום נזילה.

וכמו בכל ביקורת, רגע אחרי שהסתיימה בדיקת החדירות האחרונה, הגיע זמן הבדיקה החוזרת לשם בחינת תיקון הליקויים שהתגלו (ותמיד מתגלים פערים בהגנת הסייבר שכן שילוב של טכנולוגיות ובני אדם חשוף במיוחד לפערים וכשלים) וחוזר חלילה.

הבדל אחד נעוץ אולי בפוטנציאל הכלכלי. יש כמה חברות סייבר ישראליות שמתמחות בתצורות וגרסאות שונות של מבדקי החדירה הללו. חברות אלה הגיעו לשווי של יותר ממיליארד דולר.

לכן, אין זה מפתיע שישראל היא כנראה המובילה בעולם גם בתחום הביקורת משולבת הסייבר. פירמות מובילות בעולם לראיית חשבון, ייעוץ וביקורת כמו דלוייט (Deloitte) ו-BDO הקימו בישראל את מרכזי הסייבר העולמיים שלהן, המיועדים למתן שירותי סייבר שונים לכלל לקוחותיהן ברחבי העולם.

משרד מבקר המדינה בישראל גם הוא מהחלוצים והמובילים בתחום בעולם, כראוי למעצמת סייבר וגם להיותנו מהמדינות המותקפות ביותר בסייבר בעולם, אם לא המותקפת ביותר פר-גולגולת. להבנתי, על בסיס ניסיון רב-שנים, זהו חלק בלתי נפרד מהצלחתה של ישראל בתחום הסייבר ומהתבססותה כמעצמה עולמית בתחום. בשנים האחרונות זהו נושא ביקורת מרכזי, ומאז פרוץ הסייבר לחיינו פורסמו עשרות דוחות בנושא, מקצתם עוסקים רק בהגנת סייבר ואבטחת מידע ומקצתם מוקדש פרק ייחודי לנושא הסייבר. במשרד המבקר בוצעו שינויים ארגוניים כדי לשפר את היכולת המקצועית והקיבולת של המשרד בתחום, ואני גאה לציין שבתפקידי כראש מערך הסייבר הלאומי יכולתי לסייע מקצועית בתהליך המבורך. המבקר בדק, והוא חוזר ובודק את המוכנות ואת רמת הגנת הסייבר של הרשויות המקומיות (מספר פעמים), מערכת הבריאות, התשתיות הקריטיות, המידע הממשלתי, מערכות חירום לאומיות ועוד. בדיקות וביקורות אלה מציבות תמונה שקשה לחלוק עליה ודוחפות את הארגונים לבחינה עצמית ולתיקון שוטף של ליקויים ופרצות. הביקורת תורמת גם להעלאת המודעות והקשב של ההנהלה הבכירה לתחום ובכך גם לשיפור המקצועיות ולהגעה לתוצאות טובות יותר באופן שיטתי. בשונה אולי מחלק מהביקורות, חלק ניכר מהארגונים מבינים את החשיבות שבקבלת ממצאי הביקורת הנוגעים לתחום הסייבר, גם אם אינם מחמיאים, ופועלים במהירות לתיקון ולשיפור כל מה שנדרש.

סיכום

הסייבר הפך לאחד האיומים המרכזיים על מדינות, ארגונים וחברות בעידן הדיגיטלי. התלות בטכנולוגיה והקישוריות הגלובלית מרחיבות את משטחי התקיפה ואת פוטנציאל הנזק הכלכלי, התפעולי והלאומי, וזאת בקצב גובר הנגזר מקצב התפתחות הטכנולוגיה הדיגיטלית ותלותנו בה. מדינת ישראל הצליחה לבסס מעמד של מעצמת סייבר עולמית בזכות שילוב ייחודי של תפיסה לאומית, הון אנושי איכותי, אקו-סיסטם מתקדם ושיתוף פעולה בין גופי ממשל, ביטחון ותעשייה. עם זאת, הצלחה זו מחייבת תחזוקה מתמדת של יכולות ההגנה והסתגלות לשינויים מהירים בזירת האיומים. הביקורת - הפנימית והחיצונית - היא מרכיב חיוני במערך ההגנה, שכן היא מאפשרת זיהוי פערים, חיזוק של ניהול הסיכונים ושיפור מתמיד של רמת המוכנות והחוסן הארגוני והלאומי. שילוב אפקטיבי בין הגנת סייבר מקצועית לבין ביקורת עצמאית ואיכותית הוא תנאי הכרחי לשימור יתרונה של ישראל בתחום הסייבר ולהבטחת ביטחונה, יציבותה הכלכלית ואמון הציבור במערכותיה.