מהו סייבר?

חלק א: על מרחב הסייבר, תקיפות סייבר והגנת סייבר

אישה מתה בשל עיכוב בטיפול בחדר מיון שנגרם בעקבות מתקפת סייבר על מערכות המִחשוב של בית החולים; האקרים מפרסמים מידע פרטי על תלמידי בית ספר; פיתוח של חיסון לנגיף הקורונה יורד לטמיון בגלל חסימת הגישה של החוקרים לדאטה שלהם; מדינה זרה מנצלת פִּרצה בתוכנת ניטור כדי לחדור למערכות הממוחשבות של רשויות ממשל. אלו הן רק דוגמאות לנזקים הפוטנציאליים של מתקפת סייבר.

רחל ארידור הרשקוביץ

תהילה שוורץ אלטשולר

עידו סיון סביליה

מחקר מדיניות 171

המכון הישראלי לדמוקרטיה

המכון הישראלי לדמוקרטיה

מחקר מדיניות 171

מהו סייבר?

חלק א
על מרחב הסייבר, תקיפות סייבר והגנת סייבר

רחל ארידור הרשקוביץ | תהילה שוורץ אלטשולר |
עידו סיון סביליה

אוקטובר 2021

What is Cyber Security?
Part One: Cyberspace, Cyber Attacks, and Cyber Protection
Rachel Aridor-Hershkovitz | Tehilla Shwartz Altshuler | Ido Sivan-Sevilla

עריכת הטקסט: חמוטל לרנר
עיצוב הסדרה והעטיפה: סטודיו תמר בר־דיין
ביצוע גרפי: נדב שטכמן פולישוק
הדפסה: גרפוס פרינט, ירושלים

מסת"ב: 978-965-519-367-1

אין לשכפל, להעתיק, לצלם, להקליט, לתרגם, לאחסן במאגר ידע, לשדר או לקלוט בכל דרך או אמצעי אלקטרוני, אופטי או מכני או אחר – כל חלק שהוא מהחומר בספר זה. שימוש מסחרי מכל סוג שהוא בחומר הכלול בספר זה אסור בהחלט אלא ברשות מפורשת בכתב מהמו"ל.

© כל הזכויות שמורות למכון הישראלי לדמוקרטיה (ע"ר), 2021
נדפס בישראל, תשפ"ב/2021

המכון הישראלי לדמוקרטיה
רח' פינסקר 4, ת"ד 4702, ירושלים 9104602
טל': 02-5300888
אתר האינטרנט: www.idi.org.il

להזמנת ספרים:
החנות המקוונת: www.idi.org.il/books
דוא"ל: orders@idi.org.il
טל': 02-5300800

כל פרסומי המכון ניתנים להורדה חינם, במלואם או בחלקם, מאתר האינטרנט.

המכון הישראלי לדמוקרטיה

המכון הישראלי לדמוקרטיה הוא מוסד עצמאי א־מפלגתי, מחקרי ויישומי, הפועל בזירה הציבורית הישראלית בתחומי הממשל, הכלכלה והחברה. יעדיו הם חיזוק התשתית הערכית והמוסדית של ישראל כמדינה יהודית ודמוקרטית, שיפור התפקוד של מבני הממשל והמשק, גיבוש דרכים להתמודדות עם אתגרי הביטחון מתוך שמירה על הערכים הדמוקרטיים וטיפוח שותפות ומכנה משותף אזרחי בחברה הישראלית רבת הפנים.

לצורך מימוש יעדים אלו חוקרי המכון שוקדים על מחקרים המניחים תשתית רעיונית ומעשית לדמוקרטיה הישראלית. בעקבותיהם מגובשות המלצות מעשיות לשיפור התפקוד של המשטר במדינת ישראל ולטיפוח חזון ארוך טווח של תרבות דמוקרטית נכונה לחברה הישראלית ולמגוון הזהויות שבה. המכון שם לו למטרה לקדם בישראל שיח ציבורי מבוסס ידע בנושאים שעל סדר היום הלאומי, ליזום רפורמות מבניות, פוליטיות וכלכליות ולשמש גוף מייעץ למקבלי ההחלטות ולציבור הרחב.

המכון הישראלי לדמוקרטיה הוא זוכה פרס ישראל לשנת תשס"ט על מפעל חיים – תרומה מיוחדת לחברה ולמדינה.

הדברים המובאים במחקר מדיניות זה אינם משקפים בהכרח את עמדת המכון הישראלי לדמוקרטיה.

תוכן העניינים

תקציר 7

מבוא 13

פרק 1. מהו סייבר 17

פרק 2. המאפיינים הייחודיים של מרחב הסייבר 21
א. ממד הזמן וקצב ההתקדמות במרחב 21
ב. טשטוש גבולות גיאוגרפיים 21
ג. העלות הנמוכה של פעילות במרחב הסייבר 22
ד. טשטוש העקבות הדיגיטליים 22
ה. היפר־קישוריות (Hyperconnectivity) 23

פרק 3. היעדר תמריצים מספקים להגנת סייבר 27
א. סוחרי מידע (Data Brokers) ונושאי מידע 27
ב. מורכבות הפרויקטים והמרוץ להיות ראשון בשוק 28
ג. החצנות שליליות (Negative Externalities) 29
ד. א־סימטריה במידע בין מפתחים ומשתמשים 29
ה. א־סימטריה במידע בין תוקפים ובין המבקשים להגן על מרחב הסייבר 30

פרק 4. מהי מתקפת סייבר 31
א. מהי חולשה? 31
ב. ניצול (Exploit) ונוזקה (Malware) 33
ג. איך נראית מתקפת סייבר? 33
ד. יעדי מתקפת הסייבר 36

פרק 5. נוזקות והשימוש בהן במתקפות סייבר 39
א. נוזקה כשירות ושוק הסייבר ההתקפי 39
ב. סוגי נוזקות עיקריים 44
ג. אופני הפצה, שילוח או הדבקה של נוזקה 49
ד. פיתוח מודולרי של נוזקות ושיפור נוזקות קיימות 52

פרק 6. הגורם האנושי במתקפות סייבר 53

פרק 7. המניעים למתקפת סייבר וזהות התוקפים 58
א. הגידול במגוון המניעים למתקפת סייבר 58
ב. מגוון המניעים למתקפות סייבר כיום 60
ג. זהות התוקפים – טשטוש ההבחנה בין שחקנים מדינתיים לשחקנים א־מדינתיים 75

פרק 8. אומדן הנזק ממתקפות סייבר 80
סיכום ביניים: הגורמים לפגיעוּת של מרחב הסייבר למתקפות 85

פרק 9. הגנת סייבר 87
א. הגדרת המונח "הגנת סייבר" 87
ב. ההתפתחות של תעשיית הגנת הסייבר 96
ג. שיטות עיקריות להגנת סייבר 100

פרק 10. סיכום 107

Abstract iii

תקציר

אישה מתה בשל עיכוב בטיפול בחדר מיון עקב מתקפת סייבר על מערכות המחשוב של בית החולים. האקרים מפרסמים מידע פרטי הכולל מספרי תעודות זהות של תלמידי בית ספר בעיר גדולה. מחקר על פיתוח חיסון לנגיף הקורונה יורד לטמיון בגלל חסימת גישה של חוקרים לדאטה שלהם. רוסיה מנצלת פרצה בתוכנת ניטור של חברת SolarWind כדי לחדור למערכות הממוחשבות של רשויות ממשל אמריקאיות, גופי ביטחון וחברות מסחריות; הנזק שנגרם לביטחון הלאומי של ארצות הברית מושווה לנזק שהסבה המתקפה על פרל הרבור במלחמת העולם השנייה.

אלו רק דוגמאות ספורות, חלקן אמיתיות וחלקן רק היפותטיות, לנזקים הפוטנציאליים של מתקפת סייבר. תחומים רבים בחיי היום־יום שלנו הולכים ומתבססים על מכשירים המחוברים למוחות מרכזיים, כגון מערכות מידע מרכזיות, עוזרים דיגיטליים, קוצבי לב ורכבים אוטונומיים, והחשש מפני מתקפת סייבר הולך וגדל. מגפת הקורונה אף העצימה את החששות בגלל התלות הגוברת של גופים רבים במערכות הנשלטות מרחוק – ממקומות עבודה ולימודים ועד בתי חולים ומוסדות מחקר.

וכך, לצד היתרונות העצומים של מרחב הסייבר עבור הכלכלה והחברה בכללותה, חלה עלייה תלולה בהיקף מתקפות הסייבר, במספר הגופים שאליהם הן מכוונות ובנזק הכלכלי שהן גורמות, וכן ברמת המיסוד של ארגוני הפשע המאורגן או המדינות העוינות שעומדות מאחוריהן. כל אלה מעוררים את הצורך בבחינת אופני ההגנה הרצויים על הפעילות במרחב הסייבר ואסדרתם בחקיקה. צורך

זה לא נעלם מעיני המחוקק הישראלי, כפי שעולה מתזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח–2018 (להלן: תזכיר חוק הסייבר), ומהניסיון לחוקק לפני הבחירות במרץ 2021 את חוק סמכויות לשם חיזוק הגנת הסייבר (הוראת שעה), התשפ"א–2021, שהוא למעשה גרסה מקוצרת וממוקדת של תזכיר חוק הסייבר במתווה של הוראת שעה לשנתיים בלבד.

לפני הדיון באסדרת ההגנה על מרחב הסייבר בישראל חיוני להסביר ולהבין את המושגים המתארים את מרחב הסייבר, הגנת הסייבר ומתקפת הסייבר ואת האתגרים הקשורים אליהם. מטרת מחקר זה היא להציג את מגוון המונחים הקשורים להגנת מרחב הסייבר כדי לתת בידי קובעי המדיניות את הידע והכלים הנחוצים להבנת יחסי הכוחות במרחב הסייבר והאתגרים הקשורים בהגנתו, כבסיס לאסדרת הנושא בישראל. במקביל לפרסום זה אנו מוציאים לאור גם מסמך העוסק באסדרת מרחב הסייבר בישראל בפרספקטיבה השוואתית, ומתמקד בין השאר בבניית מערך הסייבר הלאומי ובתזכיר חוק הסייבר.

המושג העיקרי והראשון שיש להבינו הוא "מרחב הסייבר": המושג מתייחס לרשת האינטרנט כפלטפורמה המרכזית להעברת מידע ונתונים ממקום למקום, ולצידה גם למגוון מערכות המתקשרות זו עם זו ומשמשות להעברת נתונים ומידע ואינן כבולות למגבלות פיזיות או גיאוגרפיות.

למרחב הסייבר כמה מאפיינים ייחודיים המקנים יתרונות רבים למשתמשים, אך גם הופכים אותו לכר פורה למתקפות: ראשית, העברת מידע במרחב הסייבר מהירה עשרות מונים מהעברתו בדרכים מסורתיות (האוויר, הים והיבשה), ואפשר להעביר מידע מקצה אחד של העולם לקצהו השני במהירות בלתי נתפסת. שנית, העלות של ביצוע פעולה במרחב הסייבר, גם אם ההשלכות של אותה פעולה מרחיקות לכת, אינה גבוהה. פעולה במרחב זה אינה מחייבת תשתית מדינתית או תקציב גדול, ואפשר לבצעה בעלות נמוכה יחסית באמצעות מחשב אישי או באמצעות קניית שירותי תקיפת סייבר מחברות פרטיות. בשל שני מאפיינים אלו, שיקולי מרחק אינם רלוונטיים במרחב הסייבר, הגבולות הגיאוגרפיים המוכרים לנו מיטשטשים ולגורמים רבים – מדינות, ארגונים תת־מדינתיים ויחידים – יש יכולות תקיפה גבוהות במרחב זה. מאפיין נוסף הוא טשטוש העקבות הדיגיטליים במרחב הסייבר, המקשה על זיהוי מהיר וחד־משמעי של מבצעי הפעולה. מעל לכל המאפיינים האלה

מרחפת ה"היפר־קישוריות" של מרחב הסייבר: היכולת של המרכיבים השונים של מרחב הסייבר – השחקנים (מדינות, חברות פרטיות קטנות, תאגידי ענק, ארגונים שלא למטרות רווח, יחידים, ארגוני פשע, ארגוני טרור) והמכשירים (מכשירים דיגיטליים כגון מחשבים וטלפונים חכמים, וכן יישומים ותוכנות) – לתקשר אלה עם אלה באופנים מגוונים וברמות שונות ולהעביר ביניהם כמויות עצומות של מידע. ככל שיותר שירותים, מערכות מידע ומוצרים מקושרים זה לזה (בטכנולוגיה המכונה "האינטרנט של הדברים") ומסוגלים לקלוט ולהעביר מידע מהסביבה וזה מזה, כך קל יותר למתקפת סייבר, שהיא כשלעצמה תוכנת מחשב, להתפשט במהירות, להגיע ליותר מערכות, שירותים ותשתיות ולגרום נזק חמור.

מאפיינים אלו של מרחב הסייבר גם אחראים להופעתם של מגוון כשלי שוק, אשר במקרים מסוימים עשויים להצדיק את התערבות המדינה לשם אסדרה והבטחה של הגנת הסייבר. השוק של מרחב הסייבר הוא שוק "דו־צדדי": בצידו האחד נמכרים או ניתנים בחינם שירותים ומוצרים; ובצידו השני נמכרים מידע על התנהגות המשתמשים במוצרים ו"זמן מסך" של אותם משתמשים לסוחרי מידע ולמפרסמים. במצב זה נאמנות התאגידים אינה נתונה למשתמשים, שהם צרכני המוצרים והשירותים, אלא למפרסמים, שהם מקור הכנסתם העיקרית. כמו כן, לתאגידים ולסוחרי המידע הפועלים במרחב הסייבר אין תמריץ גבוה להשקיע באבטחת מידע ובהגנה על המשתמשים. כשלי השוק המובילים להשקעה הנמוכה בהגנת הסייבר נובעים מגורמים נוספים, כמו המורכבות של כתיבת תוכנה והמרוץ להיות הראשון שמשווק מוצר תוכנה חדשני כדי להשיג דומיננטיות בשוק; העובדה שמפתחי מוצר תוכנה שאינו מאובטח ומוגן כראוי ועלול לאפשר מתקפת סייבר אינם נושאים בעצמם או לבדם במלוא ההשלכות של מעשיהם (תופעה המכונה "החצנות שליליות"), ולכן אינם רואים בסיכון למתקפת סייבר סיכון משמעותי המצדיק השקעת משאבים בשיפור הגנת הסייבר ואבטחת המידע; וא־סימטריה אינהרנטית במידע בין תוקפי סייבר ובין אלו המבקשים להגן על מרחב הסייבר: לתוקף מספיק לזהות חולשת סייבר אחת המאפשרת לו לפתוח במתקפת סייבר, אך הרוצה להגן על מרחב הסייבר נדרש לזהות ולאתר כל חולשה פוטנציאלית מבעוד מועד ולמנוע את ניצולה.

נוסף על כשלי השוק הנובעים ממאפייניו הייחודיים של מרחב הסייבר, יש לתת את הדעת על כך שהגורם האנושי במרחב הסייבר, כלומר עובדים או קבלני משנה

של הארגון המותקף, הוא החוליה החלשה בהגנת הסייבר בארגון. רוב התקפות הסייבר המוצלחות מנצלות את הנטייה שלא להטמיע עדכוני אבטחה חשובים באופן קבוע ושגרתי, ואחד מאפיקי ההפצה המרכזיים לניצול חולשה ולהפצתה של נוזקה הוא דיוג (phishing), המנצל את נטייתם של גולשים ומשתמשי דוא"ל להקיש על קישורים או לפתוח קבצים מבלי לבדוק אם הם נגועים בנוזקה. העלאת המודעות של המשתמשים לסכנות שבמרחב הסייבר ואימוץ עקרונות ונהלים להפחתת הסיכון חיוניים לשם מזעור הפגיעה הפוטנציאלית של הגורם האנושי כחוליה החלשה במערכת הגנת הסייבר.

הבנת מורכבותה של מתקפת סייבר חיונית אף היא להתוויית מדיניות להגנת מרחב הסייבר. מתקפת סייבר מורכבת משלבי פעולה שונים ודינמיים שלעיתים מבוצעים על ידי שחקנים שונים במרחב הסייבר בזמנים שונים תוך קיום מסחר פעיל ביניהם. השלב הראשון במתקפת סייבר מכונה "איסוף מודיעין", ובמהלכו התוקף אוסף בעצמו או רוכש מן המוכן בשוק הסייבר ההתקפי את מרב המידע האפשרי על המערכות שהוא מבקש לתקוף במטרה לאתר חולשות: פרצות טכנולוגית או התנהגות בלתי צפויה של מערכת המחשוב המאפשרות לתוקף פוטנציאלי לקבל גישה או לבצע פעולות שלא אמורה להיות לו הרשאה לביצוען. בשלב השני, המכונה "חימוש", התוקף מכין או רוכש את הנוזקה שבה יעשה שימוש לשם ניצול החולשה שמצא וביצוע מתקפת הסייבר. קיימים סוגים שונים של נוזקות: רוגלה, שהיא תוכנת מעקב; סוס טרויאני – נוזקה שמתחזה לתוכנת מחשב לגיטימית ושימושית; "בוט" – נוזקה הגורמת למערכת המחשב המותקפת לפעול כרובוט הנשמע לפקודות הניתנות לו מרחוק; ונוזקת כופר, המצפינה את הקבצים במערכת המחשב המותקפת ומתנה את שחרורם בתשלום כופר לתוקף. בשלב השלישי הנוזקה נשלחת ליעד המתקפה, הקוד בנוזקה האחראי לניצול החולשה מופעל והרשאות הגישה מושגות. באמצעותן מתקין התוקף במערכת המותקפת "דלת אחורית" (backdoor) המאפשרת לו לשלוט בה מרחוק ולפעול למיצוי מטרת התקיפה (מחיקת קבצים, מניעת גישה אליהם, זריעת הרס במערכת הממוחשבת המותקפת, איסוף והעתקת מידע מהמערכת, התפשטות למערכות אחרות המקושרות למערכת המותקפת או התקנת תוכנת מעקב וריגול העוקבת אחר המשתמש במערכת).

המניעים למתקפת סייבר מגוונים: החל ממניעים כלכליים וריגול תעשייתי לשם רכישת יתרון תחרותי, עבור בזריעת הרס ופחד ממניעים טרוריסטיים,

וכלה בניסיונן של מדינות לאסוף מודיעין לשם השגת רווחים כלכליים, פוליטיים וביטחוניים וכאמצעי לחימה לכל דבר. קשה לאמוד במדויק את מכלול הנזקים הישירים והעקיפים העלולים להיגרם ממתקפת סייבר, אך ההערכות המפורסמות מעת לעת מצביעות על נזק כלכלי לא מבוטל. כך, למשל, בשנת 2018 פרסמו המרכז למחקרים אסטרטגיים ובינלאומיים וחברת הייעוץ מקינזי הערכה משותפת האומדת את הנזק השנתי לכלכלה העולמית עקב פשיעת סייבר בכ־600 מיליארד דולר.

הנזקים הפוטנציאליים של מתקפת סייבר רבים ומגוונים: עלות ההחלפה של תשתיות חומרה ותוכנה, נזק לתשתיות, אובדן חיי אדם כאשר הפגיעה היא בשירותי הרפואה הדחופה, העלות של התמגנות מחודשת (למשל התקנת תוכנות אנטי־וירוס חדשות), שיפוי לקוחות, קנסות המשולמים לגופים רגולטוריים מדינתיים, עלות ההפרעה לתפקוד התקין של העסק, עלות גניבת זהויות והמאבק בתופעה, עלות הפגיעה באמון הלקוחות ועלות שיקום המוניטין של החברה, עלות חשיפת מידע סודי של העסק, עלות הפגיעה בחדשנות ובתחרותיות והעלות של אובדן הזדמנויות עסקיות; וכן נזקים ברמה הסוציאלית והתודעתית – למשל הפרעה של ממש לחיי היום־יום עקב פגיעה בשירותים חיוניים, פגיעה באמון הציבור בשלטון ובמערכותיו, ערעור האמון ביכולת לברר את המציאות לאשורה וקיטוב ציבורי בין דעות שונות.

הגנת סייבר היא אפוא כורח המציאות, אולם אין לה הגדרה קוהרנטית ברורה והדבר מקשה על אימוץ מדיניות ציבורית בתחום. למול עיניהם של קובעי המדיניות עומדת שורה של הגדרות שונות שכל אחת מהן מדגישה את החשיבות של הגנת הסייבר לתחומים שונים: ביטחון לאומי ואישי, דיפלומטיה ויחסי חוץ, כלכלה, תעסוקה והתפתחות התעשייה.

לשיטתנו, יש להגדיר "הגנת סייבר" כמכלול פעולות שונות, פרואקטיביות וריאקטיביות, שמטרתן להתמודד עם איומים על השלמות, האמינות והזמינות של המידע הנמצא במחשבים, במערכות מידע ורשתות מחשבים ובתשתיות דיגיטליות אחרות, וכן לסייע למערכות אלו לשוב לתפקוד תקין במקרה של מימוש איומים כאלה. חשוב להדגיש את מה שלא נכלל בהגדרה: הגנת סייבר אינה מתייחסת לאיומים הגלומים במידע עצמו, כגון ביטויי שנאה, דיבה ולשון

הרע, העלבת עובדי ציבור, פגיעה בפרטיות, הפצת מידע אסור בפרסום מטעמים ביטחוניים ואחרים, השפעה על בחירות וכיוצא באלה.

תהא הגדרת המונח "הגנת סייבר" אשר תהא, יש לתת את הדעת ליחס שבינה ובין זכות היסוד לפרטיות. הגנת סייבר היא תנאי מקדמי חיוני למימוש זכותו של אדם לפרטיות, אף שהיא כוללת מגוון נושאים שאינם קשורים להגנה על מידע אישי ופרטיות – למשל הגנה על תשתיות ועל ביטחון כלכלי. משום כך, לעיתים מתעורר ניגוד אינטרסים בין פרטיות ובין הגנת סייבר המשקף בבסיסו את ההתנגשות בין חירות לביטחון. המקרה הבולט ביותר להתנגשות שכזו הוא היכולת לעשות שימוש בשירותים במרחב הסייבר באופן אנונימי. מחד גיסא, גלישה אנונימית היא מימוש של הזכות לפרטיות ומאפשרת לאדם להשתמש במרחב הסייבר מבלי להזדהות. מאידך גיסא, גלישה אנונימית עומדת בניגוד למטרת הגנת הסייבר לאפשר שימוש בטוח במרחב הסייבר, והדבר בא לידי ביטוי ברצונן של רשויות האכיפה לזהות כל גולש וגולש כדי למנוע פשיעת סייבר או לאתר בדיעבד את האחראים לפשע סייבר.

מבוא

אישה מתה בשל עיכוב בטיפול בחדר מיון עקב מתקפת סייבר על מערכות המחשוב של בית החולים. האקרים מפרסמים מידע פרטי הכולל מספרי תעודות זהות של תלמידי בית ספר בעיר גדולה. מחקר על חיסון לנגיף הקורונה יורד לטמיון בגלל חסימת גישה של החוקרים לדאטה שלהם. השלכות אלו של מתקפות סייבר, שחלקן אף התרחשו במציאות, מצטרפות לחששות מפני פגיעה בתשתיות חשמל ומים, גניבת זהות וכרטיסי אשראי וכן חדירה למאגרי מידע גדולים של פרטים אישיים כדי להשפיע באמצעותם על תוצאות הבחירות.[1] תחומים רבים בחיי היום־יום שלנו הולכים ומתבססים על מכשירים המחוברים ל"מוחות" מרכזיים, כגון עוזרים דיגיטליים, קוצבי לב ורכבים אוטונומיים, והחשש מפני מתקפת סייבר הולך וגדל. מגפת הקורונה העצימה את החששות בגלל התלות הגוברת של גופים רבים במערכות הנשלטות מרחוק – ממקומות עבודה ולימודים ועד בתי חולים ומוסדות מחקר. וכך, לצד היתרונות העצומים של מרחב הסייבר עבור הכלכלה והחברה בכללותה, חלה עלייה תלולה בהיקף מתקפות הסייבר, במספר הגופים שאליהם הן מכוונות ובנזק הכלכלי שהן גורמות, וכן ברמת המיסוד של ארגוני הפשע המאורגן או המדינות העוינות שעומדות מאחוריהן. כל אלה מעוררים את הצורך בבחינת אופני ההגנה הרצויים על הפעילות במרחב הסייבר.

מרחב הסייבר הוא כינוי מטפורי לרשת האינטרנט. הרשת נבנתה כבר בשנות השישים של המאה הקודמת, בעיצומה של המלחמה הקרה, כמערכת מבוזרת של מערכות מחשב ותקשורת שמטרתה לאפשר תעבורת מידע סודית, חלופית לתעבורה דרך התווך הפיזי, בין מערכות צבאיות, ביטחוניות וממשלתיות, גם במקרה שאלו נתונות למתקפה פיזית.[2]

1 ראו למשל Nicole Perlroth & David E. Sanger, *Ransomware Attacks Take on New Urgency Ahead of Vote*, The New York Times (Sept. 27, 2020)

2 כמה חוקרים עבדו באותו זמן, ללא קשר זה לזה, על הרעיון של תעבורת מידע באופן סודי בין מכוני מחקר ובין גורמי ביטחון. רשת האינטרנט נולדה הודות למעבר הטכנולוגי ממודל של רשתות מחשבים סגורות ואוטונומיות למודל של רשתות מבוזרות שיכולות לתקשר זו עם זו ללא תלות במידע קודם או בסנכרון במקום מרכזי. ראו Berry M. Leiner et al., *A Brief History of the Internet*, 39 (5) ACM SIGCOMM Computer Communication Review 22 (2009); Ben Tarnoff, *How the Internet Was Invented*, The Guardian (July 15, 2016)

לאורך השנים הוצעו בשיח המדיניות הציבורית והאסדרה של רשת האינטרנט מטפורות נוספות, כגון "אוטוסטרדת המידע" (information superhighway), שהדגישה את המהירות והכמות של מוצרי המידע המועברים על גבי רשת האינטרנט; "סייבר אקוסיסטם" (cyber ecosystem), המתארת את ההיפר־קישוריות ויחסי הגומלין בין השחקנים השונים ברשת האינטרנט, בדומה למערכת אקולוגית בטבע; ו"מרחב הסייבר" (cyberspace), המשקפת את הרצון להתייחס לרשת האינטרט כאל מקום, בדומה למקום פיזי, במטרה לפשט את הדיון המושגי בהחלת חוקים ונורמות התנהגות המקובלות בעולם הפיזי על רשת האינטרנט.[3]

לאורך השנים הורחבה משמעותו של המונח "מרחב הסייבר", וכיום הוא אינו מתייחס לרשת האינטרנט בלבד אלא למכלול של מערכות, שרשת האינטרנט היא המרכזית שבהן, המשמשות להעברת מידע ונתונים שאינה מוגבלת בשל אילוצים פיזיים או גבולות גיאוגרפיים.

מפתחיה הראשונים של רשת האינטרנט לא צפו שהיא תשמש מיליארדי משתמשים ותאפשר תעבורת מידע בהיקפים עצומים, ועל כן לא הקדישו תשומת לב יתרה לאבטחת תעבורת המידע על גבי הרשת. מרחב הסייבר הוא כיום מקור לפריחה כלכלית ורווחה חברתית ומאפשר נגישות חסרת תקדים למידע; אולם התלות החברתית הגוברת בו בשילוב עם הארכיטקטורה הביזורית הן כר פורה למתקפות סייבר למטרות פשיעה, ריגול, הרתעה ואפילו השפעה על דעת קהל.

3 Raymond Gozzi, Jr., *The Cyberspace Metaphor*, 51 Rev. of General Semantics 218 (1994); Paul C. Adams, *Cyberspace and Virtual Places*, 87 The Geographical Rev. 155 (1997); Clay Calvert, *Regulating Cyberspace: Metaphor, Rhetoric, Reality, and the Framing of Legal Options*, 20 Hastings Comm. & Ent. L. J. 541, 544-549 (1997); Niva Elkin-Koren & Eli M. Salzberger, Law, Economics and Cyberspace 20-22 (2004); Julie E. Cohen, *Cyberspace as/and Space*, 107 Colum. L. Rev. 210 (2007); Adriane Lapointe, *When Good Metaphors Go Bad: The Metaphoric "Branding" of Cyberspace* 2-8 (Center for Strategic & International Studies 2011); Frank Hsu, *Building a Secure and Sustainable Cyberspace Ecosystem: An Overview*, *in* Advances in Cybersecurity: Technology, Operation and Experiences 15 (Frank Hsu & Dorothy Marinucci eds., 2013)

בשנות השישים והשבעים של המאה העשרים התמקדה תשומת הלב בסיכון לדליפת מידע מסווג שאוחסן במערכות ממוחשבות ובצורך להתגונן מבעוד מועד מפני דליפת מידע כזו.[4] רק במהלך שנות השמונים התחדדה ההבנה שאפשר לפתח מערכות ממוחשבות לתקיפה של מערכות ממוחשבות אחרות, ושיש צורך להתגונן מפני מתקפות שכאלו ולנסות למנוע אותן.[5] עם הפיכת מערכות המידע הממוחשבות למוקד מרכזי של חיי המדינה, החברה והכלכלה גבר השימוש במרחב הסייבר למטרות התקפיות, ופותחו יכולות מדינתיות ופרטיות לניצול חולשות מובנות למטרות שונות.

עד שלהי שנות התשעים היה מקובל להשתמש בביטוי "אבטחת מידע" (information security) לתיאור הגנת מערכות ממוחשבות מפני מתקפות סייבר. הפרשנות המקובלת של הביטוי היא מכלול הפעולות הדרושות כדי להבטיח את הסודיות, האמינות והזמינות של המידע המצוי על גבי המערכות הממוחשבות (Confidentiality, Integrity, Availability; CIA).

השימוש במושג "הגנת סייבר" החל עם החדירה הגוברת של טכנולוגיות המחשוב לחיי היום־יום, לנוכח ההבנה שהמושג "אבטחת מידע" מצומצם מידי ואינו משקף את מכלול האיומים הטמונים בשימוש בטכנולוגיות דיגיטליות. איומים אלו רחבים מפגיעה באדם מסוים או בחברה מסחרית מסוימת, ומגיעים לכדי אפשרות של פגיעה בביטחון הלאומי, ביציבות הכלכלית או בסדר הציבורי. משום כך, בהדרגה הפך המושג "הגנת סייבר" לביטוי שגור הן בקרב אנשי טכנולוגיה הן בקרב חוקרי מדע המדינה ומקבלי החלטות, כחלק מהשיח הפוליטי.[6]

4 אחד המחקרים פורצי הדרך בתחום היה מחקרו של החוקר ויליס וור ממכון ראנד, שפרסם בשנת 1967 מאמר על סיכוני ביטחון ופרטיות במערכות ממוחשבות: Willis H. Ware, *Security and Privacy in Computer Systems* (RAND Corporation, 1967)

5 Michael Warner, *Cybersecurity: A Pre-history*, 27 Intelligence & Nat'l Sec. 781 (2012)

6 Samantha Adams et al., *The Governance of Cybersecurity: A Comparative Quick Scan of Approaches in Canada, Estonia, Germany, the Netherlands and the UK*, 15–16 (Tilburg University, 2015)

עם זאת, השינוי בטרמינולוגיה לא הוביל לחידוד משמעות המונחים "מרחב הסייבר", "מתקפת סייבר" ו"הגנת סייבר", והשימוש בהם תדיר אך אינו ממוקד. לתפיסתנו, דבר זה מקשה על קיום דיון ענייני ומעמיק באסדרת הגנת הסייבר בישראל.[7]

מטרת פרסום זה היא לנסות ולהבהיר את המושגים המתוארים, למקם אותם בתוך ההקשר המתאים ולתאר את האתגרים הקשורים בהם. במקביל לפרסום זה אנו מוציאים לאור גם מסמך העוסק באסדרת מרחב הסייבר בישראל בפרספקטיבה השוואתית, המתמקד בין השאר בבניית מערך הסייבר הלאומי ובתזכיר חוק הסייבר.[8]

בחלקו הראשון של המסמך שלפניכם נסקור את המאפיינים הייחודיים של מרחב הסייבר, ולאחר מכן את כשלי השוק המובילים להיעדר תמריצים מספקים להגנת סייבר במוצרים ובשירותים טכנולוגיים. בהמשך נסביר מהי מתקפת סייבר וכיצד היא מתבצעת, מהן נוזקות וכיצד הן משמשות למתקפה ולאיסוף מידע, ומה תפקידו של הגורם האנושי במתקפות סייבר. נסביר מהם המניעים למתקפות סייבר וכיצד מזהים את התוקפים, ונעסוק גם באומדן הנזק ממתקפות אלו.

בחלק השני של המסמך נסביר מהי הגנת סייבר, ונבחן כיצד התפתחה תעשיית הגנת הסייבר ומהן השיטות המרכזיות לממש הגנה זו. כן נבהיר את היחס בינה ובין המונח "אבטחת מידע" והגנה על הזכות לפרטיות.

ענבל מנדלר סייעה לנו בכתיבת הגרסה הראשונה של המסמך, ועל כך מסורה לה תודתנו. אנו מודים להוצאה לאור של המכון הישראלי לדמוקרטיה ולעורכת חמוטל לרנר על העבודה המסורה. תודה לעו"ד עמית אשכנזי, לפרופ' יובל שני ולד"ר נדיב מרדכי על הערותיהם החשובות.

7 Michael Daniel, *Why Is Cybersecurity So Hard?*, Harv. Bus. Rev. (May 22, 2017)

8 לדיון באסדרת הגנת מרחב הסייבר ראו רחל ארידור הרשקוביץ ותהילה שוורץ אלטשולר **אסדרת מרחב הסייבר: סקירה השוואתית והתמקדות בישראל** (המכון הישראלי לדמוקרטיה, בהכנה).

פרק 1

מהו סייבר

בשנים האחרונות קשה להתעלם מן השימוש התכוף במושג ״סייבר״. המילה ״סייבר״ מופיעה במושגים רבים הקשורים במרחב הדיגיטלי, כגון פשיעת סייבר (cybercrime), לוחמת סייבר (cyberwarfare), בריונות במרחב הסייבר (cyberbullying) והמושג המרכזי והכוללני ״הגנת מרחב הסייבר״ (cybersecurity). אבל נדמה שכמו מטבעות לשון אחרים גם מושג זה עבר ״זיהום מושגי״, ולכן בבואנו לבדוק את המדיניות הציבורית המתאימה לטיפול בנושא הגנת הסייבר חשוב להגדיר את המושג במדויק.[9]

המושג ״סייבר״ מוכר כיום בעיקר בהקשרים טכנולוגיים, אולם אין זה מושג חדש. מקור המושג במילה יוונית שמשמעותה ״היכולת למשול ולנווט״,[10] ובשנת 1948 שימש המושג ״סייבר״ את המתמטיקאי והפילוסוף האמריקאי נורברט ווינר לתיאור שליטה ופיקוח עצמי במערכות סבוכות של תקשורת בין בעלי חיים שונים ואף בין מכונות תעשייתיות.[11]

בשנות השישים השתמשו רקדנים במושג ״סייבר״ לתיאור ריקוד חופשי ומאולתר.[12] בשנת 1984 תיאר ויליאם גיבסון, סופר המדע הבדיוני הקנדי־אמריקאי, את ״מרחב הסייבר״ (cyberspace) כמרחב מסועף ודיגיטלי המכיל מיליארדי יישויות הפועלות יחדיו בחופשיות וללא תכנון מוקדם, אולם נשלטות דרך בקרי שליטה.[13] תיאור זה משלב בין המשמעויות השונות שניתנו למושג ״סייבר״ במהלך השנים – **ניווט בתוך מערכות מורכבות ושליטה בהן, יחד עם אלתור וזרימה חופשית**. זהו גם התיאור הקרוב ביותר להגדרת ״מרחב הסייבר״

9 לדיון באסדרת הגנת מרחב הסייבר ראו ארידור הרשקוביץ ושוורץ אלטשולר, **לעיל** ה״ש 8.

10 ENISA, Definition of Cybersecurity: Gaps and Overlaps in Standardisation 17 (V1.0, 2015)

11 Norbert Wiener, Cybernetics: Or Control and Communication in the Animal and the Machine (1948)

12 ENISA, **לעיל** ה״ש 10, בעמ׳ 10.

13 William Gibson, Neuromancer (1984)

במדינות המערב כיום – מרחב המורכב מאוסף של מערכות מידע מקושרות, שכל אחת מהן מאפשרת אינטראקציה וקישוריות עם מערכות אחרות, עם המשתמשים ועם המפעילים והמפתחים של הטכנולוגיה או המערכת.[14] כלומר ההגדרה של מרחב הסייבר אינה מזוהה בהכרח עם טכנולוגיה מסוימת.

במזכר מטעם מזכיר ההגנה האמריקאי משנת 2008 הוגדר מרחב הסייבר כ"מרחב גלובלי הכולל רשתות עצמאיות של תשתיות טכנולוגיית מידע, לרבות רשת האינטרנט, רשתות טלקומוניקציה ומערכות מחשב".[15] במסמך מדיניות רשמי של ממשלת גרמניה ההגדרה מתמקדת בתשתיות מידע הזמינות באמצעות האינטרנט מעבר לגבולות מדינתיים,[16] אך גם ב"מרחבים וירטואליים נוספים הנוצרים ממערכות מידע ממוחשבות"; ובמסמך תשתית של ממשלת בריטניה בעניין הגנת מרחב הסייבר משנת 2011 הוגדר מרחב הסייבר כ"מרחב אינטרקטיבי של מערכות דיגיטליות המשמשות לאחסון, שינוי והעברה של מידע". הגדרה זו כוללת את רשת האינטרנט אך מתייחסת גם למערכות אחרות שחברות מסחריות משתמשות בהן.[17]

14 Adams et al., **לעיל** ה"ש 6, בעמ' 17–18.

15 "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers"; ראו Noah Shachtman, *26 Years After Gibson, Pentagon Defines "Cyberspace"*, WIRED (May 23, 2008)

16 באסטרטגיה להגנת מרחב הסייבר משנת 2011 הוגדר מרחב הסייבר כך: "Cyberspace includes all information infrastructures accessible via the internet beyond all territorial boundaries". ראו Federal Ministry of the Interior, *Cyber Security Strategy for Germany* 2 (2011)

17 באסטרטגיה להגנת מרחב הסייבר משנת 2011 הוגדר מרחב הסייבר כך: "Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also other information systems that support our business, infrastructure and services". ראו The UK Cyber Security Strategy, *Protecting and Promoting the UK in a Digital World* 10 (2011)

בהחלטת ממשלת ישראל משנת 2011 הוגדר מרחב הסייבר כ"המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה".[18]

המושג סייבר שולב במטפורות שונות ששימשו לאורך השנים בעיקר כדי לפשט אותו ולהשוות את האתגרים בתחום הסייבר לאתגרים בתחומים אחרים, שמקבלי ההחלטות מכירים ומנוסים בתמודדות איתם ובאסדרתם.[19] כך, המטפורה "מרחב הסייבר" (cyberspace) שטבע גיבסון בספרו משנת 1984[20] יצרה השוואה **בין רשת האינטרנט למקום פיזי**, ולמעשה אפשרה להחיל נורמות וחוקים המאסדרים את התנהגותם של הפרטים בעולם הפיזי על התנהגויותיהם ברשת האינטרנט.[21] ההבנה של מרחב הסייבר כאוסף של מערכות מידע מקושרות, מוסדות חברתיים ושחקנים מהעולם הלא וירטואלי, המקושרים ומתקשרים זה עם זה באופנים שונים, מתבטאת יפה במטפורת ה"סייבר אקוסיסטם" (cyber ecosystem), המשווה בין מרחב הסייבר למערכת אקולוגית דינמית המורכבת ממשתתפים מגוונים המקושרים זה לזה בדרכים שונות.[22]

באופן הפשטני ביותר, מושג הסייבר הוא מטפורה המתארת מרחב וירטואלי שהיקפו זהה לזה של רשת האינטרנט, אותה רשת פיזית המחברת בין רשתות שונות של מחשבים ושרתים ומאפשרת תעבורת מוצרי מידע ביניהם באופן גלובלי. כל פעולה המתבצעת על גבי רשת האינטרנט – שליחת דואר אלקטרוני, השתתפות במשחק משותף על גבי רשת האינטרנט או ביקור באתר אינטרנט –

18 החלטה 3611 של הממשלה ה־32 "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.2011).

19 Hsu, **לעיל** ה"ש 3, בעמ' 15; Lapointe, **לעיל** ה"ש 3; CISA, *Enabling Distributed Security in Cyberspace* (March 23, 2011); Jada F. Smith, *Cyberattack Exposes I.R.S. Tax Returns*, The New York Times (May 26, 2015)

20 Gibson, לעיל ה"ש 13.

21 Gozzi, **לעיל** ה"ש 3; Adams, **לעיל** ה"ש 3; Cohen, **לעיל** ה"ש 3; Elkin-Koren & Salzberger, **לעיל** ה"ש 3, בעמ' 20–22.

22 Lapointe, **לעיל** ה"ש 3, בעמ' 2.

מתרחשת גם במרחב הסייבר. כפי שספר הוא אמצעי להעברת מידע מהמחבר לקורא, כך רשת האינטרנט היא פלטפורמה להעברת מידע בין שני מחשבים או בין מחשב לשרת. כאשר הקורא קורא את הספר הוא מדמיין בעיני רוחו את הסיפור ויוצר מעין מציאות וירטואלית שבה הסיפור מתרחש. באופן הפשטני ביותר אותה מציאות וירטואלית משולה למרחב הסייבר.[23]

לאורך השנים הורחבה משמעות המושג במסמכי מדיניות שונים, ועתה היא חורגת מגבולות המושג "רשת האינטרנט" או "המרחב הווירטואלי" לבדו. מרחב הסייבר כולל, לפי הגדרות אלו, את רשת האינטרנט כפלטפורמה המרכזית להעברת מידע ונתונים ממקום למקום, אך הוא אינו משקף אך ורק את הממד הווירטואלי של אותן העברות. מרחב הסייבר כולל מגוון מערכות, לצד רשת האינטרנט, המתקשרות זו עם זו ומשמשות להעברת נתונים ומידע, ואינן מוגבלות בשל אילוצים פיזיים או גבולות גיאוגרפיים. הבנת המשמעות הרחבה של המושג "מרחב הסייבר" חשובה להבנת ההשלכות שעשויות להיות למהלכי אסדרה מדינתיים שונים, ויש לתת עליהן את הדעת בטרם אימוץ אמצעי אסדרה.

23 *The Difference Between Cyberspace & The Internet*, Cyber Security Intelligence (May 22, 2017)

פרק 2

המאפיינים הייחודיים של מרחב הסייבר

למרחב הסייבר מאפיינים ייחודיים שבגללם הוא נתפס כמרחב פעולה חדש, לצד מרחבי הפעולה ה"מסורתיים" המוכרים לנו בהיבטים של תנועה ושל שימוש בכוח: היבשה, הים, האוויר והחלל. הבנת מאפיינים ייחודיים אלו חיונית לשם התוויית כיווני חשיבה בנוגע לאסדרת ההגנה על מרחב זה.[24]

א. ממד הזמן וקצב ההתקדמות במרחב

התנועה במרחב הסייבר מתרחשת באמצעות העברת סיביות בין ישויות דיגיטליות. סיביות הן יחידות הנתונים הבסיסיות של מחשבים וקצב התקדמותן יכול להיות קרוב למהירות האור – מהירות הגבוהה עשרות מונים מזו של העברת מידע, אנשים או תחמושת באמצעים שהיו נהוגים בעבר. בדרך זו אפשר להעביר מידע מקצה אחד של העולם לקצהו השני במהירות בלתי נתפסת ובעלות נמוכה יחסית בהשוואה למשך הזמן והעלות של פעולה צבאית, כגון הנעת ספינות על פני הים. שלא כמו הריסה פיזית של מפעל, במרחב הסייבר אפשר למחוק מאגר נתונים של ארגון תוך דקות בודדות.

ב. טשטוש גבולות גיאוגרפיים

על פי רוב שיקולי מרחק גיאוגרפי אינם רלוונטיים במרחב הסייבר, ומרחק של אלפי קילומטרים מתגמד לשניות בודדות של העברת הסיביות דרך סיבי האינטרנט התת־ימיים באוקיינוסים.[25] ביצוע פעולה במרחב הסייבר מחייב מחשוב וידע טכנולוגי, אולם אינו דורש בהכרח גישה פיזית אל המטרה. האקר המתגורר בעיר קטנה בצפון קוריאה ורוצה להשתמש בכרטיס האשראי של

24 לדיון באסדרה של הגנת מרחב הסייבר ראו אריאל הרשקוביץ ושוורץ אלטשולר, **לעיל** ה"ש 8.

25 Daniel, **לעיל** ה"ש 7.

גברת עשירה בלונדון, או מדינה שרוצה לפגוע בתשתיות של מדינה אחרת המרוחקת ממנה אלפי קילומטרים, יכולים להגיע אל יעדם בקלות. במרחבים אחרים, להאקר הקוריאני כנראה לא היה הממון הדרוש כדי להגיע לאנגליה או היכולת לפרוץ לדירתה של הגברת העשירה בלונדון; את התקיפה שהמדינה הייתה מתכננת היו מגלים כנראה בדרך הארוכה אל היעד באוויר או בים.

ג. העלות הנמוכה של פעילות במרחב הסייבר

פעולה במרחב הסייבר, שעשויות להיות לה השלכות מרחיקות לכת, אינה מחייבת תשתית מדינתית או תקציב גדול, ואפשר לבצעה במחיר נמוך יחסית באמצעות מחשב אישי או קנייה של שירותי תקיפת סייבר מחברות פרטיות. בניגוד למלחמה הקרה, שבה היכולות הצבאיות והטכנולוגיות פותחו בידי שתי מעצמות שהיו להן המשאבים לכך, היום יש לגורמים רבים מאוד – מעל מאה מדינות, כמו גם יחידים וארגונים תת־מדינתיים רבים מספור – יכולות תקיפה נרחבות במרחב הסייבר,[26] והשיח על שליטה ודומיננטיות של מדינות בודדות במרחבים שלמים, כגון ים ואוויר, כבר אינו רלוונטי כפי שהיה.[27]

ד. טשטוש העקבות הדיגיטליים

מרחב הסייבר מאפשר טשטוש של העקבות הדיגיטליים בעזרת אמצעי הצפנה והתממת זהות התוקפים, באופן המקשה על זיהוי חד־משמעי מהיר של מבצעי הפעולה. עם זאת, יש להודות כי חשיבותו של מאפיין זה תלך ותפחת ככל שמרחב הסייבר יכלול יותר ויותר פרטי מידע, כיוון שהצלבתם של פרטי המידע השונים תאפשר זיהוי של אנשים ותבניות מתקפה תוך הסרת מעטה האנונימיות מעל תוקפים או יחידים.

26 Fergus Hanson, *Waging (Cyber)war in Peacetime*, Brookings (Oct. 22, 2015)

27 Joseph S. Nye, Jr., *Cyber Power* (Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010)

שיטות מקובלות לטשטוש העקבות הדיגיטליים הן למשל שימוש בדפדפנים מוצפנים, כגון דפדפן TOR, ותקיפת מחשבים תמימים ושימוש בהם כשלוחים (proxies) או כשרשראות של שלוחים: כל מחשב משמש כשער גישה למחשב הבא בשרשרת עד שהתוקף מגיע באמצעותם למחשב המטרה לשם ביצוע מתקפת הסייבר. כדי לאתר את התוקף יש לעבור את שרשרת השלוחים שבה עשה שימוש ולזהות שמדובר במחשבים תמימים שהופעלו בידי תוקף.[28]

נכון לעכשיו, המאמצים להשגת אמצעים וכלים דיגיטליים, הן עבור מדינות והן עבור הציבור הרחב, במטרה להעלים או לחשוף עקבות דיגיטליים בצורה יעילה, נמצאים בעיצומם.[29]

ה. היפר־קישוריות (hyperconnectivity)

"היפר־קישוריות" היא היכולת של המרכיבים השונים של מרחב הסייבר – השחקנים (מדינות, חברות פרטיות קטנות, תאגידי ענק, ארגונים שלא למטרות רווח, יחידים, ארגוני פשע, ארגוני טרור) והמכשירים (מכשירים דיגיטליים כגון מחשבים וטלפונים חכמים, וכן יישומים ותוכנות) – לתקשר אלה עם אלה באופנים מגוונים וברמות שונות ולהעביר ביניהם כמויות עצומות של מידע.

האינטרנט של הדברים (IoT) הוא אחת הדוגמאות של ההיפר־קישוריות: מכשירים מסורתיים, כגון מקרר, מזגן, שעון יד, תנור, מצלמת אבטחה, תרמוסטט

28 Josh Chin, *Cyber Sleuths Track Hacker to China's Military*, The Wall Street Journal (Sep. 23, 2015); *Hacking the Hacker: Attribution of Cyber Attacks*, Synergia Foundation (Oct. 4, 2020)

29 Stuart A. Thompson & Charlie Warzel, *One Nation, Tracked*, The New York Times (Dec. 19, 2019); James Orenstein, *I'm a Judge. Here's How Surveillance Is Challenging Our Legal System*, The New York Times (June 13, 2019)

או מכונית, הופכים למכשירים האוספים ושומרים מידע ואף מעבירים אותו אל מוחות מרכזיים,[30] ואפשר לזהותם ולשלוט בהם מרחוק.

הוספת חיישנים מקושרים למוצרים רבים, או אפילו לכל המוצרים (לכן האינטרנט של הדברים מכונה לעיתים "האינטרנט של כל דבר"), אומנם מאפשרת נוחות והתייעלות, אך גם מגבירה את הסיכון לשימוש במכשירים אלו כפלטפורמה למתקפות סייבר למטרות שונות, לרבות לשם סחר במידע אישי. ככל שיותר שירותים, מערכות מידע ומוצרים מקושרים זה לזה ומסוגלים לקלוט ולהעביר מידע זה מזה ומהסביבה, כך קל יותר למתקפת סייבר, שהיא כשלעצמה תוכנת מחשב, להתפשט במהירות, להגיע למספר גדול של מערכות, שירותים ותשתיות ולגרום נזק חמור.[31] כאשר המכשירים החכמים מוטמעים בשירותים שמספקים גורמי רפואה במערכת הבריאות, מתקפות סייבר עשויות לסכן את ביטחון הציבור ולא רק כל פרט בפני עצמו. כך, למשל, מתקפת סייבר על בית חולים בארצות הברית לא אפשרה שימוש במערכות ממוחשבות לשם מתן שירות, והובילה להפניית כל הטיפולים הלא דחופים לבתי חולים אחרים. יכולתו של בית החולים להעניק שירותים רפואיים לקהילה באזור נפגעה קשות;[32] מתקפות סייבר על מכשירים חכמים המובילות לחשיפת מידע רפואי רגיש ואף למסחר בו עלולות לפגוע מאוד באמון הציבור בנותני השירות הרפואי מתוך תפיסה שהשירות אינו מאובטח דיו, ואף להביא להימנעות מפנייה לקבלת טיפול רפואי. בשל כך עשויה להיפגע מאוד היעילות והשמישות של השירות

30 Rolf H. Weber, *Internet of Things: New Security and Privacy Challenges*, 26 Comp. L. & Sec. Rev. 23, 23 (2010); Francis daCosta, Rethinking the Internet of Things: A Scalable Approach to Connecting Everything 3-5 (2013); Vijay Madisetti & Arshdeep Bahga, Internet of Things (A Hands-on Approach) 19-22 (2014); Michael E. Porter & James E. Heppelmann, *How Smart, Connected Products Are Transforming Competition*, Harv. Bus. Rev. (Nov. 2014); Samuel Greengard, The Internet of Things (2015); Tatiana Tropina, *Public-Private Collaboration: Cybercrime, Cybersecurity and National Security*, *in* Self- and Co-regulation in Cybercrime and National Security 1 (2015)

31 Madisetti & Bahga, **לעיל** ה"ש 30, בעמ' 19–22; daCosta, **לעיל** ה"ש 30, בעמ' 3–5; Greengard, **לעיל** ה"ש 30; Weber, **לעיל** ה"ש 30, בעמ' 23.

32 Justin Snair, *Risks of Cyber Attacks on Healthcare Sector Leave Public Health of Communities Vulnerable*, Naccho Voice (Oct. 24, 2013)

הרפואי, אשר יפגעו בציבור בכללותו; מתקפת סייבר המשבשת את זמינות מוקדי החירום עלולה לשבש או להשבית לחלוטין אספקה של שירותי חירום רפואיים לאורך זמן וכך לפגוע בחלקים נרחבים מהציבור; יתרה מכך, מגפת הקורונה הובילה להכרה בחיוניות מערכת הבריאות ולהגדלת תלות הציבור והממשל בתפקודה התקין. בנסיבות אלו מתקפת סייבר על שירותי הבריאות עלולה להוביל לפאניקה בציבור, לפגיעה באמון הציבור בממשל ולערעור יציבות השלטון.[33]

לדוגמה, חברת האבטחה פרופפוינט (Proofpoint) זיהתה שמתקפת סייבר בינלאומית שהתרחשה ב־2013 בוצעה באמצעות למעלה מ־100,000 מכשירי חשמל ביתיים חכמים, כגון טלוויזיות, רמקולים, מקררים ונתבי תקשורת. המכשירים הפכו לרשת בוט־נטים (bot-nets), כלומר לרשת של מערכות מחשב שנשלטות מרחוק על ידי האקרים.[34] המכשירים הללו שלחו יותר מ־750,000 מסרי דואר אלקטרוני זדוניים.[35]

בשנת 2015 הצליח צמד חוקרי אבטחה לפרוץ למערכות של מכונית מסוג קרייזלר, ולשלוט לא רק במערכות מיזוג האוויר או הרדיו במכונית אלא גם במנוע ובבלמים.[36] עקב כך הכריזה חברת פיאט־קרייזלר על "ריקול" לכ־1.4 מיליון כלי רכב מתוצרתה.[37] בשנת 2016 פרסמו חוקרים מקנדה וממכון ויצמן

33 Daniel J. Barnett et al., *Cyber Security Threats to Public Health*, 5 World Med. & Health Policy 37 (2013); Naresh Persaud, *Security and Access Management*, CSO Online (Dec. 22, 2017); Alex Berezow, *Cyberattacks as a Public Health Threat* (American Council on Science and Health, Oct. 28, 2020)

34 Kaspersky *What is a Botnet?*. להרחבה בנוגע לבוט־נטים ולשימוש אפשרי בהם ראו הטקסט הנלווה להערות שוליים 92–94, 169–176.

35 *Proofpoint Uncovers Internet of Things (IoT) Cyberattack*, Proofpoint (Jan. 16, 2014)

36 Nicole Perlroth, *Security Researchers Find a Way to Hack Cars*, The New York Times (July 22, 2015)

37 Aaron M. Kessler, *Fiat Chrysler Issues Recall Over Hacking*, The New York Times (July 25, 2015)

כי הצליחו לתקוף נורות "חכמות", להפיץ את הווירוס התוקף מנורה לנורה ולשלוט על כיבוין והדלקתן.[38]

מתקפת הסייבר המפורסמת ביותר עד כה על מכשירים חכמים בוצעה באוקטובר 2016 באמצעות עשרות אלפי מכשירי חשמל ביתיים חכמים, כגון נתבים, מקליטי וידיאו דיגיטליים (DVR) ומצלמות אבטחה חכמות, שמשתמשיהם לא החליפו את סיסמאות האבטחה של היצרן. התוקפים ניצלו חולשה זו והפכו את כלל המכשירים לצבא שלם של בוט־נטים אשר יצרו יחד מתקפת מניעת שירות מבוזרת (DDoS) רבת משתמשים, שהתמקדה בחברת Dyn המספקת מערכת שמות מתחם (Domain Name System, DNS) לאתרים רבים ברשת האינטרנט. מטרתה של מתקפת מניעת שירות היא למנוע מהמערכות המותקפות לתפקד באופן תקין ולספק את השירות שהן אמורות לספק.[39] ואכן, עקב המתקפה הושבתה למשך יום שלם פעילותם של 85 מהאתרים הגדולים בעולם, כגון נטפליקס, טוויטר, פייפאל וסוני. בעלי מכשירי החשמל הביתיים החכמים כלל לא ידעו כי המכשירים מעורבים במתקפה כלשהי, מאחר שהמכשירים תפקדו כהלכה.[40]

38 Eyal Ronen et al., *IoT Goes Nuclear: Creating a ZigBee Chain Reaction*, 16 (1) IEEE Security & Privacy 54 (2018)

39 להסבר על מתקפת מניעת שירות ראו "מהן מתקפות מניעת שירות מבוזרות (DDoS)" **מערך הסייבר הלאומי** (16.5.2017).

40 Brian Solomon, *Hacked Cameras Were Behind Friday's Massive Web Outage*, Forbes (Oct. 21, 2016)

פרק 3

היעדר תמריצים מספקים להגנת סייבר

משבר הגנת הסייבר וההתפרצות של מתקפות סייבר בשנים האחרונות נובעים בראש ובראשונה מהעלייה החדה בשימושים הדיגיטליים בעולם. ואולם, הסבר נוסף לכך הוא שבתעשיית התוכנה, החומרה, המוצרים והשירותים הטכנולוגיים המתנהלת במרחב הסייבר לא הושקעו די משאבים בפיתוח של מוצרים ושירותים מאובטחים, בשל כשלי שוק המובילים לתמריצים נמוכים להשקעה מסוג זה. בחלק זה נמפה את כשלי השוק האלה כדי להבין את הצורך בהתערבות מדינתית לשם התמודדות עימם ופתרונם.

א. סוחרי מידע (data brokers) ונושאי מידע

רוב שווקי התעשייה הדיגיטלית כיום הם שווקים המכונים "דו־צדדיים". בשווקים אלה פועלים תאגידים המעניקים שירותים או מוצרים למשתמשים בצד אחד, לרוב בחינם, ומוכרים את "זמן המסך" של המשתמשים או מידע על התנהגותם של המשתמשים לסוחרי מידע ולמפרסמים בצד השני. סוחרי המידע מוכרים את המידע האישי – מזוהה ושאינו מזוהה – ללקוחות שונים כגון מפרסמים, מכוני מחקר וחברות ביטוח. אם כן, למי נאמנים התאגידים בשווקי התעשייה הדיגיטלית? האם למשתמשים ולמידע עליהם, או שמא למפרסמים ולסוחרי המידע, שהם מקור ההכנסה שלהם? הואיל והתשובה היא כמובן האפשרות השנייה, נוצרה כלכלת מידע שבה תאגידים רבים המספקים שירותים שונים (כגון מנוע חיפוש, רשת חברתית או דואר אלקטרוני) מחזיקים וסוחרים בכמויות עצומות של מידע אישי על יחידים, בדרך כלל ללא ידיעת נושאי המידע עצמם ומבלי שאלו יכולים לשלוט במידע הנאסף אודותיהם ובמסחר בו.[41] כשל השוק

41 על פי הערכות פועלות בארצות הברית 2,500–4,000 חברות הסוחרות במידע – data brokers. ראו Paul Boutin, *The Secretive World of Selling Data About You*, Newsweek (May 30, 2016); Ramona Pringle, *"Data is the New Oil": Your Personal Information Is Now the World's Most Valuable Commodity*, CBC News (Aug. 25, 2017); Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, Wired (Feb. 15, 2019)

נוצר בשל הצירוף בין הנאמנות של הכלכלה הדיגיטלית למפרסמים ולסוחרי המידע ובין ידיעת התאגידים שרוב ציבור המשתמשים, נושאי המידע, אינו מבין את משמעות איגום המידע עליו; אינו לקוח ישיר של סוחרי המידע; ואינו יכול תמיד להפסיק להשתמש בשירותיהם. לכן, למעשה אבטחת מידע, מניעת דליפה שלו והגנה על נושאי המידע אינן צעד משתלם כלכלית עבור אותן חברות.[42]

ב. מורכבות הפרויקטים והמרוץ להיות ראשון בשוק

כתיבת תוכנה היא פעולה מורכבת שמבוצעת על ידי מספר רב של מתכנתים העובדים בשיתוף פעולה ובמהירות. בשל מספר המתכנתים המעורבים בכתיבת התוכנה וקצב עבודתם המהיר, ניהול סיכוני אבטחה במערכות מידע הוא משימה קשה וגוזלת משאבים התלויה גם בעלות של הוספת רכיבי אבטחה ושל אחסון מוגן ומבוקר של מידע.[43] כמו כן, המרוץ להשגת דומיננטיות בשוק גובר לעיתים על ההתייחסות לאבטחת מידע. כך נוצר מצב של "התקדמות עכשיו והתנצלות אחר כך", כלומר רק לאחר שמוצר זוכה בנתח שוק משמעותי מוטמעות בו תוספות של אבטחה. משום כך, במרחב הדיגיטלי קיימות תוכנות רבות אשר רמת האבטחה ההתחלתית שלהן אינה מספקת, ומשתמשיהן אינם מודעים להכרח בהתקנת תיקוני תוכנה ועדכוני תוכנה הכוללים פעמים רבות עדכוני אבטחה חשובים.[44]

42 עם כניסתן לתוקף של התקנות החדשות של האיחוד האירופי בדבר הגנת מידע במאי 2018 (EU General Data Protection Regulation 2016/679; להלן: GDPR) התעוררה השאלה אם סוחרי מידע יכולים לעמוד בדרישות התקנות. ראו למשל Amit Katwala, *Forget Facebook, Mysterious Data Brokers are Facing GDPR Trouble*, Wired (Nov. 8, 2018)

43 Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems (2001)

44 האִמרה המוכרת בהקשר זה היא: "Ship on Tuesday and get it right by version 3"; וראו Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 Science 610, 611 (2006); Sabyasachi Mitra & Sam Ransbotham, *Information Disclosure and the Diffusion of Information Security Attacks*, 26 Inf. Sys. Res. 565, 567-568 (2015)

ג. החצנות שליליות (negative externalities)

החצנות שליליות הן העלויות או ההשלכות השליליות של פעולה מסוימת המוטלות על גורמים אחרים, חיצוניים למבצע הפעולה עצמה. במרחב הסייבר החצנות שליליות הן גורם נוסף להיעדר תמריצים מספקים לאבטחת מידע: ארגונים העושים שימוש בתשתיות מידע שאינן מאובטחות כראוי אינם נושאים בעצמם או לבדם במלוא ההשלכות של מעשיהם.[45] מוצר תוכנה שאינו מאובטח עלול לאפשר מתקפת סייבר רחבת היקף, אך המשתמש במוצר, המפתח שלו או המפיץ שלו אינם נפגעים מכך או נפגעים קלות בלבד.[46] לכן, הסיכון הגלום באי־השקעה באבטחת מידע אינו נתפס כגבוה בעיני מנהלי חברות, ובבחירה בין השקעה באבטחת מידע ובין נשיאה מודעת בסיכון וחיסכון במשאבים, הם יעדיפו על פי רוב לחסוך. גם משתמשי הקצה לרוב אינם נושאים בעלויות מתקפת הסייבר המבוצעת תוך שימוש במוצר התוכנה או החומרה הלא מוגן שבבעלותם, ולכן אין להם כל תמריץ לרכוש תוכנת הגנת סייבר ולהתקין אותה על המכשיר, או אפילו לשנות את סיסמת הגישה הגנרית אליו. למשל, בשנת 2016 השתמשה מתקפת הסייבר המכונה Mirai במכשירי אינטרנט של הדברים, כמו מצלמות רשת ונתבי רשת, כצבא בוט־נטים במתקפת מניעת גישה. המשתמשים במכשירים הנגועים לא ניזוקו כלל ואפילו לא היו מודעים לשימוש המזיק שנעשה במכשיר שברשותם.[47]

ד. א־סימטריה במידע בין מפתחים ומשתמשים

הואיל ומשתמשים אינם יכולים לרוב להעריך את רמת האבטחה של מוצר תוכנה או מוצר הגנה שהם רוכשים, נוצר מה שמכונה בספרות "שוק לימונים" – שוק

45 Pascal Brangetto & Mari Kert-Saint Aubyn, *Economic Aspects of National Cyber Security Strategies* (Project Report, CCDCOE, 2015)

46 שם.

47 Michel van Eeten, *Patching Security Governance: An Empirical View of Emergent Governance Mechanisms for Cybersecurity*, 19 Digital Policy, Regulation and Governance 429, 434, 439–441 (2017)

שבו הצרכנים אינם יודעים להעריך את ההבדל בין מוצרים שונים. בשוק כזה התמריצים לפתח ולשווק מוצרי תוכנה הכוללים רכיבי אבטחת מידע נמוכים.[48]

ה. א־סימטריה במידע בין תוקפים ובין המבקשים להגן על מרחב הסייבר

ביצוע תקיפת סייבר מוצלחת דורש איתור וניצול של חולשה אחת במערכת מידע, שדרכה אפשר להשיג גישה לא מורשית למערכת. מרגע השגת הגישה התוקף יכול להשתמש בה לצרכים שונים: גרימת נזק פיזי, מניעת גישה למידע, שינוי, העתקה או מכירה של המידע או שימוש בו לצרכיו.

מנגד, מפתחי מערכות להגנת מרחב הסייבר אינם מחזיקים במידע על הפגיעה המתוכננת ועליהם להשקיע משאבים כספיים ואנושיים רבים באיתור חולשות במערכות המידע ובהגנה מפני כלל הפגיעות האפשריות. כך נוצרים חסמי כניסה נמוכים עבור תוקפים לעומת עלויות הגנה גבוהות. תופעה זו מועצמת משום שאפשר לנצל חולשות ולפתח נוזקות על בסיס כלי תקיפה קיימים שכבר עבדו בהצלחה בעבר.[49] עם זאת, יש לסייג את האמור ולהדגיש כי העלויות הכרוכות במימוש מתקפת סייבר ובהגנה מפניה תלויות בגורמים נוספים, כמו המבנה הארגוני של התוקף ושל המגן; אופי התעשייה הספציפית; המטרה של המתקפה ומטרת ההגנה; איכות המערכות המותקפות; ונכונות מפתחי התוכנה או המערכת המותקפת לספק למשתמשים בה עדכוני תוכנה (patches) כדי לתקן את החולשה שנתגלתה בה ולמנוע את ניצולה.[50]

48 Anderson & Moore, **לעיל** ה"ש 44, בעמ' 610–611.

49 למשל, אנו עדים לשוק משגשג של ניצול חולשות zero-day ברשת האפלה – אלו חולשות שטרם פותח עבורן עדכון אבטחה מתאים ושימוש בהן מאפשר גישה לא מורשית למערכות בהסתברות גבוהה.

50 Rebecca Slayton, *What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment*, 41 (3) Int'l Sec. 72 (2017)

פרק 4

מהי מתקפת סייבר

ברמה הפשטנית ביותר מתקפת סייבר היא פעילות בתוך מרחב הסייבר או באמצעותו שמטרתה להזיק לגורם המותקף[51] באמצעות ניצול חולשה (vulnerability) בפלטפורמה טכנולוגית כלשהי. החולשה מאפשרת רמות שונות של גישה לא מורשית למערכת מידע, ובאמצעותה התוקף יכול לבצע פעולות שונות בהתאם לאינטרסים שלו ולמערכת היחסים שלו עם הגורם המותקף.

א. מהי חולשה?

חולשה היא פרצה טכנולוגית או זיהוי התנהגות בלתי צפויה של מערכת המחשוב, המאפשרת לתוקף פוטנציאלי לקבל גישה למערכת או לבצע בה פעולות שלא אמורה להיות לו הרשאה לביצוען. "איכותה" של חולשה נמדדת ברמת ההרשאות המתקבלת עקב ניצולה. מערכת הפעלה שלא הותקנו בה עדכוני אבטחה או מערכת הפעלה המאפשרת בשוגג לכל משתמש להתחבר אליה מרחוק ללא צורך בסיסמה הן דוגמאות לחולשות שאפשר לנצל לקבלת גישה לא מורשית למערכת המחשב העושה שימוש במערכות הפעלה אלו. כך, למשל, במתקפת הסייבר NotPetya בשנת 2017 נעשה שימוש במרחב הסייבר כדי לפגוע בתשתיות ובשירותים בעולם הפיזי. המתקפה גרמה, בין השאר, לשיתוק מערכות המחשב של חברת השילוח הבינלאומית מרסק (Maersk), שבעטיו נוצרו פקקי ענק בכניסה לנמלים ימיים בארצות הברית ובמדינות אחרות, מזון שהובל במכולות בלב ים התקלקל וחברות רבות לא קיבלו את הסחורה שלה המתינו. עקב כך נגרם עיכוב בביצוע פרויקטים אחרים. חברות העוסקות בשיווק ומכירה של מוצרי צריכה בכל העולם ספגו הפסדים כבדים.[52] אחד הגורמים להצלחתה של NotPetya היה השימוש במערכת הפעלה

51 שמואל אבן ודוד סימן טוב **לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל** (מזכר 109, המכון למחקרי ביטחון לאומי 2010).

52 Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired (Aug. 22, 2018) (להלן: Greenberg, *The Untold Story*).

"חלונות" משנת 2000 ברוב המחשבים של חברת מרסק. מיקרוסופט לא תמכה במערכת הפעלה זו זה כמה שנים, ועל כן המערכת נותרה ללא עדכוני אבטחה.[53]

מקובל להבחין בין חולשות שנחשפו ושמפתחי התוכנה הוציאו עדכון אבטחה המונע את ניצולן, ובין אלו המכונות חולשות "יום אפס" (zero-day): חולשות שנחשפו אולם אין עדיין עדכון אבטחה המתאים למניעת ניצולן. לרשות מפתחי התוכנה עומדים למעשה אפס ימים לפתח עדכון שכזה בטרם תנוצל החולשה למטרות זרות.[54] עם זאת, רק 5% מחולשות יום אפס שמתגלות בשנה מנוצלות לרעה; חברת מיקרוסופט מובילה במספר החולשות המנוצלות על ידי האקרים, אחריה לינוקס, ושלישית ברשימה ניצבת אפל.[55]

מרבית החולשות המנוצלות למטרות תקיפת סייבר אינן חולשות יום אפס, שכן איתורן דורש מאמץ והשקעה ניכרת של משאבים כלכליים ואנושיים. מרבית התוקפים מעדיפים להימנע מהשקעה זו ולנסות לנצל דווקא חולשות ידועות, אלו שחברות התוכנה הוציאו להן עדכוני אבטחה. תקיפת סייבר המנצלת חולשה ידועה מתאפשרת מכיוון שמרבית המשתמשים, אנשים פרטיים וארגונים, נוטים שלא להטמיע במהירות עדכוני תוכנה, לרבות עדכונים קריטיים.[56] מומחי אבטחת מידע טוענים כי בממוצע חולפת לפחות שנה מרגע הוצאת עדכון אבטחה על ידי חברת תוכנה ועד להטמעת העדכון בארגון.[57]

מספר החולשות המתגלות בכל שנה הולך ועולה. בשנת 2018 נקבע שיא של 16,555 חולשות באבטחת מערכות מחשב שנחשפו במהלך השנה, כ־45

53 שם.

54 *Zero-Day Vulnerability: What It Is, And How It Works*, Norton (Aug. 28, 2019)

55 Lillian Ablon & Andy Bogart, Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits (RAND Corporation, 2017)

56 להרחבה על חלקו של הגורם האנושי ראו פרק 6.

57 Roger A. Grimes, *Zero-Days Aren't the Problem – Patches Are*, CSO Online (June 1, 2016); Natasha Turak, *The Next 9/11 Will Be a Cyberattack, Security Expert Warns*, CNBC (June 1, 2018); Suzanne Widup et al., 2018 Verizon Data Breach Investigations Report 50 (2018)

חולשות בממוצע ליום, לעומת 14,712, כ־40 חולשות ליום, בשנת 2017.[58] 80% ממתקפות הסייבר במחצית הראשונה של 2020 ניצלו חולשות שדווח עליהן כבר בשנת 2017 או קודם לכן. יתרה מכך, למעלה מ־20% מהמתקפות ניצלו חולשות בנות 7 שנים ויותר.[59]

ב. ניצול (exploit) ונוזקה (malware)

ניצול (exploit) הוא מונח מקובל בתחום מדעי המחשב והגנת מרחב הסייבר לתיאור השלב במתקפת סייבר שבו מופעל במחשב המותקף קטע הקוד שמטרתו לנצל את החולשה שהתגלתה כדי להשיג הרשאות גישה לא מורשות למערכת הממוחשבת שהתוקף מבקש לתקוף. הרשאות הגישה מאפשרות את המשך התקיפה, שכן בעזרתן התוקף יכול להתקין בתוך המערכת הממוחשבת את שאר הנוזקה (malware), שהיא תוכנת המחשב הזדונית המשמשת אותו להשגת מטרתו – שיבוש, איסוף או העתקה של מידע, ואף המשך הפצת הנוזקה למערכת נוספת.

ג. איך נראית מתקפת סייבר?

מקובל לתאר את האופן שבו מתנהלת מתקפת סייבר באמצעות מודל של שבעה שלבים המכונה "שרשרת ההרג" (kill chain),[60] כמפורט להלן:[61]

58 *Number of Common IT Security Vulnerabilities and Exposures (CVEs) Worldwide from 2009 to 2018*, Statistica (2019)

59 Check Point Research, Cyber Attack Trends: 2020 Mid-Year Report 19 (2020) (להלן: מגמות תקיפת סייבר 2020).

60 מודל שרשרת ההרג (kill chain) פותח על ידי חברת לוקהיד מרטין כדי לחקור ולהבין את השלבים השונים בתקיפות סייבר. ראו *The Cyber Kill Chain*, Lockheed Martin

61 Darren Death, *The Cyber Kill Chain Explained*, Forbes (Oct. 5, 2018)

תרשים 1
שלבי שרשרת ההרג (kill chain)

מקור: התרשים מבוסס על תרגום תרשים שרשרת ההרג שהוצג במקור על ידי חברת לוקהיד מרטין. ראו *The Cyber Kill Chain*, ה"ש 60.

השלב הראשון – איסוף מודיעין (reconnaissance)

בשלב זה התוקף בוחן את הארגון שהוא מבקש לתקוף ואוסף עליו את מרב המידע האפשרי, לרבות סוג הארגון, אופן פעולתו והפלטפורמות שבהן הוא עושה שימוש. מטרת שלב זה היא לאתר חולשות, למשל שימוש בתוכנה ללא עדכוני אבטחה או עובד בארגון המוריד למחשבי הארגון קבצים הנשלחים אליו ממקור לא מזוהה בדואר אלקטרוני.

השלב השני – חימוש (weaponization)

בשלב זה התוקף מכין את הנוזקה (malware) שבה הוא רוצה להשתמש בהתאם לחולשות שאיתר בשלב הראשון. התוקף יכול להשתמש בנוזקה מוכנה או לשנות נוזקה מוכנה לצרכיו, או להכין נוזקה חדשה מאפס. תהליך שכזה יכול לקחת ימים עד שנים, בהתאם למטרת התקיפה.

השלב השלישי – הפצה (delivery)

בשלב זה התוקף משלח את הנוזקה שפיתח או רכש בשלב השני, בהתאם לאיסוף המודיעין ואיתור החולשות שביצע בשלב הראשון. שילוח הנוזקה יכול להיעשות באמצעות דואר אלקטרוני או אתר אינטרנט, וכן באמצעות מכשירים חכמים במסגרת האינטרנט של הדברים, כגון מוצרי חשמל חכמים ומכשירים לבישים המחוברים לאינטרנט. כך, למשל, אפשר להחדיר נוזקה באמצעות מדפסת המחוברת לרשת האינטרנט, טלפון חכם או שעון חכם.[62]

השלב הרביעי – ניצול (exploitation)

בשלב זה מופעל במחשב היעד קטע הקוד בנוזקה שנכתב במטרה לנצל את החולשה שהתגלתה בשלב הראשון של איסוף המודיעין, כדי לספק לתוקף הרשאות גישה בלתי מורשות ראשוניות.

השלב החמישי – התקנה (installation)

ברגע שניצול החולשה הסתיים בהצלחה והושגו הרשאות הגישה, הנוזקה מתקינה את עצמה במערכת הממוחשבת המותקפת ולעיתים אף מתחילה בהורדת תוכנות נוספות הדרושות לשם המשך הפעלתה.

השלב השישי – שליטה ובקרה (command and control, C2)

בשלב זה התוקף מתקין במערכת המותקפת "דלת אחורית" (backdoor), דהיינו קוד תוכנה המאפשר לו לחדור למערכת המותקפת תוך עקיפת אמצעי ההגנה המותקנים בה ומבלי להתגלות או לעורר חשד, ולשלוט בה מרחוק, לרבות

62 *Malware Attack Vectors: What to Expect in 2018*, LastLine (Dec. 6, 2017)

גישה לעומק המערכת המותקפת והעתקת מידע השמור בה, שינוי של המידע, חסימת הגישה אליו או הריסת המערכת כולה או חלקה.

השלב השביעי – פעולות להשגת מטרת התקיפה (actions on objectives)

בשלב זה התוקף מבצע את הפעולות הדרושות להשגת מטרותיו, כגון מחיקת קבצים, מניעת גישה אליהם, זריעת הרס במערכת הממוחשבת המותקפת, איסוף והעתקה של מידע מהמערכת, התפשטות למערכות אחרות המקושרות למערכת המותקפת או התקנת תוכנת מעקב וריגול העוקבת אחר המשתמש במערכת. תוכנה מסוג זה יכולה לעקוב אחר מסרים כתובים ומצולמים שהמשתמש שולח או מקבל, ואף לרגל אחר המשתמש באמצעות שימוש בחיישנים המצויים על גבי המכשיר עצמו, כגון חיישן GPS, ואף במצלמת המכשיר כאשר המערכת המותקפת היא מכשיר טלפון נייד.

יצוין כי מתקפת סייבר אומנם מתבצעת על פי השלבים שתוארו, אך היא דינמית: מרגע החדרת הנוזקה למערכת המחשב לשם ניצול החולשה שזוהתה התוקפים ממשיכים בעדכון הנוזקה ובשיפורה, לרבות חיפוש חולשות חדשות הניתנות לניצול, בתגובה לתיקוני אבטחה ולניסיונות מערכת המחשב המותקפת להדוף את ההתקפה.[63]

ד. יעדי מתקפת הסייבר

מחשבים אישיים הם יעד נפוץ למתקפות סייבר מפני שהם עוצבו ויוצרו בעיקר לפי שיקולים של נוחות המשתמש ופחות לפי שיקולי אבטחה. כמו כן, מותקנות בהם מערכות הפעלה בעלות יכולות התממשקות נרחבות אשר הופכות אותם לנוחים לשימוש מחד גיסא, אך גם לפגיעים למתקפות סייבר מאידך גיסא.[64] ככל

63 Check Point Research, Cyber Attack Trends: 2018 Mid-Year Report (2018) (להלן: מגמות תקיפת סייבר 2018).

64 Jethro Carr, *Attack Vectors on Personal Computers*, Jethro Carr (June 15, 2013)

שמערכת ההפעלה פופולרית יותר כך היא מהווה מטרה ליותר מתקפות סייבר, כלומר שיעור מתקפות הסייבר על מערכת הפעלה מסוימת מתוך כלל מתקפות הסייבר תואם את נתח השוק של אותה מערכת הפעלה.[65] משום כך, מערכת ההפעלה חלונות של חברת מיקרוסופט היא מערכת ההפעלה המותקפת ביותר. 51.08% מהנוזקות החדשות שפותחו ב־2018 התמקדו במערכת ההפעלה חלונות, 22.10% כוונו לדפדפני אינטרנט, 4.12% – למערכות הפעלה מבוססות אנדרואיד ו־22.7% מהנוזקות החדשות התמקדו במערכות הפעלה אחרות, כגון אפל אוינוקס. 74.49% מהנוזקות החדשות שפותחו ברבעון הראשון של 2019 התמקדו בתקיפת מערכת ההפעלה חלונות, 10.73% – בדפדפני אינטרנט, 2.77% כוונו למערכות הפעלה מבוססות אנדרואיד ו־12.01% – למערכות הפעלה אחרות.[66]

עם השנים גוברות מתקפות הסייבר המתמקדות במכשירי טלפון ניידים ומבוססות על נוזקות ואפליקציות בלתי רצויות פוטנציאליות (potentialy unwanted applications, מכונות גם "grayware", להלן: אפליקציות אפורות). אפליקציות אלה אינן זדוניות באופן ברור ואינן נחשבות לנוזקה או לווירוס מחשב, אולם הן עשויות להיות טורדניות ואף מזיקות – למשל אפליקציה למיטוב השימוש בסוללה, המבצעת לצד הפעולה הלגיטימית והרצויה שלה גם פעולה בלתי רצויה, כגון מעקב אחר התנהגות המשתמש ברשת האינטרנט או שליחת פרסומות למשתמש.[67] כ־1.87 מיליון אפליקציות אפורות פותחו למערכת ההפעלה אנדרואיד ב־2018, וכ־2.63 מיליון בשנת 2019. כמו כן, לפי דוח של חברת האבטחה צ'ק פוינט חלה עלייה ניכרת במספר הנוזקות המתמקדות באפליקציות בנקאיות ובאפליקציות תשלומים באמצעות מכשירים ניידים.[68]

65 *Adoption Rate and Popularity*, Kaspersky

66 AV-Test, Security Report 2018/19; *Operating Systems Most Affected by Malware as of 1st Quarter 2019*, Statistica (2019)

67 AV-Test, **לעיל** ה"ש 66; Norton Team, *What is Grayware?* Norton UK Blog

68 Check Point Research, Cyber Attack Trends: 2019 Mid-Year Report 7, 9 (2019) (להלן: מגמות תקיפת סייבר 2019).

במחצית הראשונה של שנת 2018 הופיעו גם נוזקות המותקנות עוד לפני מכירת מכשיר הטלפון החכם ללקוח הקצה. האקרים מצליחים לחדור לשרשרת הבנייה וההרכבה של המכשיר ולהבטיח כי נוזקה מתוחכמת מטעמם תופעל בו כבר עם רכישתו. למשל, נוזקת הבוט־נט RottenSys התחזתה לאפליקציית מערכת לשירות האינטרנט האלחוטי והצליחה לחדור לכמעט חמישה מיליון מכשירי אנדרואיד של חברות כגון וואווי, שיאומי וסמסונג.[69]

בנק המטרות של מתקפות סייבר צפוי לגדול בשנים הקרובות, ומעריכים כי הן יתמקדו לא רק במחשבים אישיים, בשרתים או במכשירי טלפון ניידים אלא גם במכשירי צריכה ביתיים ואישיים מסוג האינטרנט של הדברים ובתשתיות רשת – למשל באמצעות התחזות לספקי שירות VPN, המאפשר חיבור מאובטח לאינטרנט על גבי רשת ציבורית.[70]

מגפת הקורונה הובילה לעלייה בשימושים הדיגיטליים של הציבור – הן בצריכה של מוצרים והן בצריכה של מידע – ובמקביל ניכרת עלייה במתקפות הסייבר העושות שימוש באופני הפצה והדבקה שונים. כך, כבר בינואר 2020 התרחשה מתקפת סייבר שהשתמשה במסמכי תוכן הקשורים למגפת הקורונה לשם הפצת נוזקה; פותחו יישומונים למכשירי סלולר ונרשמו שמות מתחם רבים בנושאים הקשורים לנגיף הקורונה אשר שימשו בפועל להונאות ולהפצת נוזקות בשיטת הדיוג (phishing); וכן נצפתה עלייה חדה במתקפות הסייבר שכוונו כלפי פלטפורמות לתקשורת וידאו, כגון זום (Zoom).[71]

69 מגמות תקיפת סייבר 2018, **לעיל** ה"ש 63, בעמ' 5–6.

70 Kaspersky Security Bulletin 2019; *Advanced Threat Predictions for 2020*, Securelist (Nov. 20, 2019)

71 מגמות תקיפת סייבר 2020, **לעיל** ה"ש 59, בעמ' 5–6.

פרק 5

נוזקות והשימוש בהן במתקפות סייבר

א. נוזקה כשירות ושוק הסייבר ההתקפי

בשנים האחרונות אנו עדים להפיכת שוק פיתוח הנוזקות לשוק עסקי, שנעשות בו פעולות של הזמנה, אספקה, קנייה ומכירה. בדיוק כפי שאפשר לרכוש תוכנה כשירות (software as a service) אפשר לרכוש נוזקה כשירות (malware as a service). למעשה, מפתחי נוזקות הפכו לשכירי חרב המספקים שירותי פיתוח נוזקות, לרבות שירות תמיכת לקוחות וליווי במהלך השימוש בנוזקה. כך, המבקשים לבצע מתקפת סייבר יכולים לבצע למעשה מיקור חוץ של היכולות הטכנולוגיות הדרושות לתקיפה ובכך להתגבר על החסמים הטכנולוגיים העומדים בפניהם. נוזקות ומידע על חולשות הניתנות לניצול זמינים להורדה ולרכישה כשירות ברשת האפלה (darknet).[72] כפלטפורמה אנונימית, הרשת האפלה מאפשרת שיתוף מידע על תכנון מתקפת סייבר, התייעצות לגבי שימוש בנוזקות קיימות או שדרוגן, רכישת מגוון רחב של נוזקות או מידע על חולשות, ואף קניית ערכה כוללת לביצוע מתקפת סייבר המכילה את כל הדרוש – החל ממידע על חולשה ומיקומה וכלה בנוזקה המתאימה ואמצעי הפצתה. מחירה של נוזקה או מידע על חולשה נע בין דולר אחד למאות אלפי דולרים, והוא משתנה לאורך השנים ותלוי ברמת מורכבות הנוזקה או החולשה.[73]

72 הרשת האפלה, המכונה גם "הרשת השקופה" או "הרשת הנסתרת", מורכבת מאתרי אינטרנט שאינם נגישים באמצעות מנוע חיפוש רגיל דוגמת גוגל. מפעילי האתרים אינם מעוניינים להנגישם לכלל משתמשי האינטרנט בעולם באמצעות מנוע חיפוש, והגישה אליהם נעשית באמצעות תוכנה ייחודית, כמו TOR (The Onion Router) או Comodo Dragon browser. ראו רנן אלעל "דארקנט: העולם התחתון של האינטרנט" **ynet** (6.4.2013); Jamie Bartlett, The Dark Net: Inside the Digital Underworld (2016)

73 Lillian Ablon, Martin C. Libicki, & Andrea A. Golay, Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar (RAND Corporation, 2014); Danny Palmer, *Criminals in the Cloud: How Malware-as-a-service is Becoming*

ככל שעולם הסייבר מתפתח שירותים אלה מגיעים אל העולם ה"אמיתי" וחברות מסחריות ברחבי העולם מציעות שירותי "סייבר התקפי". כמה מהחברות המרכזיות בתחום הן קבוצת גמה, שבבעלות אנגלית־גרמנית; Hacking Team, שבבעלות איטלקית; ו־NSO מישראל.[74]

אין מדובר רק בשירותי סייבר התקפי המתמקדים במניעת גישה למערכות ממוחשבות עד לתשלום כופר, פגיעה בתשתיות קריטיות או מתקפה המכוונת לאיסוף פרטי כרטיסי אשראי ומכירתם. רבות מחברות הסייבר ההתקפי עוסקות באיסוף, ריגול ומעקב באמצעות סוגים שונים של נוזקות ומתקפות סייבר. חשוב להבין כי אין מדובר באיסוף המידע השיטתי הנאגם על כל אחד מאיתנו בכל יום ובכל דקה באמצעות יישומונים המותקנים לאחר קבלת רשותנו במכשיר הטלפון הנייד האישי שלנו, כגון רשת חברתית, עוזר דיגיטלי או מנוע חיפוש. אף שמדובר באיסוף מטריד ביותר, הוא נעשה על פי רוב בהסכמתנו, גם אם זו ניתנת באופן אוטומטי ומבלי להבין את השלכותיה עד תום.[75] איסוף המידע, המעקב והריגול שמבצעות חברות סייבר התקפי נעשה על פי רוב שלא בידיעת נושא המידע, ובוודאי שלא בהסכמתו, באמצעות החדרת נוזקה למכשיר הסלולרי האישי שלו.

שוק הסייבר ההתקפי משגשג בישראל,[76] ומונה כמה חברות פרטיות אשר פועלות בחשאי והמידע עליהן מועט. על פי רוב הן מגייסות את מרבית עובדיהן מקרב יוצאי יחידות מודיעין מובחרות בתחום לוחמת הסייבר, ובדומה לחברות סייבר התקפי אחרות בעולם, גם אלו הישראליות מוכרות בעיקר אמצעי איסוף, מעקב וריגול.

אחת מחברות אלו היא "בלאק קיוב", שהוקמה על ידי יוצאי קהילת המודיעין הישראלית למטרות מודיעין עסקי, ומשלבת שירותי סייבר התקפי לצד יכולות

---

the Tool of Choice for Crooks, ZDNet (April 21, 2016); Rasa Juzenaite & Daniel Dimov, *Malware-as-a-service*, Infosec (June 5, 2017)

74 *Offering Software for Snooping to Governments is a Booming Business*, The Economist (Dec. 14, 2019) (להלן: *Offering Software*).

75 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (2019)

76 *Offering Software*, **לעיל** ה"ש 74.

מודיעיניות מוכרות מתחום המודיעין האנושי (יומינט) ומודיעין האותות (סיגינט). החברה מספקת שירותי תמיכה בליטיגציה משפטית, איסוף מודיעין עסקי וראיות, ייעוץ אסטרטגי בסכסוכים משפטיים, מתן מודיעין לאיתור נכסים וזיהוי סימני שחיתות או ניגוד עניינים. סוכני החברה מסוגלים לאסוף מידע ולעקוב אחר מטרותיהם באמצעות גישה לחשבונות בנק, דוחות כרטיסי אשראי, ניטור חשבונות הרשתות החברתיות של מושא המעקב וחבריו ומעקב אחר נתוני המיקום של מכשיר הטלפון הנייד שלו. באפריל 2017 נעצרו שני עובדי החברה בחדר מלון ברומניה, ונטען כי ניסו להשיג דגימות DNA של ראשת הרשות למלחמה בשחיתות ברומניה ואף ביצעו תקיפת סייבר נגדה באמצעות פריצה לחשבונות דוא"ל של כמה ממקורביה. בהמשך הסתבכה החברה בניסיון לברר את מניעיה של המתלוננת הראשונה שטענה כי המפיק והבמאי האמריקאי הרווי ויינסטין אנס אותה.[77]

חברה נוספת היא חברת NSO, שנחשבת לחברת הסייבר ההתקפי הגדולה בישראל על פי הערכות של היקף פעילותה ומספר העובדים בה. NSO פועלת גם בשוק בישראל, אך היא התפרסמה בעיקר בגין מכירת נשק הסייבר שהיא מפתחת למדינות דיקטטוריות כגון סין, איחוד האמירויות וסעודיה, לשם מעקב אחר פעילי זכויות אדם, עיתונאים ומתנגדים למשטר במדינות אלה. על פי הדיווחים, תוכנת פגסוס (Pegasus) שהחברה פיתחה מאפשרת למשתמש בה לקבל גישה מרחוק למכשיר הטלפון הנייד של מושא המעקב ולאסוף ממנו מידע, לרבות הודעות טקסט, לוג שיחות ונתוני מיקום. לדברי החברה היא משווקת את מוצריה לממשלות, רשויות אכיפת חוק וסוכנויות מודיעין מדינתיות בלבד.[78]

77 יובל הירשהורן "בתוך הקופסה השחורה" **פורבס** (8.11.2017); יואב סטולר ואור הירשאוגה "חברת הסייבר המסתורית בשירות משרד הביטחון" **כלכליסט** (29.3.2018); Ronen Bergman & Scott Shane, *The Case of the Bumbling Spy: A Watchdog Group Gets Him on Camera*, The New York Times (Jan. 28, 2019); Ronan Farrow, *The Black Cube Chronicles: The Private Investigators*, The New Yorker (Oct. 7, 2019)

78 Ben Gilbert, *Meet the Shadowy Security Firm from Israel Whose Technology is Believed to be at the Heart of the Massive WhatsApp Hack*, Business Insider (May 14, 2019); Ronan Farrow, *The Black Cube Chronicles: The Double Agent*, The New Yorker (Oct. 9, 2019)

חברת קנדירו, הנחשבת השנייה בגודלה בשוק הסייבר ההתקפי בישראל, מספקת, לפי דיווחים בתקשורת, מערכת מלאה למתקפת סייבר הכוללת סל של שירותים: זיהוי חולשה, ממשק משתמש שמאפשר ללקוח לראות כמה יעדים נחדרו ואיזה מידע הושג, ומגוון נוזקות – ואף פיתוח נוזקות חדשות אם אלה הקיימות במערכת אינן מספיקות. למשל, קנדירו מספקת פלטפורמה שאינה ניתנת לאיתור המשמשת לחדירה למערכות מחשב, לרשתות ולמכשירי טלפון ניידים. בין השאר, המערכת מאפשרת למשתמש בה לשלוט מרחוק ולבצע מניפולציות במיקרופון, במצלמה ובמקלדת של מכשיר הטלפון הנייד, ואף לצלם צילומי מסך, להאזין לשיחות VoIP ולצותת לתוכנות מסרים מיידיים. קנדירו משווקת את מוצריה לממשלות בכל רחבי העולם, למעט בישראל, ארצות הברית, רוסיה וסין.[79]

חברת PICSIX עוסקת אף היא, לפי הדיווחים בתקשורת, בסייבר התקפי ובעיקר במעקב והאזנה ברשתות סלולר. גם חברות ישראליות נוספות, כגון Rayzonre, Wintego, Septier, ורינט ואלביט מערכות, עוסקות בסייבר התקפי.[80]

כלי סייבר התקפי נחשבים במדינת ישראל כלי נשק לכל דבר, ועל כן חברות הסייבר ההתקפי בשוק כפופות לאגף הפיקוח על היצוא הביטחוני במשרד הביטחון. אולם פיקוח זה מתמקד בעיקרו בשמירה על ביטחון המדינה ובמניעת מכירת כלי נשק העשויה לפגוע בביטחון המדינה; הפיקוח אינו עוסק כלל בהשלכות הסחר בנשק סייבר התקפי על זכויות אדם במדינות אחרות ועל המשטר הדמוקרטי בהן. יתרה מזו, משרד הביטחון בישראל יצר הליך אישור מהיר למכירת כלי סייבר התקפי אשר קיצר מאוד את משך הזמן לקבלת רישיון יצוא – משנה לארבעה חודשים. משרד הביטחון גם צמצם את ההגבלות על מערכות אלו, וכעת חברות סייבר התקפי יכולות לקבל פטור מקבלת רישיון לשיווק ולמכירה של מוצרים מסוימים למדינות ספציפיות. מדיניות מקילה זו

79 אמיתי זיו "'גאווה' כחול לבן: חברת הסייבר קנדירו משווקת כלי פריצה לטלפונים סלולריים" **TheMarker** (2.9.2020); Thomas Brewster, *Mysterious Mercenaries Hacking Apple and Microsoft PCs For Profit*, Forbes (Oct. 3, 2019)

80 אמיתי זיו "חברת הסייבר המסתורית שמשלמת להאקרים שלה 80 אלף שקל בחודש" **TheMarker** (3.1.2019) (להלן: זיו "חברת הסייבר המסתורית").

ספגה ביקורת מהאו"ם ומארגוני זכויות אדם והגנת פרטיות בעולם, הסבורים שעל מדינת ישראל להגביל את מתן רישיונות היצוא לכלי סייבר התקפי שעלול להיעשות בהם שימוש לרעה לשם הפרת זכויות אדם במדינות דיקטטוריות, כמו סעודיה, סין, סודן, מלזיה ואיחוד האמירויות.[81]

אומנם הטענה המרכזית של חברות הסייבר ההתקפי היא שכלי הנשק שהן מפתחות יכולים ואמורים לשמש למטרות לגיטימיות, כמו אכיפת חוק, מניעת סחר בסמים ולוחמה בטרור. NSO, למשל, אף אימצה מדיניות המבוססת על העקרונות המנחים של האו"ם לעסקים ולזכויות אדם, ואוסרת בתנאי השימוש שלה שימוש בתוכנה שבפיתוחה העלול לפגוע בזכויות אדם מסוימות, כגון הזכות לחיים ולביטחון אישי.[82] אולם בפועל, לאחר המכירה של כלים לזיהוי ולניצול חולשה במערכת ממוחשבת או מתן רישיון לשימוש בהם יכול להיעשות בהם גם שימוש לרעה, בעיקר כאשר הם נמכרים לחברות שערכי הדמוקרטיה וזכויות האדם אינם בראש סדר העדיפויות שלהן.[83]

ואכן, חברות סייבר התקפי מישראל מצאו עצמן לאחרונה מושא לביקורת ציבורית במדינות המערב עקב מעורבותן לכאורה בניהול מתקפות סייבר שונות. כך, למשל, באוקטובר 2018 הגיש העיתונאי הסעודי עומר עבדול עזיז תביעה לבית המשפט המחוזי בתל אביב נגד חברת NSO, בטענה שזו מכרה רישיון לשימוש בתוכנת הריגול הסלולרי שלה, פגסוס, למשטר הסעודי, אשר השתמש בה כדי לעקוב אחר העיתונאי הסעודי ג'מאל אחמד ח'אשוקג'י. לטענת עבדול עזיז, מעקב זה סייע למשטר הסעודי ברציחתו של ח'אשוקג'י.[84] NSO מתמודדת בימים אלו גם עם תביעה שהגישה נגדה חברת פייסבוק בארצות

81 **שם**; *Offering Software*, **לעיל** ה"ש 74; משה גורלי "בלאק קיוב לא לבד" **כלכליסט** (9.6.2019); שוקי טאוסיג "מנוולים, חובבנים ובריונים" **העין השביעית** (7.6.2019).

82 *Offering Software*, **לעיל** ה"ש 74; William Turton & Davide Scigliuzzo, *Facebook Sues Israel's NSO on Alleged WhatsApp Malware Hack*, Bloomberg (Oct. 29, 2019)

83 עומר כביר "חברות סייבר התקפי מקלות על האקרים ופושעים לפרוץ לנו לחיים ולשבש אותם" **כלכליסט** (1.9.2019).

84 *Offering Software*, **לעיל** ה"ש 74.

הברית, בטענה ש־NSO השתמשה בחשבונות ואטסאפ מזויפים כדי להפיץ ולהחדיר את תוכנת פגסוס. לפי כתב התביעה, התוכנה שימשה למעקב אחר עורכי דין, עיתונאים, פעילי זכויות אדם, מתנגדים למשטר, דיפלומטים ובעלי תפקידים בכירים בממשלות זרות.[85] ביולי 2021 פורסם תחקיר מקיף בנושא זה, אשר חשף כי סוכנויות ממשלתיות של כמה מדינות (בדרגות שונות של דמוקרטיה, בין השאר קזחסטן, אזרבייג'ן, הונגריה וסעודיה) השתמשו בתוכנת פגסוס של NSO כדי לעקוב אחר כ־180 עיתונאים.[86] כמו כן, ביוני 2018 הטיל משרד האוצר האמריקאי סנקציות על שתי חברות סייבר ישראליות, Embedi ו־ERPScan, עקב מעורבותן לכאורה בסיוע למתקפות סייבר שביצעה ממשלת רוסיה נגד מוסדות אמריקאיים גדולים.[87]

ב. סוגי נוזקות עיקריים

מקובל להבחין בין כמה סוגים עיקריים של נוזקות נפוצות במרחב הסייבר:

(**1**) **נוזקה המבוססת על תוכנת פרסום** (adware) המציגה פרסומות בבאנרים קופצים על מסך המחשב של המשתמש.

(**2**) **רוגלה** (spyware): תוכנת ריגול העוקבת אחר פעילות המשתמש באינטרנט ואוספת עליו מידע כדי למכור אותו, בין השאר לשם התאמת פרסומות.[88]

(**3**) **וירוס**: נוזקה המתוכנתת לשכפל את עצמה בהיחבא באמצעות תקיפת קבצים קיימים במערכת המותקפת. וירוסים הם הנוזקות הוותיקות ביותר, אך השפעתם והשימוש בהם פחתו לאורך השנים עם הופעתן של נוזקות מסוגים חדשים.

85 Turton & Scigliuzzo, **לעיל** ה"ש 82.

86 Phineas Rueckert, *Pegasus: The New Global Weapon for Silencing Journalists*, Forbidden Stories (July 18, 2021)

87 זיו "חברת הסייבר המסתורית", **לעיל** ה"ש 80; יוסי הטוני "ישראל מקלה את ההגבלות על יצוא סייבר התקפי – וחוטפת ביקורת" PC **אנשים ומחשבים** (26.8.2019).

88 מגמות תקיפת סייבר 2018, **לעיל** ה"ש 63, בעמ' 5.

(**4**) **תולעת**: נוזקה אשר בדומה לווירוס מתוכנתת לשכפול עצמי בהיחבא, אך היא משכפלת ומפיצה את עצמה מבלי לעשות שימוש בקבצים הקיימים במערכת המחשב המותקפת; לעיתים היא מוחקת קבצים קיימים.

(**5**) **סוס טרויאני**: נוזקה שמתחזה לתוכנת מחשב לגיטימית ושימושית. המשתמש התמים מתקין את התוכנה מבלי לדעת שזוהי בעצם נוזקה בתחפושת. כך חודרת הנוזקה למערכת המחשב ומתקיפה אותה. מטרת נוזקה מסוג סוס טרויאני היא בדרך כלל ליצור "דלת אחורית" המאפשרת לתוקפים גישה בלתי מורשית למערכת המחשב המותקפת ולקובצי מידע אישי, כמו למשל שמות משתמש וסיסמאות, פרטי חשבון בנק ופרטי כרטיסי אשראי.

(**6**) **"בוט" (bot)**: נוזקה הגורמת למערכת המחשב המותקפת לפעול כרובוט הנשמע לפקודות הניתנות לו מרחוק. נוזקת הבוט גם משכפלת את עצמה באופן עצמאי או בתגובה לפעולה של המשתמש ומתפשטת במערכות מחשב מקושרות. בדרך זו נוצר "צבא" בוט־נטים הנשמעים לפקודות הניתנות להם ממרכז השליטה של ההאקר התוקף מרחוק. פעמים רבות במתקפות מסוג זה המחשב המותקף למטרות הפיכתו לבוט ממשיך לפעול כרגיל והמשתמש כלל אינו מודע למתקפת הסייבר שמחשבו האישי משתתף בה.

צבאות של בוט־נטים משמשים, למשל, לביצוע מתקפות מניעת שירות מבוזרות (Distributed Denial of Service, DDoS). מתקפת סייבר מסוג זה מנצלת את העובדה שלכל שרת המאחסן אתר אינטרנט יש קיבולת מסוימת ומוגבלת לתקשורת מול משתמשים חיצוניים. במתקפת מניעת שירות מבוזרת השרת המאחסן את אתר האינטרנט שאת הגישה אליו התוקפים מבקשים למנוע מוצף בפניות סרק המבקשות גישה לאתר, עד שאינו מסוגל יותר להתמודד עם עומס הפניות ופעולתו מואטת או מופסקת לחלוטין.[89]

בשנים 2013–2012 הותקפו בנקים אמריקאיים בגלים של מתקפות מניעת שירות. התקיפה גרמה למערך הבנקאות האמריקאית נזק המוערך בעשרות מיליוני דולרים, הנובע מהפגיעה ביכולתם של לקוחות לבצע פעולות ולקבל

89 *Denial of Service (DoS) Guidance*, National Cyber Security Centre (published March 16, 2016; reviewed Nov. 15, 2018)

שירותים מהבנקים, מאובדן האמון במערכת הבנקאית וכן מהמאמצים למגר ולמזער את התקיפות.[90]

שימוש נוסף בבוט־נטים הוא לשם הפצה מסיבית של מידע בניסיון להטות את השיח ברשתות חברתיות ולתמרן את דעת הקהל, בעיקר בהקשרים פוליטיים. שימוש כזה בבוט־נטים נעשה, לדוגמה, במשאל העם בבריטניה על היציאה מהאיחוד האירופי (ברקזיט) ובמערכת הבחירות לנשיאות ארצות הברית בשנת 2016. בשני המקרים השתמשו רשתות בוט־נטים בפלטפורמות הרשתות החברתיות טוויטר, פייסבוק, אינסטגרם ויוטיוב להפצת כתבות חדשותיות מזויפות וחצאי אמיתות, כגון הודעות שנשלחו לבוחרים המסבירות להם שביכולתם להצביע בהודעת טקסט; וכן להפצת מסרים חתרניים המכוונים לקהלים מסוימים במטרה להעמיק שסעים חברתיים, כמו למשל עידוד הצבעה למועמד שאין כל סיכוי שייבחר, קריאה להימנעות כללית מהצבעה כדרך לבטא את חוסר שביעות רצון הבוחרים מהמצב הפוליטי הקיים, ומסרים המכוונים לקהילה האפריקאית־אמריקאית בארצות הברית שנועדו להגביר את חוסר האמון של בני הקהילה במועמדת המפלגה הדמוקרטית הילרי קלינטון.[91] באותה מערכת בחירות אף נטען שאחד מכל ארבעה ציוצים בטוויטר הוא ציוץ שהופק על ידי בוט, ושמספר הבוט־נטים שהופעל מטה הבחירות של טרמאפ היה גדול הרבה יותר מזה שהפעיל מטה הבחירות של קלינטון.[92] גם בישראל בוט־נטים תורמים להפצת מידע שקרי כדי להשפיע ולעצב את דעת

90 Joseph Menn, *Cyber Attacks Against Banks More Severe than Most Realize*, Reuters (May 18, 2013)

91 Renee DiResta et al., The Tactics & Tropes of the Internet Research Agency (2019)

92 יעקב הכט "תרומתן של תוכנות האנשה להתפתחות התרבות" **איגוד האינטרנט הישראלי** (6.9.2017); John Markoff, *Automated Pro-Trump Bots Overwhelmed Pro-Clinton Messages, Researchers Say*, The New York Times (Nov. 17, 2016); Alessandro Bessi & Emilio Ferrara, *Social Bots Distort the 2016 U.S. Presidental Election Online Discussion*, 21 (11) First Monday (2016); Sam Earle, *Trolls, Bots and Fake News: The Mysterious World of Social Media Manipulation*, Newsweek (Dec. 17, 2019)

הקהל, בעיקר לפני בחירות לכנסת.[93] חשוב לציין שהשימוש ברשתות לצורך הפצת דיס־אינפורמציה רחב יותר מהפעלת בוטים בלבד וכולל כמובן גם שימוש בחשבונות מזויפים, טרולים, רשתות הדהוד ומנגנונים מייצרי ויראליות אחרים.[94]

(**7**) **נוזקת כופר** (ransomware): נוזקה מסוג זה מצפינה את הקבצים במערכת המחשב של המשתמש המותקף. מפתח ההצפנה נמצא אצל התוקף, והוא מעמיד דרישת תשלום מוגבלת בזמן כנגד מסירת המפתח ומתן גישה לקובצי הנתקף. בחברת אבטחת המידע קספרסקי התייחסו אליהן כאיום מרכזי בשנת 2016.[95] ברבעון הרביעי של שנת 2017 זיהתה חברת האבטחה מקאפי גידול של כ־35% בשימוש בנוזקות כופר לעומת הרבעון הזהה בשנת 2016.[96] מתקפות הסייבר הגדולות של 2017, WannaCry, NotPetya ו־Petya, עשו שימוש בנוזקות כופר. WannaCry, למשל, הביאה להשבתת מחשביהן ועקב כך פעולתן של חברות כמו יצרנית העוגיות אוראו (Oreo), בתי חולים בפנסילבניה, בריטניה ואינדונזיה אשר נאלצו לדחות טיפולים ובדיקות שונות, מפעל נפט בברזיל, מפעל שוקולד בטסמניה, חברת הטלקומיוניקציה טלפוניקה (Telefonica) בספרד וחברת השילוח פדקס (FedEx) בארצות הברית.[97] במחצית

93 הגר בוחבוט "שדה הקרב של הבחירות: זה מה שיקרה ברשתות החברתיות" **ynet** (28.12.2018); עודד ירון "בפוליטיקה הישראלית הבוטים הרוסים הם רק קצה הקרחון" **הארץ** (31.8.2018); איתמר גרנות ורנאד עיד "2019 – פרשת 'הבוטים' והסדרת תעמולת הבחירות ברשתות החברתיות" **משרד המשפטים** (6.5.2019).

94 להרחבה ראו תהילה שוורץ אלטשולר וגיא לוריא **תעמולה דיגיטלית והאיום על הבחירות** (מחקר מדיניות 155, המכון הישראלי לדמוקרטיה 2020).

95 Anton Ivanov, David Emm, Fedor Sinitsyn, & Santiago Pontiroli, *Kaspersky Security Bulletin 2016; Story of the Year: The Ransomware Revolution*, Securelist (Dec. 8, 2016)

96 McAfee Labs, McAfee Labs Threats Report (March 2018); John Love, *Malware Types and Classifications*, LastLine (March 28, 2018); Roger A. Grimes, *8 Types of Malware and How to Recognize Them*, CIO (July 25, 2018)

97 Jon Ungoed-Thomas, Robbin Henry & Dipesh Gadher, *Cyber-Attack Guides Promoted on YouTube*, The Sunday Times (May 14, 2017); Alex Hern, *WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017*, The Guardian (Sep. 30, 2017); Danny Palmer, *WannaCry Ransomware Crisis,*

הראשונה של שנת 2018 נרשמה ירידה של 57% במספר מתקפות הכופר על שירותי בריאות.[98] עם זאת, לפי דוח של חברת מקאפי, ברבעון הראשון של שנת 2019 גדל המספר הכולל של מתקפות הכופר ב־118%.[99] לפי התחזיות תחול ירידה במספר מתקפות הכופר הגלובליות, אך צפויה עלייה במספר מתקפות הכופר הממוקדות – מתקפות שיכוונו למערכות ממוחשבות של ארגונים ותאגידים שצפוי שישלמו סכומי כסף ניכרים כדי להציל את המידע שלהם. כמו כן, מומחים מעריכים כי לצד מתקפות כופר על מחשבים אישיים ושרתים צפויה עלייה במספר מתקפות הכופר על מכשירי צריכה ביתיים או אישיים מסוג האינטרנט של הדברים, כגון טלוויזיה חכמה, בתים חכמים או מכוניות חכמות.[100] ואכן, במחצית הראשונה של 2020 זוהתה עלייה במספר מתקפות הכופר שהתמקדו בשירותי בריאות ובחברות תרופות, תוך ניצול חוסר יכולתם של גופים אלו להתמודד עם מתקפות מסוג זה בעיצומה של מגפת הקורונה.[101]

(**8**) **נוזקה "נעדרת קבצים"** (fileless): נוזקה העושה שימוש בכלי תכנות הקיימים במערכות ההפעלה השונות כדי להשיג הרשאות גישה למערכות ולעשות בהן שימוש לצורכיהן. השימוש בנוזקות מסוג זה נמצא במגמת עלייה החל מהמחצית הראשונה של 2018. הנוזקה המוכרת מסוג זה מכונה "פאוורשל" (PowerShell), שכן היא עושה שימוש בכלי הקידוד העונה לכינוי זה של חברת מיקרוסופט המשולב במערכת ההפעלה חלונות. העובדה שנוזקות אלו עושות שימוש בכלי התכנות הקיימים במערכות ההפעלה מקשה על זיהוין ואיתורן.[102]

One Year On: Are We Ready for the Next Global Cyber Attack?, ZDNet (May 11, 2018)

98 Fred Donovan, *Despite Flashy Attacks, Healthcare Ransomware Attacks Decline*, Health IT Security (July 23, 2018)

99 McAfee Labs, McAfee Labs Threats Report (August 2019)

100 Kaspersky Security Bulletin 2019; *Advanced Threat Predictions for 2020*, **לעיל** ה"ש 70.

101 מגמות תקיפת סייבר 2020, **לעיל** ה"ש 59, בעמ' 5–6.

102 *Fileless Malware Execution with PowerShell is Easier than You May Realize*, McAfee (Technical Brief, March 2017); *What You Can Do About Powershell Threats*, Broadcom (Dec. 26, 2017)

ג. אופני הפצה, שילוח או הדבקה של נוזקה

קיימות כמה שיטות עיקריות לניצול חולשה ולהפצת נוזקה:

(**1**) הפצה באמצעות פרסומת ("malvertising"): בשיטה זו הנוזקה מוטמעת בפרסומות המופיעות באתרי אינטרנט ובאפליקציות, לרבות כאלו הנחשבים אמינים, כמו רויטרס, יוטיוב, הניו יורק טיימס וספוטיפיי.[103] על פי ההערכות, נוזקות המוטמעות בפרסומות גורמות לנזק בהיקף של כ־1.1 מיליארד דולר בשנה.[104] לעיתים די בצפייה בפרסומת בעת ביקור באתר האינטרנט או בעת השימוש באפליקציה כדי להביא להפעלת הנוזקה. בשנים האחרונות גבר השימוש באמצעי הדבקה זה להפצת נוזקות המשמשות לכריית מטבעות דיגיטליים.[105]

(**2**) הורדת הנוזקה למחשב האישי ללא ידיעת המשתמש (drive-by download): בשיטה זו די בצפייה באתר אינטרנט כדי להביא להורדת הנוזקה ללא ידיעת המשתמש. ההורדה מתאפשרת בשל ניצול חולשה בדפדפן האינטרנט, גלישה באמצעות גרסת דפדפן ישנה שלא הותקנו בה עדכוני תוכנה או שימוש במערכת הפעלה מיושנת ולא מעודכנת.[106]

(**3**) התקנה מרצון של תוכנה שהמשתמש אינו מודע לכך שהיא נגועה בנוזקה, למשל תוכנה המתחזה דווקא לתוכנת אנטי־וירוס[107] או תוכנה לגיטימית הנגועה בנוזקה ללא ידיעת מפיץ התוכנה המורשה. למשל, אחת הדרכים

103 Gonzalo Torres, *Three Real-Life Horror Stories Your Antivirus Could Have Prevented*, Avast (Oct. 26, 2017)

104 *Digital Ad Industry Will Gain $8.2 Billion by Eliminating Fraud and Flows in Internet Supply Chain, IAB & EY Study Shows*, IAB News (Dec. 1, 2015)

105 *Malware Attack Vectors*, **לעיל** ה"ש 62.

106 **שם**.

107 **שם**.

להפצת הנוזקה מסוג סוס טרויאני המכונה Havex הייתה הדבקתה לתוכנות לגיטימיות עוד באתר ספק התוכנה ללא ידיעתו.[108]

(**4**) דיוג (phishing): שיטת הדבקה ותיקה שהשימוש בה החל כבר באמצע שנות התשעים של המאה הקודמת, ונחשבת זולה וקלה ליישום גם ללא ידע טכנולוגי נרחב. בשנת 2017, 54.6% מכלל מסרי הדוא"ל הכילו נוזקות שהופצו בשיטת הדיוג.[109] בשיטה זו מפתים את הגולש או משתמש שירות הדואר האלקטרוני להקליק על קישור המוביל להתקנת נוזקה או להוריד צרופה שנשלחה בדואר אלקטרוני המכילה נוזקה, תוך ניצול הטיות פסיכולוגיות אנושיות. למשל, התוקף משתמש בקישורים מפתים המופצים ברשתות החברתיות,[110] יוצר זהות בדויה שמקיימת קשרים עם הגורם האנושי או מתחזה למקור מהימן בתכתובת דואר אלקטרוני, כמו מסר מהבנק או הודעה מעמית לעבודה או מאדם אחר שהמשתמש מופיע באנשי הקשר שלו.[111] גם מתקפת הסייבר על המפלגה הדמוקרטית בארצות הברית במהלך מערכת הבחירות לנשיאות בשנת 2016, אשר הובילה לחשיפת מסרי דוא"ל סודיים שמאוחר יותר פורסמו ברבים על ידי אתר ויקיליקס והסבו נזק להילרי קלינטון, התאפשרה באמצעות דיוג: מסר דוא"ל שהכיל נוזקה נשלח לחשבון הג'ימייל האישי של מנהל מטה הבחירות של קלינטון, ג'ון פודסטה.[112] במחצית הראשונה של 2020 נמצא ש־78% ממתקפות הסייבר מבוססות קבצים הופצו באמצעות מסרי דואר אלקטרוני.[113]

108 Rachael King, *DHS Investigating Havex Trojan Which Targets Energy Companies*, Wall Street Journal (June 26, 2014)

109 Symantec, Internet Security Threat Report (vol. 23, 2018)

110 תומר טלר "לפרוץ למוח האנושי: הסיכון הגדול ביותר לאבטחת מידע הוא הנדסה חברתית" **Geektime** (16.5.2012).

111 Martin C. Libicki, Cyberdeterrence and Cyberwar (2009); Will Yakowicz, *The 3 Biggest Phishing Scams of 2018*, Inc (Jul. 6, 2018); Josh Fruhlinger, *What Is Phishing? How This Cyber Attack Works and How to Prevent It*, CSO Online (Aug. 9, 2018)

112 Ben Gilbert, *Hillary Clinton's Campaign Got Hacked by Falling for the Oldest Trick in the Book*, Business Insider (Oct. 31, 2016); Luke Harding, *Top Democrat's Emails Hacked by Russia After Aide Made Typo, Investigation Finds*, The Guardian (Dec. 16, 2016)

113 מגמות תקיפת סייבר 2020, **לעיל** ה"ש 59, בעמ' 11.

(**5**) חיבור התקן זיכרון נייד (USB) הנגוע בנוזקה: אופן הדבקה זה מאפשר הפצה של נוזקה במערכות שאינן מקושרות ובדרך כלל מבודדות מטעמי אבטחה. כך, למשל, מומחים מעריכים שהנוזקה סטקסנט (Stuxnet), שפגעה במתקני הגרעין של איראן, הועברה באמצעות התקן זיכרון נייד.[114]

(**6**) שתילת קובץ הפעלה בתוכנת הביוס (Basic Input Output System, BIOS), בדרך כלל באמצעות סוס טרויאני או תולעת: תוכנת הביוס היא התוכנה המופעלת ראשונה עם הדלקת המחשב ותפקידה לשלוט בכמה פעולות בסיסיות והתחלתיות של המחשב, כגון אתחול ושליטה במקלדת. שילוח והרצה של הנוזקה דרך תוכנת הביוס מאפשרים לנוזקה לחמוק ממוצרי אנטי־וירוס ומסריקות סטנדרטיות של מערכת ההפעלה, שכן אלו נכנסים לשימוש ומנטרים את מערכת המחשב רק לאחר כניסת מערכת הביוס לפעולה. כמו כן, נוזקה התוקפת את מערכת הביוס נהנית מהרשאות גישה מרחיקות לכת לחומרת המחשב. הנוזקה הראשונה המוכרת מסוג זה אותרה בשנת 2011 וכוונה לתקוף משתמשים סיניים.[115]

שילוח הנוזקה יכול להיעשות בדרכים שונות במקביל. למשל, הנוזקה המכונה Havex תקפה תשתיות קריטיות במגזר האנרגיה בארצות הברית ובאירופה משנת 2010 עד שנת 2013 בשלושה שלבים. בשלב הראשון ההדבקה בנוזקה נעשתה באמצעות דיוג (phishing) ומטרות המתקפה היו איסוף מודיעין על מטרות התקיפה; בשלב השני הנוזקה הופצה באמצעות אתרי אינטרנט לגיטימיים אשר הפנו לשרתים שהכילו את הנוזקה; ובשלב השלישי והאחרון הנוזקה הייתה מסוג סוס טרויאני והופצה באמצעות הורדת תוכנה לגיטימית לכאורה למחשב האישי של המשתמש.[116] כאשר שילוח הנוזקה נעשה בכמה דרכים במקביל והמערכת המותקפת היא רשת מחשבים, הפגיעה הצפויה עלולה להיות קשה אף יותר כיוון שהנוזקה תוכל לפעול בקלות בתוך רשת המחשבים מרגע קבלת הרשאות הגישה המתאימות.

114 Josh Fruhlinger, *What is Stuxnet, Who Created it and How Does it Work?* CSO Online (Aug. 22, 2017)

115 נוזקה זו זכתה לשם Mebromi Virus. ראו Marco Giuliani, *Mebromi: The First BIOS Rootkit in the Wild*, Webroot (Sep. 13, 2011)

116 King, **לעיל** ה"ש 108.

ד. פיתוח מודולרי של נוזקות ושיפור נוזקות קיימות

בעבר יכלה נוזקה אחת לבצע פעולות שונות אך כולן היו צריכות להיות מוכנות ומתוכננות מראש. בשנים האחרונות הפכו נוזקות למודולריות, כלומר אפשר להוסיף לנוזקה תוכנות לביצוע פעולות נוספות. בדרך זו התוקף יכול להתאים מרחוק את הנוזקה לאחר החדרתה למערכת הממוחשבת המותקפת, בהתאם לצרכיו ולהגדרות המערכת המותקפת.[117] פיתוח מודולרי של נוזקות מאפשר לתוקף להסתיר את מלוא יכולותיו ומקשה מאוד על גילוי הנוזקה במערכת המותקפת, תחקור אופן פעולתה והתגוננות מפניה.

נוזקות רבות הנמצאות בשימוש הן בעצם שימוש מחדש בחלקים נרחבים מנוזקות קודמות. ההפצה של נוזקה ברבים מאפשרת החלפת מידע בין תוקפים ופיתוח אסטרטגיות יצירתיות. כך, למשל, מניתוח מתקפת הסייבר המכונה WannaCry נמצא כי הנוזקה הייתה מבוססת על שילוב של גרסאות קודמות של נוזקות אחרות: נוזקה אשר שימשה למתקפת הסייבר על תאגיד סוני בנובמבר 2014 ולמתקפת כופר על בנק בבנגלדש במאי 2016,[118] נוזקה שפותחה בעבר על ידי הסוכנות לביטחון לאומי בארצות הברית (NSA) למטרות ריגול והועתקה שלא כדין,[119] ונוזקה שיועדה לשיפור תפוצת הנוזקות הללו על פי לקחים ממתקפות סייבר גלובליות קודמות.[120]

117 John Bryk, *The Next Wave? Modular Component Malware Against Industrial Control Safety Systems*, CSO Online (Dec. 15, 2017); Proofpoint Staff, *New Modular Downloaders Fingerprint Systems, Prepare for More – Part 1: Marap*, Proofpoint (Aug. 16, 2018)

118 Security Response Team, *What You Need to Know About the WannaCry Ransomware*, Symantec (Oct. 23, 2017)

119 Scott Shane, Nicole Perlroth, & David E. Sanger, *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core*, The New York Times (Nov. 12, 2017)

120 Danny Palmer, *Hackers Are Making Their Malware More Powerful by Copying WannaCry and Petya Ransomware Tricks*, ZDNet (July 28, 2017)

פרק 9

הגורם האנושי במתקפות סייבר

בדומה לזירות אחרות,[121] גם במרחב הסייבר הגורם האנושי הוא החוליה החלשה האחראית לרוב הכשלים והתקלות.[122] נכון לשנת 2017, כ־52% מבעלי העסקים בארצות הברית הכירו בסיכון למתקפת סייבר בגלל הגורם האנושי, כלומר בגלל מעשה או מחדל של מי מעובדי הארגון.[123]

חולשתו של הגורם האנושי מנוצלת פעמים רבות על ידי תוקפים, כפי שמעידה העובדה שרוב התקפות הסייבר המוצלחות מנצלות את הנטייה שלא להטמיע עדכוני אבטחה חשובים באופן קבוע ושגרתי, ושאחד מאפיקי ההפצה המרכזיים של נוזקה הוא דיוג, המנצל את נטייתם של גולשים ומשתמשי דוא"ל להקיש על קישורים או לפתוח קבצים מבלי לבדוק אם הם נגועים בנוזקה. כך, למשל, מתקפות הסייבר WannaCry ו־NotPetya ניצלו חולשה במערכת ההפעלה של חברת מיקרוסופט, שהייתה ידועה ושהוצא עדכון אבטחה כדי לתקנה, אולם חברות רבות לא עדכנו את מערכותיהן כנדרש ונותרו חשופות.[124] הבנק האמריקאי ג'יי פי מורגן צ'ייס הותקף באביב 2014 על ידי תוקפים שהצליחו להעתיק את הרשאות הכניסה של אחד מהעובדים במחלקת המחשוב של הבנק, והחדירו את הנוזקה לאחד משרתיו של הבנק שהגדרות האבטחה שלו לא עודכנו. התקיפה הובילה לחשיפת פרטיהם של 7 מיליון עסקים קטנים ו־80 מיליון לקוחות פרטיים. חברת ביטוח הבריאות האמריקאית אנת'ם (Anthem)

121 הגורם האנושי אחראי לכ־90% מהטעויות בבקרת תעופה, לכ־50% מהכשלים במפעלים תעשייתיים ולכ־37% מזמן ההשבתה של חברות תרופות. ראו Israel Levy, *The Human Factor: The Unspoken Threat in Cybersecurity*, IT ProPortal (April 19, 2017)

122 Mahmood Sher-Jan, *Data Indicates Human Error Prevailing Cause of Breaches, Incidents*, IAPP (June 26, 2018); Ponemon Institute & Accenture Security, The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study 9 (2019) (להלן: The Cost of Cybercrime).

123 *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within*, Kaspersky (להלן: Kaspersky, *The Human Factor*).

124 **שם**; Greenberg, *The Untold Story*, **לעיל** ה"ש 52.

הותקפה בדצמבר 2015 ופרטיהם של 78.8 מיליון משתמשים נחשפו. לפי ההערכות, מתקפת הסייבר בוצעה על ידי מדינה זרה והחלה כבר בחודש פברואר 2014 באמצעות הפצת הנוזקה בשיטת הדיוג: משתמש של אחת מחברות הבת של אנת׳ם פתח דואר אלקטרוני שהכיל נוזקה, הנוזקה נשמרה על מחשבו האישי של אותו משתמש ואפשרה לתוקפים גישה מרחוק למערכות המידע של חברת אנת׳ם. אלו המשיכו בהפצת הנוזקה תוך ניצול חשבונותיהם והרשאות הגישה של לפחות 50 משתמשים או עובדים נוספים.[125]

על פי מחקר של חברת IBM ומכון פונמון (Ponemon Institute), 25% מכלל מתקפות הסייבר בשנת 2017 היו תוצר של רשלנות הגורם האנושי, כלומר של עובדים או של קבלני משנה של הארגון המותקף.[126] חברת ורייזון מצאה ש־17% ממתקפות הסייבר בשנת 2018 נגרמו בשל טעות אנוש, כמו עובד ששיתף מידע סודי או שלח תכתובת דואר אלקטרוני חסויה לכתובת הלא נכונה; כמו כן נמצא כי בממוצע 4% מכל העובדים בארגון פותחים תכתובת דואר אלקטרוני המכילה נוזקה המופצת בשיטת הדיוג. בחלוקה לתעשיות נמצא שבתעשיית המוסדות הפיננסים נגרמו 19% מתקיפות הסייבר על ידי עובדים, ובתעשיית שירותי הרפואה היו 56% מתקיפות הסייבר תוצאת מעשה או מחדל של גורם אנושי מתוך התעשייה.[127] חברת קספרסקי מצאה שרשלנות או חוסר מודעות של עובדים תרמו לכ־46% מתקיפות הסייבר נגד עסקים בארצות הברית במהלך שנת 2017, וכי אחת מכל עשר מתקפות הסייבר החמורות באותה שנה עירבה רשלנות של עובדים בארגון המותקף. כמו כן, ב־40% מהארגונים הסתירו העובדים את פריצתה של מתקפת הסייבר. עובד שאינו מדווח לממונים עליו

125 Jeffrey Roman, *Chase Breach Affects 76 Million Households*, Bank Info Security (Oct. 2, 2014); James A. (Sandy) Winnefeld, Jr., Christopher Kirchhoff, & David M. Upton, *Cybersecurity's Human Factor: Lessons from the Pentagon*, Harv. Bus. Rev. (Sep. 2015); Marianne Kolbasuk McGee, *A New In-Depth Analysis of Anthem Breach*, Bank Info Security (Jan. 10, 2017)

126 Ponemon Institute & IBM Security, 2017 Cost of Data Breach Study: Global Overview 14 (June 2017)

127 Widup et al., **לעיל** ה"ש 57, בעמ' 3.

בארגון או לאחראי הגנת הסייבר שפרצה מתקפת סייבר מייד עם היוודע לו הדבר עלול להביא להחמרת תוצאותיה.[128]

במרבית המקרים הפרטים שבגללם נגרמות מתקפות הסייבר אינם פועלים מתוך כוונה זדונית ליזום מתקפת סייבר ולפגוע במערכות הממוחשבות של הארגון. חולשת הגורם האנושי נובעת מחוסר הבנה של העובדים בארגון באשר לחשיבות אבטחת המידע ובאשר להשלכות התנהגויותיהם על הסיכון למתקפת סייבר, וכן מהיעדר מודעות של העובדים לנושאים אלו, התעלמות או חוסר אכפתיות בנוגע לרמת הסיכון האפשרית או פעולה בתנאי לחץ ובחוסר תשומת לב, והכול במסגרת קבלת הרשאות גישה רחבות שלא לצורך.[129]

כך, למשל, מחשבה האישי של יועצת משפטית בחברה הותקף באמעות נוזקת כופר. העובדת החליטה לטפל בבעיה בעצמה ומבלי לעדכן את מחלקת המחשוב בחברה, שילמה את הכופר הדרוש וקיבלה בחזרה גישה לכל הקבצים האישיים והעסקיים שבמחשבה האישי. אולם היא לא הייתה מודעת לכך שנוזקת הכופר המשיכה לשכון במחשבה האישי, ועם התחברותה מרחוק למערכת המחשב של החברה הופצה הנוזקה ותקפה את מערכות המחשב של כלל החברה.[130]

ככל שמערכות המחשוב של הארגון מורכבות יותר כך גובר הסיכוי לטעות אנוש העשויה לפגוע בהגנת הסייבר של הארגון.[131] לפיכך, נדבך מרכזי בהגנת הסייבר הוא השקעה נבונה בהכשרת הגורם האנושי: הגברת מודעות עובדי הארגון לסכנות במרחב הסייבר, הרחבת ידיעותיהם בנוגע לדרכי ההגנה על המידע וחשיבותן, יצירת מנגנונים שיסייעו להם לקבל החלטות שקולות כדי למזער

128 Kaspersky, *The Human Factor*, **לעיל** ה"ש 123.

129 **שם**; Levy, **לעיל** ה"ש 121; Mohd Anwar et al., *Gender Difference and Employees' Cybersecurity Behaviors*, 69 Computers in Human Behavior 437 (2017); Lee Hadlington, *The "Human Factor" in Cybersecurity: Exploring the Accidental Insider*, *in* Psychological and Behavioral Examinations in Cyber Security 46, 47 (John McAlaney, Lara A. Frumkin, & Vladlena Benson, eds., 2018)

130 Kaspersky, *The Human Factor*, **לעיל** ה"ש 123.

131 Levy, **לעיל** ה"ש 121.

את החשיפה לתקיפות סייבר ויצירת תמריץ חיובי לדיווח על מתקפת סייבר מייד כשמתעורר חשד, לצד חיזוק המומחיות של צוותי אבטחת המידע ובניית הון אנושי מיומן הלומד בקצב תדיר את האיומים החדשים ודרכי ההגנה. מזעור וניהול של הסיכון הטמון בגורם האנושי בחברה מהווים שכבת הגנה נוספת במכלול הגנת הסייבר, שיש לאמץ ולהטמיע בהתאם למיפוי האיומים והסכנות למתקפת סייבר ולנוכח הנכסים האסטרטגיים שעליהם רוצים להגן.[132]

הצבא האמריקאי וכן משרד ההגנה האמריקאי החלו כבר בשנת 2014 בפעולות להגברת הגנת הסייבר באמצעות מזעור מרחב הטעות של הגורם האנושי, מתוך תפיסה שהשקעה בהכשרת האנשים וביצירת תרבות ארגונית של הגנת סייבר חשובה לא פחות מהטכנולוגיה עצמה. ראשיתו של התהליך בשנת 2004, עת הוטמעו בצבא ובמשרד ההגנה מערכות מידע מתקדמות המאחדות את מערכות המחשוב, התקשורת והמכשירים השונים לכדי מערכת שליטה אחת, המסוגלת לנטר את כלל המערכות בו זמנית ולהבחין בפעילות חריגה העשויה להעיד על מתקפת סייבר. ואולם, מערכת השליטה המרכזית הקלה על הפצת נוזקות והגדילה את טווח ההפצה האפשרי, ואכן התרחשו באותן שנים כמה מתקפות סייבר שניצלו חוסר תשומת לב אנושית כדי להשיג דריסת רגל בתוך מערכות המחשוב המסווגות. למשל, בשנת 2008 נפרצה רשת צבאית מסווגת כאשר חייל חיבר למחשב מאובטח, בניגוד לנהלים, התקן נייד (disk on key) שהכיל נוזקה.[133] ב־2013 פורסם כי מדינה זרה חדרה לרשת הארגונית הלא מסווגת של חיל הים האמריקאי ושהתה שם במשך ארבעה חודשים, תוך ניצול חולשה מוכרת שלא תוקנה בזמן באתר האינטרנט הציבורי של חיל הים.

כדי להתמודד עם קשיים אלה אומצה בצבא האמריקאי מדיניות הגנת סייבר המבוססת על דרישה שהעובדים, בכל הדרגים בארגון, ימלאו אחר עקרונות בסיסיים של יושרה ומחויבות לנהלים, אי־הסתרת טעויות ודיווח אמין על פעולות. כן נקבע כי יש להכשיר עובדים עם כניסתם לתפקיד ובאופן עיתי

132 Kaspersky, *The Human Factor*, **לעיל** ה"ש 123; Federal Information Systems Security Educators' Association, *Cybersecurity – The Human Factor* (2014)

133 Winnefeld, Kirchhoff, & Upton, **לעיל** ה"ש 125.

ולוודא שהם מבינים את כלל היבטי המערכת שעל הפעלתה הם מופקדים, כך שיוכלו לזהות באופן מהיר ומיידי התנהלות חריגה. הוגדר גם נוהל שלפיו פעולות רגישות העלולות להוות סיכון ממשי למערכות חייבות להתבצע על ידי לפחות שני עובדים בדרגים שונים, שכל אחד מהם מוסמך לעצור את הפעולה בכל עת אם לדעתו מתעוררת בעיה. לצד כל אלה הונהגו תהליכי פיקוח ובקרה ונעשו צעדים לטיפוח תרבות ארגונית המעודדת בחינה פנימית ומחויבות לנהלים.[134]

העקרונות והנהלים שיש לאמץ כדי להפחית את הסיכון הנשקף מהגורם האנושי עשויים להיות שונים מארגון לארגון בהתאם לגודלו, הסיכון שלו ליפול קורבן למתקפת סייבר והרגישות של פעולותיו או של המידע המצוי בידו. עם זאת, הדעה הרווחת היא שרק כך אפשר למזער את הפגיעה הפוטנציאלית של הגורם האנושי כחוליה החלשה במערכת הגנת הסייבר.

134 שם.

פרק 7

המניעים למתקפת סייבר וזהות התוקפים

א. הגידול במגוון המניעים למתקפת סייבר

לאורך השנים השתנו אופי מתקפות הסייבר, מטרותיהן והאחראים להן. בעוד בעבר היה המניע העיקרי למתקפות סייבר מחקרי־אקדמי, לצד הרצון לזכות בתהילה אישית, כיום מתקפות סייבר יכולות להתבצע ממגוון מניעים נוספים: להפקת רווח כלכלי, לזריעת הרס ופחד כאמצעי טרור, או לשם איסוף מודיעין בידי מדינות למטרת השגת רווחים כלכליים או פוליטיים וביטחוניים וכאמצעי לחימה לכל דבר.[135]

בשנות השבעים והשמונים של המאה העשרים, כאשר האינטרנט היה בחיתוליו, אנשי אקדמיה פיתחו תוכנות מחשב שפעלו כווירוסים. התוכנות פותחו כחלק מניסיון להבין את מבנה האינטרנט והיקפו, וככל הנראה מתוך חוסר מודעות לנזק שהן עלולות לגרום. למשל, בשנת 1971 פיתח החוקר בוב תומס תוכנת מחשב, שכונתה "קריפר" (Creeper), במטרה להפיצה ברשת הארפאנט (ARPANET), אותה רשת שהפכה כעבור שנים לרשת האינטרנט המוכרת לנו. קריפר עברה בין מחשבי הרשת והותירה רק סממן מילולי – המשפט "אני הקריפר: תפוס אותי אם תוכל". חוקר אחר בשם ריי תומלינסון הצליח לאתר את הקוד של קריפר ולשפרו כך שיעתיק עצמו לצורך הפצה, וכך נוצר וירוס התולעת הראשון.[136]

בשנת 1983 הדגים פרד כהן, אז תלמיד מחקר במדעי המחשב מאוניברסיטת דרום קליפורניה, כיצד בעזרת תוכנה שכתב הוא מסוגל לעקוף את מנגנוני האבטחה ולהשתלט על מערכות מחשבים מרכזיות מסוג מיינפריים (mainframe). אף

135 van Eeten, **לעיל** ה"ש 47, בעמ' 440–441.

136 *The History of Cyber Security: Everything You Ever Wanted to Know*, SentinelOne (Feb. 10, 2019)

שתוכנות שפעלו כווירוסים פותחו עוד לפני כן, התוכנה שפיתח כהן נחשבת וירוס המחשב הראשון.[137] בשנת 1986 התגלה וירוס המחשבים שכונה "המוח" (Brain), אשר פותח על ידי שני אחים מפקיסטן שביקשו להדביק מחשבים אישיים מתוצרת IBM. הווירוס השתלט על המחשב המותקף והציג הודעה עם פרטיהם של המפתחים ודרכי יצירת הקשר עימם לשם רכישת "חיסון" לאחר הידבקות המחשב בווירוס.[138] כשנתיים אחר כך פרצה "תולעת מוריס" (The Morris Worm), שפיתח רוברט מוריס, אז סטודנט למדעי המחשב באוניברסיטת קורנל, במטרה למדוד את גודלה של רשת האינטרנט. תולעת מוריס התפשטה במהירות וגרמה להאטה ניכרת בתעבורה ברשת האינטרנט. הייתה זו מתקפת הסייבר הראשונה מסוג מניעת שירות (DDoS).[139]

לאחר התפרצות תולעת מוריס חלה האטה בקצב פיתוח וירוסים. אולם באמצע שנות התשעים שבו מתקפות הסייבר לפרוח, לנוכח התפוצה הנרחבת של מחשבים אישיים, העלייה בנוחות השימוש בהם באמצעות תוכנת חלונות 98 הידידותית למשתמש והעלייה בשימוש בשירותי דואר אלקטרוני, שסייעו בשכלול אופני ההפצה של נוזקות במהירות ובהיקפים גדולים. בשנת 1999 הופיע הווירוס "מליסה" (Melissa virus), שצורף כקובץ להודעות דואר אלקטרוני והדביק כ־250,000 מחשבים. עם זאת, הנזק שגרם היה מזערי: כל אימת שהתאריך והשעה במחשב המודבק תאמו את זה המוגדר בווירוס הופיע על מסך המחשב המודבק ציטוט מתוכנית הטלוויזיה "משפחת סימפסון".

כשנה אחר כך, בשנת 2000, פרץ וירוס האהבה ("i love you") הטורדני, שפיתח סטודנט מהפיליפינים. הווירוס הופיע כקובץ המצורף למסר דואר אלקטרוני שכותרתו "אני אוהב אותך". לחיצה על הקובץ המצורף הביאה להפעלת הנוזקה ולשליחת דואר אלקטרוני זהה לכל אנשי הקשר של אותו משתמש, וכן להורדתו ולהתקנתו של סוס טרויאני על מחשב המשתמש. הסוס הטרויאני אסף שמות

137 Kim Zetter, *Nov. 10, 1983: Computer "Virus" Is Born*, Wired (Nov. 10, 2009) (להלן: Zetter, *Computer Virus*); Bruce Middleton, A History of Cyber Security Attacks: 1980 to Present 29–32 (2017)

138 Zetter, *Computer Virus*, **לעיל** ה"ש 137.

139 **שם.**

משתמש וסיסמאות שאוחסנו על גבי המחשב ושלח אותם לכתובת דואר אלקטרוני בפיליפינים. הווירוס נחל הצלחה מסחררת: הוא הדביק כ־2.5 מיליון מחשבים אישיים באירופה ובארצות הברית וגרם נזק בהיקף של כ־10 מיליארד דולר בתוך שש שעות בלבד.[140]

ב. מגוון המניעים למתקפות סייבר כיום

1. רווח כלכלי

ארגוני פשיעה החלו לפעול במרחב הסייבר בתחילת שנות האלפיים עם העלייה המטאורית בשימוש ברשת האינטרנט, בידיעה שמעטה האנונימיות שהרשת מקנה למשתמשיה ממזער את הסיכוי שזהותם האמיתית תתגלה. ככל שיותר עסקים ושירותים פיננסיים החלו לספק שירותים במרחב הסייבר, כך גברה גם פשיעת הסייבר בצורות שונות: הונאת רשויות הרווחה והמס; מכירת המידע שהועתק לפושעים אחרים העושים בו שימוש; סחיטה – בשנים האחרונות בעיקר באמצעות נוזקות כופר, שמצפינות את הקבצים במערכת המחשב המותקף עד לתשלום סכום הכופר הנדרש;[141] כריית מטבעות דיגיטליים וסחר במוצרים בלתי חוקיים או גנובים ב"רשת האפלה", שהגישה אליה אינה מתאפשרת באמצעות מנועי החיפוש המוכרים, והפעילות בה נעשית בתוך רשת מוצפנת ותחת מעטה אנונימיות המקשה על ניטור פעילות המשתמשים בה וזיהוים.[142]

רוב מתקפות הסייבר ממניע כלכלי בוצעו בעבר בידי שחקנים א־מדינתיים מאורגנים, ברובם ארגוני פשע שהיגרו למרחב הסייבר מתוך הבנת היתרונות שהוא מציע לפעילותם העבריינית ותוך שכירת שירותי מתכנתים או רכישת

140 רויטל סלומון "20 שנים של וירוסים" **הארץ** (29.1.2006); Zetter, *Computer Virus*, **לעיל** ה"ש 137; Middleton, לעיל ה"ש 137, בעמ' 33–38.

141 לדיון מעמיק בנוזקת כופר ראו סעיף ב(7) בפרק 5.

142 Check Point Research, *Under the Hood of Cyber Crime: The Rise of Stealthy and Targeted Cyber Attacks*, 2 Security Report (2019)

נוזקות.[143] אולם בשנים האחרונות עולה גם המעורבות של שחקנים מדינתיים במתקפות סייבר המכוונות להפקת רווח כלכלי, מתוך רצון לממן פעולות שונות של המשטר במדינה.[144]

הנזק הכספי המוערך של מתקפות סייבר ממניעים כלכליים עולה מידי שנה בשנה. בשנת 2017 הוערך הנזק העולמי השנתי של פשיעת סייבר לכל מגזר תעשייתי ב־11.7 מיליון דולר בממוצע, ואילו בשנת 2018 ההערכה עלתה לכ־13 מיליון דולר. במגזר הבנקאות, למשל, הערכת הנזק השנתי הממוצע של פשיעת סייבר עמדה בשנת 2018 על 8.371 מיליון דולר, ואילו במגזר הבריאות – 11.82 מיליון דולר. בחתך מדינתי, הנזק השנתי הכולל של פשיעת סייבר בשנת 2018 בארצות הברית הוערך בכ־27.4 מיליון דולר, ביפן – 13.6 מיליון דולר, ובבריטניה – 11.46 מיליון דולר.[145]

שני הסוגים הרווחים ביותר של מתקפות סייבר ממניעים כלכליים הם כריית מטבעות וירטואליים ואיסוף של מידע, נתונים פיננסיים ונתוני אשראי.

I. כריית מטבעות וירטואליים

מטבעות וירטואליים אינם נשמרים בבנק אלא ב"ארנק אלקטרוני". לא קיימת מערכת כלכלית רגילה העוקבת אחר הסליקה והעברת המטבעות בין החשבונות, בדומה למערכת הסוויפט (swift) המשרתת את הבנקים. מערכת הפקת המטבעות הווירטואלים היא מערכת מבוזרת, והמעקב אחר המטבעות הווירטואליים והעסקאות בהם מתבצע על ידי המשתמשים עצמם באמצעות יצירת רשומות אלקטרוניות של כל העסקאות. רישום מסודר ורציף של כלל העסקאות מחייב כוח מחשוב רב, שאף הולך וגדל ככל שערך המטבע הווירטואלי הרלוונטי עולה ולכן כמות העסקאות בו מתרחבת. כל המחשבים המעורבים בתהליך נדרשים לבצע חישוב מתמטי מסובך שחוזר על עצמו בכל כמה דקות. משתמש אשר תורם מכוח המחשוב שלו לתהליך הרישום מתוגמל במטבעות

143 לדיון בנוזקות כשירות ראו סעיף א בפרק 5.

144 The Cost of Cybercrime, **לעיל** ה"ש 122, בעמ' 7.

145 **שם**, בעמ' 11; James Lewis, Economic Impact of Cybercrime – No Slowing Down (CSIS & McAfee 2018)

וירטואליים, וכך הופכת פעולת העיבוד המתמטי המכונה "כריית מטבעות" לפעולה שיש בצידה גמול כספי ניכר.

נוזקה שמטרתה כריית מטבעות וירטואליים מוטמעת במחשב האישי, במערכות מחשוב ענן (cloud) או במכשיר הטלפון הנייד המותקף, ומסיטה את משאבי המחשוב של המכשיר המותקף למטרת כריית מטבעות וירטואליים. מתקפות אלו מובילות בסופו של דבר לפגיעה קשה בתפקודן הרגיל של מערכות המחשב המותקפות ומניבות רווח כספי גבוה מאוד לתוקפים, המוערך בכ־2.5 מיליארד דולר במחצית הראשונה של שנת 2018. במחצית השנייה של שנת 2018 חלה עלייה ניכרת בהיקף השימוש בנוזקות לשם כריית מטבעות וירטואליים, וסביר שגם הרווח הכספי של התוקפים עלה בהתאם.[146]

II. העתקת מידע אישי והרשאות שימוש

בסוג זה של מתקפות סייבר נעשה שימוש בנוזקות כדי להעתיק מידע אישי לשם גניבת זהות או סיוע בגיבוש הרשאות גישה, למשל למערכות פיננסיות. מדובר, למשל, בחדירה למערכות מידע והעתקת מידע אישי רגיש, כגון שם, כתובת, שמות קרובי משפחה, מקום לידה, מספר תעודת זהות, מספר רישיון נהיגה, מספר כרטיס אשראי וכדומה, ומכירתם בשוק השחור או שימוש בפרטים לשם הונאת אשראי או הונאת בנקים; מכירת הרשאות כניסה לחשבון הבנק; או גניבת זהות לצורך התחזות וגישה למשאבים פיננסיים באמצעות צימוד של שם מלא, תאריכי לידה, כתובות, מספרי רשיון נהיגה ומספרי תעודות זהות או ביטוח לאומי.[147] פרטי כרטיס אשראי גנוב יימכרו בשוק השחור ב"רשת האפלה" בסכום של 4–80 דולרים, תלוי בסוג הכרטיס ובמסגרת האשראי.[148]

בשנים האחרונות העתקת מידע אישי נעשית לא רק באמצעות חדירה למערכות מחשב שקיימות פיזית בארגון, אלא גם באמצעות חדירה לשירותי הענן שבהם הארגון משתמש. שירותי מחשוב ענן מוצעים בתשלום ושלא

146 עודד ירון "אז מה זה לעזאזל כרייה? ולמה דווקא מונרו" **הארץ** (9.10.2017); מגמות תקיפת סייבר 2018, **לעיל** ה"ש 63, בעמ' 4; Leonard Kleinman, *A New Age of Malware – Cryptocurrency Mining*, Forbes (Jun 7, 2018)

147 Secureworks, 2016 Underground Hacker Markets Annual Report (2016)

148 שם.

בתשלום ומאפשרים אחסון, גיבוי ועיבוד של כמויות עצומות של מידע מרחוק. הענן מופעל, מתוחזק ומנוהל על ידי ספק שירותי הענן דוגמת אמזון, גוגל, מיקרוסופט ו־IBM.[149]

לשימוש בשירותי הענן יתרונות רבים: הם מאפשרים גישה מרחוק לקבצים מסוגים שונים מכל מכשיר ומכל מקום בעולם. בכך הם מגבירים את הפרודוקטיביות של המשתמש ומאפשרים לו לגשת למסמכים הנחוצים לו לעבודה או לפנאי מכל מקום תוך ניצול יעיל של הזמן. למשל, עובד יכול לעבוד בחופשיות על קבצים המאוחסנים בשירותי הענן של מקום עבודתו גם בזמן נסיעתו לעבודה ברכבת, ואין צורך בהעברת מסמכים בדוא"ל או בהעברת הקבצים הרצויים להתקן אחסון נייד. כמו כן, כאשר קבצים מאוחסנים בענן יכולים כמה משתמשים לעשות בהם שימוש בו בזמן, וכל אחד מהם רואה את השינויים שעושה האחר.[150]

אולם הפופולריות הגוברת של שירותי ענן הביאה עימה גם עלייה במתקפות הסייבר המתמקדות במידע רגיש המאוחסן בענן, וחלקן מצליחות עקב הגדרות לא מתאימות וניהול כושל של שירותי הענן עצמם. כ־51% מהארגונים הבינלאומיים, לרבות חברות ענק כגון פדקס והונדה, חוו במחצית הראשונה של 2018 מתקפות סייבר למטרות העתקת מידע שהן מחזיקות בשירותי ענן.[151] באפריל 2019 נחשפו על ידי צד שלישי חצי מיליארד רשומות שכללו מידע אישי על משתמשי פייסבוק, שאוחסנו על גבי שרתי ענן לא מוגנים של חברת אמזון; במרץ 2019 נחשף שחשבונות שהוגדרו באופן שגוי בשירות Box.com הובילו לזליגה של טרה־בייטים של מידע רגיש ביותר מחברות רבות שעשו שימוש בשירותי ענן אלו; ומידע פיננסי רגיש של 80 מיליון אמריקאים שאוחסן על הענן של חברת מיקרוסופט נחשף במהלך שנת 2019 ברשת האינטרנט.[152]

149 המעבר מאחסון ועיבוד על המחשב האישי לאחסון ועיבוד ב"ענן", כלומר מחשבים של ארגון אחר שאפשר לגשת אליהם באמצעות רשת האינטרנט, החל בתעשיית הסרטים והמוזיקה. בעבר האזנו למוזיקה וצפינו בסרטים שנשמרו על מחשבנו האישי, ואילו היום ההאזנה למוזיקה והצפייה בסרטים נעשות באמצעות שירות הזרמה (streaming) של קובצי האודיו והווידאו המאוחסנים על שרתים מרוחקים.

150 Eric Griffith, *What Is Cloud Computing?* PCMAG (June 29, 2020)

151 מגמות תקיפת סייבר 2018, **לעיל** ה"ש 63, בעמ' 5.

152 מגמות תקיפת סייבר 2019, **לעיל** ה"ש 68, בעמ' 6.

מגפת הקורונה הובילה לעלייה חדה ומיידית בשימוש בשירותי ענן, אשר לוותה בעלייה במתקפות הסייבר שכוונו נגד שירותים אלו.[153]

2. תחרות

אחד המניעים למתקפות סייבר הוא העתקת קניין רוחני לשם צמצום הפערים במחקר ופיתוח טכנולוגיות מתקדמות ורכישת יתרון כלכלי.[154] בשנת 2016 הוערך שכ־26% ממתקפות הסייבר באותה השנה היו ממניע זה.[155] בשנת 2017 נמצא שכ־47% מכלל מתקפות הסייבר על מפעלים באותה השנה בוצעו למטרת העתקת קניין רוחני לשם השגת יתרון תחרותי.[156]

כך, למשל, סין פעלה במשך שנים (וייתכן שאף עדיין פועלת) בתחום הסייבר במה שכונה "העברת העושר הגדולה בהיסטוריה".[157] מתקפות סייבר שמקורן בממשל הסיני שימשו להעתקת הקניין הרוחני של חברות מערביות רבות. לדוגמה, הממציא הבריטי ג'יימס דייסון טען שמתקפת סייבר הביאה להעתקת הקניין הרוחני שלו ולפיתוח וייצור שואבי אבק סיניים בעיצוב זהה לשלו. כמו כן, תוכניות הפיתוח של חברת בואינג למטוס המשא הצבאי האמריקאי היקר ביותר שפותח אי פעם, ה־C-17, והתוכניות של חברת לוקהיד מרטין למטוס התקיפה היקר והמשוכלל F-35, שימשו לפיתוח ולייצור של גרסאות דומות של מטוסים עבור צבא סין – מטוס משא ומטוס תקיפה המכונה F-31.[158]

153 מגמות תקיפת סייבר 2020, **לעיל** ה"ש 59, בעמ' 11.

154 Emily Mossburg, J. Donald Fencher, & John Gelinne, *The Hidden Costs of an IP Breach: Cyber Theft and the Loss of Intellectual Property*, 19 Deloitte Review 106 (2016)

155 Jeff Desjardins, *Why Hackers Hack: Motives Behind Cyberattacks*, Visual Capitalist (Jan. 3, 2018)

156 Widup et al., **לעיל** ה"ש 57.

157 כך כינה זאת ב־2012 קית' אלכסנדר, מנהל הסוכנות האמריקאית לביטחון לאומי (NSA) דאז; ראו Garrett M. Graff, *How the US Forced China to Quit Stealing – Using a Chinese Spy*, Wired (Nov. 10, 2018) (להלן: Graff, *How the US*).

158 **שם**; Amanda Macias, *America's Most Expensive Weapons System, the F-35, is a Key Symbol of Trump's Trade Gripe with China*, CNBC (March

גם חברת התרופות האמריקאית Charles River Laboratories דיווחה באפריל 2019 על פרצה באבטחת המידע בחברה שהובילה להעתקת מידע בקנה מידה נרחב. המידע שהועתק כלל מידע על לקוחות החברה אך לא כלל מידע אישי רגיש, לרבות מידע רפואי, ומשום כך חושדים כי מתקפת הסייבר כוונה להעתקת קניין רוחני כאמצעי לרכישת יתרון תחרותי בשוק התרופות.[159]

באוקטובר 2019 דווח שהאקרים מאיראן תקפו החל משנת 2013 ובמשך 4 שנים כ־170 אוניברסיטאות ברחבי העולם והצליחו להעתיק קניין רוחני בשווי 3.4 מיליארד דולר ולמכור אותו ללקוחות איראנים.[160] בשנת 2016 טענו גורמים אמריקאים שמתקפות סייבר שמקורן בסין הביאו להעתקת סודות מסחריים של חברות אמריקאיות הקשורים לייצור פלדה קלת משקל, ואלו שימשו לשכלול ייצור הפלדה בסין.[161]

מגפת הקורונה הביאה גם לעלייה בכמות מתקפות הסייבר המכוונות נגד חברות תרופות שונות ברחבי העולם העוסקות במחקר ובפיתוח תרופות וחיסונים לנגיף. על פי ההערכות המתקפות מתמקדות בכמה חברות תרופות ומאחוריהן עומדות קבוצות תוקפים המזוהות עם רוסיה וצפון קוריאה. מטרת המתקפות היא העתקת הקניין הרוחני – ממצאי המחקרים שחברות התרופות עורכות.[162]

22, 2018); Siobhan Gorman, August Cole, & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*, The Wall Street Journal (April 21, 2009)

159 Marianne Kolbasuk McGee, *Drug Lab Cyberattack Puts Spotlight on IP Theft Threat*, Bank Info Security (May 3, 2019)

160 Significant Cyber Incidents Since 2006, Center for Strategic & International Studies (2020)

161 Kevin L. Jackson, *China Linked to Lockheed Martin Cyber Attack*, Forbes (Jun. 8, 2011); Dennis C. Blair & Keith Alexander, *China's Intellectual Property Theft Must Stop*, The New York Times (Aug. 15, 2017)

162 Tara Seals, *Nation-State Attackers Actively Target COVID-19 Vaccine-Makers*, Threat Post (Nov. 13, 2020); Robert McMillan, *Covid-19 Vaccine Makers Face Russian, North Korean Cyberattacks, Microsoft Says*, The Wall Street Journal (Nov. 13, 2020); Alfred Ng, *Russian and North Korean Hackers are Targeting COVID-19 Vaccine Researchers*, Cnet (Nov. 13, 2020)

3. לוחמת תודעה

מניע נוסף למתקפות סייבר הוא לוחמת תודעה: רצון לעורר מודעות למאבק או לרעיון, להשפיע על דעת הקהל בנושא מסוים או להטות את השיח לטובת אינטרס מסוים, לזרוע פחד ולגרום לתחושה של אובדן הביטחון האישי.

לוחמת תודעה אינה תופעה ייחודית למרחב הסייבר; תעמולה הייתה רכיב יסוד באסטרטגיית השלטון של האימפריה הרומית, ובמלחמת העולם הראשונה היה תפקיד חשוב לתעמולה ולשימוש בתקשורת לצורכי השלטון.[163]

אולם המאפיינים של מרחב הסייבר ושל תעבורת המידע בו שינו ללא הכר את השימוש בלוחמת תודעה, והתפתחותן של טכנולוגיות לאיסוף, עיבוד והפצה של מידע שכללו עד מאוד את היכולת להשפיע על תודעת המונים ויחידים אף מבלי לנקוט פעולה במרחב הפיזי. הפצת תוכן במרחב הסייבר יעילה, פשוטה, מהירה ומקיפה יותר מאשר במרחב הפיזי; עלות הפצת מידע ברשת האינטרנט, לרבות פרסום פוסט ברשת חברתית, היא אפסית, ולעת עתה אפשר להפיץ מידע במרבית הרשתות החברתיות אף ללא מתווכים שיש בכוחם למנוע את פרסום התוכן מראש. כאשר כ־67% מהאמריקאים ניזונים בעיקר ממידע המפורסם ברשתות חברתיות ולא מאתרי חדשות מוכרים ומקצועיים קל מאוד להפיץ מסרים מטעים או שקריים (פייק ניוז), שכן חלק לא קטן מהציבור אינו מייחס חשיבות לאמינות המידע.[164]

לוחמת תודעה במרחב הסייבר מתבצעת באמצעות מנעד רחב של פעולות, הכולל העתקה, חסימה או מחיקה של מידע לצד שתילה והפצה של מידע רב ושקרי במגוון דרכים, כגון פוסטים ברשתות חברתיות, תגוביות, מאמרי חדשות ואתרי אינטרנט ייעודיים המתחזים לאתרי חדשות אמינים.[165]

163 רון שלייפר **לוחמה פסיכולוגית: ויישומיה בהיסטוריה העולמית ובמזרח־התיכון** (2007); רון שלייפר "יוצאים למלחמה פסיכולוגית" **הידען** (4.3.2009).

164 Joshua Danielson, *The Current State of Information Warfare*, Forbes (Feb. 15, 2018)

165 Susan McCorriston, *Memes That Kill: The Future of Information Warfare*, Constella Intelligence (April 30, 2020)

כמו כן, המידע האישי הרב שנמצא ברשת האינטרנט מאפשר פילוח של מאפייני האישיות של כל אחד ואחד מאיתנו. הפילוח משמש זה מכבר לשם התאמה אישית של פרסומות, אולם נעשה בו גם שימוש למטרות לוחמת תודעה. בדרך זו אפשר להתאים את המסר ולהפנות אותו (לטרגט) לקבוצות משתמשים או למשתמש ספציפי הרלוונטיים לו ביותר או הצפויים להיות מושפעים ממנו במידה הרבה ביותר. כך אפשר לבצע מניפולציות אינדיבידואליות ולהשפיע על קהלי יעד שונים במהירות, ביעילות ובהיקפים חסרי תקדים.[166]

כך, למשל, בפרשת "קיימברידג' אנליטיקה" נעשה ניסיון לבצע מניפולציות על קהלים מסוימים או משתמשים מסוימים בהתאם למאפייני האישיות שלהם, כפי שנלמדו מהשימוש ברשתות חברתיות. חברת קיימברידג' אנליטיקה השיגה באופן בלתי מורשה מידע אישי על 50 מיליון משתמשי פייסבוק, ועל בסיסו הפיקה ניתוחי אישיות של משתמשי הרשת החברתית. בהמשך נשכרה החברה על ידי מטה הבחירות של דונלד טראמפ כדי להתאים מסרי תעמולה אישיים לקבוצות מסוימות של בוחרים, בעיקר אלו שפילוח האישיות שלהם הצביע על מאפייני אישיות חרדתיים.[167]

מרבית מתקפות הסייבר למטרות לוחמת תודעה מבוצעות בשימוש בבוט־נטים, המתחזים למשתמשים אנושיים או מופעלים לצורך תפעול מתקפות מניעת שירות רבות משתמשים. מתקפות אלו משמשות להפלת אתרי אינטרנט

166 גבי סיבוני "מלחמת התודעה הראשונה" **הערכה אסטרטגית 2017-2016** 193, 194 (המכון למחקרי ביטחון לאומי 2016); David Stupples, *What is Information Warfare?*, World Economic Forum (Dec. 3, 2015); Dragan Z. Damjanovic, *Types of Information Warfare and Examples of Malicious Programs of Information Warfare*, 65 Military Technical Courier 1044 (2017); Alex Zaheer, *Information Warfare: Western Democracies' Waterloo?*, Stanford Politics (Oct. 27, 2017)

167 Matthew Rosenberg, Nicholas Confessore, & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, The New York Times (March 17, 2017); Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, The Guardian (March 17, 2018)

של רשויות המדינה או של חברות גדולות, במטרה לזרוע פחד בציבור ולגרום לאובדן תחושת הביטחון האישי.[168]

מתקפות סייבר מסוג זה מקורן לרוב במדינות, אבל לוחמת תודעה אינה מוגבלת רק לזו המופעלת בין ממשלות או צבאות. ממשלות מפעילות עובדי ממשל, חברות פרטיות, אזרחים הפועלים תמורת תשלום ומתנדבים כחלק ממערך לוחמת תודעה המכוונת כלפי אזרחי המדינה, במטרה לשכנע את האחרונים בצדקת פעולותיו של השלטון הנוכחי; מועמדים לתפקידים ציבוריים או פוליטיים נוקטים פרקטיקות של לוחמת תודעה במהלך מערכת הבחירות; ארגוני טרור מנסים להשפיע על תודעת האויב או להניע פעילים פוטנציאליים לצאת ולבצע מעשי טרור; וארגונים לא ממשלתיים (NGOs) משתמשים בלוחמת תודעה כדי להביא לידיעת הציבור נושאים שונים.[169] התוקפים מנצלים את היכולת להעביר מסרים, לרבות מסרים שקריים, במהירות ובתפוצה רחבה, בעיקר באמצעות בוט־נטים, וכך להשפיע על דעת הקהל או ליצור פאניקה בציבור.[170] כמו כן, במרחב הסייבר לוחמת התודעה אינה מוגבלת רק למצב מלחמה, אלא היא מתרחשת גם בעיתות שגרה.[171]

על פי ההערכות, במהלך מערכת הבחירות לנשיאות ארצות הברית בשנת 2016 שתלה רוסיה חדשות כוזבות התומכות במועמדותו של טראמפ, והפעילה טרולים ובוט־נטים בהיקפים גדולים אשר פעלו ברשתות החברתיות והפיצו תמונות ופוסטים שהכילו מסרים המעודדים תמיכה בטראמפ או מציגים באור

168 דור צח ומישל אודי "מלחמת האקרים נמשכת: אתר הבורסה ואתר אל־על נפלו" **כלכליסט** (16.1.2012).

169 סיבוני, **לעיל** ה"ש 166, בעמ' 194; Desjardins, **לעיל** ה"ש 155; Samantha Bradshaw & Philip N. Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation* 15–16 (University of Oxford, Computational Propaganda Research Project, Working Paper No. 2017.12, 2017)

170 הכט, **לעיל** ה"ש 92; Markoff, **לעיל** ה"ש 92; Bessi & Ferrara, **לעיל** ה"ש 92; Earle, **לעיל** ה"ש 92.

171 רן בר זיק "צבא בוטים שהגיב לטובת בוגי יעלון נתפס ברשת" **Internet Israel** (19.8.2018); Keir Giles, Handbook of Russian Information Warfare 4 (NATO Defence College Fellowship Monograph Series 9, 2016)

שלילי את הילרי קלינטון. בעזרת פילוח מאפייני אישיות לפי מידע אישי גלוי ברשתות החברתיות התאימו הרוסים את המסרים לקבוצות המתאימות. כך, למשל, בקבוצות של נוצרים אדוקים הופצה תמונה של הילרי קלינטון בדמות השטן נאבקת בישו בצירוף הכיתוב "עשה לייק אם אתה רוצה שישו ינצח!", ואילו בקבוצות של חיילים, אנשי מילואים ויוצאי צבא הופצה תמונה של יוצא צבא עני וחסר בית לצד מהגר בריא למראה הלובש חולצה שעליה הכיתוב "לא מתועד, לא מפחד, לא מתנצל", בשילוב הכיתוב "יוצא צבא זה לא מקבל דבר, ואילו מהגר בלתי חוקי זה מקבל הכול; לייק אם אתה חושב שזו חרפה".

כמו כן, מתקפת סייבר על מחשבו האישי של ג'ון פודסטה, מנהל מטה הבחירות של הילרי קלינטון, שבוצעה על פי הערכות על ידי יחידות מצבא רוסיה, הביאה לחשיפת דברים שנשאה קלינטון בהרצאות סגורות לקהלים שונים טרם התמודדותה. חלקים מהרצאות חסויות אלו הודלפו בתזמון מושלם לפני עימותים טלוויזיוניים בין המועמדים, ואף שולבו במסרים ישירים לבוחרים שבהם נטען כי על אף הרטוריקה הליברלית שלה, בפועל קלינטון תומכת בוול סטריט, שהמסחר בה נתפס באותה עת כמושחת וכמעצים את האי־שוויון החברתי והכלכלי בארצות הברית.[172]

מקרים נוספים של שימוש במתקפות סייבר לשם השפעה על תודעה ודעת קהל התרחשו לאחר הפלת המטוס המלזי מעל אוקריאנה בשנת 2015. עיתונאי בריטי פרסם ראיות המצביעות כי רוסיה מעורבת בהתרסקות המטוס, ובתגובה

172 Jane Mayer, *How Russia Helped Swing the Election for Trump*, The New Yorker (Sep. 24, 2018); Kathleen Hall Jamieson, Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't and Do Know (2018); Molly Mckew, *Did Russia Affect the 2016 Election? It's Now Undeniable*, Wired (Feb. 16, 2018); David E. Sanger, *Putin Ordered "Influence Campaign" Aimed at U.S. Election, Report Says*, The New York Times (Jan. 6, 2017). בעגה המקצועית יש מונחים רבים לתיאור פעילויות שמטרתן השפעה על התודעה: מבצעי תודעה, לוחמת תודעתית, לוחמה פסיכולוגית ו־"hacking the people". כשמתייחסים לשימוש בכלי סייבר לצורך פעילויות אלו, המינוח הנפוץ הוא זה הרוסי – לוחמת מידע. ראו Giles, **לעיל** ה"ש 171, בעמ' 7; P. W. Singer & Emerson T. Brooking, *How the Kavanaugh Information War Mirrors Real Warzones*, Wired (Oct. 2, 2018). ראו גם שוורץ אלטשולר ולוריא, **לעיל** ה"ש 94; רון שמיר ואלי בכר **התקפות סייבר על הבחירות – איך מתמודדים?** (מחקר מדיניות 136, המכון הישראלי לדמוקרטיה 2019).

פרסמו כלי תקשורת ברוסיה חדשות ומאמרים המטילים ספק באמינותו ובעבודתו של אותו עיתונאי והתוקפים אותו אישית.[173] גם לאחר סיפוח האי קרים השתמשה רוסיה בלוחמת תודעה בניסיון ליצור ערפל ולמנוע את החשיפה של גודל הכוח הצבאי שהיה מעורב במבצע ושל מספר ההרוגים במהלך הלחימה וניסיונות הסיפוח.[174] בכיר בנאט"ו תיאר את פעילות לוחמת התודעה הרוסית בזמן העימות באי קרים: "אם מסתכלים על הפעילות של הרוסים בעת סיפוח חצי האי קרים והפלישה למזרח אוקראינה, השימוש בלוחמת מידע היה מרכזי, וכלל לא רק שינוי הנרטיב לטובת הרוסים אלא גם שיבוש, הטעיה ושיטוי במידע, ממש כמו מיסוך עשן".[175]

במחצית הראשונה של 2020 הביאה מגפת הקורונה לעלייה בהיקף מתקפות הסייבר למטרות מלחמת תודעה, בעיקר בהקשר של ניסיונן של מדינות להכפיש זו את זו בכל הקשור לטיפול במגפה, השקיפות של סין באשר להתפרצות המגפה, תרופות אפשריות לטיפול במגפה וזמינותם של חיסונים.[176]

4. הפקת רווח פוליטי, ביטחוני או מדיני

מתקפות סייבר יכולות להניב לתוקפים רווח פוליטי, ביטחוני או מדיני בדרכים נוספות פרט ללוחמת תודעה.

I. איסוף מודיעין ומידע רגיש

מטרת האיסוף היא השגת מידע בנושאים שונים, כגון יכולות צבאיות של מדינות, תוכניות עתידיות של הארגון המותקף או מידע סודי אחר שיקנה יתרון אסטרטגי למי שיחזיק בו.

173 Ellen Nakashima, *Russian Hackers Harassed Journalists Who Were Investigating Malaysia Airlines Plane Crash*, The Washington Post (Sep. 28, 2016)

174 Gabriela Baczynska, *Russia Says No Proof It Sent Troops, Arms to East Ukraine*, Reuters (Jan. 21, 2015)

175 House of Commons Defence Committee, Russia: Implications for UK Defence and Security (2016)

176 מגמות תקיפת סייבר 2020, **לעיל** ה"ש 59, בעמ' 11.

מתקפות סייבר למטרות איסוף מודיעין מבוצעות לרוב על ידי מדינות, בשל המשאבים הדרושים לשם כך והיכולת לפעול מתוך ראייה אסטרטגית ארוכת טווח. מתקפת סייבר לאיסוף מודיעין מחייבת לרוב חדירה לרשתות מחשב מבודלות, שאינן מחוברות לרשת חיצונית, ושבהן על פי רוב מאוחסן מידע רגיש. חדירה לרשתות כאלה דורשת השקעת משאבים, שימוש ביכולת טכנולוגית מתקדמת ולעיתים אף מעורבות של סוכני מודיעין אשר נמצאים פיזית ביעד המותקף.[177]

מתקפות סייבר למטרות איסוף מודעין עושות שימוש בשיטות הפצה מוכרות, כמו דיוג.[178] בחלק מהמתקפות משמשות נוזקות המכונות "air-gap malware", המופצות באמצעות התקן נייד (דיסק און קי), גלי רדיו[179] או צלילים ממיקרופון המחשב, ואף באמצעות רעשי הפעילות של הדיסק הקשיח שאוזן אנושית איננה שומעת.[180] ייחודן של נוזקות אלה, כאמור, ביכולתן לשלוף מידע מרשתות סגורות.[181] למשל, נוזקת סטקסנט (Stuxnet) הוחדרה אל מערכת המחשבים הסגורה של תוכנית הגרעין האיראנית באמצעות התקן נייד, שכנראה חובר על ידי סוכן של רשות מודיעין מדינתית לאחד מהמחשבים שלא היה מחובר לאינטרנט.[182] לפי המידע שהדליף אדוארד סנודן, הסוכנות לביטחון לאומי (NSA)

177 Sam Pudwell, *Q&A: Staying Alert for State-Sponsored Cyber Attacks*, ITProPoratal (Nov. 11, 2016); Kim Zetter, *Hacker Lexicon: What is an Air Gap?* Wired (Aug. 12, 2014) (להלן: Zetter, *Hacker Lexicon*).

178 Graff, *How the US*, **לעיל** ה"ש 157.

179 David E. Sanger & Thom Shanker, *N.S.A. Devises Radio Pathway into Computers*, The New York Times (Jan. 15, 2014); Wikileaks (@wikileaks), Twitter (June 22, 2017, 12:14 pm)

180 Mordechai Guri, Matan Monitz, & Yuval Elovici, *Bridging the Air Gap Between Isolated Networks and Mobile Phones in a Practical Cyber-Attack*, 8 (4) ACM Transactions on Intelligent Systems and Technology (2017)

181 Zetter, *Hacker Lexicon*, **לעיל** ה"ש 177; Guri, Monitz & Elovici, **שם**. על פי רוב גופים אלו מאחסנים את המידע הרגיש שברשותם במערכות סגורות שאינן מונגשות או מחוברות לרשת האינטרנט הפומבית.

182 Zetter, *Hacker Lexicon*, **לעיל** ה"ש 177.

וסוכנות הביון המרכזית (CIA) האמריקאיות משתמשות בגלי רדיו כאמצעי לאיסוף מודיעין מרשתות סגורות.[183]

II. שיתוק תשתיות קריטיות במדינה או החלשה של העורף

תשתיות קריטיות הן המערכות, השירותים והנכסים הפיזיים או הווירטואליים החיוניים לתפקודה התקין של מדינה, לביטחונה הלאומי, ליציבותה הכלכלית ולבריאות תושביה.[184] התחבורה היבשתית, הימית והאווירית, מערכות החשמל, המים, הגז והבנקאות, שירותי החירום ומערכת הבריאות נחשבים כולם תשתיות קריטיות.[185]

מרבית התשתיות הקריטיות בארץ ובעולם מנוהלות ומופעלות באמצעות מערכות בקרה ושליטה דיגיטליות (Supervisory Control and Data Acquisition, ובקיצור "SCADA") המתווכות בין העולם הפיזי למרחב הסייבר באמצעות בקרים לוגיים מתוכנתים. מערכת SCADA מאפשרת בחלק מהמקרים גם גישה מרחוק. למשל, במקרה של מערכות מים תיתכן שליטה מרחוק בהפעלתן וכיבוין של משאבות השואבות מים ממאגרי מים, בהתאם לכמות המים במאגר, וכן שליטה בזרימת מים בסכר ובמידת הצורך גם סגירה שלו.

מתקפות הסייבר המיועדות לפגוע בתשתיות קריטיות מתמקדות לרוב במערכות ה־SCADA. על פי רוב מבוצעת מתקפת סייבר על תשתיות קריטיות על ידי שחקנים מדינתיים, שכן ביצועה מחייב השקעת משאבים אנושיים וכספיים רבים, ופעמים רבות היא עושה שימוש בחולשות יום אפס. המניע למתקפות אלה הוא בדרך כלל השגת מטרות מדיניות, כחלק ממאבק מזוין

183 Sanger & Shanker, **לעיל** ה"ש 179.

184 Ryan K. Baggett & Brian K. Simpkins, Homeland Security and Critical Infrastructure Protection 3–5 (2018); Eldar Haber & Tal Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis*, 44 Fla. St. U. L. Rev. 515, 518–520 (2017)

185 תוספת ראשונה עד תוספת חמישית לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1998, ס"ח 348; *Presidential Policy Directive: Critical Infrastructure Security and Resilience* (2013)

בין מדינות מסוכסכות או כפעילות של ארגון טרור. ואולם, לעיתים מבוצעות מתקפות סייבר מסוג זה על ידי ארגוני פשיעה לצורך הפקת רווח כלכלי.[186]

כך, למשל, מתקפת הסייבר על מערכת הפקת האורניום האיראנית באמצעות נוזקת סטקסנט, שהופעלה באתרי הגרעין באיראן בין השנים 2010–2007, פגעה במערכת ה־SCADA. הנוזקה גרמה למתן הוראה להאצת קצב הסיבוב של הצנטריפוגות המעשירות את האורניום עד להתרסקותן, תוך הסתרת ההתרחשות מצגי הבקרה של מערכת ה־SCADA, אשר הציגו כל אותה עת דיווחים על פעילות תקינה.[187] כך הביאה הנוזקה לעיכוב בתוכנית הגרעין האיראנית ועוררה פאניקה בקרב אנשי תוכנית הגרעין ומקבלי ההחלטות באיראן, מחשש לחדירה למערכותיהם ולחשיפת סודות ביטחוניים רגישים.[188] לפי דיווח של משרד ההגנה האמריקאי ממרץ 2018, נמצא שתוקפים המזוהים עם הממשל הרוסי ניסו במשך כשנתיים להתקיף תשתיות קריטיות בארצות הברית בדרכים שונות, כגון דיוג וסוסים טרויאניים, בין השאר על ידי תקיפת מערכות ממוחשבות של צדדים שלישיים ששימשו קבלני משנה של בעלים או מפעילים של תשתיות קריטיות בארצות הברית, והכול במטרה להשיג גישה למערכות הממוחשבות של התשתיות הקריטיות המותקפות.[189] האיראנים תקפו בשנת 2012 את מערכות המחשב של ארמקו הסעודית (Saudi Aramco), אחת מחברות הנפט הגדולות בעולם, ואת תאגיד האנרגיה הקטארי ראסגז (RasGas).[190] בחג המולד של שנת 2015 הצליחה ממשלת רוסיה להביא לקריסת אספקת החשמל בבתים רבים באוקראינה באמצעות מתקפת סייבר. המניע

186 אלדר הבר וטל ז'רסקי "דרכי ההגנה על תשתיות חיוניות במרחב הסייבר בישראל" **משפט וממשל** יח 99, 107–106 (2017).

187 Nicolas Falliere, Liam Murchu, & Eric Chein, *W32.Stuxnet Dossier*, Symantec (2011)

188 גבי סיבוני וסמי קרוננפלד "לוחמת הסייבר של איראן" **צבא ואסטרטגיה** 4 (3), 76 (2012).

189 *Alert (TA18-074a): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, US-CERT (March 16, 2018)

190 יוסי הטוני "הגבינה זזה: מתקפת סייבר תגבה מחיר בחיי אדם" **PC אנשים ומחשבים** (14.6.2018).

לתקיפה, לפי אחת הסברות, היה מאבק ממשלת רוסיה בסירובה של אוקראינה להשלים עם הפלישה הרוסית לחצי האי קרים.[191] לפי דיווחים בתקשורת, בשנת 2013 ניסה ארגון סורי לתקוף באופן דומה את מערכת המים בחיפה. באפריל 2020 הותקפו בישראל מערכות ה־SCADA של מתקני מים של תאגידי מים וביוב, במתקפת סייבר שמאחוריה עומדת איראן.[192]

גם כאשר אין מדובר בתשתיות קריטיות, מתקפות סייבר על חברות וארגונים יכולות להחליש מאוד את תחושת הביטחון של אזרחי המדינה. מתקפות נרחבות ולאורך זמן על חברות ביטוח, עסקים בינוניים וכיוצא באלה יכולות ליצור אפקט חברתי וציבורי הדומה ל"טפטוף" של מתקפות בנשק קונבנציונלי, כגון טילים על העורף.

5. נקמה

חלק ממתקפות הסייבר מבוצעות על ידי או בהוראת לקוחות כועסים, עובדים לשעבר בארגון המותקף או אנשים אחרים הרוצים מנימוקים אישיים שונים לנקום באדם או בארגון המותקפים. נכון לשנת 2016 היה זה המניע לכ־20% מכלל מתקפות הסייבר בעולם.[193]

6. תהילה ורווח אישי של התוקף, צבירת מוניטין בקרב קהילת ההאקרים

שיעור קטן יחסית ממתקפות הסייבר מבוצעות מתוך הנאה או רצון לצבור מוניטין בקרב קהילת ההאקרים, או כדי להוכיח מקצועיות וניסיון בתחום.[194]

191 גבי סיבוני וצבי מגן "מתקפת סייבר נגד תשתית החשמל באוקריאנה – קריאת אזהרה (נוספת)" **מבט על** 798 (המכון למחקרי ביטחון לאומי 2016).

192 "ארגון סורי ערך מתקפת סייבר נגד מערכת המים" **ynet** (25.5.2013); אחיה ראב"ד "חשד למתקפת סייבר חריגה על שורת מתקני מים בישראל" **ynet** (26.4.2020); ליאור גוטמן "מתקפת הסייבר על תשתיות המים חושפת כאוס בסמכויות החירום" **כלכליסט** (24.5.2020).

193 Desjardins, **לעיל** ה"ש 155.

194 *Denial of Service (DoS) Guidance*, לעיל ה"ש 89.

ג. זהות התוקפים - טשטוש ההבחנה בין שחקנים מדינתיים לשחקנים א־מדינתיים

עם השתכללות מטרותיהן של מתקפות הסייבר היטשטשה ההבחנה המקובלת בין מתקפות סייבר המבוצעות בידי שחקנים א־מדינתיים, בעיקר ארגוני פשיעה, לאלו המבוצעות ביוזמת מדינות ריבוניות. הראשונות היו ממוקדות בהשגת רווח כלכלי, בעוד האחרונות נועדו להשיג הישגים גיאו־פוליטיים. לצד המטרות השונות, הייתה מקובלת גם הבחנה בין ההיקף השונה של מתקפות הסייבר: מתקפות שמומנו או שבוצעו על ידי מדינות דרשו משאבים כספיים ואנושיים גדולים יותר ועל כן היו מורכבות ומתוחכמות יותר, כללו איסוף מודיעין נרחב וחשיפת חולשות "יום אפס" והתמקדו בפגיעה בתשתיות קריטיות של המדינה היריבה.[195]

ואולם, כיום מקובל שבכל הנוגע להגנת מרחב הסייבר אין לייחס חשיבות יתרה לזהות התוקפים ולהבחנה בין מתקפת סייבר במימון מדינה ריבונית למתקפת סייבר במימון ארגוני פשיעה, מכמה סיבות. ראשית, זיהוי העומדים מאחורי מתקפת סייבר קשה ומאתגר ומחייב השקעת משאבי מחקר לא מבוטלים. ההאקרים פועלים תחת זהויות בדויות, מנצלים טכניקות המאפשרות אנונימיות ברשת ומנסים לטשטש את עקבותיהם.[196] כך, למשל, אתר ההיכרויות "אשלי מדיסון", הפונה לאנשים נשואים, היה נתון למתקפת סייבר שהובילה לחשיפת פרטי משתמשיו ביולי 2015. התקיפה בוצעה על ידי קבוצה שזיהתה את עצמה בשם "אימפקט טים" (Impact Team). עד כה לא הצליחו החוקרים לאתר את זהות התוקפים.[197]

195 Rajiv Gupta, *These Types of Hackers are Driving Cyber Attacks Now*, Fortune (March 21, 2016); Nick Ismail, *Money, Terrorism or Nation State Snooping – How Understanding the Real Motives Behind Cyberattacks Can Help to Prevent Them*, InformationAge (June 30, 2017)

196 Louise Matsakis, *To Identify a Hacker, Treat Them Like a Burglar*, Wired (Aug. 12, 2018)

197 Mark Ward, *Ashley Madison: Who Are the Hackers Behind the Attack?* BBC News (Aug. 20, 2015); Nate Lord, *A Timeline of the Ashley Madison Hack*, DataInsider (July 27, 2017)

שנית, הנזק העשוי להיגרם ממתקפת סייבר המבוצעת על ידי יחידים או ארגוני פשע אינו פעוט. מסיבה זאת הגדיר פורום הכלכלה העולמי את מתקפות הסייבר כאחד מארבעת הסיכונים העיקריים לכלכלה הגלובלית, מבלי להבחין בין מתקפות המבוצעות במימון מדינה ריבונית למתקפות המבוצעות על ידי ארגוני פשיעה או האקרים עצמאים.[198]

שלישית, ארגוני פשיעה פועלים פעמים רבות במהירות להשגת רווח כלכלי, ומשום כך גוברת הסכנה כי יפעלו באופן חובבני ויגרמו נזק כבד לתשתיות קריטיות אף מבלי שהתכוונו לכך. למשל, מתקפת סייבר שאורגנה כנראה על ידי ארגון פשע עשתה שימוש בנוזקה מסוג תולעת שהופצה באמצעות בוט־נטים, והביאה להפסקת פעילותו של מפעל להפקת נפט וגז בערב הסעודית למשך זמן מה.[199] כמו כן, ככל שיגדל מספרן של מתקפות הסייבר הגורמות נזק כלכלי כבד יפחת אמון הציבור באמינותן של מערכות ממוחשבות, וחברות וארגונים יתקשו לחזור לשווי הכלכלי שלהם קודם למתקפה. הצטברותם של נזקים שכאלו עשויה להביא לפגיעה בכלכלתה של מדינה הדומה בהשפעתה לפגיעה בתשתית קריטית.[200]

רביעית, לפעמים קיימת חפיפה גם במטרות מתקפת הסייבר, ומתקפת סייבר במימון מדינה ריבונית עשויה להתמקד בהשגת רווח כלכלי. לדוגמה, מתקפת הסייבר WannaCry, שהתרחשה במאי 2017, עשתה שימוש בנוזקת כופר

198 World Economic Forum, The Global Risks Report 2018, 61 (13th Edition, 2018)

199 Derek Hawkins, *The Cybersecurity 202: These Researchers Worry More About Cybercriminals Hacking the Grid than Nation-State Hackers*, The Washington Post (Aug. 29, 2018)

200 Pierluigi Paganini, *Two-factor Authentication for SMBs*, Security Affairs (July 1, 2013); Yong Wu, Gengzhog Feng, Nengmin Wang, & Huigang Liang, *Game of Information Security Investment: Impact of Attack Types and Network Vulnerability*, 42 Expert Sys. with Applications 6132, 6132-6133 (2015); Symantec, Internet Security Threat Report (vol. 20, 2015); Wojciech Mazurczyk, Szymon Drobniak, & Sean Moore, *Towards a Systematic View on Cybersecurity Ecology*, *in* Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities 17, 17-18, 22-27 (Babak Akhgar & Ben Brewster eds., 2016)

ואורגנה על פי ההערכות על ידי המשטר בצפון קוריאה כדי להשיג מימון לפעילותו. על פי הדיווחים הניבה מתקפת הסייבר למשטר הצפון־קוריאני 140,000 דולר בביטקוין.[201]

חמישית, פעמים רבות התוקפים כלל אינם שולטים בנתיב התפוצה של הנוזקה. מתקפת הסייבר NotPetya מדגימה זאת: המתקפה אורגנה על ידי רוסיה במטרה לפגוע באוקריאנה ולהרתיע בעלי עסקים ומדינות אחרות מיצירת קשרים עסקיים עימה. בפועל, מתקפת הסייבר התפשטה במהירות וביעילות ופגעה אפילו בחברת הנפט רוסנפט (Rosneft) שבבעלות ממשלת רוסיה. קשה להאמין שרוסיה רצתה בכך כאשר הנוזקה שוחררה לרשת האינטרנט.[202]

שישית, קיימת זליגת ידע בין המגזר העסקי למגזר הציבורי ולהפך, עקב היחסים הקרובים בין גופי המודיעין המדינתיים לאקדמיה ולתעשייה, המעבר של מומחי סייבר מהמגזר הציבורי למגזר הפרטי והדלפות על שיטות איסוף המודיעין.[203] בשל זליגת ידע זו מיטשטשת ההבחנה בין יכולות מדינתיות לאיסוף מודיעין, לפיתוח נוזקה ולהפצתה ובין יכולותיהם של חברות ואנשים פרטיים. עם האחרונים נמנות למשל חברות העוסקות במתן שירותי סייבר התקפי,[204] המספקות איסוף, מעקב וריגול במרחב הסייבר ברמה הבינלאומית ועשויות אף למכור כלי איסוף מודיעין ונוזקות, בדרך כלל למדינות עולם שלישי.[205] חברות

201 Danny Palmer, *WannaCry Ransomware: Hackers Behind Global Cyberattack Finally Cash Out Bitcoin Windfall*, ZDNet (Aug. 3, 2017); Ellen Nakashima & Philip Rucker, *U.S Declares North Korea Carried Out Massive WannaCry Cyberattack*, The Washington Post (Dec. 19, 2017)

202 Greenberg, *The Untold Story*, **לעיל** ה"ש 52.

203 כמו המידע שהדליף ב־2013 אדוארד סנודן, עובד לשעבר ב־NSA, וחשיפות שיטות איסוף המודיעין של ה־CIA באתר ויקיליקס; עידו סיון־סביליה "היזהרו, המדינה היא סוכן כפול" **TheMarker** (28.3.2017); Ewen Macaskill & Gabriel Dance, *NSA Files: Decoded, What the Revelations Mean for You*, The Guardian (Nov. 1, 2013)

204 ראו הדיון בטקסט הנלווה להערות שוליים 75–88 בנוגע לחברות המפתחות סייבר התקפי.

205 Bill Marczak & John Scott-Railton, *The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender*, The Citizen Lab (Aug. 24, 2016)

אלו מסוגלות למפות את איומי הסייבר ומתקפות הסייבר ברמה הגלובלית, לזהות את מקור האיום במרחב הסייבר ומאפייניו הטכנולוגיים, ולסייע בתיקון החולשות במרחב הסייבר ברמה המדינתית. להבדיל מחברות פרטיות אלו, למדינות אין בהכרח הכלים והיכולות הדרושים כדי לבצע חקירות בינלאומיות רחבות, או לחלופין – הן אינן רוצות לחשוף כלים אלה. חברות הסייבר ההתקפי וענקיות אבטחת המידע הפכו במידה מסוימת ל"אינטרפול של מרחב הסייבר", ללא רגולציה וללא פיקוח.

כמו כן, לא רק שאין ערובה לניטרליות של חברה המונעת משיקולים פנימיים שלה, כלכליים ומקצועיים, לעיתים חברות אבטחת מידע או סייבר התקפי אף מזוהות עם מדינה מסוימת. לדוגמה, חברת אבטחת המידע קספרסקי נחשבת שחקן מרכזי בתחום המודיעין במרחב הסייבר, שכן יש לה יכולת לחקור את מאפייני הנוזקה, לקשר אותה לנוזקות אחרות ולאתר את מקורה. אולם לאחרונה היא הואשמה ביחסים קרובים עם הממשל הרוסי ובריגול לטובתו דרך מוצריה המותקנים על מיליוני מחשבים ברחבי העולם.[206] החששות למעורבות ממשלות מסוימות בפעולתיהן של חברות אבטחת מידע מדגישים עוד יותר את טשטוש ההבחנה בין יכולות מדינתיות ליכולות א־מדינתיות.

משום כך, בזמן אמת פעולות ההגנה מתמקדות בהפסקת המתקפה, במזעור נזקיה ובחזרה לתפקוד שגרתי של המערכות המותקפות; המצוד אחר התוקפים והענשתם נעשים ברמה המדינתית בשלב מאוחר יותר. לדוגמה, כשמונה חודשים לאחר מתקפת הסייבר NotPetya, אשר החלה בפגיעה במערכות מחשב ותשתיות קריטיות באוקראינה אולם במהרה שיתקה חברות וממשלות ברחבי העולם, הכריזו שירותי הביטחון באנגליה ובארצות הברית כי מאחורי התקיפה עומדת מדינה – רוסיה.[207] הבולשת הפדרלית האמריקאית

206 Olivia Solon, *US Government Bans Agencies from Using Kaspersky Software Over Spying Fears*, The Guardian (Sep. 13, 2017); Jack Stubbs, *Kaspersky Lab to Open Swiss Data Center to Combat Spying Allegations*, Reuters (May 15, 2018); *Dutch Government Dropping Kaspersky Software Over Spying Fears*, VOA News (May 15, 2018)

207 Ellen Nakashima, *Russian Military was Behind "NotPetya" Cyberattack in Ukraine, CIA Concludes*, The Washington Post (Jan. 13,

(FBI) מחזיקה ברשימה של 59 האקרים מבוקשים, שמרביתם נחשדים בביצוע מתקפות סייבר במימון מדינה ריבונית כגון רוסיה, איראן, סין וצפון קוריאה; אחד מהמבוקשים הוא פקיסטני החשוד בביצוע מתקפת סייבר במסגרת פשע מאורגן.[208]

בשנים האחרונות החלו חברות פרטיות וגם מדינות לנקוט את שיטת הסייבר ההתקפי כאמצעי הגנה עצמית (פעולה המכונה hackback) למטרות שונות, כגון להביא לסיומה של מתקפת סייבר נגדם, לזהות את התוקף או להרוס את המידע שהועתק מהם במסגרת המתקפה. החוקיות והלגיטימיות של ביצוע פעולות מסוג זה בידי חברות פרטיות מצויה בדיון זה כמה שנים. מחד גיסא, לפעולת סייבר התקפי יש יתרונות כאמצעי הגנה עצמית, כיוון שהיא עשויה להביא למזעור הנזק לחברה המותקפת ולהרתעת מתקיפים. מאידך גיסא, פעולה שכזאת עשויה לצאת מכלל שליטה במהרה, לפגוע במערכות ממוחשבות של גופים חפים מפשע ולהביא להידרדרות כללית. בשנת 2017 הוצעה בארצות הברית הצעת חוק שבה הוטל על משרד המשפטים לקבוע כללים שבמסגרתם תוכל לפעול חברה המבקשת לתקוף בחזרה את מי שתקף אותה כאמצעי הגנה, במטרה למחוק ממחשבי התוקפים קניין רוחני או מידע פיננסי שהועתק ממנה. כן הוצע להחריג מתחולת החוק הפלילי מתקפות סייבר הנעשות למטרות הגנה עצמית.[209] ההצעה לא הבשילה לכדי חוק וספגה ביקורת רבה. היא הועלתה שוב ב־2019 אך גם אז לא הושלם תהליך החקיקה.

2018); Andy Greenberg, *The White House Blames Russia for NotPetya, the "Most Costly Cyberattack in History"*, Wired (Feb. 15, 2018)

208 *Cyber Most Wanted – Noor Aziz Uddin*, FBI (July 6, 2017)

209 יוסי גורביץ "ההגנה הטובה ביותר היא התקפה" **כלכליסט** (17.7.2016); Robert Chesney, *Hackback Is Back: Assessing the Active Cyber Defense Certainty Act*, Lawfare (June 14, 2019); Rob Lemos, *Why the Hack-Back is Still the Worst Idea in Cybersecurity*, TechBeacon

פרק 8

אומדן הנזק ממתקפות סייבר

הבנת מכלול הנזקים האפשריים ממתקפות סייבר חיונית להגדרת מדיניות ציבורית להגנת סייבר.[210] אכן, מתקפת סייבר עשויה לגרום לנזקים ישירים ועקיפים. כך, למשל, ענקית הקמעונאות Target הייתה יעד למתקפת סייבר שהחלה בסוף נובמבר 2013 ונחשפה בסוף דצמבר באותה השנה, שיא עונת מכירות החגים בארצות הברית. הנזק הכולל שגרמה מתקפה זו מוערך בכ־420 מיליון דולר, לרבות שיפוי, עלות הנפקת כרטיסי אשראי חדשים, שכר טרחת עורכי דין וניטור האשראי של מיליוני לקוחות.[211]

נזקים ישירים ועקיפים עשויים לכלול עלות החלפת תשתית חומרה ותוכנה, עלות התמגנות מחודשת (למשל העלות הכרוכה בהתקנת תוכנות אנטי־וירוס חדשות), שיפוי לקוחות, קנסות המשולמים לגופים רגולטוריים מדינתיים, עלות ההפרעה לתפקוד התקין של העסק, עלות גניבת זהויות והמאבק בתופעה, עלות הפגיעה באמון הלקוחות ועלות שיקום המוניטין של החברה, עלות חשיפת מידע סודי של העסק, עלות הפגיעה בחדשנות ובתחרותיות, עלות אובדן הזדמנויות עסקיות ועלות הירידה האפשרית באמון המשתמשים בשירותים במרחב הסייבר.[212]

קשה לאמוד במדויק את היקפם של מרבית מהנזקים הישירים והעקיפים, מבחינת עלותם הכלכלית וטווח פגיעתם, מכמה סיבות. ראשית, חברות וארגונים רבים עושים כל שביכולתם כדי שלא לחשוף את עצם העובדה

210 Jeff Kosseff, *Defining Cybersecurity Law*, 103 Iowa L. R. 985, 989 (2018)

211 Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime 18 (2014) (להלן: Net Losses); Oxford Economics, Cyber-attacks: Effects on UK Companies 39 (2014)

212 **שם**, בעמ' 39; Ross Anderson et al., *Measuring the Cost of Cybercrime*, *in* The Economics of Information Security and Privacy 265 (Rainer Böhme ed., 2013); Paul Dreyer et al., Estimating the Global Cost of Cyber Risk: Methodology and Examples (RAND Corporation, 2018)

שמתקפת סייבר כוונה כלפיהם או את הנזק שנגרם להם, כדי למזער את הפגיעה באמון הלקוחות, במוניטין החברה ובשווי מנייתה. כך, למשל, בשנת 2010 דיווחה חברת גוגל כי הייתה נתונה למתקפת סייבר; כ־34 חברות נוספות מתחומי תעשייה שונים, כולן מבין 500 החברות המדורגות ראשונות על ידי כתב העת פורצ'ן ("Fortune 500"), הותקפו גם הן אך נמנעו מלדווח על התקיפה. היעדר מידע על חברות אחרות שנפגעו ממתקפת סייבר ועל הנזק הנגרם להן מקשה על אומדן מדויק של הנזק הכולל.[213]

יש לציין כי המנהג להסתיר את קיומן של מתקפות סייבר עשוי לבוא אל קיצו בשנים הקרובות לאור חובת הדיווח על מתקפות סייבר הקבועה בתקנות החדשות של האיחוד האירופי בדבר הגנת מידע, שנכנסו לתוקפן במאי 2018,[214] וכן לנוכח חובת הדיווח בתיקון לחוק הגנת הפרטיות האוסטרלי,[215] וחובת הדיווח אשר אומצה גם בתקנות אבטחת מידע בישראל.[216]

סיבה שנייה לקושי לאמוד את נזקיהן של מתקפות סייבר היא היעדר הגדרה אחידה המבחינה בין נזקים הנגרמים מתקיפת סייבר ונזקים שנגרמים מסיבות אחרות.[217] כמו כן, מאחר שמרחב הסייבר, ועימו גם סוגי מתקפות הסייבר,

213 Net Losses, **לעיל** ה"ש 211, בעמ' 18; Oxford Economics, **לעיל** ה"ש 211, בעמ' 10; Brian Cashell et al., *The Economic Impact of Cyber-Attacks* (CRS Report for Congress 2004); Tucker Bailey, Andrea Del Miglio, & Wolf Richter, *The Rising Strategic Risks of Cyberattacks* 4-5, McKinsey Quarterly (May 2014); Jart Armin et al., *2020 Cybercrime Economic Costs: No Measure No Solution*, *in* 2015 10th International Conference on Availability, reliability and Security 701, 701-702 (2015)

214 GDPR, **לעיל** ה"ש 42, בסעיפים 33 ו־34.

215 Privacy Act 1988, § WF26

216 סעיף 11(ד) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, ק"ת 1022.

217 Net Losses, **לעיל** ה"ש 211, בעמ' 18; Oxford Economics, **לעיל** ה"ש 211, בעמ' 39; Anderson et al., **לעיל** ה"ש 212; Bailey, Del Miglio, & Richter, **לעיל** ה"ש 213, בעמ' 4-5; Cashell et al., **לעיל** ה"ש 213; Armin et al., **לעיל** ה"ש 213, בעמ' 701-702; Sören Preibusch, *Guide to Measuring Privacy Concern: Review of Survey and Observation Instruments*, 71 Int. J. Hum. Comput. Stud. 1133, 1134 (2013); Sarah Spiekermann et al., *The Challenges of*

מטרותיהן ואופן פעולתן, משתנים ומשתכללים ללא הרף, קשה לפתח מודל כלכלי אחיד להערכת הנזק הצפוי ממתקפת סייבר.[218]

הקושי באומדן ההיקף הכלכלי של הנזק בא לידי ביטוי בהערכות שונות של חברות מחקר. למשל, בשנת 2014 העריך המרכז למחקרים אסטרטגיים ובינלאומיים (The Center for Strategic and International Studies, CSIS) שפשיעת סייבר גרמה לכלכלה העולמית נזק בגובה 375–575 מיליארד דולר באותה שנה, לרבות הנזק לביצועיהן של חברות מסחריות והנזק לתעסוקה, למסחר, לתחרותיות, לחדשנות ולצמיחה הכלכלית של כל מדינה.[219] לפי חברת מקאפי, נכון לשנת 2014 הוערך הנזק הכלכלי העולמי השנתי מפשיעת סייבר ביותר מ־400 מיליארד דולר, וסכום זה צפוי לגדול ככל שיותר עסקים ויחידים ישתמשו בפלטפורמות מקוונות.[220] חברת הייעוץ מקינזי העריכה ב־2014 כי בשנים 2014–2019 יעמוד הנזק השנתי לכלכלה העולמית מפשיעת סייבר על 9–21 טריליון דולר.[221] בשנת 2018 פרסמו המרכז למחקרים אסטרטגיים ובינלאומיים וחברת הייעוץ מקינזי הערכה משותפת האומדת את הנזק השנתי לכלכלה העולמית עקב פשיעת סייבר בכ־600 מיליארד דולר.[222]

בעתיד, ככל שיגדל שוק הביטוח מפני נזקי מתקפות סייבר, ייתכן שיהיה אפשר להתגבר באמצעותו על הקושי לאמוד במדויק את מכלול הנזקים

Personal Data Markets and Privacy, 25 Electronic Markets 161, 161 (2015); Alessandro Acquisti, Curtis Taylor, & Liad Wagman, *The Economics of Privacy*, 52 J. of Econ. Literature 38 (2016)

218 Davey Winder, *Calculating the Cost of Cyber-Risk*, Raconteur (April 25, 2018)

219 Net Losses, **לעיל** ה"ש 211, בעמ' 3, 6.

220 **שם**.

221 Bailey, Del Miglio, & Richter, לעיל ה"ש 213, בעמ' 4–5.

222 Lewis, **לעיל** ה"ש 145.

הכלכליים של מתקפות סייבר; אולם לעת עתה גם בשוק הביטוח מתקשים לאמוד במדויק את היקף הנזק האפשרי.[223]

על אף הקושי הנדון, ההערכה הרווחת היא שהנזק ממתקפות סייבר עשוי לפגוע קשות בכלכלתן של מדינות ובכלכלה הגלובלית. בדוח של הפורום הכלכלי העולמי (The World Economic Forum) משנת 2019 דורגו מתקפות סייבר במקום השביעי ברשימת עשרת הסיכונים הגלובליים החמורים ביותר לכלכלת העולם המפותח – מקום גבוה מזה של אסונות סביבתיים מעשה ידי האדם או מגפות, ונמוך רק מעט מזה של אסונות טבע.[224]

נוסף על הנזקים הכלכליים, מתקפת סייבר עלולה לגרום לנזקים נוספים שאינם כלכליים, כגון נזקים פיזיים – למשל נזק לתשתיות או אובדן חיי אדם בשל פגיעה בשירותי הרפואה הדחופה; נזקים פסיכולוגיים – תחושות של מבוכה, בושה, בלבול או דיכאון עקב חשיפת קניין רוחני או מידע אישי, כפי שאירע לדוגמה עקב מתקפת הסייבר על אתר ההיכרויות אשלי מדיסון; ונזקים ברמה החברתית – למשל כאשר מתקפת הסייבר גורמת להפרעה של ממש בחיי היום־יום עקב פגיעה בשירותים חיוניים, מקטינה את אמון הציבור בשלטון או בטכנולוגיה או מובילה לפגיעה מורלית קשה בקרב עובדי ארגון המצוי תחת מתקפת סייבר.[225] כמו כן, למתקפת סייבר עלול להיות אפקט מצנן על חופש הביטוי, כפי שאירע בעקבות מתקפת הסייבר על תאגיד סוני בנובמבר 2014 לקראת צאת סרט בהפקתו העוסק בניסיון לרצוח את מנהיג צפון קוריאה, קים ג'ונג און. בעקבות מתקפת הסייבר עיכבה סוני את יציאתו של הסרט לאקרנים. כמה חודשים אחר כך דווח שחברת דיסני התקשרה בחוזה להקמת ערוץ חדשות חדש, ובו נקבע שחברת החדשות תשפה את דיסני בגין כל נזק העלול

223 OECD, *Cyber Insurance Market Challenges*, *in* Enhancing the Role of Insurance in Cyber Risk Management 93 (2017); Rob Marvin, *What Is Cyber Insurance and Should You Get It?*, PCMag (Jan. 24, 2018)

224 World Economic Forum, The Global Risk Report 2019 (14th Edition, 2019)

225 Loaanis Agrafiotis et al., *A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate*, 4 (1) J. of Cybersecurity (2018)

להיגרם לה מהפקה של תוכנית טלוויזיה שיש בה פגיעה במדינה, בשלטון או במנהיג באופן העלול לחשוף את מערכותיה של דיסני למתקפה.[226]

נוסף על כל אלה, הבחירות לנשיאות ארצות הברית בשנת 2016 העלו לסדר היום הציבורי את השימוש במתקפות סייבר למטרת גרימת נזק שאינו כלכלי אלא תודעתי: פגיעה באמון הציבור בשלטון ובמערכותיו, ערעור האמון ביכולת לברר את המציאות לאשורה וקיטוב ציבורי בין דעות שונות, הכול במסגרת לוחמת תודעה.

קשה לכמת את הנזק של לוחמת תודעה במרחב הסייבר, משום שלוחמה מסוג זה מנסה להשפיע על חוסנו של הציבור בכללותו, לדכא את רוח הלחימה של חיילים בצבאות, וכן להשפיע על התנהלותם, דעותיהם והחלטותיהם של יחידים בעלי רקע ואינטרסים שונים, לרבות על מקבלי החלטות בחברה ובממשל.[227] יתר על כן – מחקרים מצאו שלניסיונות של מתקפות סייבר להחדיר רעיונות תעמולתיים ולשנות באמצעותם מציאות יש אפקטיביות נמוכה, בעיקר עקב חוסר הדיוק בהפעלת לוחמת התודעה; ובכל מקרה השפעת מתקפות סייבר שכאלו מוגבלת בזמן. נטען, למשל, כי הבוט־נטים הרוסים אינם מדייקים בשימוש בשפות אחרות, דוגמת אנגלית ופינית, וכי קיים חוסר תיאום בין מרכזי הלוחמה התודעתית הרוסים השונים.[228]

לצד הנזק התודעתי, חשוב לתת את הדעת לכך שהסכנה הגדולה ביותר הטמונה בלוחמת תודעה במרחב הסייבר היא פגיעה בחופש הבחירה ובדמוקרטיה. גם המקרה של פרסום ממוקד אישית הנשען על ניתוח מאפייניו האישיים של הצרכן, כפי שנעשה היום באופן נרחב בשיתוף הפעולה המסחרי שבין פלטפורמות דיגיטליות כגון גוגל ופייסבוק, סוחרי מידע ומפרסמים, עלול להוביל, בסופו של דבר ובמצבי קיצון, לתוצאה הבעייתית של אובדן

226 Kosseff, **לעיל** ה"ש 210, בעמ' 992–993.

227 סיבוני, **לעיל** ה"ש 166, בעמ' 195; גבי סיבוני וגל פרל פינקל "מאמץ התודעה הישראלי: משלים למאמץ הקינטי" **מבט על** 1028 (המכון למחקרי ביטחון לאומי 2018).

228 Peter Suciu, *Why Cyber Warfare is So Attractive to Small Nations*, Fortune (Dec. 21, 2014); Maria Snegovaya, Russia Report I: Putin's Information Warfare in Ukraine (Institute for the Study of War, 2015)

חופש הבחירה האמיתי של הצרכן. אין ספק שיש לבחון דרכים למזער פגיעה זו ולמנוע ככל האפשר את הפגיעה בחופש הבחירה הצרכני. אולם כאשר מדובר בלוחמת תודעה המובילה לפגיעה בחופש הבחירה הנזק עלול להיות חמור אף יותר: אזרחים עלולים לאבד אמון בשיטה הדמוקרטית מתוך ההבנה שבפועל לא באמת ניתן בידם חופש בחירה, אלא דעותיהם והחלטותיהם הושפעו ממסרים שהועברו אליהם לאחר שהותאמו לקווי האופי שלהם. לוחמת תודעה במרחב הסייבר משמשת להחרפת המחלוקות והשסעים בציבור ולזריעת כאוס. שלטון דמוקרטי נעשה תלוי באמינות ובמהימנות של המידע שאליו נחשפים בוחריו.[229]

פרשת ״קיימברידג׳ אנליטיקה״ מחזקת את החשש לפגיעה בדמוקרטיה עקב שימוש בלוחמת תודעה במרחב הסייבר. לכאורה, כאשר נעשה שימוש מתוחכם כל כך בלוחמה כזאת ציבור הבוחרים הופך ללא ידיעתו לכלי שרת בידי המועמד או המדינה, המנצלים את תעבורת המידע הקלה, היעילה והמהירה ברשת האינטרנט כדי להשיג את מטרותיהם.[230]

סיכום ביניים: הגורמים לפגיעות של מרחב הסייבר למתקפות

התרשים שלהלן מציג את מכלול הגורמים שנסקרו בפרקים הקודמים המגדילים את החשיפה של מרחב הסייבר למתקפות סייבר.

229 Evelyn Rupert, *Report: Russian Propaganda Efforts Propelled Fake Election News*, The Hill (Nov. 24, 2016); *Experts Discuss Cyber Espionage, Propaganda, and Russia*, SIPA News Magazine (March 9, 2017); Garrett M. Graff, *A Guide to Russia's High Tech Tool Box for Subverting US Democracy*, Wired (Aug. 13, 2017); Brian Klaas, *Stop Calling It "Meddling." It's Actually Information Warfare*, The Washington Post (July 17, 2018)

230 להרחבה על פרשת קיימברידג׳ אנליטיקה ולוחמת מידע מותאמת אישית ראו הדיון בטקסט הנלווה להערת שוליים 168.

תרשים 2
הגורמים המגדילים את החשיפה של מרחב הסייבר למתקפות

פרק 9

הגנת סייבר

עד כה סקרנו את המאפיינים הייחודיים של מרחב הסייבר המקילים את ביצועה של מתקפת סייבר, פירטנו את השלבים של מתקפת סייבר, המגמות הבולטות בתחום ואופני ההפצה השונים, תיארנו את המניעים הנפוצים לביצוע מתקפות סייבר ואמדנו את הנזק הכלכלי והתודעתי שלהן. בפרק זה נסקור את תמונת הראי של נושאים אלו ונדון באופני ההגנה השונים על מרחב הסייבר.

א. הגדרת המונח "הגנת סייבר"

למונח "הגנת סייבר" אין הגדרה קוהרנטית אחת ברורה ומוסכמת. הדבר מקשה על אימוץ מדיניות ציבורית להגנת מרחב הסייבר, שכן כל אחת מההגדרות שבנמצא מדגישה היבטים שונים הקשורים להגנת סייבר, כגון חשיבות הגנת הסייבר לביטחון הלאומי והאישי; הצורך בחינוך ובהכשרה מקצועית להגברת המודעות לסכנות שבמרחב הסייבר; החשיבות של יכולות הגנת סייבר, כמו גם של יכולות תקיפת סייבר, ביחסים בין מדינות; וההשלכות של הגנת סייבר מוצלחת או קלוקלת על מצבה הכלכלי ויציבותה הכלכלית של המדינה.[231]

ההגדרה של הגנת סייבר במילון אוקספורד מדגישה מצב תגובתי: הגנת סייבר היא מוגנות מפני שימוש עברייני או לא מורשה במידע אלקטרוני.[232] בשנת 2014 קבעה קבוצת חוקרים קנדית כי הגנת סייבר היא "ארגון ואיסוף משאבים, תהליכים ומבנים המשמשים להגנת מרחב הסייבר ולהגנת מערכות העושות בו

231 Kosseff, **לעיל** ה"ש 210, בעמ' 987–988; Dan Craigen, Nadia Diakun Thibault, & Randy Purse, *Defining Cybersecurity*, 4 (10) Technology Innovation Management Rev. 13, 13–14 (2014); Myriam Dunn Cavelty & Florian J. Egloff, *The Politics of Cybersecurity: Balancing Different Roles of the State*, 15 (1) St. Anthony's Int'l Rev. 37, 38 (2019)

232 *Cybersecurity*, Oxford Online Dictionary (2019)

שימוש מפני התרחשויות העשויות לפגוע, הלכה למעשה, בזכויות קניין".[233] זוהי הגדרה רחבה, שאינה מגבילה את מאמצי הגנת הסייבר לטכנולוגיה מסוימת או לאסדרה ממשלתית מסוימת, ובכך טמון יתרונה. עם זאת, התמקדותה בפגיעה בזכויות קנייניות אינה מביאה בחשבון מתקפות סייבר העשויות לפגוע בזכות לפרטיות, בחדשנות או בביטחון הלאומי, או לגרום נזק תודעתי. חברת אבטחת המידע קספרסקי הגדירה את המונח כ"מכלול הטכנולוגיות, התהליכים ואופני הפעולה הנהוגים בתעשייה לשם הגנה על רשתות, מכשירים, מחשבים אישיים, מכשירי טלפון נייד, שרתים, מערכות אלקטרוניות, תוכנות ומידע מפני מתקפות סייבר, נזק או גישה בלתי מורשית".[234] הגדרה זו מוגבלת לאמצעים הטכנולוגיים להגנת הסייבר, ואינה מביאה בחשבון את האפשרות של אסדרה ממשלתית לשם הגנת מרחב הסייבר.

1. היחס בין הגנת סייבר ובין אבטחת מידע ואבטחת נתונים

במקרים רבים נעשה שימוש במונחים אבטחת מידע (information security), אבטחת נתונים (data protection) והגנת סייבר (cybersecurity) כמונחים חליפיים,[235] אולם לכל אחד מהם משמעות שונה.

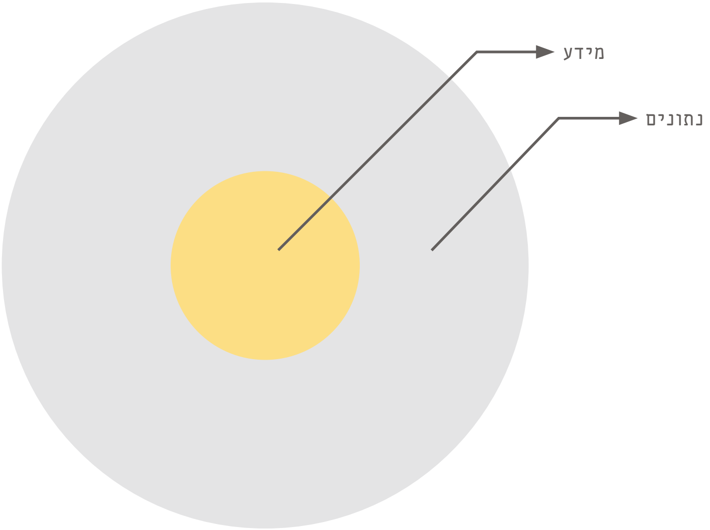
אבטחת נתונים ואבטחת מידע הם מושגים דומים שהשוני ביניהם נעוץ בשאלה על מה מגינים. מידע (information) הוא נתון (data) שיש לו משמעות. למשל, צבר הספרות 271259 הוא נתון שיהפוך להיות מידע אם נדע שהוא תאריך לידה, כלומר צבר ספרות בעל משמעות. אבטחת נתונים היא אפוא ההגנה המוענקת לכל הנתונים באשר הם, ואילו אבטחת מידע היא הגנה על נתונים שיש להם משמעות.

233 Craigen, Diakun Thibault, & Purse, **לעיל** ה"ש 231, בעמ' 17.

234 Juliana De Groot, *What is Cyber Security? Definition, Best Practices & More*, DigitalGuardian (Oct. 5, 2020); *What is Cyber-Security*, Kaspersky

235 Luke Irwin, *Do You Know the Difference Between Cyber Security and Information Security?*, IT Governance (Aug. 9, 2018); Jake Olcott, *Cybersecurity Vs. Information Security: Is There A Difference?* BitSight (Sep. 15, 2019)

תרשים 3
היחס בין מידע לנתונים



אבטחת מידע מוגדרת כהגנה על הסודיות, האמינות והזמינות של המידע ("משולש ה־CIA" – confidentiality, integrity, availability), ללא קשר לפורמט שבו הוא מאוחסן. מקובל להבחין בשני סוגים של אבטחת מידע:

(**1**) **במרחב הפיזי:** מניעת גישה פיזית לא מורשית למידע, כלומר למקום שבו המידע מאוחסן, כדי לשמור על הסודיות, האמינות והזמינות שלו.

(**2**) **במרחב הסייבר:** מניעת גישה לא מורשית למידע במרחב הסייבר כדי לשמור על סודיותו, אמינותו וזמינותו.[236] זו גם נקודת החפיפה בין אבטחת מידע להגנת סייבר, כפי שיוסבר להלן.

236 Irwin, **לעיל** ה"ש 235; William C. Barker, *Guideline for Identifying an Information System as a National Security System* (NIST Special Publication 800-59, 2003); Tim Maurer & Robert Morgus, Compilation of

בחלק מן המדינות אין הגדרה למונח "הגנת סייבר", או שהיא רחבה ועמומה,[237] ובדברי חקיקה שונים בעולם העדיפו המחוקקים להימנע ממתן הגדרה ברורה בחוק למונח זה. לדוגמה, חוק הגנת הסייבר האמריקאי משנת 2015 מגדיר מגוון מונחים כגון איום סייבר, חולשת אבטחה ומטרת הגנת סייבר – שהיא הגנה על מערכת מידע או על מידע המאוחסן על גבי מערכת מידע, מעובד על ידה או מועבר באמצעותה, מפני איום סייבר או חולשת אבטחה[238] – אך אינו כולל הגדרה ברורה למונח "הגנת סייבר".[239]

Existing Cybersecurity and Information Security Related Definitions 35-37 (Policy Paper, New America 2014)

237 Eric Luiijf, Kim Besseling, & Patrick Graaf, *Nineteen National Cyber Security Strategies*, 9 (1) Int'l J. of Critical Infrastructures 3 (2013)

238 להלן כמה מההגדרות בחוק Cybersecurity Information Sharing Act, 6) U.S.C Chapter I, 2015). סעיף 102(4) מגדיר "Cybersecurity Purpose" כך: "[...] the purpose of protecting an information system or information that is stored on, processed by or transiting an information system from cybersecurity threat or security vulnerability". סעיף 102(5) מגדיר "Cybersecurity Threat" כך:

(A) IN GENERAL.–Except as provided in subparagraph (B), the term "cybersecurity threat" means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.
(B) EXCLUSION.–The term "cybersecurity threat" does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

סעיף 102(17) מגדיר "Security Vulnerability" כך: "[...] any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control"

239 Kosseff, **לעיל** ה"ש 210, בעמ' 987–988.

עם זאת, לפי מסמכי מדיניות הגנת הסייבר באיחוד האירופי[240] ובמדינות שונות, כגון רוסיה,[241] אנגליה,[242] ארצות הברית,[243] פינלנד,[244] גרמניה,[245]

240 ראו את ההגדרה באיחוד האירופי אצל Maurer & Morgus, **לעיל** ה"ש 236, בעמ' 31:

> Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein (European Union, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013, p. 3).

241 ראו את ההגדרה ברוסיה (בתרגום מרוסית) אצל Maurer & Morgus, **לעיל** ה"ש 236, בעמ' 26: "A set of conditions under which all components of cyberspace are protected from the maximum number of threats and impacts with undesirable consequences" (Russia, Concept Strategy for Cybersecurity of the Russian Federation, p. 2)

242 ראו את ההגדרה באנגליה אצל Maurer & Morgus, **לעיל** ה"ש 236, בעמ' 26: "Cyber security embraces both the protection of the UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers [...]" (United Kingdom, Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space, 2009, p. 9)

243 ראו את ההגדרה בארצות הברית אצל Maurer & Morgus, **לעיל** ה"ש 236, בעמ' 26: "The ability to protect or defend the use of cyberspace from cyber attacks" (United States of America, Committee on National Security Systems National Information Assurance Glossary, 2010, p. 22; United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 58)

244 ראו את ההגדרה בפינלנד אצל Maurer & Morgus, **לעיל** ה"ש 236, בעמ' 28: "Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured" (Finland, Finland's Cyber Security Strategy, 2013, p. 13)

245 ראו את ההגדרה בגרמניה אצל Maurer & Morgus, **לעיל** ה"ש 236, בעמ' 27:

> (Global) cyber security is the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum. Hence, cyber security in Germany is the desired objective of the IT security situation, in which the risks of the German cyberspace have been reduced to an acceptable

הונגריה[246] וישראל,[247] נראה שההגדרה המקובלת של הגנת סייבר מתייחסת להגנה על כל מה וכל מי שאפשר לגשת אליו דרך מרחב הסייבר, ומטרתה להגן על האינטרס הציבורי של שימוש בטוח ויעיל במרחב הסייבר ולמזער כל השפעה שלילית שעשויה להיות לשימוש בו. כלומר הגנת סייבר מגינה על מידע זמין או נגיש במרחב הסייבר, על נתונים שאינם מידע ועל דברים שאינם מידע, למשל מכוניות, רמזורים או מוצרי חשמל שנגישים באמצעות מרחב הסייבר.[248]

ההגדרה מתמקדת בהגנה על כל מה שבמרחב הסייבר, בעוד אבטחת מידע מתמקדת בהגנה על מידע בכל פלטפורמה או מרחב שבו הוא מצוי. משום כך יש חפיפה מסוימת בין הגנת מידע להגנת סייבר: ככל שמדובר במידע הנגיש באמצעות מרחב הסייבר יחולו עליו הן מנגנוני אבטחת מידע והן מנגנוני הגנת סייבר.

---

minimum. Cyber security (in Germany) is the sum of suitable and appropriate measures. Civilian cyber security focuses on all IT systems for civilian use in German cyberspace. Military cyber security focuses on all IT systems for military use in German cyberspace (Germany, Cyber Security Strategy for Germany, 2011, p. 15; Germany, Federal Office for Information Security (BSI): Glossary/Terminology).

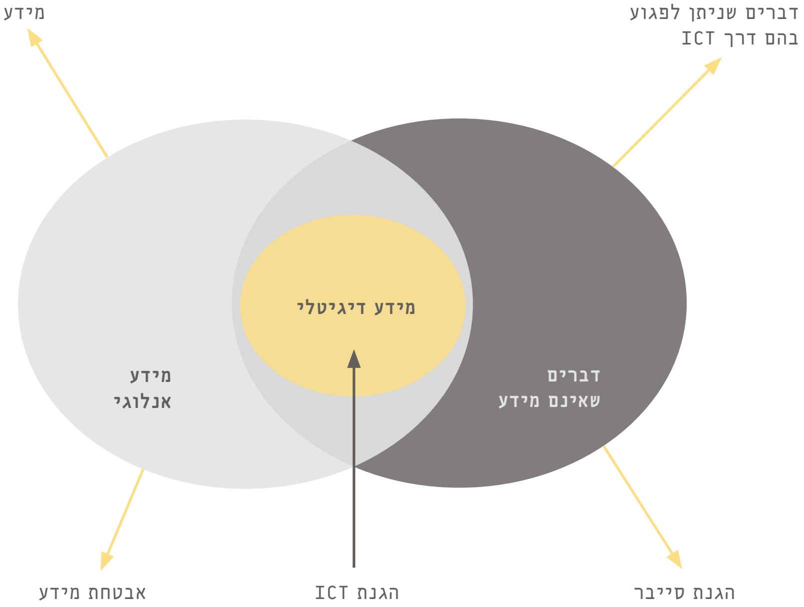
246 ראו את ההגדרה בהונגריה אצל Maurer & Morgus, **לעיל** ה"ש 236, בעמ' 29:

Cyber security is the continuous and planned taking of political, legal, economic, educational, awareness-raising and technical measures to manage risks in cyberspace that transforms the cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace (Hungary, Annex 1 to Government Decision No. 1139 / 2013 National Cyber Security Strategy of Hungary, 2013, p. 13).

247 מדינת ישראל הגדירה בהחלטת ממשלה משנת 2015 את המושג "הגנת סייבר" באופן רחב כ"מכלול הפעולות למניעה, לנטרול, לחקירה ולהתמודדות עם איומי סייבר ואירועי סייבר ולצמצום השפעתם והנזק הנגרם מהם, וזאת בטרם התרחשותם, במהלכם ולאחריהם"; ראו החלטה 2444 של הממשלה ה־33 "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.2015). תזכיר חוק הסייבר מגדיר את המונח כ"מכלול הפעולות הנדרשות למניעה, להתמודדות ולטיפול בתקיפת סייבר או איום סייבר, לצמצום השפעתם והנזק הנגרם מהם, במהלכם ולאחריהם, ובכלל זה פעולות אבטחת מידע". ראו סעיף 1 לתזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי.

248 NIST, Guide for Conducting Risk Assessments (Special Publication 800-30 Rev. 1, 2012)

תרשים 4
תחולת הגנת סייבר ואבטחת מידע



מקור: Ihor Chernobai, *Cybersecurity vs. Information Security*, Protectimus (April 24, 2018)

גישה אחרת אינה מבחינה בין נתונים למידע. לפי גישה זו אבטחת מידע היא הגנה על האמינות, הסודיות והזמינות של כל נתון שהוא, ללא קשר לפורמט שהוא מאוחסן בו, מפני גישה ושימוש לא מורשים. הגנת סייבר היא הגנה על האמינות, הסודיות והזמינות של כל נתון ששמור בפורמט אלקטרוני;[249] במובן זה הגנת סייבר היא תת־קבוצה של אבטחת מידע.

249 זו, למשל, ההגדרה המקובלת באוסטרליה, בניו זילנד ובארגון התקינה הבינלאומי. ראו את ההגדרה באוסטרליה אצל Maurer & Morgus, **לעיל** ה"ש 236, בעמ' 30: "Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means" (Australia, Cyber Security Strategy 2009, p. 5)

לפי גישה זו, לאבטחת מידע ולהגנת סייבר שני מאפיינים דומים:

(**1**) שתיהן מורכבות מהגנה פיזית ומהגנה במרחב הסייבר: במסגרת אבטחת מידע מתקינים מנעול על דלת החדר הסגור שבו הנתונים מאוחסנים; במסגרת הגנת סייבר יותקן מנעול על דלת החדר שבו נמצאים השרתים שעליהם מאוחסנים הנתונים.

(**2**) בשתיהן רמת ההגנה נמצאת ביחס ישר לערך המיוחס לנתונים המוגנים.[250]

2. היחס בין הגנת סייבר, אבטחת מידע והגנה על הזכות לפרטיות

פרטיות, לפי התיאוריות המקובלות, היא השליטה של האדם על המידע האישי עליו, והיא הכרחית לבחירה החופשית של אדם ולאוטונומיה שלו. במובן זה, אבטחת מידע היא מכשיר למימוש זכותו של אדם לפרטיות ובלעדיה לא תמומש זכות זו.[251]

בנקודת החפיפה בין הגנת סייבר לאבטחת מידע, כלומר כשמדובר בהגנה על מידע הנגיש במרחב הסייבר, הגנת הסייבר גם היא מכשיר או אף תנאי מקדמי למימוש זכותו של אדם לפרטיות.[252] הבנה זו באה לידי ביטוי, למשל, בסעיף 25

ראו את ההגדרה בניו זילנד, אצל Maurer & Morgus, **לעיל** ה"ש 236, בעמ' 30: "The practice of making the networks that constitute cyber space as secure as possible against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them" (New Zealand, New Zealand's Cyber Security Strategy, 2011, p. 12).
ראו את ההגדרה בארגון התקינה הבינלאומי, אצל Maurer & Morgus, **לעיל** ה"ש 236, בעמ' 32: "Cyberspace security [is] defined as the preservation of confidentiality, integrity and availability of information in Cyberspace" (International Organization for Standardization, ISO / IEC 27032:2012)

250 De Groot, **לעיל** ה"ש 234.

251 Mark R. Heckman, *The Difference Between Data Security and Privacy,* United States Cybersecurity Magazine (2017)

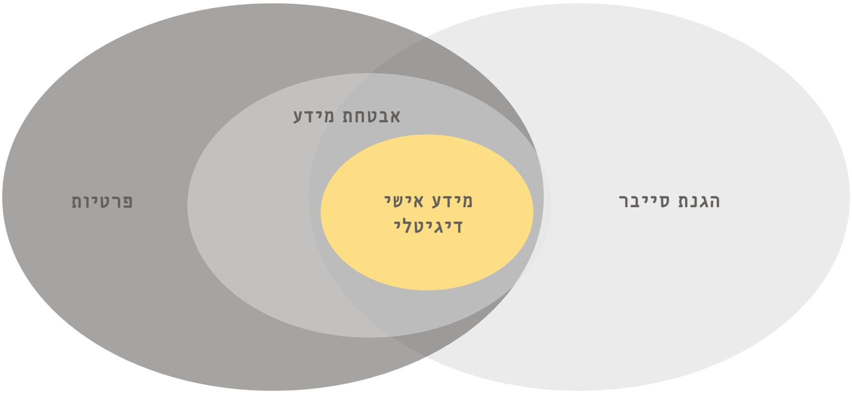
252 Wolf J. Schünemann & Max-Otto Baumann, *Introduction: Privacy, Data Protection and Cybersecurity in Europe*, *in* Privacy, Data Protection and Cybersecurity in Europe 1-14 (Wolf J. Schünemann & Max-Otto Baumann eds., 2017)

לתקנות הגנות המידע החדשות של האיחוד האירופי (ה־GDPR), המחייב את בעל השליטה במידע או מעבד המידע לנקוט את האמצעים הטכניים והארגוניים המתאימים לשם הגנה על זכויותיו של נושא המידע.[253]

עם זאת, הגנת סייבר כוללת מגוון נרחב של נושאים שאינם קשורים בהגנה על מידע אישי ופרטיות – למשל הגנה על תשתיות ועל ביטחון כלכלי. משום כך, לעיתים מתעורר ניגוד אינטרסים בין פרטיות להגנת סייבר, המשקף בבסיסו את ההתנגשות בין חירות ובין ביטחון. המקרה הבולט ביותר של התנגשות שכזו הוא היכולת לעשות שימוש אנונימי בשירותים במרחב הסייבר. מחד גיסא, גלישה אנונימית היא מימוש של הזכות לפרטיות ומאפשרת לאדם לעשות שימוש בשירותים במרחב הסייבר מבלי להזדהות. מאידך גיסא, גלישה אנונימית אינה מאפשרת לזהות כל גולש וגולש כדי למנוע פשיעת סייבר או לאתר בדיעבד את האחראים לפשע סייבר, ומכאן שהיא מנוגדת למטרת הגנת הסייבר לאפשר שימוש בטוח במרחב הסייבר.[254]

התרשים שלהלן מתאר את היחס בין פרטיות, אבטחת מידע והגנת סייבר:

תרשים 5
היחס בין פרטיות, אבטחת מידע והגנת סייבר



253 GDPR, **לעיל** ה"ש 42.

254 **שם**.

3. מהי הגנת סייבר?

פרופ' ג'ף קוסף הציע שלא להתמקד במונח "הגנת סייבר" אלא להגדיר דווקא "מדיניות הגנת סייבר": המסגרת המשפטית שמטרתה הגנה על הסודיות, האמינות והזמינות של מידע אישי וציבורי במערכות ורשתות, באמצעות אסדרה צופה פני עתיד ומערך תמריצים שמטרתם הגנה על זכויות הפרט, אינטרסים כלכליים והביטחון הלאומי.[255] קבוצת מומחים שבחנה את הנושא מטעם נציבות האיחוד האירופי הציעה להגדיר הגנת סייבר כ"הבטחת הסודיות, הנכונות והזמינות של המידע האישי, וכן הגנה על הזכות לפרטיות והשגת חוסן במובן של יכולת התאוששות מהירה לאחר פגיעה".[256]

לאור המתואר, בחרנו להגדיר כך את המושג "הגנת סייבר": מכלול פעולות שונות, פרואקטיביות וריאקטיביות, שמטרתן להתמודד עם איום על השלמות, האמינות, הזמינות והפרטיות של מידע הנמצא במחשבים, במערכות מידע ורשתות מחשבים ובתשתיות דיגיטליות אחרות, וכן סיוע למערכות אלה לשוב לתפקוד תקין במקרה של מימוש איום כזה.

מתוך הגדרה זו חשוב להדגיש את מה שלא נמצא בה: הגנת סייבר אינה מתייחסת לאיומים הגלומים במידע עצמו, כגון ביטויי שנאה, דיבה ולשון הרע; העלבת עובדי ציבור; פגיעה בפרטיות; הפצת מידע אסור בפרסום מטעמים ביטחוניים ואחרים; השפעה על בחירות וכיוצא באלה.

ב. ההתפתחות של תעשיית הגנת הסייבר

תעשיית הגנת הסייבר החלה להתפתח בסוף שנות השמונים ותחילת שנות התשעים של המאה העשרים. העיקרון שהנחה את תעשיית הסייבר עם הקמתה היה שמניעת מתקפת סייבר עדיפה על ריפוי נזקיה לאחר התפרצותה. משום כך, תוכנות האנטי־וירוס הראשונות התמקדו בניסיונות לזהות וירוסים

255 Kosseff, **לעיל** ה"ש 210, בעמ' 995–1010.

256 ENISA, **לעיל** ה"ש 10, בעמ' 28.

על פי חתימתם, מעין טביעת אצבע דיגיטלית של הווירוס, בטרם ייכנסו לפעולה.[257] חסרונותיהן של תוכנות אלו מאפיינים את תעשיית הגנת הסייבר גם היום: מתן תחושת ביטחון מוטעית למשתמשים ושימוש במשאבי מחשוב רבים בעת הפעלתן.[258]

לצד חברות פרטיות שביקשו לתת מענה לצורך להתגונן מפני מתקפות סייבר, הקים הממשל האמריקאי בשנת 1988 את המרכז הארצי לניהול אירועי סייבר (Computer Emeregency Response Team, להלן: CERT) באוניברסיטת קרנגי מלון. ה־CERT הוקם בעקבות התפרצות תולעת מוריס,[259] שהובילה להכרת הממשל האמריקאי בצורך לרכז בידי גוף ציבורי או פרטי את ניהול התגובה למתקפת סייבר והשיקום ממנה. ה־CERT הוא מרכז מחקר המספק מידע לציבור בנושאי נוזקות, חולשות טכנולוגיות ופרקטיקות להתגוננות מפני מתקפות סייבר, מזעור הנזק ממתקפת סייבר והבטחת המשך תפקודן של תשתיות קריטיות על אף מתקפות סייבר.[260]

במהלך השנים אימצו כ־100 מדינות נוספות את המודל האמריקאי והקימו מרכזים ארציים לניהול אירועי סייבר. גופים אלה הם גם פלטפורמה להעברת מידע על איומי סייבר ומתקפות סייבר מהתעשייה לממשל ומהממשל, לאחר עיבוד וניתוח, למגזרים נוספים בתעשייה ולעיתים אף לכלל הציבור. כך, בשנת 2014 הקימה אנגליה את CERT-UK, אשר אחראי לניהול התגובה הלאומית למתקפות סייבר, לתמיכה בהתגוננות מפני מתקפות סייבר על תשתיות קריטיות במדינה ולקידום המודעות לסכנות שבמרחב הסייבר בקרב התעשייה, האקדמיה והמגזר הציבורי, ומשמש כפלטפורמה לשיתוף פעולה בינלאומיים

257 Ted Julian, *Defining Moments in the History of Cyber-Security and the Rise of Incident Response*, InfoSecurity Magazine (Dec. 4, 2014)

258 *The History of Cyber Security*, **לעיל** ה"ש 136.

259 להרחבה על "תולעת מוריס" ראו הטקסט הנלווה לה"ש 139.

260 *The History of Cyber Security*, **לעיל** ה"ש 136.

עם גופי CERT אחרים.[261] בישראל הוקם CERT-IL בשנת 2015, והוא פועל מבאר שבע במסגרת מערך הסייבר הלאומי.[262]

שוק הגנת הסייבר הלך השתכלל עם השנים. כיום זיהוי של נוזקות לפי החתימה הידועה שלהן הוא רק חלק קטן ממכלול המשימות שמבצעות מערכות הגנת סייבר, ביניהן ניטור עבודת מערכת המחשב, רשתות מחשבים ורשת האינטרנט עצמה לשם זיהוי פעילות לא רגילה; מתן מענה למספר רב ככל האפשר של סוגי נוזקות, לרבות וירוס, רוגלה או סוס טרויאני; ואספקת פלטפורמה לגלישה בטוחה ואנונימית באינטרנט (Virtual Private Network). התפתחות זו היא תולדה של העלייה בכמות הנוזקות הפעילות, כפי שתיארנו בפרק 5, מנוזקה חדשה אחת לחודש בסוף שנות השמונים למציאות שונה לגמרי. לפי נתונים שפרסמה חברת סימנטק, בשנת 2018 אחת מכל 10 כתובות אינטרנט הייתה כתובת זדונית; בממוצע הותקפו 4,800 אתרי אינטרנט מסחריים בחודש למטרת העתקת מידע דיגיטלי; 1.3 מיליון מתקפות סייבר שמקורן באתרי אינטרנט נחסמו ביום במכשירי קצה; אחד מכל 412 מסרי דוא"ל הכיל נוזקה (בישראל היה השיעור נמוך בהרבה, ורק אחד מכל 1,112 מסרי דוא"ל הכיל נוזקה); 545,231 מתקפות כופר דווחו; אחד מכל 36 מכשירים ניידים הכיל אפליקציות מזיקות, ובממוצע חסמה סימנטק 10,573 אפליקציות זדוניות למכשירים ניידים ביום; אחת מכל 54 מתקפות סייבר זוהתה כמתקפת בוט־נט; ובסך הכול אירעו 57,553 מתקפות סייבר על מכשירי האינטרנט של הדברים (IoT).[263]

לאחרונה נראה שתעשיית הגנת הסייבר עוברת שינוי נוסף, לנוכח ההבנה שמניעה מוחלטת של מתקפות סייבר אינה אפשרית ועל כן יש לרכז מאמצים גם בתגובה למתקפת סייבר, כלומר סיוע בהתמודדות עם מתקפת סייבר בזמן

261 *UK Launches First National CERT* (Cabinet Office and the RT Hon. Lord Maude of Horsham Press Release, March 31, 2014)

262 המרכז הארצי לניהול אירועי סייבר (CERT), **מערך הסייבר הלאומי**.

263 Eric Domage, *The Evolution of Anti-virus*, InfoSecurity Magazine (Jan. 1, 2009); Paul Gillin, *How Virus Protection Software Has Evolved with the Threat Landscape*, SecurityIntelligence (July 17, 2017); Symantec, Internet Security Threat Report (vol. 24, 2019)

אמת, התגברות על מתקפת הסייבר ושיקום המערכות לחזרה לפעולה רגילה ושגרתית במהירות האפשרית.[264]

כמו כן, מתקפות הסייבר WannaCry ו־NotPetya הוכיחו שמתקפת סייבר עשויה לגרום נזקים חמורים גם אם אינה ממוקדת בתקיפת ארגון מסוים, אלא מופצת באופן רוחבי ובמהירות בין ארגונים ומערכות שונות ורחוקות. בעקבות זאת החלה לחלחל ההבנה שהגנת סייבר אינה שירות משני בחשיבותו או הוצאה שאפשר לוותר עליה. ואכן, בשנת 2018 הגיעה ההוצאה על מוצרים ושירותים של הגנת סייבר לכדי כ־114 מיליארד דולר – עלייה של 12.4% בהשוואה לשנת 2017. מכון גרטנר צפה שבשנת 2019 תעלה ההוצאה השנתית העולמית הממוצעת על הגנת סייבר בכ־10.5%. בסקר שנערך בשנת 2020 הצהירו 62% מהארגונים המשתתפים כי בכוונתם להגדיל את ההוצאה השנתית להגנת סייבר. הגידול בביקוש לשירותי ענן והצורך לעמוד בדרישות רגולטוריות בתחום הגנת הפרטיות במידע, בעיקר לנוכח התקנות החדשות להגנת הפרטיות במידע שנכנסו לתוקפן במאי 2018 באיחוד האירופי,[265] הביאו אף הם להתפתחויות וחידושים בתחום הגנת הסייבר. התעשייה עלתה מדרגה, ותפסה את קדמת הבמה מבחינת מרכזיותה במכלול הטכנולוגיות החדשניות המפותחות בימים אלו. בשנת 2020 הוערך השווי של שוק הגנת הסייבר העולמי ב־173 מיליארד דולר, והוא צפוי להגיע לשווי של 270 מיליארד דולר בשנת 2026. יתרה מכך, בשל העברת חלקים ניכרים מהתעשייה לעבודה מרחוק עקב מגפת הקורונה העולמית גדלו ההוצאות של ארגונים על הגנת סייבר. למשל, 79% מבעלי העסקים באנגליה הגדילו את הוצאות הגנת הסייבר של הארגונים שלהם במהלך שנת 2020.[266]

264 Julian, **לעיל** ה"ש 257.

265 GDPR, **לעיל** ה"ש 42.

266 Nick Ismail, *Securing the Future: The Evolution of Cyber Security in the Wake of Digitalisation*, InformationAge (Feb. 13, 2018); MarketWatch, Cyber Security Market 2018 Global Analysis, Segments, Size, Share, Industry Growth and Recent Trends by Forecast to 2023 (2018); *Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019*, Gartner (Aug. 15, 2018); Louis Columbus, *2020 Roundup Of Cybersecurity Forecasts and Market Estimates*, Forbes (April 5, 2020); Rodika Tollefson, *Cybersecurity Budgeting and Spending Trends 2020: How Does Yours Compare?*, Infosec (May 19, 2020)

בשוק הגנת הסייבר הבינלאומי המתפתח יש לתעשיית הגנת הסייבר בישראל מקום מרכזי. נכון לסוף 2017 היו בישראל למעלה מ־300 חברות הגנת סייבר פעילות, וישראל אף נחשבת למובילת החדשנות בתחום זה ומייצאת מוצרים ושירותים בשווי של יותר מ־3.5 מיליארד דולר. שתיים מעשר החברות המובילות בעולם בתחום הגנת הסייבר הן חברות ישראליות: צ'ק פוינט וסייברארק.[267] בשנת 2017 הייתה ישראל היעד השני בעולם, אחרי ארצות הברית, של השקעות פיננסיות בחברות הזנק בתחום הגנת הסייבר: 16% מכלל ההשקעות בחברות העוסקות בהגנת סייבר בעולם הושקעו בחברות הגנת סייבר ישראליות.[268] בשנת 2018 גדל שיעור זה ועמד על 20%.[269] בישראל פועלת גם תעשיית סייבר התקפי ענפה, כפי שהוסבר בפרק 5.[270]

ג. שיטות עיקריות להגנת סייבר

הואיל ומתקפת סייבר עשויה להתרחש בכל אחת מן החוליות המרכיבות את שרשרת אספקת המידע – החל בחומרה, עבור במערכת ההפעלה וכלה בתוכנה של צד שלישי שהותקנה על גבי המערכות או בספק השירות – הגנת הסייבר של ארגון צריכה להתקיים בכל אחת מן החוליות. לאורך השנים התפתחו כמה שיטות מרכזיות המשמשות ארגונים וממשלות למטרת הגנת סייבר. נסקור אותן כעת.

267 *Israel: A Global Center for Cyber Security*, Start-Up Nation Central

268 Aharon Aharon, *How Israel Is Accelerating Cybersecurity Innovation*, The Times of Israel (Nov. 12, 2018); Ofer Schreiber & Iren Reznikov, *The State of Israel's Cybersecurity Market*, TechCrunch (Jan. 14, 2018); Shoshanna Solomon, *Israel Wins Second-Largest Number of Cybersecurity Deals Globally*, The Times of Israel (April 15, 2018); Yoav Leitersdorf & Ofer Schreiber, *A Look Back at the Israeli Cybersecurity Industry in 2018*, TechCrunch (Jan. 6, 2018)

269 Gil Press, *Israeli Startups Shine In The $92 Billion Cybersecurity Market*, Forbes (Feb. 26, 2019)

270 ראו הטקסט הנלווה להערות שוליים 77–88.

1. מניעת גישה כברירת מחדל (whitelisting)

עקרון מניעת הגישה כברירת מחדל הוא העיקרון המוביל בעולם האבטחה הפיזית והוא מיושם גם בעולם הגנת הסייבר: רק משתמשים שנמצאים ברשימת מורשי הגישה יכולים לגשת למערכות המחשב של הארגון; הודעות דואר אלקטרוני מתקבלות רק מכתובות הנמצאות ברשימה; ורק אפליקציות שנמצאות ברשימה ניתנות להורדה למחשבי הארגון. הבדיקה אם תוכנה, יישום או משתמש נמצא ברשימת מורשי הגישה מתבצעת באחד משני אופנים: באמצעות בקרת גישה רשתית (Network Access Control, NAC) או מערכת חומת אש (firewall), המאפשרות גישה לאזורים שונים במערכות המחשב של הארגון רק לפי הגדרת הרשאות הגישה של המשתמש; או באמצעות אימות חד־חד־ערכי של זהות מבקש הגישה באמצעות סיסמה, תעודה דיגיטלית, כרטיס חכם או נתון ביומטרי. הנחת העבודה של עיקרון זה היא היעדר אמון (zero trust): כל כתובת, שם מתחם או ישות שאינה ברשימה אינם בטוחים ויש למנוע מהם את הגישה למערכות.[271]

לעקרון מניעת הגישה כברירת מחדל יש יתרונות בולטים. ראשית, יישומו קל יחסית: אומנם הוא דורש היכרות מעמיקה עם מורשי הגישה, אולם הוא אינו מחייב חיפוש מתמיד של נוזקות במרחב הסייבר. שנית, הוא מאפשר לעשות שימוש במכשירי קצה המתחברים למערכות הארגון, כגון מחשב נייד או טלפון נייד, ובלבד שהשימוש בהם נעשה בהתאם להנחיות אבטחת המידע בארגון.[272] אולם לעקרון מניעת הגישה כברירת מחדל יש גם כמה חסרונות. החיסרון הראשון הוא הקושי בהגדרת רשימת מורשי גישה, הצורך לעדכנה בקביעות והבירוקרטיה הנלווית ליישומה. על המערכת להכיר את כל מורשי הגישה בארגון ואת מכלול הפעילויות שכל אחד מהם מורשה לבצע בכל זמן נתון. דרישה זו יוצרת עומס רב על העובדים האמונים על הגנת הסייבר בארגון.

271 Finjan Team, *Blacklisting vs. Whitelisting – Understanding the Security Benefits of Each*, Finjan Cybersecurity Blog (May 1, 2017); Elizabeth Mack, *What is Whitelisting and How Should You Implement It?* Springboard Blog (June 11, 2018); Erin Brereton, *Whitelisting May Be the Future of System Security*, FedTech (Jul. 5, 2018)

272 Mack, **לעיל** ה"ש 271.

החיסרון השני הוא ההסתמכות המשמעותית על הגורם האנושי, שחסרונותיה נדונו בפרק 6.[273] החיסרון השלישי הוא שתוקפים עשויים להצליח לחדור לתוך מערכות הארגון באמצעות התחזות לישות מורשית גישה.

2. התרת גישה כברירת מחדל (blacklisting)

לפי שיטה זו הגישה למערכות הארגון מותרת לכל ישות אלא אם היא מופיעה ברשימת מנועי הגישה שמתעדכנת בקביעות. למשל, תוכנת האנטי־וירוס תתריע רק כאשר חתימת נוזקה הידועה לה מופיעה במחשב שעליו היא מותקנת, ותוכנת סינון תחסום מסרי דואר אלקטרוני המוגדרים כדואר זבל או גישה לכתובות IP מסוימות (למשל, כחלק מחסימת פרסומות).

העיקרון של התרת גישה כברירת מחדל מוכר גם הוא בעולם האבטחה הפיזי במקומות ציבוריים מסוימים: למשל, בבתי קזינו הבעלים מעוניינים לאפשר גישה לכלל הציבור למעט אנשים מסוימים; בעמדת ביקורת גבולות נמנעת כניסתם של פושעים מוכרים לתחומי המדינה.[274]

חסרונו המרכזי של עיקרון זה הוא במתן הגנה רק נגד נוזקות ידועות ומוכרות – נוזקה חדשה שאינה מוכרת, נוזקה המנצלת חולשת יום אפס או נוזקה קיימת שבוצע שינוי קל באופן פעולתה ובחתימתה לא ייחסמו.[275] כמו כן, כדי לספק הגנה יעילה יש להתעדכן כל העת בגילוי של חולשות ונוזקות חדשות. במציאות שבה נכון לשנת 2017 התגלו בממוצע 360,000 נוזקות חדשות בכל יום,[276] ובשנת

273 להרחבה בנוגע לפגיעות הגורם האנושי ראו פרק 6.

274 Finjan Team, **לעיל** ה"ש 271.

275 Bruce Schneier, *Whitelisting vs. Blacklisting*, Schneier On Security (Jan. 28, 2011)

276 Tara Seals, *360k New Malware Samples Hit the Scene Every Day*, InfoSecurity Magazine (Dec. 14, 2017)

2020 יותר מ־11 מיליון נוזקות בחודש בממוצע,[277] קיים קושי אובייקטיבי לספק הגנה יעילה תוך עדכון אמיתי ומהיר של רשימת מנועי הגישה.[278]

אף שלכאורה עקרון התרת הגישה כברירת מחדל נראה כסותר את העיקרון של מניעת הגישה כברירת המחדל, פעמים רבות שני עקרונות אלו מיושמים זה לצד זה במערכות ממוחשבות. לדוגמה, ארגון עשוי להטמיע מערכות של בקרות גישה, כגון כניסה מוגנת בסיסמה ומערכות חומת אש המאפשרות גישה רק לישויות המוגדרות ברשימה, לצד מערכות אנטי־וירוס המתריעות כאשר חתימת נוזקה הידועה להן הופיעה במחשב שעליו הן מותקנות.

3. הטמעת עדכוני אבטחה

הטמעת עדכוני אבטחה באופן רציף ומיידי היא חלק חשוב מהגנת סייבר, והיא נדרשת כדי למזער את הסיכוי של ניצול חולשה במערכות המחשב לשם ביצוע מתקפת סייבר. חברות תוכנה רבות מפרסמות עדכוני אבטחה באופן תדיר.[279] עדכוני אבטחה אלו מצביעים על חולשות שזוהו ותוקנו, אך בכך טמון גם חסרונו המרכזי של הנוהג לשחרר במהירות מוצר תוכנה ולעדכנו מאוחר יותר: עדכוני התוכנה הכוללים פירוט מדויק של החולשה שזוהתה ומתוקנת על ידי העדכון חושפים בפני תוקפים פוטנציאליים אפשרויות תקיפה של מערכות שטרם התקינו את עדכוני האבטחה. באופן זה, פרסום עדכוני אבטחה שם למטרה ארגונים המתמהמהים בהטמעת עדכונים במערכותיהם.[280]

277 *Malware*, AV-TEST

278 Finjan Team, **לעיל** ה"ש 271.

279 חברת מיקרוסופט, למשל, מפרסמת את עדכוני האבטחה למערכות שלה מדי יום שלישי בשבוע. כריסטופר באד, אחד ממומחי האבטחה בחברה, מספר על האופן שבו מוסדר התהליך בארגון: Christopher Budd, *Ten Years of Patch Tuesdays: Why It's Time to Move On*, GeekWire (Oct. 31, 2013)

280 *Why Software Updates Are So Important*, McAfee (Sep. 19, 2017); Steve Symanovich, *5 Reasons Why General Software Updates and Patches Are Important*, Norton (Jan. 23, 2021)

4. סקירת חולשות

שיטה זו מבוססת על סקירות תקופתיות לאיתור חולשות במערכות, המבוצעות באופן אוטומטי באמצעות תוכנות ייעודיות. חסרונה המרכזי הוא חוסר היכולת לספק מענה ודאי ומלא, שכן לנוכח הדינמיות של מתקפות סייבר, תוכנת סריקה אינה מעודכנת בכל זמן נתון בכל החולשות הקיימות, ועל כן ייתכן שלא תתריע על קיומה של חולשה חדשה שעלולה להיות מנוצלת לטובת מתקפת סייבר.

5. ניהול וניתוח של התיעודים (logs) של הפעילות הרשתית והדיגיטלית במערכות ממוחשבות

מערכות דיגיטליות מתעדות כל אירוע ופעולה המתרחשים בהן, לרבות אירועי אבטחה. כמות התיעודים עצומה וגדלה ללא הרף, ועל כן נדרש ניהול נכון של התיעודים, כלומר הליך ברור לתיעוד, העברה, אחסון וניתוח תקופתי של תיעודים הנוגעים לאבטחת מידע ולהגנת הסייבר. במסגרת הליך שכזה יש לקבוע מראש גם מהי רמת הפירוט הנדרשת בכל תיעוד. בדרך זו אפשר לזהות פעילות חריגה ואנומליות סמוך ככל האפשר להתרחשותן, למשל חדירה בלתי מורשית למערכות הממוחשבות של הארגון, שימוש מואץ וחריג במשאבי המערכת, ניטור תוכנות המורצות על גבי המערכות הממוחשבות של הארגון או התחברות של מחשב חדש לרשת הארגון.[281]

במדינות מסוימות, למשל הולנד, ניהול התיעודים נעשה במסגרת מרכזי מידע שהוקמו בשיתוף בין ספקי שירות (ISPs) והממשלה. ספק שירות שמבחין בנתונים המעידים כי מנוי קצה שלו עושה שימוש חריג או מואץ באפשרות הגישה לאינטרנט המסופקת לו חוסם את הגישה של אותו מנוי לאינטרנט. כך אפשר לזהות ולחסום מכשירי קצה המשמשים כחלק מצבא בוט־נטים.[282]

281 Karen Kent & Murugiah Souppaya, *Guide to Computer Security Log Management* (NIST Special Publication 800-92, 2006)

282 van Eeten, **לעיל** ה"ש 47, בעמ' 441-442.

6. גיבוי מחזורי ותוכניות לשיקום וחזרה לשגרה לאחר מתקפת סייבר

מדיניות גיבוי מחזורית של מערכות המחשב של הארגון היא חלק חשוב מהגנת הסייבר. הגיבוי הוא עותק המידע שהיה קיים במערכות המחשב של הארגון במועד מסוים, ולכן הוא ההגנה האחרונה מפני אובדן מידע בשל מתקפת סייבר. הגיבוי מקנה יכולת לשחזר את המידע המקורי במועד הסמוך ביותר האפשרי לפרוץ מתקפת הסייבר, וכך מסייע לארגון להשתקם במהרה ממתקפה.[283]

7. "מלכודות דבש" (honeypots)

שיטה נוספת הננקטת בידי אחראי הגנת הסייבר היא הצבה של "מלכודות דבש" – מחשבים או מערכות מחשוב המדמים מטרות נוחות למתקפת סייבר. מטרת מלכודות הדבש היא למשוך אליהן תוקפים במטרה להטעותם, וכך לאתר ולחסום מתקפות סייבר פוטנציאליות; לנתח את האופן שבו תוקפים פועלים, כלומר כיצד הם מאתרים חולשה ומנצלים אותה כדי להחדיר נוזקה לתוך מערכות המחשב המותקפות; לזהות חולשות אפשריות במערכות המחשב הקיימות; ולהבין טוב יותר מהם אמצעי ההגנה היעילים יותר.

בשנת 1986 נעשה לראשונה שימוש במלכודת דבש לשם איתור והפסקה של מתקפת סייבר, כאשר מנהל הרשת במעבדות הלאומיות של מוסד לורנס ברקלי זיהה כניסה בלתי מורשית לרשת הארגון. הוא אסף 50 מחשבים במשרדו וחיבר אותם לקו הטלפון של המשרד. כאשר התוקף התקשר לבסוף, מנהל הרשת איתר את השיחה ואת מקורה – סוכן ק.ג.ב.[284]

באמצעות מלכודות דבש שהוטמעו במכשירי האינטרנט של הדברים למדו מומחים מאילו מדינות יוצאות רוב מתקפות הסייבר ומהן הסיסמאות שתוקפי הסייבר מחשיבים כשכיחות ומנסים לחדור למערכות מחשב באמצעותן, וכן

283 *What Is Backup and Recovery?* NetApp

284 Cliff Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage (2005)

נמצא שיש חשיבות גדולה לאימוץ סטנדרט הגנה אחיד בקרב כל היצרנים של מכשירי האינטרנט של הדברים.[285]

לפיכך יתרונותיה של שיטת מלכודת הדבש הם האפשרות לאסוף מידע על שיטות תקיפה ואופני פעולה של מתקפות סייבר, וכן היתרון שהיא מעניקה לממונה על הגנת הסייבר בארגון לעומת התוקפים: הממונה על הגנת הסייבר בארגון מסוגל לאתר ולחסום מתקפת סייבר לפני שהיא מצליחה לחדור למערכות הארגון ואילו התוקפים נופלים במלכודת. כאשר מלכודת הדבש ממוקמת במערכות הארגון מאחורי חומת אש או אמצעי הגנה אחר המיישם התרעה או מניעה של גישה כברירת מחדל, היא משמשת גם קו הגנה אחורי נוסף במקרה שאמצעי ההגנה הקדמיים יותר נפרצים.[286]

אחד האתגרים המרכזיים בשימוש במלכודות דבש הוא כיצד ליצור מלכודת דבש אמינה דייה בעיני התוקף הפוטנציאלי, כך שישתכנע שמדובר במערכת ממוחשבת ארגונית לגיטימית ובת תקיפה, ובו בזמן להטמיע אמצעי הגנת סייבר ברמה מספקת שלא יאפשרו לתוקף חדירה קלה מידי למערכות הארגון ויעוררו את חשדו שמדובר במלכודת דבש, אך גם לא יהיו קשים מדי לפריצה כך שהתוקף יוותר ויחפש מערכות קלות יותר לפריצה.[287]

285 Steve Symanovich, *What is a Honeypot? How It Can Lure Cyberattackers*, Norton (May 26, 2020); Caleb Townsend, *What is a Honeypot*? United States Cybersecurity Magazine

286 Yifat Mor, *Using Dynamic Honeypot Cyber Security: What Do I Need to Know?* Guardicore (Oct. 10, 2018)

287 שם.

פרק 10

סיכום

חשיבותו של מרחב הסייבר בחיי היום־יום שלנו התעצמה בשני העשורים האחרונים, ומשבר הקורונה, שהביא לאימוץ נרחב של מתכונת עבודה ומסחר מרחוק, העצים אותה עוד יותר. הפעילות במרחב הסייבר רלוונטית לכל תחומי החיים ולכן טומנת בחובה סיכונים הולכים וגדלים, שאינם מתמצים בגניבת פרטי כרטיס אשראי ומכירתם בשוק השחור או בחסימת הגישה לקבצים במחשב ביתי. מתקפות הסייבר שאירעו בשנים האחרונות מלמדות שהסיכונים במרחב הסייבר גדולים מאוד בהיקפם, בהשלכותיהם ובנזק הכלכלי או הפיזי שהם עלולים לגרום.

בנסיבות אלה מדינות רבות, ובכללן ישראל, מבקשות לתת מענה לסיכונים ולהתוות אסדרה מתאימה להגנת מרחב הסייבר. ללא ספק, האתגרים העומדים בפני גיבוש אסדרה מסוג זה הם בראש ובראשונה אתגרים טכנולוגיים, למשל הצורך להעריך את מידת האפקטיביות של פעולות להגנת מרחב הסייבר ושל הרצף הנכון שלהן. ואולם, בשל מורכבות הנושא והעובדה שהסכנות אינן ייחודיות למגזר מסוים או לתעשייה מסוימת יש צורך לפעול בשיתוף פעולה עם גורמים מתחומים נוספים, כגון כלכלה, פסיכולוגיה, משפטים, מדעי המדינה וסוציולוגיה. בשל כך אנו סבורים כי אסדרה מיטבית ושקולה של ההגנה על מרחב הסייבר דורשת אוריינות דיגיטלית מצד מקבלי ההחלטות: הבנה של מרחב הסייבר, מאפייניו הייחודיים, השלבים של מתקפת סייבר, דרכי פעולה אפשריות של תוקפים ודרכי הגנה מפניהם. אחרת קיים חשש שמקבלי החלטות לא יוכלו להבין לאשורם את אתגרי האסדרה, מצד אחד, ולא את החששות מפני אסדרה בלתי אחראית, מצד אחר.

מחקר זה הוא הראשון מתוך שני מחקרים העוסקים בנושא. במחקר זה בחרנו שלא להיכנס לעובי הקורה של פרטי האסדרה ושל ההסדרים ההשוואתיים אלא לפרוׂש עבור הקוראים את התשתית המושגית שהם נדרשים לה כיום. החלק השני יעסוק במנגנוני האסדרה ובפרטי הצעות החוק המונחים כיום על שולחנם של מקבלי ההחלטות בארץ ובחלק ממדינות העולם המערבי.

לפיכך במחקר הנוכחי הסברנו את המאפיינים הייחודיים של מרחב הסייבר המשפיעים הן על אופן השימוש בו הן על הסכנות הטמונות בו: קצב התנועה האדיר; העלות הנמוכה של ביצוע פעולות; וה"היפר־קישוריות", כלומר היכולת של סוגים רבים של שחקנים במרחב הסייבר (מדינות, חברות פרטיות קטנות, תאגידי ענק, ארגונים שלא למטרות רווח, ארגוני פשיעה, ארגוני טרור, יחידים וכלל המכשירים המקושרים לרשת האינטרנט) לתקשר אלה עם אלה ולהעביר כמויות עצומות של מידע ביניהם.

עוד עסקנו בכשלי השוק היוצרים היעדר תמריצים להשקעה בפיתוח של מוצרים מאובטחים מפני מתקפות, וגורמים לכך שחברות מוציאות לשוק מוצרים ושירותים שרמת האבטחה שלהם אינה מספקת – בין השאר משום שמי שמייצר את המוצרים האלה אינו נושא בהשלכות של הנזק שהוא גורם. כך גם באשר למי שמייצר מוצרי אבטחת מידע, שיודע שהוא פועל בשוק שבו הצרכנים אינם יכולים להעריך את האיכות של אותם מוצרים.

בהמשך הסברנו מהי מתקפת סייבר – שרשרת פעולות היוצרות נזק, ומכונות לכן "שרשרת הרג". עסקנו גם בגורם האנושי, שהוא חוליה חלשה בהגנת סייבר, וכן בא־סימטריה במידע בין מי שמבקשים לבצע תקיפות ובין המגינים מפניהן. עבור תוקף מספיקה היכרות עם חולשת אבטחה אחת במערכת מידע כדי לממש תקיפת סייבר מוצלחת. לעומת זאת, על מפתחי מערכות ההגנה להשקיע משאבים רבים – בכוח אדם ובכסף – כדי לאתר את כלל החולשות במערכות המידע ולהגן עליהן מפני כלל הפגיעות האפשריות.

לבסוף, עסקנו בהגנת סייבר והסברנו את היחס בינה ובין אבטחת מידע, אבטחת נתונים והגנת הפרטיות. הגדרנו הגנת סייבר כמכלול הפעולות שמטרתן להתמודד עם איום על השלמות, האמינות, הזמינות והפרטיות של מידע הנמצא במחשבים, במערכות מידע ורשתות מחשבים ובתשתיות דיגיטליות אחרות, וכן לסייע למערכות אלה לשוב לתפקוד תקין במקרה של מימוש איום כזה. סקרנו גם שיטות עיקריות להגנת סייבר, כגון מניעת גישה למי שאין לו הרשאה, התרת גישה רק למי שמורשה לכך, הטמעת עדכוני אבטחה וניהול יומן תיעודי הפעילות הדיגיטלית בארגונים.

המסקנה המרכזית העולה ממחקר זה היא שהסיכונים שמתקפות סייבר עשויות לייצר, יחד עם כשלי השוק המייצרים תת־הגנה, מחייבים התערבות ממשלתית ותמריצים רגולטוריים. ואולם, אסדרה מדינתית איננה תרופת פלא והיא מלווה בחששות ובאתגרים. למדינה כובעים רבים במרחב הסייבר, ולפעמים יש ניגודי אינטרסים בין תפקידיה השונים: היא הבעלים של תשתיות קריטיות; האחראית לביטחון הלאומי ואמורה להגן על התשתית הקריטית עצמה; פועלת כרגולטור עבור גופי המגזר הפרטי המחזיקים בתשתיות במרחב הסייבר ואחראים להגנתו; שחקנית הלוקחת חלק בשיתופי פעולה ציבוריים ופרטיים להגנת מרחב הסייבר; נציגה במישור הבינלאומי ופועלת עם ומול מדינות אחרות במטרה להגן על מרחב הסייבר, מאחר שמדובר במרחב שהגבולות הגיאוגרפיים בו מטושטשים; יצרנית ומפיצה של ידע ומידע בנוגע להגנת מרחב הסייבר; ולבסוף, פעמים רבות המדינה היא גם התוקפת במרחב הסייבר, היוצרת בעצמה איומים. כל אלה מחייבים את מקבלי ההחלטות לפעול בסביבה מורכבת, שהבנתה היא הבסיס הראשוני לכל מדיניות ויישומה.

יתרה מזו, מורכבות המרחב מובילה לכך שאסדרה אפקטיבית תהיה כזאת המטילה אחריות על כתפי שחקנים רבים, במגזר הציבורי וגם במגזר הפרטי, התעשייה והאקדמיה. לכן, האוריינות הדיגיטלית נדרשת עבור כלל השחקנים, ואנו תקווה שמחקר זה ימלא את החלל הקיים היום בשפה העברית בנושא זה.

THE ISRAEL
DEMOCRACY
INSTITUTE

Policy Paper 171

WHAT IS CYBER SECURITY?

Part One
Cyberspace, Cyber Attacks, and Cyber Protection

Rachel Aridor-Hershkovitz | Tehilla Shwartz Altshuler | Ido Sivan-Sevilla

October 2021

Text Editor [Hebrew]: Hamutal Lerner
Series and Cover Design: Studio Tamar Bar Dayan
Typesetting: Nadav Shtechman Polischuk
Printed by Graphos Print, Jerusalem

ISBN: 978-965-519-367-1

No portion of this book may be reproduced, copied, photographed, recorded, translated, stored in a database, broadcast, or transmitted in any form or by any means, electronic, optical, mechanical, or otherwise. Commercial use in any form of the material contained in this book without the express written permission of the publisher is strictly forbidden.

Copyright © 2021 by the Israel Democracy Institute (RA)
Printed in Israel

The Israel Democracy Institute
4 Pinsker St., P.O.B. 4702, Jerusalem 9104602
Tel: (972)-2-5300-888
Website: en.idi.org.il

To order books:
Online Book Store: en.idi.org.il/publications
E-mail: orders@idi.org.il
Tel: (972)-2-5300-800

The views expressed in this policy paper do not necessarily reflect those of the Israel Democracy Institute.

All IDI publications may be downloaded for free, in full or in part, from our website.

Abstract

A woman dies due to a delay in treatment in the emergency room following a cyber attack on the hospital’s computer systems. Hackers publish personal information about students in a school in a major city, including their identity card numbers. A study on the development of a vaccine against Covid-19 comes to naught because researchers’ access to their data is blocked. Russia exploits a breach in the SolarWinds monitoring software to infiltrate the computer systems of American government agencies, security services, and private companies; the damage to US national security is said to be comparable to that caused by the attack on Pearl Harbor in World War II.

These are just a few examples, some real and others just hypothetical, of the potential harm of cyber attacks. As many aspects of our daily lives become based more and more on instruments connected to central brains, such as central information systems, digital assistants, pacemakers, and self-driving cars, concern about cyber attacks is increasing. The Covid-19 pandemic has further intensified these concerns due to the growing dependence of many entities—from workplaces and schools to hospitals and research institutes—on remotely controlled systems.

Thus, alongside the tremendous advantages of cyberspace for the economy and society as a whole, there has been a sharp increase in the scope of cyber attacks, in the number of targets, and in the economic damage caused, as well as in the degree of effectiveness of the organized crime groups or hostile countries behind the attacks. Due to all these factors, it is necessary to look into the best methods of protecting cyberspace activity and their regulation through legislation. This need has not gone unnoticed by Israeli legislators, as we see from the memorandum on the Cyber Defense and National Cyber Directorate Law, 2018 (hereafter: the Cyber Law Memo), and from the effort, before the March 2021 elections, to pass the Authority for Strengthening Cyber Protection Bill (Provisional Measure), 2021—essentially an abridged, narrowly focused version of the Cyber Law Memo in the form of a provisional measure that would be in effect for just two years.

Before we discuss the regulation of cyber protection in Israel, it is necessary to explain and understand the terms used to describe cyberspace, cyber protection, and cyber attacks and the related challenges. The purpose of this study is to present the various terms associated with the protection of cyberspace in order to give policymakers the knowledge and tools needed to understand the balance of power in cyberspace and the challenges associated with protecting it, as a basis for regulating the issue in Israel. Along with this publication, we are publishing a document on the regulation of cyberspace in Israel from a comparative perspective, focusing, inter alia, on the development of the National Cyber Directorate and the Cyber Law Memo.

The first and most important concept that must be understood is "cyberspace": The term refers to the internet as the main platform for transferring information and data from place to place, as well as a range of interrelated systems used for data and information transfer that are not bound by physical or geographical limitations.

Cyberspace has several unique characteristics that offer users many advantages, but also make it fertile ground for attacks: First, transferring information in cyberspace is many times faster than transferring it by traditional means (air, sea, and land); information can be sent from one end of the world to the other at inconceivable speed. Second, the cost of carrying out an action in cyberspace, even one with far-reaching consequences, is not high. Action in cyberspace does not require political infrastructure or a large budget and can be carried out at relatively low cost on a personal computer or by purchasing cyber-attack services from private companies. Due to these two features, considerations of distance are irrelevant in cyberspace, the familiar geographical borders are blurred, and many actors—countries, substate organizations, and individuals—have powerful attack capabilities. Furthermore, digital traces are erased in cyberspace, making rapid, unambiguous identification of perpetrators difficult. And above all these characteristics hovers the "hyperconnectivity" of cyberspace: the ability of the various components of cyberspace—the players (countries, small private companies, giant corporations, nonprofit organizations, individuals, organized crime groups, terrorist organizations) and the instruments (digital devices such as computers and smartphones, as well as applications and software)—to communicate with one another in diverse ways and on various levels and to transfer huge quantities of information between them. As more and more services, information systems, and products become interconnected (by the technology known as "the Internet of Things") and capable of absorbing and transferring information from their environment and from one another, it becomes easier for a cyber attack, which is waged by a computer program to spread rapidly, to reach more systems, services, and infrastructure, and to cause major damage.

These characteristics of cyberspace are also responsible for various market failures, which in some cases may justify government intervention in order to regulate and secure cyber protection. The cyberspace market is

"two-sided": on one side services and products are sold or given away for free; and on the other side information about the behavior and "screen time" of users of products is sold to information vendors and advertisers. In this situation, the corporations are loyal not to the users, i.e., the consumers of their products and services, but to the advertisers, who are their main source of income. Moreover, corporations and information vendors operating in cyberspace have no great incentive to invest in information security and user protection. The market failures leading to low investment in cyber protection stem from additional factors as well, including the complexity of writing software and the race to be the first to market a novel software product so as to achieve market dominance. Another factor is the fact that developers of a software product that is not secure and properly protected and is therefore vulnerable to cyber attacks are not held responsible, personally or wholly, for the consequences of their actions (a phenomenon known as "negative externalities") and therefore they do not consider the danger of a cyber attack significant enough to justify investing resources in improving cyber protection and information security. A third factor is the inherent asymmetry in information between cyber attackers and cyberspace defenders: for the attacker it suffices to identify one cyber weakness in order to launch a cyber attack, but in order to protect cyberspace one has to identify and locate every potential weakness in advance and prevent exploitation of it.

In addition to the market failures that stem from the unique characteristics of cyberspace, it is important to bear in mind that the human factor in cyberspace (the employees or subcontractors of the organization attacked) is the weak link in cyber protection in an organization. Most successful cyber attacks take advantage of the tendency not to install important security updates regularly and routinely. One of the main distribution channels for exploiting weaknesses and spreading malware is phishing, which takes advantage of the tendency of internet and email users to click on links or open files without making sure they do not contain malware.

Raising users' awareness of the dangers in cyberspace and adopting principles and procedures for reducing the risk are vital for minimizing the potential harm that can be caused by the human factor as the weak link in the cyber protection system.

Understanding the complexity of a cyber attack is also essential to drafting cyber protection policy. A cyber attack consists of several dynamic stages of activity that may be carried out by different players in cyberspace at different times, while maintaining active relations with each other. The first stage of a cyber attack is known as "reconnaissance." In this stage attackers personally gather as much information as possible on the system that they want to attack or purchase it ready-made in the cyber attack marketplace in order to identify weaknesses: technological breaches or unanticipated behavior of a computer system that enables potential attackers to gain access or carry out actions that they are not authorized to carry out. In the second stage, known as "weaponization," attackers prepare or purchase the malware that they will use to exploit the weakness found and to carry out the cyber attack. There are various kinds of malware: spyware, i.e., tracking software; Trojans, i.e., malware disguised as legitimate, useful software; bots, i.e., malware that causes the computer system being attacked to act as a robot and obey orders given remotely; and ransomware, which encrypts the files in the computer system under attack, thereby locking them until ransom is paid to the attacker. In the third stage, the malware is delivered to the target of the attack, the code in the malware responsible for exploiting the weakness is activated, and access authorizations are obtained. Using them, attackers install a "backdoor" in the system being attacked that enables them to control it remotely and accomplish the goal of the attack (deleting files, preventing access to them, destroying the computer system, gathering and copying information from the system, spreading to other systems connected to the attacked system, or installing spyware that tracks the user of the system).

The motives for cyber attacks are varied: companies try to obtain a competitive advantage and therefore financial gain through industrial espionage; terrorists sow destruction and fear in order to achieve their objectives; and countries gather intelligence for the purpose of economic, political, and security gains or as a full-fledged means of warfare. It is hard to determine the total direct and indirect damage that can be caused by a cyber attack with any precision, but estimates published from time to time point to significant economic damage. In 2018, for example, the Center for Strategic and International Studies and the McKinsey consulting firm published a joint estimate putting the annual damage to the global economy due to cybercrime at $600 billion.

The potential damage that cyber attacks can cause is wide-ranging: the cost of replacing hardware and software, damage to infrastructure, loss of human lives when emergency medical services are attacked, the cost of resuming protection (e.g., installing new antivirus software), compensation of customers, fines paid to state regulatory bodies, the cost of interference with the proper functioning of a business, the cost of identity theft and the fight against it, the cost of losing customers' trust and rehabilitating the company's reputation, the cost of exposure of trade secrets, and the cost of impairment of innovation and competitiveness and of lost business opportunities, as well as psychological harm and harm to society—such as actual disruption of daily life due to attacks on essential services, loss of public confidence in the government and its systems, loss of confidence in the ability to determine reality accurately, and public polarization between different opinions.

Cyber protection is therefore essential, but the fact that it has no clear, coherent definition makes it difficult to adopt a public policy in this regard. Policymakers are faced with a series of definitions, each emphasizing the importance of cyber protection to certain fields: national and personal security, diplomacy and foreign relations, the economy, employment and industrial development.

As we see it, “cyber protection” should be defined as an aggregate of activities, both proactive and reactive, aimed at contending with threats to the integrity, reliability, and availability of the information stored in computers, information systems and computer networks, and other digital infrastructure, and helping these systems resume normal functioning if such threats are carried out. It is important to stress what is not included in the definition: Cyber protection does not concern threats inherent in the information itself, such as expressions of hatred, libel and slander, insults to public servants, violations of privacy, dissemination of information that is under a publication ban for security or other reasons, or attempts to influence elections.

However we define the term “cyber protection,” we have to bear in mind how it relates to the fundamental right to privacy. Cyber protection is an essential precondition for exercising the right of individuals to privacy, even though it includes a range of topics that have nothing to do with protection of personal information and privacy—for example, protection of infrastructure and economic security. For this reason, a conflict of interest sometimes arises between privacy and cyber protection, reflecting an underlying clash between freedom and security. The most salient case of such a clash is the ability to use services in cyberspace anonymously. On the one hand, using cyberspace without identifying oneself is a way of exercising one’s right to privacy. On the other hand, anonymous internet use runs counter to the goal of cyber protection—namely, to make the safe use of cyberspace possible, and therefore enforcement authorities have an interest in identifying every user so as to prevent cybercrimes or to identify those responsible for cybercrimes after the fact.

אישה מתה בשל עיכוב בטיפול בחדר מיון שנגרם בעקבות מתקפת סייבר על מערכות המִחשוב של בית החולים; האקרים מפרסמים מידע פרטי על תלמידי בית ספר; פיתוח של חיסון לנגיף הקורונה יורד לטמיון בגלל חסימת הגישה של החוקרים לדאטה שלהם; מדינה זרה מנצלת פִּרצה בתוכנת ניטור כדי לחדור למערכות הממוחשבות של רשויות ממשל. אלו הן רק דוגמאות לנזקים הפוטנציאליים של מתקפת סייבר. תחומים רבים בחיי היום־יום שלנו מתבססים יותר ויותר על מכשירים המחוברים למוחות מרכזיים, כגון מערכות מידע מרכזיות, עוזרים דיגיטליים, קוצבי לב ורכבים אוטונומיים, והחשש מפני מתקפות סייבר הולך וגדל. מגפת הקורונה העצימה את החששות בגלל התלות הגוברת של גופים רבים במערכות הנשלטות מרחוק.

מטרת המחקר המוגש כאן היא לתת בידי קובעי המדיניות את הידע והכלים הנחוצים להבנת יחסי הכוחות במרחב הסייבר והאתגרים הקשורים בהגנתו כבסיס לאסדרת הנושא בישראל. לפיכך הוא מתאר את המושגים הנוגעים למרחב הסייבר, להגנת הסייבר ולמתקפת הסייבר; את המאפיינים הייחודיים של מרחב הסייבר ההופכים אותו לכר פורה למתקפות; את המניעים למתקפת סייבר ואת הנזקים הכרוכים בה; את השלבים של מתקפה כזאת; את הדרכים לביצוע הגנת סייבר ואת היחס בינה לבין הגנת המידע הפרטי שתוקפים מבקשים להשיג. מחקר זה הוא חלק ראשון בסדרה של שני מחקרים. החלק השני עוסק באסדרת מרחב הסייבר בישראל בפרספקטיבה השוואתית ומתמקד בבניית מערך הסייבר הלאומי ובתזכיר חוק הסייבר.

ד"ר רחל ארידור הרשקוביץ היא חוקרת בתוכנית "דמוקרטיה בעידן המידע" של המכון הישראלי לדמוקרטיה. עבודת הדוקטור שלה עסקה במסגרות לשיתופי פעולה בין הממשל לתעשייה לשם הגברת ההגנה על מרחב הסייבר. מומחית למשפט וטכנולוגיה, בדגש על הזכות לפרטיות.

ד"ר תהילה שוורץ אלטשולר היא עמיתה בכירה במכון הישראלי לדמוקרטיה וראשת התוכנית "דמוקרטיה בעידן המידע". חברת מועצת הארכיונים העליונה ולשעבר חברת נשיאות מועצת העיתונות. עמיתת מחקר בכירה במרכז פדרמן למשפט וסייבר באוניברסיטה העברית בירושלים. מומחית לאסדרת תקשורת ואתיקה עיתונאית ולממשק שבין טכנולוגיה, משפט ומדיניות.

ד"ר עידו סיון סביליה הוא חבר סגל במחלקה ללימודי מידע באוניברסיטת מרלינד (UMD). עוסק באופן שבו התפתחות טכנולוגית בתחומי הגנת הסייבר, פרטיות המידע והבינה המלאכותית מאתגרת מושגי יסוד בתחום המינהל והמדיניות הציבורית כגון עיצוב מדיניות, אכיפה ואחריותיות.

מחיר מומלץ: 45₪

אוקטובר 2021

מסת"ב:
978-965-519-367-1

0 4500001245 5
דאנאקוד 450-1245

www.idi.org.il