לוחמת הסייבר בארצות הברית: השלכות על גופי סייבר מבצעיים ועל קביעת מדיניות הסייבר

עמרי הייזלר

מאמר זה מתמקד בשני מרכיבים מרכזיים של מרחב הסייבר ולוחמת הסייבר בארצות הברית. תחילה הוא יסקור שלושה אירועי סייבר בתקופות שונות, שבמהלכן חלה התפתחות הדרגתית בתשתיות, במנגנונים ובמדיניות ארצות הברית בתחום הסייבר. במסגרת זו ינתח המאמר את ההתפתחות התפיסתית, המבצעית והמשפטית שהובילה למבנה הארגוני של תחום הסייבר האמריקאי ולתהליך הנוכחי של קבלת ההחלטות בו. בהמשך יבחן המאמר את המדיניות ואת שיטות הפעולה של קהילת המודיעין האמריקאית וכן את המבנה של המערכת המבצעית של תחום הסייבר בארצות הברית. במסגרת זו ייסקרו הרקע, תחומי האחריות והמשימות של קהילת המודיעין של ארצות הברית לפני מתקפת סייבר, במהלכה ואחריה, תוך התעכבות על המבנה הארגוני, וספציפית על הארכיטקטורה הארגונית שלה. כמו כן יסקור המאמר בקצרה את איומי הסייבר הנוכחיים על ארצות הברית ויפרט כמה מהאסטרטגיות וכללי המדיניות שמשמשים אותה למתן מענה הולם לאיומים אלה. לבסוף, המאמר ינתח את מרחב הסייבר ברמת המקרו, תוך התייחסות לתיאום בין סוכנויות המודיעין האמריקאיות וביניהן למוסדות הפדרליים, המדינתיים והפרטיים הרלוונטיים לטיפול במשברי סייבר.

מילות מפתח: Moonlight Maze, תולעת מוריס, סטוקסנט, מתקפות סייבר, קהילת המודיעין האמריקאית, משבר סייבר, איומי סייבר, משילות אינטרנט, מדיניות אינטרנט, אסטרטגיית סייבר

עומרי הייזלר הוא קצין צה"ל ועובד משרד ראש הממשלה לשעבר. בוגר תואר שני מטעם בית הספר ליחסים בינלאומיים וציבוריים של אוניברסיטת קולומביה (SIPA).

תולדות לוחמת הסייבר

ניתן לחלק את התפתחות לוחמת הסייבר לשלושה שלבים היסטוריים: שלב התהוות, במהלך העידן המוקדם של האינטרנט; שלב הנסיקה, במהלך תקופת הביניים שלפני מתקפת 11 בספטמבר 2001 ואחריה, כאשר מתקפות הסייבר היו ברובן עדיין בעלות אופי של איסוף מידע; ושלב המיליטריזציה הנוכחי, שבו לוחמת סייבר יכולה לפגוע ביכולות אסטרטגיות ובתשתיות אמריקאיות קריטיות, בדומה למתקפה קינטית בקנה מידה נרחב.[1] הטבלה שלהלן מתארת שלבים אלה.

טבלה 1. שלבים היסטוריים בלוחמת הסייבר

שלבים	התהוות	נסיקה	מיליטריזציה
מסגרת זמן	1980–1998	1998–2003	2003 – כיום
דינמיקות	לתוקפים יש יתרון על המותקפים	לתוקפים יש יתרון על המותקפים	לתוקפים יש יתרון על המותקפים
למי יש יכולות?	ארה"ב ועוד כמה מעצמות־על	ארה"ב ורוסיה ועוד שחקנים קטנים רבים	ארה"ב, רוסיה, סין, ועוד שחקנים קטנים רבים עם יכולות משמעותיות
יריבים	האקרים	האקטיביסטים, האקרים פטריוטים, וירוסים ותולעים	ניאו־האקטיביסטים (Neo-Hakctivists), סוכני ריגול, תוכנות זדוניות, צבאות של מדינות, מרגלים ושלוחיהם, האקטיביסטים (Hacktivists)
אירועים מרכזיים	"ביצת הקוקייה" (1986), "תולעת מוריס" (1988), האקרים הולנדים (1991), מעבדות רומא (1994), "סיטיבנק " (1994)	"Eligible Receiver", "Solar Sunrise", "Moonlight Maze", "Allied Force",	"Titan Rain", אסטוניה, גיאורגיה, "Buckshot Yankee", "סטוקסנט"
הדוקטרינה האמריקאית	לוחמת מידע	מבצעי מידע	לוחמת סייבר

מתקפות סייבר כזרז להתפתחות ארגונית

כל אחת מהתקופות שתוארו בטבלה שלעיל מתאפיינת בדוקטרינה שונה מהותית, הן בהתייחס להתקדמות הטכנולוגית ולסוגי האיומים והן בהתייחס למדיניות

הסייבר של הממשל האמריקאי. חלק ממתקפות העבר רמזו על אתגרי הסייבר העתידיים ושימשו כסימני אזהרה לפגיעויות של ארגונים ולמצב האבטחה הבלתי מספק השורר בהם. ככל שהתלות של החברה בטכנולוגיה עלתה, כך גם גברו ההשלכות האפשריות של אבטחה בלתי מִספקת על פגיעויות ספציפיות במרחב הסייבר.

שלב ההתהוות – "תולעת מוריס"

אירוע סייבר זה שימש כקריאת ההשכמה הראשונה לקהילת המודיעין האמריקאית, לקובעי המדיניות ולחוקרים באקדמיה. אמנם, לא הייתה זו מתקפת הסייבר הראשונה על מערכות מחשב אמריקאיות (מתקפת ריגול הסייבר המשמעותית הראשונה הייתה החדירה בשנת 1986, שזכתה לכינוי Cuckoo's Egg בה היה מעורב הקג"ב הסובייטי), אולם הדעה הרווחת היא ש"תולעת מוריס" הייתה המתקפה הראשונה בקנה מידה גדול, וזאת מבחינת השתלשלות האירועים המהירה, היקפם והשלכותיהם. "תולעת מוריס" שוגרה במקור כמעשה קונדס ממעבדה באוניברסיטת קורנל, במטרה לפגוע בכמה שיותר מחשבים מבלי להתגלות. התולעת הביאה לקריסה של 6,000 מחשבים, שבשנת ההתקפה, 1988,[2] היוו כמעט עשרה אחוזים מרשת האינטרנט. המשרד לפיקוח על התקציב (US Accountability Office) העריך את הנזק שנגרם כתוצאה מ"תולעת מוריס" בין מאה אלף דולר לעשרה מיליון דולר – פער מספרי הממחיש את הקושי הקיים עד היום להעריך את הנזקים ממתקפות סייבר.[3]

ההשלכות החמורות של "תולעת מוריס" סיפקו אזהרה חשובה לקהילת המודיעין האמריקאית מעצם הפניית הזרקור לנזק הפוטנציאלי לרשתות מחשבים עתירות חיבורים, והדגישו את הצורך ליצור יכולות ארגוניות ומנגנונים בני הגנה במרחב הסייבר. למעשה, "תולעת מוריס" פעלה כזרז לגיבוש השלבים הראשונים בדרך לפיקוח טוב יותר על מרחב הסייבר והובילה לשינויים דרמטיים מבחינה תפיסתית ויישומית גם יחד:

- **שינוי בפרדיגמה**: במועד בו התרחש אירוע "תולעת מוריס" עשה האינטרנט את צעדיו המשמעותיים הראשונים ונחשב כ"מקום ידידותי". "תולעת מוריס" סייעה לחשוף את נוכחותם של אנשים בעלי כוונות זדוניות במרחב הסייבר. האירוע היה הפעם הראשונה שבה העיסוק בסייבר עבר מהתמקדות בנושא הקישוריות לחששות בתחום האבטחה.
- **מבצעיות**: בעקבות אירוע "תולעת מוריס" הקימה "הסוכנות לפרויקטי מחקר מתקדמים בתחום ההגנה" (DARPA) באוניברסיטת קרנגי מלון את "המרכז להתמודדות עם איומי סייבר" (CERT). מהלך זה המחיש את המעבר ממתן

פתרונות אד־הוק להקמת צוותים מקצועיים מאומנים ומצוידים כנדרש, לתיאום אירועים ולמתן הערכות ופתרונות למתקפות סייבר.[4]

- **רגולציה ותקנות**: במקביל לשינוי התפיסתי באבטחת הסייבר, חוקק הקונגרס האמריקאי בשנים שלאחר אירוע "תולעת מוריס" כמה חוקים, ביניהם חוק הפרטיות בתקשורת האלקטרונית ב־1986 וחוק ביטחון המחשבים ב־1987, שנועדו להבטיח, באמצעות הגנות משפטיות, את הפרטיות בתחומי הסייבר.[5] היוצר של "תולעת מוריס", רוברט טאפאן מוריס, היה האדם הראשון שהורשע על פי החוק נגד מעשי הונאה ושימוש לרעה במחשבים שנחקק בשנת 1986.[6]

שלב הנסיקה – אירוע "Moonlight Maze"

ב־1998 גילו גורמים אמריקאיים רשמיים בדרך מקרה דפוס של "גישוש" (probing) מתמשך במערכות המחשב של הפנטגון, באוניברסיטאות פרטיות, בנאס"א, במשרד האנרגיה ובמעבדות מחקר. עד מהרה הם הבינו כי פעולת הגישוש התרחשה באופן רציף במשך כמעט שנתיים. אלפי מסמכים שאמנם לא היו מסווגים, אך כללו מידע רגיש שקשור לטכנולוגיות בעלות יישומים צבאיים, נחשפו או נגנבו, לרבות מפות של מתקנים צבאיים, מערכי חילות ותוכניות חומרה.[7] למרות שמשרד ההגנה של ארצות הברית הצליח לזהות את עקבות הפולשים כמובילות למחשב מרכזי שנמצא בברית המועצות לשעבר, הגורמים שיזמו את המתקפה נותרו עלומים. רוסיה הכחישה כל מעורבות בה, והחשדות מעולם לא הוכחו חד־משמעית.[8]

המתקפה שקיבלה את הכינוי "Moonlight Maze" נחשבת בעיני רבים כמתקפת ריגול הסייבר הגדולה הראשונה מצד גורם מדינתי מאורגן וממומן. המתקפה תוכננה היטב, שכן התוקפים הותירו "דלתות אחוריות" כדי לאפשר להאקרים לחדור למערכת במועדים שונים, השאירו מעט מאוד עקבות ופעלו במשך זמן רב מבלי שהתגלו.[9] אירוע "Moonlight Maze" הבליט את התפקיד שממלאות רשויות מדינתיות בהפקה, במימון או לפחות בהשתתפות פסיבית באירועי ריגול מתוחכמים ורחבי היקף. יתרה מכך, האירוע ציין את הפגיעות של מרחב המידע, שבו יריבים יכולים לא רק לגרום לשיבוש השירות, אלא גם לשים את ידם על מידע רגיש. הוא הוכיח את הצורך החיוני ב"חומות אש" ובהצפנות, ומעל לכל – את הקושי בזיהוי מתקפה ובייחוסה לגורם עוין ספציפי.

אירוע "Moonlight Maze" היה שלב חשוב בהתפתחות לוחמת הסייבר ואבטחת הסייבר, וזאת בזכות ההשלכות האפשריות שלו על עימותים עתידיים.[10] הוא הצביע על השינוי הצפוי בשדה הקרב המודרני – ממלחמה קינטית, שבה לאויבים יש שמות, מיקומם הפיזי ידוע, המתקפות נראות בעין וניתן להעריך את נזקן, לעבר לוחמה אסימטרית המאופיינת במבצעי סייבר התקפיים, שהמתקפות בהם בלתי נראות, האויבים לא ידועים והנזק קשה לכימות. "Moonlight Maze"

הוביל לשינויים דרמטיים בגישתו של הממשל האמריקאי לאבטחת סייבר, כפי שיתואר בהמשך.

השינוי בפרדיגמה

המודעות של קובעי המדיניות בארצות הברית לאיומי טרור ותמיכתם ביוזמות למלחמה בטרור גם לאחר פיגועי 11 בספטמבר 2001 היו מוגבלות. אירוע "Moonlight Maze" הביא לחשיבה מחודשת על אסטרטגיית הגנת הסייבר האמריקאית, לוחמת סייבר, הרתעת סייבר וההגנה על רשתות רגישות ולא מוצפנות, כגון NIPERnet (רשת נתב פרוטוקול אינטרנט לא מאובטח – הרשת הלא מסווגת של הפנטגון). לראשונה התעוררו שאלות פוליטיות וחוקתיות בנוגע לביטחון, לפרטיות, לרעיונות בדבר ניטור אקטיבי ולסכנה של חשיפה לאיומים על־לאומיים.[11] אירוע "Moonlight Maze" הביא את ארצות הברית להבנה כי נדרשות מדיניות ואסטרטגיה ברורות ללוחמה האסימטרית, למרחב העתידי של איסוף מידע מודיעיני וריגול ולהשלכות הטכנולוגיות שנגזרות מכך.

פעולות חקיקה

הצו הנשיאותי מספר 63 להגנה על תשתיות קריטיות היה בחלקו תוצאה של אירוע "Moonlight Maze". היה זה מסמך מדיניות חלוצי שהגדיר את הכללים, תחומי האחריות והיעדים להגנה בתחום השירותים הציבוריים, תשתיות התחבורה והפיננסים וכל תשתית חיונית אחרת של ארצות הברית.[12] לצו הנשיאותי מספר 63 היו שתי השלכות אסטרטגיות מרכזיות: האחת, הקמת "מרכז ההגנה הלאומי נגד אירועים" (NIPC) – גוף חוצה סוכנויות, בעל סמכות לפקח על התשתיות הקריטיות הממשלתיות והאזרחיות של המדינה מפני מתקפות מחשב;[13] השנייה, הקמת "כוח המשימה המשותף להגנה על רשתות מחשב" (JTF-CND) – גוף שהופקד על הובלה ותיאום התגובות למתקפות סייבר ברמה הארצית, המרַכז תחתיו את ההגנה על רשתות מחשב צבאיות.[14]

פעולות מבצעיות

משרד ההגנה של ארצות הברית הוביל את בנייתם של מנגנוני תגובה לאירועי הסייבר והקים מוסדות לדיווח עליהם. דיווחים בנושאים צבאיים טופלו מאז ברמה המקומית, דרך מרכזי אבטחה ותפעול רשתות (NOSC) שפעלו בהכְוונה של "הסוכנות למערכות מידע של משרד ההגנה" (DISA). בנוסף לכך, מרכזי CERT אזוריים, שפעלו כמנגנוני פיקוד ושליטה, הפכו למובילים בתחום הערכת ההשלכות של מתקפות סייבר ברמות האישית והאזורית. גורמים נוספים שהוקמו לסיוע בתיעול מידע הם "כוח המשימה המשותף לתפעול רשתות מחשב" (JTF-CNO)

ו"המרכז הגלובלי לביטחון ותפעול רשתות" (GNOSC) של "הסוכנות למערכות מידע של משרד ההגנה".

שלב המיליטריזציה – "סטוקסנט"

מתקפת "סטוקסנט" נחשבת לאחת המתקפות המתוחכמות ביותר של תוכנות זדוניות עליהן נודע לציבור. מומחים רבים סבורים שרק מדינה יכולה הייתה ליצור ולשגר מתקפה כזאת, למרות שלא ניתן לאמת את הדבר. בערוצי תקשורת רבים אף הועלתה סברה שהיה זה שיתוף פעולה ישראלי־אמריקאי.[15]

התוכנה הזדונית, שנחשבת לאחת ממתקפות הסייבר ההרסניות ביותר שניהלו מדינות ריבוניות, הסבה נזק לצנטריפוגות של איראן ועיכבה את פעילות העשרת האורניום שלה. מרגע שהתוכנה הוחדרה לרשת, היא עשתה שימוש במגוון מנגנונים כדי להפיץ עצמה למחשבים נוספים בתוך אותה רשת ולהשתלט על הנעשה בה. המנגנונים שבהם השתמשה "סטוקסנט" כללו ניצול של פגיעויות מוכרות וכאלו שכבר טופלו ותוקנו, אך גם ארבע פגיעויות שלא היו ידועות ולא תוקנו עד למועד שחרור התולעת (וידועות בשם "מתקפות יום אפס" – zero-day exploits).[16] הקהילה הבין־לאומית ממשיכה לתהות מה היו המקור והמטרה המדויקים של וירוס ה"סטוקסנט", אך בכל מקרה האירוע העלה את המודעות לפגיעויות העיקריות הקיימות ברשתות המחשבים.[17]

"סטוקסנט" זוהה בשנת 2010. מקורו הלא ודאי והשפעתו המחישו את הקושי בזיהוי מתקפת סייבר והביאו למסקנה שלא ניתן להשיג הגנה מלאה ברמת המדינה על כל משאביה החיוניים.[18] כתוצאה מכך התעורר הכרח ללמוד את הדינמיקות של מצבים דמויי קרב בלוחמת הסייבר של העידן המודרני, שבהם אפילו מתקפת ענק לא בהכרח מיוחסת לתוקף ידוע ומוגדר, ואולי אף לא מותירה עקבות כלל. פירוש הדבר הוא שקובעי המדיניות עשויים לעמוד בפני השלכות של מתקפה בשדות הקרב הלא קינטיים של העידן הנוכחי (החל ממניעת שירות ועד הרס תשתיות קריטיות של מדינה) מבלי שיהיה להם "אקדח מעשֵן" או כלי פוליטי או חוקי להילחם בעזרתו. תופעה זו מחייבת את המחוקק והרשויות להתחיל לגבש אופציות תגובה כבר עתה, במקום לנסות לפתח אפשרויות התמודדות אד־הוק במהלך המשבר עצמו.

לוחמת הסייבר שלאחר שנת 2013 העתיקה את גישת מתקפת־הנגד מהרמה המבצעית[19] לרמה האסטרטגית־דיפלומטית, שבה המדיניות, החוק הבין־לאומי, המשילות באינטרנט והסכמים משחקים תפקיד משמעותי ביותר בסביבת הסייבר הפרוצה. שלושה הסכמים מרכזיים ומאמצי שיתוף פעולה בנושא המשילות באינטרנט ברמה הרב־לאומית גובשו מאז אותה שנה:

- **הסכם הסייבר בין ארצות הברית לסין**: הסכם זה קבע כי אף ממשלה "לא תבצע ולא תתמוך ביודעין בגניבה של קניין רוחני דרך הסייבר, לרבות סודות מסחריים או מידע עסקי סודי אחר, למען יתרון מסחרי".[20] אמנם, זהו הסכם בסיסי בלבד שאינו מבטיח סביבת סייבר בטוחה בין שתי המדינות, אולם חשיבותו נובעת מהיכולת להתבסס עליו בשנים הבאות ולהשתמש בו כמחווה של רצון טוב.
- **מפגש הפסגה העולמי של האו"ם בנושא חברת המידע (WSIS+10)**: פסגה זו חידשה את "פורום המשילות באינטרנט" (IGF) – מסגרת שבה המדינות החברות, החברה האזרחית והמגזר העסקי דנו בנושאי מדיניות האינטרנט, אבטחת סייבר, מעקב ופיקוח, קניין רוחני וזכויות יוצרים. המדינות החברות חיזקו במעמד זה ערוצים דיפלומטיים קיימים בתחום מדיניות הסייבר, ואשררו את מחויבותן לגשר על פערים דיגיטליים ולשפר את הגישה לטכנולוגיות מידע ותקשורת, וזאת באמצעות אישור המסמך שגובש בפסגת WSIS+10.[21]
- **הסכם "המעגן הבטוח" (Safe Harbor)**: הסכם זה נחתם בין משרד המסחר האמריקאי ובין האיחוד האירופי, והסדיר לראשונה את האופן שבו חברות אמריקאיות רשאיות לייצא ולטפל בנתונים אישיים של אזרחים אירופיים.[22]

מבנה מרחב הסייבר האמריקאי

מרחב הסייבר האמריקאי רווי במוסדות, בענפי צבא, במכוני מחקר ובגורמי אקדמיה, ממשל והמגזר העסקי. הדבר נובע ממורכבות התיאום, מתחומי האחריות המפוצלים ומגורמי פיקוח חופפים.

ברמה הלאומית ניצבת קהילת המודיעין האמריקאית, עם יכולות הגנה והתקפה במרחב הסייבר. קהילת המודיעין גם נושאת באחריות העליונה לטיפול בכל הסוגיות הקשורות בלוחמת הסייבר המודרנית, למתן מענה להן ולמעקב אחריהן. היא גם זו שמחזיקה למעשה באחריות המבצעית על כל היבטיו של מרחב הסייבר בארצות הברית, בין אם מדובר במתקפה נגד רשויות צבאיות או ממשלתיות, ובין אם מדובר במתקפה גדולה נגד מוסד פרטי או תשתית קריטית.

קהילת המודיעין האמריקאית במתכונתה הנוכחית הוקמה ב־1981 ומהווה פדרציה של 17 סוכנויות ממשל אמריקאיות הפועלות בנושאי מודיעין, הן ביחד והן בנפרד.[23] הארגונים החברים בקהילה כוללים סוכנויות מודיעין, את המודיעין הצבאי, את המודיעין האזרחי וכן גופי מחקר בתוך משרדי ממשלה פדרליים. בראש כל 17 הגופים עומד מנהל המודיעין הלאומי, שמדווח ישירות לנשיא ארצות הברית.[24] מרבית הסוכנויות המודיעיניות הן משרדים או לשכות בתוך משרדי הממשלה. תשע מתוכן פועלות במסגרת משרד ההגנה ואחראיות למימוש 85 אחוזים מסך כל תקציב המודיעין האמריקאי.

איסוף מסורתי של מידע מודיעיני למלחמה בטרור מבוסס על סדרה של דרכים ושיטות, הכוללת מודיעין אנושי (HUMINT), מודיעין אותות (SIGINT), מודיעין חזותי (IMINT) ומודיעין מדידות וחתימות (MASINT). כל הדיסציפלינות האלו דרושות כדי לבנות הערכת מודיעין כוללת, ויחד עם זאת, ככל שההון האנושי והמשאבים דורשים השקעות גדולות יותר מצד אחד, וההסתמכות האנושית על הטכנולוגיה הולכת וגוברת מצד שני, כך מתחזקת ההכרה ביכולותיו של מרחב הסייבר.

קהילת המודיעין האמריקאית מתמקדת כיום בשלושה היבטים בתחום אבטחת הסייבר: **ארגון**, **גילוי** ו**הרתעה**. גופים שונים בתוך הקהילה עוסקים במשימות שונות בתחום זה:[25] משרד מנהל המודיעין הלאומי עומד בראש כוח משימה המתאם את המאמצים לזיהוי מקורותיהן של מתקפות סייבר עתידיות; המשרד לביטחון המולדת (DHS) מוביל את מאמצי ההגנה על מערכות המחשוב הממשלתיות; משרד ההגנה מתכנן את האסטרטגיות למתקפות־נגד בסייבר; "הסוכנות לביטחון לאומי" (NSA) מנטרת, מזהה, מדווחת ומגיבה לאיומי סייבר; הבולשת הפדרלית (FBI) מובילה את המאמצים הלאומיים לחקירה ולהעמדה לדין של מבַצעי פשעי סייבר. בתקופת משבר, 17 הסוכנויות המרכיבות את קהילת המודיעין האמריקאית אחראיות הן לדווח והן להעריך את המודיעין שלהן, שלאחר מכן מתורגם להמלצות על ידי מנהל המודיעין הלאומי. יש ארגוני סייבר רבים נוספים הפועלים מחוץ למטרייה של קהילת המודיעין האמריקאית, הנותנים מענה לאיומי סייבר. הבולטת שבהם היא "מפקדת הסייבר האמריקאית" (USCYBERCOM).

ג'יימס קלאפר, מנהל המודיעין הלאומי של ארצות הברית, האחראי על קהילת המודיעין האמריקאית ועל התיאום המורכב בין כל זרועותיה, פרסם בתחילת 2015 הערכת סיכונים, לפיה איומי הסייבר עומדים בראש רשימת האיומים הגלובליים.[26] היה זה השינוי הראשון בהגדרת האיום הגלובלי הראשי, שמאז מתקפת 11 בספטמבר 2001 היה איום הטרור הפיזי. עם זאת, קלאפר התייחס לאפשרות של אירוע בממדים של "יום הדין של הסייבר" (מצב שקיבל גם את הכינוי "פרל הרבור של הסייבר" או "11 בספטמבר של הסייבר")[27] בסבירות נמוכה ורחוקה, למרות שמתקפות סייבר נגד ארצות הברית מתרחשות כל הזמן ומספרן נמצא בעלייה.[28]

במקום תרחיש של "יום הדין של הסייבר" שיפגע בכלל התשתיות האמריקאיות, קהילת המודיעין של ארצות הברית צופה שהאתגר בתחום הסייבר יהיה שונה. התחזית שהיא פרסמה כוללת סדרה ארוכה של מתקפות סייבר בעצימות נמוכה עד בינונית, ממגוון מקורות ולאורך זמן. סדרת מתקפות זו תגרום לעלויות מצטברות, שישפיעו על יכולת התחרות הכלכלית של ארצות הברית ועל ביטחונה הלאומי.[29]

התפוצה של תוכנות זדוניות ברחבי העולם מגבירה את הסיכון לרשתות המחשב האמריקאיות, לתשתיות רגישות ולנתונים. פעולת סייבר שנועדה לשבש

או להרוס לחלוטין, ומופנית נגד תאגיד פרטי, מערכת בקרה תעשייתית או מערכת הגנה, אמנם מחייבת שהאויב הפוטנציאלי יהיה בעל מומחיות ניכרת כדי להוציאה לפועל, אך היא לא דורשת מימון של מדינה או כישרון מבצעי ברמה בין־לאומית. שחקן מסוים, בין אם ברמת המדינה ובין אם ברמה של ארגון שאינו מדינתי, יכול לרכוש בשוק השחור תוכנה זדונית, תוכנת ריגול, תוכנת "יום האפס" (zero-day) או כל תוכנה אחרת, ולשלם למומחים כדי שיחפשו נקודות פגיעות ויפתחו יכולות לתקוף אותן.[30]

למרות העלייה בפעילות הסייבר מצד ארגונים כמו דאע"ש, בכירים במודיעין האמריקאי עדיין מאמינים כי גורמים מדינתיים הם האיום הגדול ביותר לאינטרסים האמריקאיים במרחב הסייבר. קהילת המודיעין של ארצות הברית מעריכה כי קיים סיכוי למשבר סייבר שייגרם על ידי שורה של גורמים, לרבות מדינות עם תוכניות סייבר מתוחכמות ביותר, כגון רוסיה או סין; מדינות עם יכולות טכניות נמוכות יותר אך בעלות כוונות הרסניות, כמו איראן או קוריאה הצפונית; גורמים לא מדינתיים עם יכולת גישה למשאבים ניכרים ומוטיבציה ליצור כאוס בסייבר; או עבריינים המונעים משאיפות לרווחים ופורצים או גורמים קיצוניים המונעים מאידאולוגיה.

לפי הערכתה של קהילת המודיעין האמריקאית, היעדים האפשריים למתקפות סייבר הם:

- **המגזר הפרטי**: לצד היותו קורבן למתקפות סייבר, המגזר הפרטי הוא גם שותף פעיל בחקירתן ובהתייחסות אליהן. לאור חשיבותם של המוסדות הפיננסיים (דוגמת "גולדמן סאקס") לכלכלה האמריקאית, קהילת המודיעין של ארצות הברית מגדירה מגזר זה כתחום חשוב להגנה במקרה של מתקפת סייבר חמורה.[31]
- **תשתיות קריטיות**: התשתיות הקריטיות – קרי הנכסים, המערכות והרשתות הפיזיים והווירטואליים החיוניים לביטחון, לבריאות ולבטיחות הכלכלה והחברה – פגיעות למתקפות סייבר מצד ממשלות זרות, גורמי פשע וגורמים הפועלים באופן עצמאי. מתקפה בקנה מידה גדול עלולה לשתק זמנית את אספקת המים, החשמל או הגז, לפגוע בתחבורה או בתקשורת ולהסב נזק למוסדות פיננסיים.[32]
- **הממשל**: חדירה למערכת קבלת ההחלטות הלאומית של ארצות הברית ולקהילת המודיעין האמריקאית תהיה תמיד יעד מרכזי עבור ישויות ריגול זרות. איום קבוע נוסף על אינטרסים אמריקאיים הוא הניסיון להשיג מידע בנושאי הביטחון הלאומי של ארצות הברית ומידע קנייני ממכוני מחקר אמריקאיים העוסקים בנושאי ביטחון, אנרגיה, כספים, טכנולוגיה בעלת שימוש כפול ותחומים נוספים.[33]
- **צבא וסוכנויות ממשל**: קו המגע הקדמי, שבאמצעותו יש להגן על משאבי ההגנה וההתקפה של הצבא האמריקאי, יותקף וייפגע במקרה של משבר סייבר.

מדיניות קהילת המודיעין האמריקאית

קהילת המודיעין של ארצות הברית מבצעת שורה של פעולות מודיעיניות מדי יום. במקביל, ארצות הברית נמצאת תחת מתקפת סייבר תמידית מצד גורמים מדינתיים ולא מדינתיים כאחד. ברמת המודיעין הלאומי, מתקפת סייבר מחייבת לא רק גיבוש מאמצי הגנה, אלא גם תכנון חלופות מבצעיות שונות לצורך פעולת גמול.

גודלה של קהילת המודיעין האמריקאית מביא אותה לקיים קשרים הדדיים ולשתף פעולה עם סוכנויות ממשל, הן ברמה המבצעית (צבא, משרד ההגנה, המשרד לביטחון המולדת) והן ברמה המדינתית (המגזר הפרטי, מחלקת המדינה, הבית הלבן).יעדי ההתכוננות וההיערכות האסטרטגית של קהילת המודיעין האמריקאית הם:[34]

- הקמה וניהול של כוחות ויכולות המוכנים להוציא לפועל מבצעי סייבר.
- הגנה על רשת המידע הפנימית שלה, אבטחת נתונים וצמצום סיכונים הניצבים בפני ביצוע משימותיה.
- היערכות להגן על אינטרסים אמריקאיים חיוניים מבית ומחוץ נגד מתקפות סייבר משבשות או הרסניות, שיש להן השלכות משמעותיות.
- הקמה וניהול של יכולות סייבר ותכנון השימוש ביכולות אלו כדי למנוע הסלמה של עימותים מצד אחד וכדי לשאוב ולאגור מידע לצורך הכנת "בנק מטרות" מצד שני.
- הקמה וניהול של שותפויות ובריתות בין־לאומיות איתנות במטרה להרתיע איומים משותפים ולחזק את היציבות והביטחון בזירה הבין־לאומית.

מדיניות קהילת המודיעין האמריקאית במענה למתקפות סייבר היא:

- **זיהוי המתקפה**: תוקפים מתוחכמים מנסים להסוות את מתקפת הסייבר שלהם. על גורמי המודיעין מוטל להכין את שדה הקרב ולהעריך במדויק את סיכויי ההצלחה והתועלת בכל סוג של מבצע נגד מתקפת סייבר, בדיוק כפי שהם עושים זאת בעימות קונבנציונלי.[35]
- **מידע**: תפקידה המרכזי של קהילת המודיעין הוא לספק מידע ולדווח, וזאת בנוסף ליכולות ההתקפיות המשמעותיות המצויות בידיה. היא חייבת להעביר מידע לזרועות המבצעיות עמן היא משתפת פעולה, וכן למחלקת המדינה. פירוש הדבר הוא שהצלחתה של קהילת המודיעין האמריקאית במהלך מתקפת סייבר תימדד בסימנים המעידים שהיא תיתן בשלב ההיערכות למתקפה, וביכולתה להיערך מולה באמצעות מתן התרעה ברגע התרחשותה.
- **הצגת חלופות**: המטרה המרכזית של קהילת המודיעין האמריקאית בזמן מתקפה היא לספק שורה של חלופות למקבלי ההחלטות ולאפשר להם גמישות אסטרטגית באמצעות הספקת מידע ערכי. במהלך מתקפה, על קהילת המודיעין

להצביע על דרכי פעולה אפשריות. המלצותיה והערכותיה נועדו לאפשר מרחב פעולה ותמרון מדיניים ואסטרטגיים־מבצעיים למקבלי ההחלטות.

- **הערכת נזקים**: שלא כמו בשדה הקרב המסורתי, מתקפת סייבר קשה לעתים לזיהוי, אפילו אם היא בקנה מידה גדול. על קהילת המודיעין מוטל לאמוד את הנזק שנגרם על ידי מתקפת הסייבר, כדי לאפשר לקובעי המדיניות לנקוט פעולת גמול מידתית. הדבר אינו מחייב אותה לבצע בהכרח מהלכים מבצעיים; אדרבא, עליה לקיים הערכות מודיעיניות ולפעול בתיאום עם משרדי ממשל אחרים, תוך החלפת מידע אתם, כך שתתאפשר זרימה הדדית שוטפת ויעילה של מידע רלוונטי.

תגובה רב־ממדית למתקפת סייבר

תפקידה של קהילת המודיעין האמריקאית חופף לא פעם לתפקידיהם של מוסדות, משרדי ממשל ויחידות צבאיות, שרבים מהם נמצאים מעבר לתחומי הסמכות והאחריות שלה. קהילת המודיעין אינה האחראית הבלעדית למתן מענה למתקפה בתחום הסייבר ברמה הארצית, המדינתית או ברמת התשתיות, ולפיכך היא תלויה במערכת היררכית ובשרשרת מורכבת של זרימת מידע. להלן מוסדות וגופים נוספים בארצות הברית המספקים מענה למתקפות סייבר:

- **המשרד לביטחון המולדת**: מופקד, במסגרת תפקידיו להגן על הטריטוריה של ארצות הברית ולהגיב למתקפות טרור, לתאונות מעשה ידי אדם ולאסונות טבע, והינו בעל אחריות על מודיעין "משמר החופים" (CGI) ועל "המשרד למודיעין ולמחקר" (I&A). "המשרד למודיעין ומחקר" אחראי לאיסוף, לניתוח ולעיבוד מודיעין, וכן להפצת המודיעין למשרד לביטחון המולדת ולשאר החברים בקהילת המודיעין האמריקאית. הוא גם הראשון להגיב על אירועים ברמה הארצית, המקומית והארגונית.[36] גופי הסייבר המרכזיים הפועלים בתוך המשרד לביטחון המולדת הינם המרכז הלאומי לאבטחת סייבר (NCSC) וחטיבת אבטחת הסייבר הלאומית ((NCSD. משרדו של מנהל המודיעין הלאומי אחראי לזרימה יעילה של מידע בין המשרד לביטחון המולדת ובין שאר גופי קהילת המודיעין, על מנת להבטיח סינרגיה של המידע במהלך מתקפת סייבר.
- **משרד ההגנה**: נחשב למוקד המבצעי של קהילת המודיעין האמריקאית ומופקד על תשע מסוכנויות הקהילה, כולל "הסוכנות לביטחון לאומי" (NSA). משרד ההגנה הוא גם המקור העיקרי למודיעין סייבר עבור משרד מנהל המודיעין הלאומי. חיוני שהמידע המבצעי יעובד באמצעות משרד מנהל המודיעין הלאומי ויועבר כהמלצות למדיניות ברמה הפדרלית. למעשה, מנהל המודיעין הלאומי מדווח למקבלי ההחלטות ולבית הלבן על סמך המודיעין שמשרדו מקבל ממשרד ההגנה (סביר מאוד להניח שמנהל המודיעין הלאומי והאדמירל מייקל רוג'רס,

שעמד הן בראש NSA והן בראש CYBERCOM, פועלים בצמידות במהלך מתקפת סייבר).

- **מחלקת המדינה**: הממשל תלוי בקהילת המודיעין במהלך משבר סייבר. שלא כמו בעימותים קונבנציונליים, בתרחיש של מתקפת סייבר סביר להניח שמקבלי ההחלטות אינם יודעים מה אירע, מי תקף, והיכן. אחריותה של קהילת המודיעין היא לספק הערכת מודיעין בזמן אמת, לעבד ולהעביר את המידע הלאה למקבלי ההחלטות. מחלקת המחקר והמודיעין (INR), העובדת עם הדיפלומטיה האמריקאית בנושאי מדיניות סייבר ומתווכת בין מחלקת המדינה לגורמי מודיעין לאומי היא הגורם המרכזי האמון על התיאום וההערכות עם קהילת המודיעין, ועל ניהול התקשורת בין המוסדות ברמה הדיפלומטית ובין הגורמים העוסקים בתחום מודיעין הסייבר.
- **המגזר הפרטי**: כאמור, מתקפות ופריצות סייבר לתשתיות הוגדרו על ידי מנהל המודיעין הלאומי כאיום מספר אחת על ארצות הברית. "המרכז לניתוח ושיתוף מידע" (ISAC) הוא הגורם המרכזי המפקח על איומי סייבר במגזר הפרטי, ומסייע לממשלים ברמה המדינתית ולממשל הפדרלי במידע הנוגע לאיומי סייבר. משברי סייבר במגזר הפרטי עשויים להשפיע על אינטרסים לאומיים (כמו במקרה של חברת "סוני"). לכן, המגזר הפרטי דורש לאמץ גישה מודיעינית מבצעית גם לגביו, וזאת בשיתוף פעולה עם המשרד לביטחון המולדת, מחלקת המדינה והבולשת הפדרלית.

מסקנות

ההיסטוריה של לוחמת הסייבר מלאה במסקנות ולקחים רבים, ויש בה כדי ללמד הן על ההתקדמות של מרחב הסייבר וכיוונו והן על תשומת הלב המקיפה שתחום זה מחייב בכל הרמות. ההתפתחות הטבעית של לוחמת הסייבר היא כלי חשוב בהתמודדות עם טעויות ואמצעי לחיזוי עתידו של מרחב המידע, הצורך בחוקים ותקנות בתחום הפרטיות, ריגול סייבר וכל הקשור באבטחת סייבר. קובעי המדיניות מתייחסים כיום למרחב הסייבר ברצינות רבה מאי פעם, ומוסדות בכל הרמות מפנים משאבים ניכרים כדי להתמודד עם איומי הסייבר הניצבים בפניהם. סוכנויות המודיעין משכללות ללא הרף את יכולות ההגנה וההתקפה שלהן בתחום הסייבר, בעוד שמוסדות פרטיים, במיוחד בתחומי הרפואה, הפיננסים, התשתיות הקריטיות והאנרגיה, וכן תאגידים מבוססי ידע, מקצים היום יותר מתמיד משאבים וכוח אדם להגנה על נתוניהם ולאבטחת הסייבר. הממשל האמריקאי מודע לסיכונים בפניהם עומדות רשתות המחשבים שלו, מה עוד והפרצות בהן נפוצות כיום יותר מתמיד. על רקע זה, ההשקעות ביצירת הגנה טובה יותר על מרחב הסייבר נמצאות כיום בשיא של כל הזמנים.

מספר הבנות מדיניות מהותיות הנוגעות לתחום הסייבר גובשו ברמה הבין־לאומית. עם זאת, מרבית קובעי המדיניות והמחוקקים אינם בעלי יכולת לטפל במתקפות סייבר בהיקף נרחב. לדוגמה, אין הגדרה כוללת אחת של "פעולה מלחמתית" במרחב הלא קינטי, וההגדרות הקיימות אינן ברורות, אינן משותפות לכול ואינן מוסכמות ברמה הבין־לאומית. זאת ועוד, אין בנמצא מנגנונים להתמודדות עם משברי סייבר בתחום הפיננסי. כתוצאה מכך, אין למדינות היכולת לקשור בין מתקפות סייבר גדולות ובין תוקפים מסוימים, דבר המאפשר לגורמים אחרים להסיר מעצמם אחריות.

יש צורך בשיתוף פעולה בין־לאומי בכל הרמות, במיוחד במישור הפיננסי, הדיפלומטי והמשפטי, שכן היעדר שיתוף פעולה כזה מונע יצירת בסיס יציב שעליו ניתן לבנות מנגנונים שיטילו את האחריות על האשמים האמיתיים. בשלוש השנים האחרונות הפכו מתקפות הסייבר למתוחכמות מאי פעם, וזאת למרות הגידול בהשקעות באבטחת סייבר בכל המגזרים. לכן, רק הסכמים מחייבים, כוללים ורב־לאומיים בתחום הסייבר, במקביל לחקיקה מתקדמת בתחום המשילות באינטרנט, יאפשרו להגיע למרחב סייבר בטוח יותר.

בהיבט הביטחוני, קהילת המודיעין האמריקאית יודעת להציג לקובעי המדיניות נרטיבים והמלצות מבצעיות, וזאת בזכות יכולות התיאום וטווח הסמכויות הרחב שלה. האתגר הגדול ביותר במהלך מתקפת סייבר הוא לזהות ולחבר את הנקודות השונות לכדי תגובה אחראית ומידתית. ללא גוף כמו קהילת המודיעין, הכמות האדירה של נתונים עתידה לרדת לטמיון במבוך המידע האינסופי. אויב עקשן עשוי לגרום לקריסתו של קו ההגנה במלחמה קיברנטית, בדומה למצב במלחמה קינטית. לעומת זאת, ובשונה משדה הקרב המסורתי, כאשר מתרחשת מתקפת סייבר, אי אפשר לראות אותה בעין, לא ניתן לייחס אותה לתוקף מסוים וקשה לזהות את השלכותיה.

ככל שחולף הזמן, טרור הסייבר עלול להפוך למקור גובר לחששות. מצב זה עשוי לחייב שיתופי פעולה מודיעיניים בין־לאומיים רחבים מתמיד. ייתכן שסוכנויות ביטחון ומודיעין לאומי במדינות שונות ייאלצו לשנות שיטות עבודה ולמקד מחדש את האסטרטגיות שלהן למלחמה באיום הסייבר. לאור כל זאת, אפשר כבר כיום לנבא שלא הנשק הגרעיני יהיה האיום העיקרי והגדול ביותר על האנושות בעתיד.

הערות

1 Jason Healey, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013).

2 Ted Eisenberg et al., "The Cornell Commission: On Morris and the Worm", *Communications of the ACM* 32, no. 6 (1989): 706-709, http://portal.acm.org/citation.cfm?id=63526.63530.

3 בית הדין לערעורים של ארצות הברית העריך במהלך הערעור בנושא "תולעת מוריס" את העלות של הסרת הווירוס מכל התקן שנפגע בין 200 ל־53,000 דולר. נראה שעל נתונים אלה התבסס דובר אוניברסיטת הרווארד, קליפורד סטול, כאשר הערך את ההשפעה הכלכלית הכוללת של התולעת בין 100,000 ל־10,000,000 דולר.

4 Eisenberg et al., "The Cornell Commission: On Morris and the Worm".

5 Michael Rustad and Diane D'Angelo, "The Path of Internet Law: An Annotated Guide to Legal Landmarks", in *Duke Law & Technology Review 2011*, ed. Beatrice Hahn (Durham: Duke University School of Law, 2011).

6 United States v. Morris, (2d Cir. 1991), upholding the conviction of a computer science graduate student under the Computer Fraud and Abuse Act.

7 *Hearing before Committee on Governmental Affairs, US Senate* (March 2, 2000) (Testimony of James Adams, Chief Executive Officer, Infrastructure Defense Inc.).

8 Adam Elkus, "Moonlight Maze" in Healy, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.*

9 Ryan Richard Gelinas, *Cyberdeterrence and the Problem of Attribution*, Master Thesis, Georgetown University, 2010, http://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/historical/gelinasRyan.pdf.

10 Marcia McGowan, "15 Years after Presidential Decision Directive (PPD) 63", *Booz Allen*, May 22, 2013, http://www.boozallen.com/content/boozallen/en_US/media-center/company-news/2013/05/15-years-after-pdd63-blog-post.html.

11 "Moonlight Maze", *PBS, Frontline*, April 24, 2003, www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/.

12 Office of the Press Secretary, "Fact Sheet: Protecting America's Critical Infrastructures, PDD 63", May 22, 1998, http://fas.org/irp/offdocs/pdd-63.htm.

13 שם.

14 שם.

15 Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishing, 2014).

16 Ralph Langner, "Stuxnet's Secret Twin: The Real Program to Sabotage Iran's Nuclear Facilities was Far more Sophisticated than anyone Realized", *Foreign Policy*, November 21, 2013, http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/.

17 שם.

18 Irving Lachow, "The Stuxnet Enigma: Implications for the Future of Cybersecurity", *Georgetown Journal of International Affairs Special Issue: Cybersecurity* (2011): 118-126.

19 לדוגמה, יצירת מוסדות נוספים המנטרים, מתאמים, מפקחים, מעריכים, מגנים ותוקפים.

20 Adam Segal, "The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement", *Council on Foreign Relations, Net Politics (blog)*, January 4, 2016, http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/.

21 Guest Blogger, "The Top Five Cyber Policy Developments of 2015: The WSIS+10 Review", *Council on Foreign Relations, Net Politics (blog)*, December

22, 2015, http://blogs.cfr.org/cyber/2015/12/22/the-top-five-cyber-policy-issues-of-2015-the-wsis10-review/.

22 Federal Trade Commission, "US-EU Safe Harbor Framework", July 25, 2016, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework.

23 Executive Order No. 12333, United States Intelligence Activities (December 4, 1981), *Central Intelligence Agency,* https://www.cia.gov/about-cia/eo12333.html.

24 "The Organizational Arrangements for the Intelligence Community", *Federation of American Scientists*, February 23, 1996, http://fas.org/irp/offdocs/int009.html.

25 Eric Rosenbach and Aki J. Peritz, "Cyber Security and the Intelligence Community", in *Confrontation or Collaboration? Congress and the Intelligence Community*, ed. Eric Rosenbach (Harvard Kennedy School: Belfer Center for Science and International Affairs, 2009).

26 *Worldwide Threat Assessment of the US Intelligence Community,* Statement for the Record by James R. Clapper, Director of National Intelligence, before the US Senate Armed Security Committee, February 26, 2015, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

27 Kristen Eichensehr, "Cybersecurity in the Intelligence Community's 2015 Worldwide Threat Assessment", *JustSecurity*, March 6, 2015, https://www.justsecurity.org/20773/cybersecurity-u-s-intelligence-communitys-2015-worldwide-threat-assessment/.

28 "Norse Intelligence Platform", *Norse,* http://map.norsecorp.com.

29 Eichensehr, "Cybersecurity in the Intelligence Community's 2015 Worldwide Threat Assessment".

30 Department of Defense, "The DoD Cyber Strategy", April 17, 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_Cyber_ Strategy_for_web.pdf.

31 שם.

32 Andrew Meola, "Cyber Attacks against our Critical Infrastructure are likely to Increase", *Business Insider*, May 26, 2016, http://www.businessinsider.com/cyber-attacks-against-our-critical-infrastructure-are-likely-to-increase-2016-5.

33 שם.

34 שם.

35 Aaron Brantly, "Defining the Role of Intelligence in Cyber", in *Understanding the Intelligence Cycle,* ed. Mark Phythian (London and New York: Routledge, 2013).

36 שם.