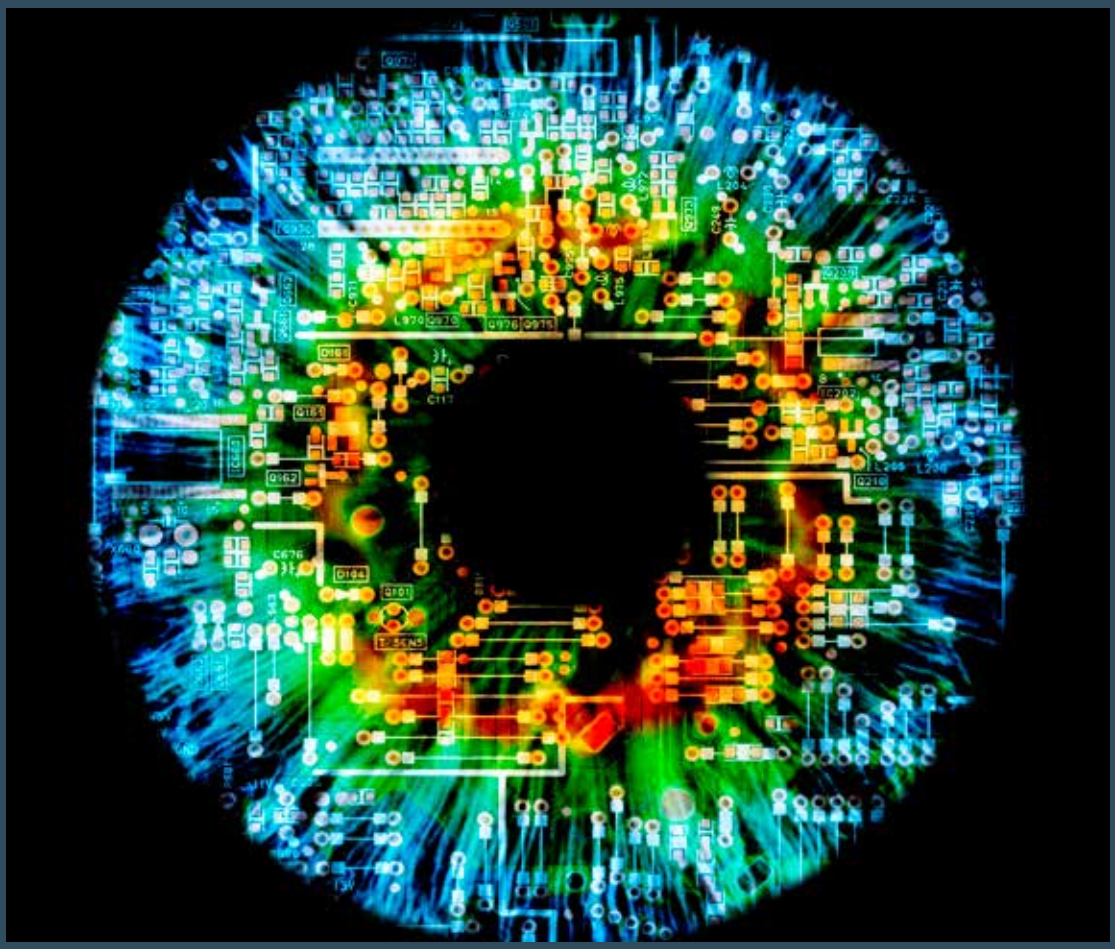


גבי סיבוני ועופר אסף

קווים מנחים לאסטרטגיה לאומית במרחב הסייבר

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

מזכר
149

גבי סיבוני ועופר אסף

קווים מנחים לאסטרטגיה לאומית במרחב הסייבר

המכון למחקרי ביטחון לאומי (חל"צ)

המכון למחקרי ביטחון לאומי, המשלב בתוכו את מרכז יפה למחקרים אסטרטגיים, הוקם בשנת 2006. למכון שתי מטרות מוצהרות: הראשונה, היא לערוך מחקרים בסיסיים בנושאי הביטחון הלאומי של ישראל, המזרח התיכון והמערכת הבינלאומית, וזאת על פי אמות המידה האקדמיות הגבוהות ביותר. המטרה השנייה, היא לתרום לדיון הציבורי ולעבודת הממשל בנושאים שנמצאים, או ראוי שיימצאו, בראש סדר היום הביטחוני של ישראל.

קהל המטרה של המכון הוא דרג מקבלי ההחלטות, מערכת הביטחון, מעצבי דעת הקהל בישראל, הקהילה האקדמית העוסקת בתחומי הביטחון בישראל ובעולם, והציבור המתעניין באשר הוא.

המכון מפרסם מחקרים שהוא מצא כראויים לתשומת הלב הציבורית, תוך שמירה על מדיניות נוקשה של אי משוא פנים. הדעות המובעות בפרסומים הן של המחברים בלבד ואינן משקפות בהכרח את עמדות המכון, נאמניו או האישים והגופים התומכים בו.

גבי סיבוני ועופר אסף

קווים מנחים לאסטרטגיה לאומית במרחב הסייבר

מזכר 149 אוקטובר 2015

המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל-אביב

Gabi Siboni and Ofer Assaf

Guidelines for a National Cyber Strategy

המכון למחקרי ביטחון לאומי (חברה לתועלת הציבור - חל"צ)

חיים לבנון 40
ת.ד 39950
רמת־אביב
תל־אביב 6997556

טל. 03-6400400
פקס. 03-7447590
דוא"ל: info@inss.org.il

אתר המכון: http://www.inss.org.il

ISBN: 978-965-7425-81-7

כל הזכויות שמורות © ספטמבר 2015

הביא לדפוס: משה גרונדמן

עיצוב גרפי: מיכל סמו־קובץ ויעל ביבר, המשרד לעיצוב גרפי, אוניברסיטת תל־אביב
עיצוב העטיפה: מיכל סמו־קובץ, המשרד לעיצוב גרפי, אוניברסיטת תל־אביב
תמונת השער: Science Photo Library / Getty Images

דפוס: אליניר, פתח תקווה

תודות

ראשית נבקש להודות לאלוף (מיל.) עמוס ידלין, ראש המכון למחקרי ביטחון לאומי, על הערותיו המועילות והממוקדות. בנוסף נבקש להודות כל מי שהאירו והעירו לנו הערות בונות ומלמדות במהלך הכתיבה ותהליך הבקרה: תא"ל (מיל') אודי דקל, סגן ראש המכון, ד"ר שמואל אבן, דודי סימן־טוב, ד"ר גליה לינדנשטראוס ויורם הכהן.

תודה לדבורה האוסן כוריאל על הבהרת רוחב היריעה ומורכבות הניתוח של הסוגיה המשפטית בסייבר (שהובילה אותנו למסקנה שיש לייחד לסוגיה זו מחקר ומסמך עמדה נפרדים), לקורין ברגר, לסימון טסיפיס וליואל קוזאק מהמכון, שתרמו לאיסוף החומר.

תודות רבות גם לג'ודי רוזן ולמשה גרונדמן על הערותיהם ופעילותם להוצאה לאור של מזכר זה, ותודה מיוחדת לד"ר ענת קורץ, מנהלת המחקר במכון למחקרי ביטחון לאומי, על סבלנותה הרבה ועל עצותיה הטובות והמלמדות לכל אורך הדרך.

נבקש גם להודות למי שסייעו להבין את הנושא הטכנולוגי המורכב – מר אבי שביט ממשרד המדען הראשי, שהפנה אותנו לתעשיות רלוונטיות ומרתקות, ואנשי התעשייה שאירחו והדגימו: מר גונן פינק ואנשיו מחברת Light cyber, מר ניר גייסט ואנשיו מחברת Nyotron, מר רון דוידזון מחברת Check Point, מר איציק ואגר מחברת Verint, מר בני רוזנבאום ז"ל מחברת Bio Catch, מר אלעד הורן מחברת enSilo, מר שמעון בקר מחברת CyberObserver. תודה לפרופסור יצחק בן־ישראל על הערותיו המלומדות.

תוכן עניינים

תקציר 9

מבוא 13

האתגר האסטרטגי 17

סקירת ספרות 21

תכנון ואסטרטגיה 21

ישראל 21

בניין הכוח 22

ארצות־הברית 23

בריטניה 26

צרפת 27

סין 29

ארגונים בינלאומיים (OECD, ENISA, European Union) 29

הגנה והרתעה 31

התמודדות עם איומי חומרה 32

הרתעה 32

התקפה 33

התקפה במסגרת עימות גלוי 33

תקיפה קיברנטית כחלק מתוכנית אופרטיבית במלחמה 34

השוואה בין מסמכי אסטרטגיה של מדינות שונות 36

הגנה 39

המענה למתקפת עומק (APT) 40

המענה לתקיפות שטחיות ומהירות (DDoS, Defacing) 44

השימוש ב'ענן' על ידי ארגונים ביטחוניים וחיוניים 45

המענה למתקפות על חומרה וקושחה 46

מניעת התקפה באמצעות הרתעה 48

התאוששות מתקיפה 48

סוגיות משלימות בהגנה 51

מבנה ארגוני עם תרבות שיתוף ושקיפות 51

רגולציה במרחב הסייבר הלאומי 56

מקצועיות עובדים, אחראי ההגנה (CISO) ואחריות מנהלים בעסקים 57

סיכום פרק ההגנה 59

התקפה 61
התקפה קיברנטית במצב גלוי ובמצב עמום 62
התקפה כאמצעי להעברת מסר 63
התקפה כחלק ממערכה חשאית 65
סיכום פרק ההתקפה 66

תובנות והמלצות 67
עיקרי ההמלצות 68
בתחום ההגנה 68
בתחום ההתקפה 69
בתחום הארגון 69

סיכום 71

נספח 75
מילון מונחים 75

הערות 79

רשימת איורים

איור 1: חלוקת מרחב הסייבר הלאומי לפי מניעי הפעולה 14
איור 2: תיחום מסמכי המדיניות והאסטרטגיה ברמה הלאומית 16
איור 3: תפיסת ההתמודדות עם תקיפות APT 41
איור 4: ציר ההגנה מול שרשרת התקיפה 42
איור 5: המחשת תהליך ניהול סיכונים 49
איור 6: התאוששות מתקיפה כחלק מובנה בהגנה 50
איור 7: מצב האסדרה (רגולציה) הארגונית בישראל 53
איור 8: אחריות מוצעת לפעולה במרחב הסייבר 55

תקציר

תחום הפעילות במרחב הסייבר התפתח במדינת ישראל בשנים האחרונות באופן מהיר ועוצמתי. ממשלת ישראל התייחסה לאתגר כבר בשנת 2002 והחליטה להקים את הרשות לאבטחת מידע. מאז העמיקה התלות של הרציפות התפקודית של מדינת ישראל (כמו במדינות אחרות בעולם) בטכנולוגיה בכלל, ובפעולה במרחב הסייבר בפרט. תלות זו מעצימה, מטבע הדברים, את האיומים על הרציפות התפקודית של ישראל. מדינות ויריבים שונים פועלים באופן שיטתי לפתח יכולות ולפעול נגד מערכות וגורמים שונים במדינה.

ממשלת ישראל השכילה להקים לפני מספר שנים את המטה הקיברנטי הלאומי, במטרה להעצים ולהסדיר את הפעילות במרחב. הקמתה של הרשות הלאומית להגנה בסייבר מהווה צעד נוסף בכיוון זה. לצד זאת, חובה לפעול לגיבושה ולניסוחה של אסטרטגיה לאומית לפעולה במרחב הסייבר, שהיא אבן הראשה בתהליך ההתעצמות הלאומית בסייבר. מסמך האסטרטגיה שייכתב צריך להוות רכיב במסמכי היסוד, כשהמוביל שבהם צריך להיות מסמך המדיניות הלאומית לפעולה בסייבר, שיגדיר את יעדי־העל של המדינה בתחום הפעולה בסייבר ואת דרכי שילובם במאמץ הביטחון, הכלכלה ושאר המאמצים הלאומיים. לבסוף, כל ארגון מדינתי הפועל במרחב זה יידרש לגבש את האסטרטגיה הארגונית שלו לפעולה במרחב.

מרחב הפעולה בסייבר כולל שלושה מרכיבי פעולה: המרכיב הראשון הוא הגנה, שמהווה יסוד עיקרי בפעולה בסייבר. ניתן לחלק את מושאי ההגנה בישראל לפי הקטגוריות הבאות: גופים העוסקים בביטחון המדינה, גופים המספקים שירותים חיוניים, גופים האחראיים לסדרי ממשל ולחיים תקינים וגופים שתקיפתם תשפיע על המורל ועל תחושות סדר, ריבונות ומשילות. אלה מאוימים על ידי מגוון גורמים וביניהם מדינות עוינות, מדינות יריבות, גורמי טרור, האקטיביסטים ואף אנשים פרטיים. לצד אלה חשופה מדינת ישראל גם לפעילות פשיעה פלילית במרחב הסייבר, לדוגמה: ריגול עסקי וגניבת קניין רוחני, פשיעה פיננסית ופעילות פלילית אחרת העושה שימוש במרחב הקיברנטי (סחר בסמים, פדופיליה, מכירת כלי נשק וכדומה).

בנוסף למרכיב ההגנה, קיים מרכיב התקיפה ברמה המדינתית. מטבע הדברים, העיסוק ברכיבים אלה בעבודה זו מוגבל למדי. מטרת מסמך זה היא להציע קווים מנחים לגיבוש אסטרטגיית סייבר לאומית בתחום ההגנה וההתקפה. קווים מנחים אלה

אינם מקיפים את כלל ההיבטים, ואינם מתייחסים להיבטים המשפטיים ולהיבטים הנוגעים לפיתוח תעשיית הסייבר הישראלית.

היעד המרכזי של אסטרטגיית הגנה לאומית בסייבר הוא שימור הרציפות התפקודית של המדינה. יעד חשוב נוסף הוא לאפשר לגורמים הרלוונטיים במדינת ישראל להחליט ולממש פעולות במרחב הקיברנטי והקינטי נגד יריבים ואויבים, מתוך ביטחון ביכולת להתמודד עם תקיפה במרחב הסייבר. מוצע להבדיל באסטרטגיית ההגנה בין שלושה סוגי מתקפות: מתקפת עומק (APT) – מתקפה מתוכננת לעומק מערך המחשבים של ארגון. מתקפה מהירה ושטחית – מתקפה שתוצאותיה ניכרות מייד, ובדרך כלל יעדיה הם גרימת שינוי באתר או מניעת גישה אליו ולשירותים שהוא מציע במרחב הקיברנטי (Defacing ,DDoS) ולבסוף מתקפת תשתית, באמצעות תקיפה על רכיבי חומרה.

בהקשר לשלושת סוגי התקיפות ניתנות ההמלצות הבאות:

1. בעניין הגנה מפני מתקפות עומק – מוצע להתבסס על שילוב בין כלים ויכולות שאינם מחייבים מידע והיכרות מוקדמים של רכיבים ושיטות תקיפה, לבין מערך היכולות המשוכלל המבוסס על היכרות מוקדמת.
2. התבססות על שקיפות בדיווחים על תקיפות בין ארגונים.
3. בניית הערכת מצב קיברנטית לאומית שוטפת ורחבה באמצעות גופים דוגמת CERT לאומי.
4. בניית גופי תגובה מהירה תוך שימוש בנתוני מחקר ולימוד על כלי תקיפה ועל קבוצות תקיפה.
5. שיתוף עם ארגוני הגנה ומודיעין מסחריים, לצד שיתוף פעולה בינלאומי.
6. פיתוח איסוף מודיעיני מתמיד על אויבים ויריבים לצורך התרעה.
7. גיבוש תוכנית לתגובה קיברנטית כחלק מממד הרתעה אפשרי.
8. פיתוח יכולת התאוששות מתקיפה במקרים שהדבר אפשרי, מתוך ההבנה שקו ההגנה לעולם ייפרץ, ולכן יש להתארגן לשיקום מהיר כתוצאה ממתקפות מוצלחות של האויב.
9. באשר לתקיפות שטחיות – מוצע להתבסס על בניית יכולות שחזור מהירות והקצאה של רוחב פס המתגבר על החסימות, תוך שילוביות עם ספקי האינטרנט במגזר האזרחי.
10. שימוש ביכולות העברה מהירה של אתרים מותקפים לאתרי אירוח חליפיים.
11. בשל הקושי הטכנולוגי הרב לזהות תקיפות של חומרה, מוצע להקים בישראל יכולת לאומית לבחינה תקיפות חומרה. זאת, לצד שימוש בחומרה מתוצרת מקומית במקרים שבהם נדרשת רמת ביטחון יוצאת דופן.

במסגרת פרק ההגנה נותחו סוגיות נוספות. כך זוהה הצורך בבניית יכולת התאוששות לאומית מתקיפה בסייבר כיכולת חיונית, מתוך הבנה שבסופו של דבר "קו ההגנה לעולם ייפרץ", ואויב נחוש יצליח לחדור הגנה משוכללת ככל שתהיה. לכן נדרש לבנות מנגנוני התאוששות וחזרה לשגרה מתאימים מבעוד מועד. בנוסף נותחה הסוגיה הארגונית, מתוך הבנת הצורך לוודא שמדינת ישראל יכולה לספק מענה הן למרחב הביטחוני והן לזה הפלילי/אזרחי. הגנת הסייבר במגזר הביטחוני נדרשת להמשיך להיות מנוהלת על ידי גורמי מערכת הביטחון, ואילו פעילות הסייבר במרחב הפלילי/אזרחי תטופל על ידי גורמי האכיפה במדינת ישראל, ובראשם משטרת ישראל. הרשות הלאומית להגנה בסייבר תידרש לסנכרן בין כלל הגופים ולוודא את קיומה ואכיפתה של רגולציה (אסדרה) במגזר האזרחי, שהוא המגזר הרגיש ביותר בישראל לפגיעה במרחב הסייבר. בהקשר זה מומלץ לאמץ תפיסת רגולציה במגזר האזרחי שתחייב את הכנסת תחום הגנת הסייבר כמרכיב מובנה בתהליכים סטטוטוריים קיימים, וזאת הן בשלבי ההקמה של מיזמים (אישור בוועדות התכנון השונות) והן בתהליך התפעול שלהם (חוק רישוי עסקים). מוצע כי במסגרת זו יידרשו עסקים להתייחס גם לנושא הגנת הסייבר הרלוונטית מבחינתם. זאת, באמצעות תסקיר/דוח עמידות סייבר. מסמך זה יהיה הכלי הסטטוטורי העיקרי לצורך איתור ובחינת חשיפתו של המיזם לאפשרות של התקפות סייבר, ולגיבוש תהליכי הגנה מפני חשיפות אלו.

מסמך זה מתייחס באופן תמציתי גם להתקפה בסייבר, ומנותחים בו מספר תרחישי תקיפה הכוללים: תקיפה במצב גלוי ועמום, תקיפה כאמצעי להעברת מסר ותקיפה כחלק ממערכה חשאית.

עיקרי ההמלצות בהקשר זה הם:

1. ארגוני הביטחון של ישראל יידרשו לשלב כלים למתקפת סייבר בדומה לשילובם של כלים קינטיים אחרים בתוכניות האופרטיביות ובהפעלת הכוח בפועל במלחמה, בחירום ובשגרה.
2. יכולת התקפית קיברנטית אינה עומדת בפני עצמה. היא צריכה להיות חלק מתוכנית כוללת כדי להשפיע בעימות גלוי כולל.
3. תקיפה אפקטיבית לא חייבת להיות תקיפת עומק מתוחכמת. רצוי למצות את היכולת לממש תקיפה קיברנטית אפקטיבית למטרה ממוקדת גם באמצעות תקיפה שטחית, מהירה ורחבה של יעדים, גם אם אינם מה שקרוי "יעדי זהב" (מטרות צבאיות, תשתיות מדינה).
4. ניתן לממש תקיפות קיברנטיות אפקטיביות באמצעות שליחים (Proxy) מבלי לקבל אחריות.
5. למתקפה קיברנטית משמעותית נדרשים בניין כוח, הכרת היעד ותכנון מוקדם.

6. תקיפה קיברנטית יכולה להוות נדבך ב"שיח" בין מדינות, כשמטרת התקיפה היא להעביר מסר.
7. מוצע לשלב תוקפים במערך המרכזי המגן על ישראל, לצורך תכנון ותפעול שוטף של מערך ההגנה.

לבסוף, המסמך ממליץ למצות את יתרון ההתנהלות הבלתי־רשמית בישראל. ההיכרות במסגרת רשתות חברתיות רחבות, ההתנהלות החברתית, הרצון לסייע, הרצון להשתתף בפעילות בעלת גוון לאומי, הרצון להיות ב"מרכז העניינים" ולהוכיח רלוונטיות אישית ומקצועית – כל אלה מובילים בישראל להתגייסותם של אנשים רבים כל אימת שנדרש, בין אם כעזרה לחברים ובין אם לצורך לאומי, ובוודאי במצב המשלב בין שתי הסיבות. הפעילות על הבסיס הלא־רשמי הזה מתרחשת כמעט תמיד, וניתן לסמוך על כך שתתרחש באחוז גבוה מאוד מהמקרים שבהם היא נדרשת. בהיותה וולונטרית, מבוססת רצון טוב ומעוגנת בתרבות בישראל, היא חזקה יותר ולעתים איכותית יותר מפעילות שיתוף פעולה שבאה כתוצאה ממחויבות מבנית, חוקית או נוהלית. רצוי יהיה לתת מקום גם למרחב התנהלות זה, שיש לו תרומה משמעותית ביותר לביטחון מרחב הסייבר במדינה.

לסיכום, מוצע שחלק נכבד מהאסטרטגיה שתגובש יהיה גלוי לציבור, ויתאפשר לו לגזור ממנה את מה שרלוונטי עבורו. מובן גם שלמסמך כזה צריכים להיות חלקים מסווגים שיעסקו בנושאים שהשתיקה יפה להם, ושיסייעו לתאם ולסנכרן ככל האפשר בין כלל ארגוני הביטחון הפועלים בישראל. זהו אתגר משמעותי וברי־השגה, שיוכל לקבע את מעמדה של ישראל כמובילה בתחום פעילות הסייבר בעולם.

מבוא

לנוכח התעצמות השימוש שנעשה במרחב הקיברנטי להשגת אינטרסים של מדינות וארגונים, ולאור העובדה שישראל כמדינה מפותחת מבחינה טכנולוגית פעילה מאוד במרחב הקיברנטי, נראה כי ראוי לדון במספר קווים מנחים עבור "אסטרטגיה להתנהלות ישראל במרחב הקיברנטי".[1] אין במסמך זה דיון מקיף בכלל הקווים המנחים ליצירת אסטרטגית סייבר לאומית, אלא התמקדות במספר קווים מנחים שנראו רלוונטיים לבחינה ולהארה עקב התפתחויות מואצות שאירעו במרחב הקיברנטי בשנים האחרונות, בדגש על מתקפות רבות ומגוונות יותר, מודעות הולכת ומתרחבת לסוגיית ההגנה בסייבר ופיתוח טכנולוגי יצירתי ומואץ.

במסמך זה מוגדר המרחב הקיברנטי כפי שהוגדר בהחלטת ממשלת ישראל באוגוסט 2011: "'המרחב הקיברנטי' – המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה".[2] המרחב הקיברנטי הוא אחד מחמישה מרחבי פעולה. האחרים הם: יבשה, ים, אויר, וחלל. אף שהוא וירטואלי ויציר מעשה אדם, הוא המשכו של העולם הקינטי במובנים רבים.[3] המרחב הקיברנטי הוא, לפיכך, מרחב נוסף שבו ישראל פועלת כדי להבטיח את יעדיה הבסיסיים שניתן לנסחם בפירוט, אך בסיסם, כמו בכל מדינה, הוא הבטחת ביטחון לאומי ואישי, ושגשוג ורווחה כלכליים לכלל אזרחי המדינה.[4] מימוש היעדים מחייב הגנה יעילה על פעילות אזרחים, ארגונים ומוסדות ישראליים במרחב הקיברנטי, ושימוש מושכל במרחב זה להשגת האינטרסים של ישראל.

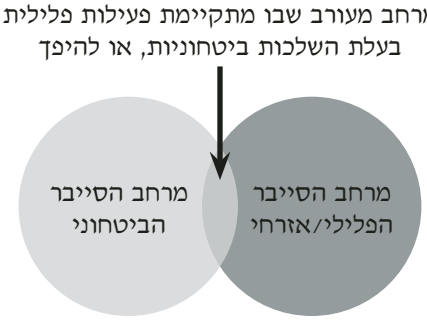
בהקשר להגנה הלאומית במרחב הסייבר, היעד העליון צריך להיות שימור הרציפות התפקודית של המדינה. הקביעה של מושאי ההגנה לצורך מימוש יעד זה היא מרכיב בסיסי, ועליו להתעדכן מעת לעת לנוכח התפתחות האיומים במרחב. מפת האיומים במרחב הסייבר נחלקת לשני תת־מרחבים עיקריים: תת־המרחב הביטחוני ותת־המרחב הפלילי. ההבדל המרכזי בין מרחבים אלה הוא המניע לפגיעה. המרחב הביטחוני מאופיין בפעולה שהמניע שלה ביטחוני/פוליטי, ואילו המרחב הפלילי מאופיין בפעולות שהמניע המרכזי שלהן פלילי כמו בצע כסף, סחיטה באיומים, גניבה, הונאה וכדומה.

להלן פירוט למרחבי משנה אלה:

א. תת־המרחב הביטחוני – איומים שהמניע המרכזי להיווצרותם נובע ממוטיבציה פוליטית וביטחונית. בקבוצה זו ניתן למצוא מדינות אויב וארגונים עוינים דוגמת איראן, חזבאללה, חמאס ודומיהם, מדינות יריבות העלולות לפעול נגד ישראל במרחב (מדינות יריבות במרחב הסייבר) כמו סין, רוסיה ועוד, וכן ארגונים, קבוצות ופרטים בעלי סדר יום פוליטי המנסים לפגוע בישראל כגון אנונימוס, קבוצות האקרים למיניהם ואנשים הפועלים נגד ישראל באופן עצמאי.

ב. תת־המרחב הפלילי – מרחב הפעולה של פשיעת סייבר לביצוע הונאות פיננסיות על ידי ארגוני פשיעה ופושעים יחידים, לביצוע גניבה וריגול עסקי ואישי על ידי חברות עסקיות, חוקרים פרטיים הפועלים באופן בלתי־חוקי וכן פעולה של עובדים ממורמרים, המבקשים לפגוע במעסיקיהם מסיבות שונות.

בתרשים להלן ניתן לראות המחשה של חלוקה זו למרחב הסייבר, כולל התייחסות לקיומו של מרחב מעורב, שבו מתממשים איומים בעלי השלכות בשני מרחבי הפעולה.



איור 1: חלוקת מרחב הסייבר הלאומי לפי מניעי הפעולה

הקווים המנחים בהקשר להגנה מציעים מגוון תפיסות פעולה וכלים שיוכלו לשרת את שני המרחבים האלה, כשכל גורם נדרש לייצר את מאפייניו הייחודיים במסגרת תפיסת הפעולה שלו, ולאפשר שיתוף פעולה במקרים שבהם האיום חוצה מרחבים. בנוסף, יש לזכור שהתיחום המתואר בתרשים לעיל מתייחס רק למרחב האיומים. מרחב הפעולה בסייבר מקיף את כלל כלכלת המשק, תאגידים ומוסדות פיננסיים, חינוך, בריאות, מחקר ופיתוח, אקדמיה ועוד. גורמים אלה יוכלו אף הם לעשות שימוש בחלק מהקווים המנחים שמסמך זה מספק.

מקובל להגדיר בצורה מדורגת שלוש רמות בתהליך – הגדרת יעדים, תכנון אסטרטגיה ותרגום לטקטיקה – כך שהגדרת היעדים תשפיע על הגדרת האסטרטגיה, שתשפיע בתורה על בחירת הטקטיקה למימוש. במציאות, כפי שכולנו חווים, הקשרים בין

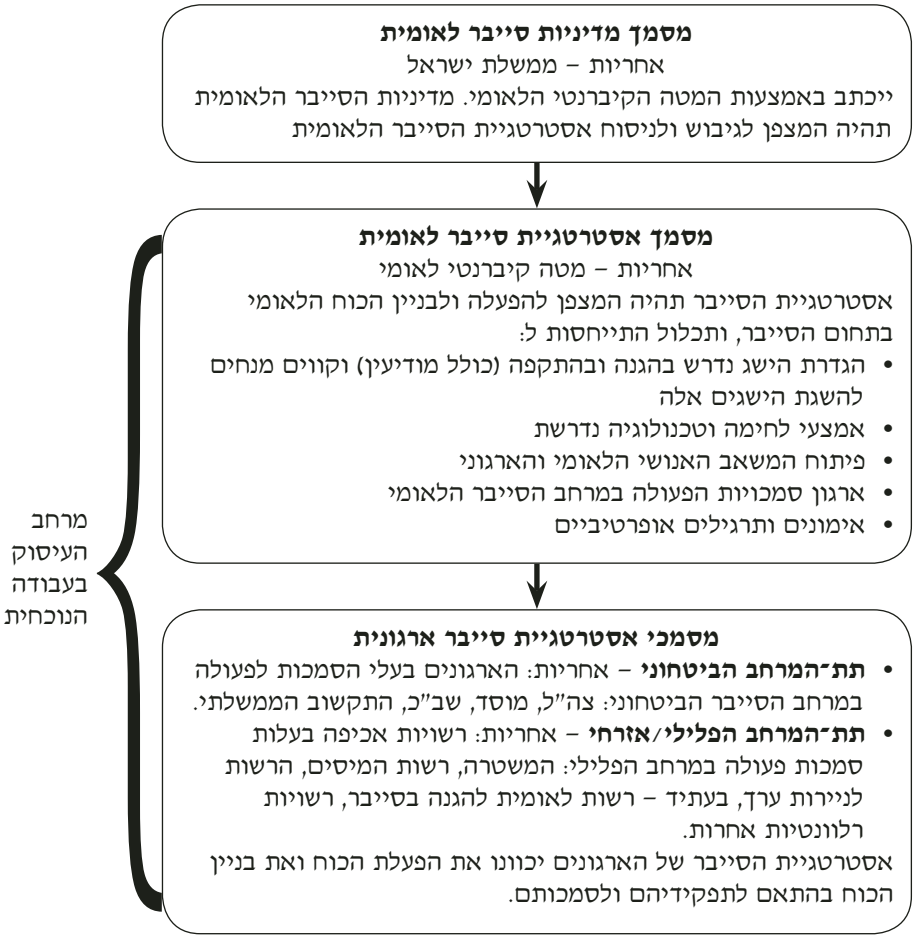
כל רמה לאחרות הם מקבילים ודו־כיווניים, והעשייה בכל רובד משפיעה כל העת על הרבדים האחרים. גם בחינת הקווים המנחים לאסטרטגיה לאומית במסמך זה נעשתה באותו אופן, והיא שואבת מתוך הטקטיקה כדי לנסח קווים מנחים ריאליים ובעלי סיכוי למימוש. העיסוק בפן המעשי יותר של הקווים המנחים מהווה אתגר משום שהעשייה בסייבר תוססת ומתעדכנת כל העת, מתפתחת ומעצבת בהתמדה את המציאות בעולם הקיברנטי. במצב כזה, חריגה מהאמירה הכללית והכוללנית עלולה ללקות בחוסר רלוונטיות, או בצורך בעדכון תוך זמן קצר. למרות זאת, משום הצורך שנראה ממשי, מוצעות כאן המלצות קונקרטיות יותר.

ככלל, יש לראות את האסטרטגיה לפעולה במרחב הסייבר כחלק אינטגרלי מהעיסוק הכולל של המדינה במרחב הקיברנטי. במסגרת עיסוק זה צריך להתקיים תהליך בניין כוח לאומי למרחב הסייבר, הכולל חמש אבני יסוד: הראשונה – אסטרטגיה ודוקטרינה לפעולה בסייבר. טכנולוגיה התומכת בהשגת היעדים וכיווני הפעולה שהוגדרו במסגרת האסטרטגיה היא אבן היסוד השנייה. אבן היסוד השלישית נוגעת לפיתוח המשאב האנושי, כדי שזה יוכל להפעיל את הכלים הטכנולוגיים. משלימה את אלה אבן היסוד הרביעית המתייחסת לארגון כוח האדם במסגרות פעולה רלוונטיות, על בסיס של יתרונות יחסיים בפעולה, ולבסוף אבן היסוד החמישית, העוסקת בהטמעה באמצעות אימונים ותרגילים, בדגש על בניית תוכניות אופרטיביות ותרגול שלהן בפועל.

מסמך זה נועד לסייע בגיבוש אבן היסוד הראשונה בבניין הכוח (אסטרטגיה ודוקטרינה לפעולה בסייבר), במטרה לאפשר את הכוונת הפעולה הלאומית במרחב הסייבר. מוצע שמסמך האסטרטגיה הלאומית יהיה חלק אינטגרלי ממדרג של מסמכים מחייבים: מסמך המדיניות הלאומית לפעולה בסייבר, שיגדיר את יעדי־העל של המדינה ואת דרכי שילובם במאמץ הביטחון והכלכלה הלאומי. ממסמך זה יש לגזור את אסטרטגיות הפעולה בסייבר, שיתייחסו לכל היבטי בניין הכוח. כל ארגון רלוונטי יידרש לגבש את האסטרטגיה הפנימית שלו לפעולה במרחב זה. תיאור מדרג המסמכים המוצע ניתן באיור 2.

מסמך זה מציע קווים מנחים לגיבוש האסטרטגיה, במטרה לסייע למי שבסמכותם ובאחריותם לגבש ולנסח את מסמך האסטרטגיה הלאומית של מדינת ישראל. בנוסף, כפי שהתרשים להלן מציג, מרכיבים במסמך זה יכולים לסייע לארגונים הרלוונטיים לגבש את האסטרטגיה הארגונית שלהם לפעולה בתחום הסייבר, וכן לסייע למגזרים אחרים מדינתיים ואזרחיים המבקשים להסדיר את פעילותם במרחב הקיברנטי.

המסמך אינו מהווה עבודת יסוד בסוגיית אסטרטגיה לפעולת ישראל במרחב הקיברנטי. קיימים מסמכים הנוגעים בהיבטים שונים של האסטרטגיה שישראל צריכה לאמץ בבואה לבחור את דרכה במרחב הקיברנטי.[5] מתקיים שיח רחב בנושא אסטרטגיית התנהלות בסייבר, בארץ ובעולם, המבוסס על ההבנה של מאפייני העידן הקיברנטי,



איור 2: תיחום מסמכי המדיניות והאסטרטגיה ברמה הלאומית

על הבנת הצורך בהתאמת המושגים, החוקים וההגדרות המקצועיות והמשפטיות, ועל יכולות התגובה והאכיפה בעידן הזה. רבות נכתב על מאפייני התקופה, מאפייני עולם המחשוב והעידן הקיברנטי. לפיכך מצאנו לנכון לא לנסח מחדש את האמירות הנכונות והשגורות זה מכבר בפי כל מי שעוסק בסייבר.[6]

הפעילות הכוללת במרחב הקיברנטי בשנים האחרונות התרחבה והתעצמה בכל המישורים, המאפיינים והכיוונים – פעילות הגנתית והתקפית, מדינתית ולא־מדינתית, ממניעי מדיניות לאומית, אידאולוגיה, אתגר טכנולוגי, פשע או טרור, גלויה וחשאית, למטרות איסוף מידע או גרימת נזק. האינטנסיביות הזו מאפשרת את לימוד המדיניות והאסטרטגיה שאימצו מדינות שונות ביחס לפעילות במרחב הקיברנטי. ההצעות

המובאות כאן מבוססות בעיקרן על השיח הרחב בארצות־הברית, על פעילויות במרחב הקיברנטי כפי שתוארו בפרסומים שונים,[7] על ממצאים שמפרסמות חברות מודיעין וביטחון סייבר בעקבות חקירות אירועים שונים,[8] על טכנולוגיות המשווקות כמענה לצורכי הפעילות במרחב הקיברנטי ועל רעיונות המובאים בכנסים ובוועידות בנושא הסייבר.

האתגר האסטרטגי

The essence of strategy is choosing to perform activities differently than rivals do.
Michael Porter[9]

דבריו של פורטר נאמרו בהקשר של קביעת אסטרטגיה לחברה עסקית המצויה בתחרות, אך דומה שהם רלוונטיים לדיון בקו מנחה מרכזי לגיבוש אסטרטגיית סייבר לאומית – ההגנה מפני תקיפות. זהו האתגר האסטרטגי המרכזי, כשמטרת־העל היא שימור הרציפות התפקודית ברמה הלאומית.

אתגר ההגנה בסייבר מרכזי מכמה סיבות. הראשונה שבהן היא יתרונו של התוקף, המועצם במרחב הקיברנטי. ליבת היתרון הזה היא היוזמה, המובילה לכך שבעצם לא תיתכן הגנה מוחלטת, הרמטית וחסרת חולשות, ותמיד ניתן יהיה לממש תקיפה מוצלחת. הסיבה השנייה היא שטרם מומשה באופן נרחב יכולת להגנה יעילה ומוכחת מפני תקיפה שמבוססת על כלים לא ידועים. העובדה הזו מביאה לניסיונות לשפר כל העת את השיטות ואת כלי ההגנה הקיימים. השיפורים הללו מועילים אך אינם משנים את תבנית ההתנהלות שבין תוקף למגן, ולכן אינם מספקים פתרון מניח את הדעת. הסיבה השלישית היא שפתרונות מהעולם הקינטי למצבים שבהם הגנה אינה הרמטית, כמו "הרתעה" ו"מאזן כוחות", טרם הוכיחו תקפות במרחב הקיברנטי. העובדה שטרם הוכחה שיטת הגנה יעילה מפני תקיפה במרחב הקיברנטי מובילה למציאות שבה העימות במרחב הזה הוא א־סימטרי באופן רב־ממדי. אין סימטריה בין תוקף למגן, אין סימטריה בין השקעה נדרשת בהגנה להשקעה הכרחית בהתקפה, אין סימטריה בין מדינה מבוססת טכנולוגיה ומחשבים למדינה דלת־תשתית טכנולוגית.

הדיון בהקשר לגיבוש אסטרטגיה עוסק גם בהתקפה במרחב הקיברנטי. מטבע הדברים, העיסוק ביכולות התקפיות למדינה אינו פתוח לדיון ציבורי, הן משום הצורך של המדינה לשמר יתרונות טכנולוגיים התקפיים לאורך זמן, ובעיקר משום שנטייתן של מדינות היא לא לקבל אחריות על התקיפות שלכאורה בוצעו על ידן. משום מיעוט הפרסומים על אסטרטגיות תקיפה מדינתיות, ההתייחסות לנושא ההתקפה תהיה מוגבלת יותר.

השיח הציבורי בישראל ובעולם עוסק בתקופה האחרונה בשתי סוגיות משמעותיות נוספות. הראשונה נוגעת לזכות לפרטיות במרחב הקיברנטי. בשל הצורך לקבל מידע על הנעשה במרחב, לרוב לטובת הגנה, יש צורך בהעברת מידע לגורמי הפיקוח הממשלתיים האחראיים על ההגנה הלאומית. העברת מידע נרחב לגורמי ממשל על פעילות אזרחים במרחב ושאלות הנגזרות ממנו, כמו מי הם הגורמים הממשלתיים שזכאים לראות את המידע הזה ומה השימוש שמותר לעשות במידע, הן שאלות שעניינן דיון ציבורי ו/או משפטי, והמסמך לא יבחן אותן ולא יעסוק בהן.[10] סוגיה שנייה היא פגיעה אפשרית באזרחים בלתי־מעורבים במהלך תקיפה קיברנטית נגד יריב, בעיקר משום התשתית האחודה והקישור בין רשתות המהוות מטרה לגיטימית לבין רשתות אזרחיות. סוגיה זו אינה ייחודית למרחב הקיברנטי, והיא רלוונטית גם בהקשרי הלחימה הפיזית באזורים מאוכלסים בצפיפות. גם נושא זה ראוי לדיון ציבורי ו/או משפטי, וגם בו מסמך זה אינו דן.

במסגרת ניתוח האתגר האסטרטגי וכדי ליצור "שפה משותפת", יש להתייחס למספר שאלות: מהם האיומים וסוגי ההתקפות הקיברנטיות? מי הם מושאי ההגנה בישראל שעבורם נבנית אסטרטגיית ההגנה? מי הם היריבים שמפניהם יש להתגונן?

התקפה במרחב הקיברנטי – מקובל להגדיר שלושה סוגי התקפות במרחב הקיברנטי. ההתקפות נבדלות במטרה שלהן, וכנגזרת, לעתים, במתווה ובכלים:

א. תקיפה לצורך פגיעה, הרס ומחיקה (Computer Network Attack – CNA) – תקיפה שתכליתה גרימת נזק למחשב/רשת ומניעה של המשך תפקודם התקין. הנזק יכול להיות ברמת השבתה לפרק זמן מוגבל, לדוגמה: מתקפה מסוג מניעת שירות (Denial of service), או שינוי חזות לאתר (Defacing) ואף מחיקה של מידע, השבתה של המחשב ושיתוק תהליכים נתמכי מחשב בארגון הנתקף בהתקפת עומק (APT– Advanced Persistent Threat).[11]

ב. תקיפה לצורך הפקת מידע/ריגול (Computer Network Exploiting – CNE) – תקיפה שתכליתה איסוף מידע. המידע יכול להיות טכנולוגי – על מבנה הרשת והמחשבים – לצורך מימוש מאוחר יותר של תקיפת CNA, או איסוף נתונים לצורך מימוש פעילות אקטיבית עתידית (כדוגמת איסוף נתוני כרטיסי אשראי או נתוני זהות של משתמשי דואר אלקטרוני), והוא יכול להיות איסוף מידע תוכני (גניבה של מידע מסחרי, מחקר ופיתוח או סודות צבא ומדינה).

ג. תקיפה לצורכי השפעה, פסיכולוגית בעיקרה (Computer Network Influence – CNI) – תקיפות מסוג זה נועדו לטעת את התחושה של חוסר ביטחון, חוסר שליטה, פגיעה בריבונות וחוסר יכולת להגן על אורח החיים הנורמטיבי. תקיפות כאלה יהיו בדרך כלל מוגבלות בזמן, ולא יגרמו נזק ממשי זולת התחושות הללו.

היריבים של ישראל – הגדרת יריבים נתפסת כמהותית בתהליך בניית יכולות ותכנון תוכניות מתאימות להגנה. בעיסוק במרחב הקיברנטי ניתן להגדיר את היריבים באופן רחב, ולבסס בניית יכולות ותוכניות הגנה על פרמטרים אחרים. יריב הוא כל מי שמבצע פעילות עוינת נגד ישראל מכל סוג ולכל מטרה במרחב הקיברנטי. היריב כולל, כמובן, אויבים מוצהרים וידועים כמו איראן, סוריה, חזבאללה, חמאס, אך יכול לכלול גם מדינות המנסות לממש פעילות עוינת למטרה נקודתית מוגדרת, למשל, ריגול או גניבת סודות טכנולוגיים, או גופים בתוך מדינות שיש להם עניין נקודתי בפעילות כזו.

מושאי ההגנה בישראל – ניתן לחלק את מושאי ההגנה[12] בישראל לפי הקטגוריות הבאות: גופים העוסקים בביטחון המדינה, גופים המספקים שירותים חיוניים, גופים האחראיים לסדרי ממשל וחיים תקינים וגופים שתקיפתם תשפיע על מורל ותחושות סדר, על ריבונות ומשילות.

א. ביטחון המדינה – כלל הגופים שפגיעה קיברנטית בהם תביא לפגיעה בביטחון המדינה, כמו גופי קביעת מדיניות חוץ וביטחון וגופי הביטחון עצמם, או חלקים מתוכם וכל הקשורים בהם.

ב. שירותים חיוניים – גופים שפגיעה קיברנטית בהם (בדרך כלל – CNA) תשבית פעילות חיונית שמשמעותה שיתוק החיים במדינה, אובדן כלכלי נרחב ואף סכנת חיים, כגון מזון, תחבורה, תקשורת, מים, אנרגיה, בריאות, מערכת מוניטרית, מסחר משמעותי, ייצור תעשייתי משמעותי וכדומה.

ג. סדרי ממשל וחיים תקינים – שיבוש אורחות החיים במדינה אך לא עד כדי שיתוק או סכנת חיים, כולל תחומים דוגמת חינוך, אקדמיה, מחקר ופיתוח, משפט, מאגרי מידע כמו מרשם האוכלוסין, רישום בעלות, רישום בטאבו, רישום פטנטים, פגיעה בחברות מסוגים שונים, פגיעה בשירותי הממשלה והשלטון המקומי.

ד. מורל וריבונות – פגיעה עתית באתרים של גופי ממשל, שליחת הודעות פוגעות לאזרחים, השבתת אתרי תקשורת לפרקי זמן מוגבלים וכל פעולה שיוצרת תדמית של פגיעה במשילות, בסדר ובארגון של המדינה.

סקירת ספרות

הלמידה מאחרים מהווה מרכיב יסוד במחקר. במסגרת זו נבחנו מגוון מקורות, ביניהם מסמכים רשמיים, מאמרים ודברים של גורמים רלוונטיים. מטבע הדברים, למידה זו אינה מלאה, וקיימים מקורות רבים שלא נסקרו במסגרת המסמך. לצד בחינת הפרסומים במדינת ישראל, הושם דגש בסקירת הספרות על בחינת הדברים במדינות דמוקרטיות מערביות, ובעיקר בארצות־הברית. התפיסות של אנגליה וצרפת מתבססות על מסמכים רשמיים, ואילו במקרה של סין מתבסס הניתוח על עבודת מחקר שבוצעה במכון למחקרי ביטחון לאומי. לצד אלה, נעשה ניסיון ללמוד גם ממסמכים של ארגונים בינלאומיים כגון OECD, ENISA והאיחוד האירופי. תהליך הלמידה כלל גם בחינה של פרסומים ומקורות גלויים בנושא הגנה והתקפה.

תכנון ואסטרטגיה

ישראל

ממשלת ישראל לא פרסמה מסמך רשמי המפרט את האסטרטגיה של המדינה בפעילותה במרחב הקיברנטי. בהחלטות הממשלה קיים כיוון כללי וחזון בנושא, ועיקרן עוסקות בסוגיית חלוקת האחריות בין הארגונים השונים בישראל.[13] החלטה זו נסמכת על המלצות מתוך עבודה שהוכנה במועצה למחקר ופיתוח בראשות יצחק בן־ישראל, במהלך השנים 2010–2011. העבודה שבוצעה במועצה הייתה מקיפה, ותכליתה "להציג תכנית עבודה למיזם לאומי להתמודדות עם האיום הקיברנטי, תוך שהוא מדגיש את המענה לצרכי הביטחון לצד המערכות הציבוריות והאזרחיות".[14] עבודת המועצה הצביעה על הצורך לגבש אסטרטגיה להגנת תחום הסייבר בישראל, ואף הצביעה על אחת הנקודות המהותיות שהאסטרטגיה תידרש להן – ההגנה על המרחב הקיברנטי הממלכתי והאזרחי של מדינת ישראל. במסגרת העבודה גובשו שתים־עשרה המלצות, מתוך כלל ההמלצות הללו פורטו בנפרד ההמלצות הבאות: הקמת המטה הקיברנטי, הרחבת סמכויות שירות הביטחון הכללי והרשות לאבטחת מידע כגוף ביצוע לטיפול במרחב האזרחי, מספר פעולות למדיניות וחקיקה לעידוד תעשיית הסייבר, עידוד מחקר ופיתוח בתחום הסייבר ומחשוב־על והקמת מרכז לאומי בתחום חישוב־על.[15] ממשלת ישראל קיבלה את המלצות המועצה למחקר ופיתוח והטילה על המטה הקיברנטי לממש אותן. המטה טרם פרסם תפיסה אסטרטגית מלאה באשר להתנהלותה של

ישראל במרחב הקיברנטי, והצעד המשמעותי היחידי שנעשה מאז היה קבלת החלטה נוספת של ממשלת ישראל, הסותרת באופן נקודתי את המלצת המועצה, ומטילה על המטה הקיברנטי להקים רשות סייבר שתהיה אחראית על הטיפול בהגנה על המרחב האזרחי.[16]

היותו של תחום הסייבר חדש יחסית ומצריך הסבר והמשגה, וכן היעדרו של מסמך רשמי המנתח את האסטרטגיה של ישראל במרחב הקיברנטי – הביאו לכתיבתן של כמה עבודות הרלוונטיות לסוגיית האסטרטגיה. שמואל אבן ודוד סימן טוב פרסמו ביוני 2011 מזכר מטעם המכון למחקרי ביטחון לאומי, שהתמודד בצורה מקיפה עם סוגיית הסייבר.[17] אבן וסימן טוב הגדירו את מטרת האסטרטגיה כקיום בטוח של המרחב הקיברנטי הישראלי.[18] לדעתם, מטרת ההגנה בסייבר היא השמירה על האינטרס הישראלי, והדרך להשגת המטרה היא גיבוש סדרי עדיפות בכל הנוגע למושאי הגנה ובניית מערך הגנה דינמי, אינטגרטיבי ומקיף, על בסיס שילוב בין מערכות הגנה פסיביות לבין מערכות הגנה אקטיביות, שילוב בין הגנה על יעדים חיוניים לבין מרכיבי "הגנה מרחבית" (תעבורה הנכנסת למדינה, צומתי תקשורת), שיפור ארכיטקטורת רשתות והידוק בין מנגנוני אבטחה פיזיים לקיברנטיים. אבן וסימן טוב מבססים את כל הפעילות על קשרי שיתוף הפעולה בין המגזר הממשלתי (הביטחוני והאזרחי) לבין המגזר הפרטי, כולל שיתוף במידע וביכולות, וכן על שיתוף פעולה הדוק עם גורמי חוץ.

בניין הכוח

מרכיב חיוני בגיבוש כיווני הפעולה של ישראל במרחב הסייבר נוגע לבניית תפיסה שיטתית של בניין הכוח.[19] סיבוני מנתח את תהליך בניין כוח לאומי בתחום הסייבר כתוצר של תכנון רב־שנתי של התעצמות באופן שיטתי ומוכוון. תהליך בניין כוח כולל מספר אבני יסוד, שהראשונה בהן היא גיבוש אסטרטגיה ותורת פעולה. רכיב זה הוא הבסיס שעליו נשען התהליך השלם, הכולל ארבעה מרכיבים נוספים: פיתוח כוח האדם וההון האנושי, פיתוח טכנולוגי של אמצעים, ארגון כוח האדם והאמצעים במסגרות מתאימות וכן קיומם של הכשרות, אימונים ותרגילים במטרה לוודא שכלל המערכים פועלים כיאות, וכדי לשכלל ולפתח את הידע. עם גיבוש עיקרי האסטרטגיה הלאומית במרחב הזה, מציע סיבוני להתייחס לתפיסת הפעלת הכוח ההגנתי, המודיעיני וההתקפי במרחב הסייבר. תורת הפעולה במרחב הסייבר נדרשת גם להתייחס למענה הלאומי בשגרה, בחירום, ובמדינות שבהן הדבר רלוונטי – גם במלחמה, כדי להגדיר היטב כיצד צריכה המדינה להתמודד לא רק עם אירועי תקיפה שבשגרה, אלא גם עם תקיפות סייבר רחבות־היקף שיופעלו במנותק או במשולב עם אירועי תקיפה פיזית.

בנוסף, פיתוח כוח האדם וההון האנושי, לצד פיתוח טכנולוגי של כלים ושיטות, נדרשים להיות משולבים ומסונכרנים באופן שימצה את כלל המשאבים הלאומיים

לטובת ביצור יכולות הסייבר של המדינה. המערך הטכנולוגי והאנושי שיפותח יידרש לתמוך ביעדיה הלאומיים של המדינה, כך גם ההשקעות בטכנולוגיה שיש לעודד, וכן בניית ההון האנושי בבתי הספר ובאקדמיה. מרכיב הארגון נוגע לאחריות ולסמכות ההפעלה של אנשים ואמצעים למימוש האסטרטגיה הלאומית במרחב הסייבר. דוגמה אפשר לראות בישראל, כשארגוני הביטחון בונים לעצמם יכולות פעולה במרחב הסייבר כדי לתמוך במשימות היסוד שלהם. לבסוף, מערך מאורגן של אנשים וכלים טכנולוגיים מחייב פיתוח טכניקות פעולה, הכשרות, אימונים ותרגילים. פיתוח התחום הזה מהווה את שיאו של תהליך בניין הכוח. ארגוני הביטחון מקיימים שגרת הכשרות, אימונים ותרגילים. יש להרחיב תחום זה גם למגזר האזרחי, שהוא החשוף ביותר לפגיעה במרחב הסייבר, ולשלב מאמצים עם שאר הארגונים כדי למצות את מלוא הפוטנציאל הלאומי.

ארצות־הברית

בארצות־הברית עוסקים בשנים האחרונות באופן אינטנסיבי למדי בעיצוב אסטרטגיה להתנהלות במרחב הקיברנטי. משרד ההגנה (Department of Defense) רואה את המרחב הקיברנטי כמגדיר מחדש את המונח "ביטחון לאומי", בשל היותו של המרחב בעל השפעה מכרעת על יכולתו של משרד ההגנה לממש את יעדיה של ארצות־הברית, ההגנתיים וההתקפיים. משרד ההגנה פרסם ביולי 2011 מסמך ובו ניתוח האסטרטגיה הבסיסית שלו להתנהלות במרחב הקיברנטי.[20] ליבת המסמך היא הגדרת חמשת העקרונות של האסטרטגיה:[21] (א) משרד ההגנה מתייחס למרחב הקיברנטי כאל מרחב מבצעי שזקוק לארגון, לאימון ולציוד, שיאפשרו למשרד ההגנה למצות את הפוטנציאל הטמון בו. (ב) אימוץ תפיסת הגנה מבצעית חדשה במטרה להגן על הרשתות והמערכות שלה. (ג) שותפות עם משרדים אחרים בממשל, עם סוכנויות ועם המגזר הפרטי כדי לממש אסטרטגיה קיברנטית ממשלתית אחודה/שלמה. (ד) בניית מערכת יחסים חזקה עם בעלי־ברית ושותפים בינלאומיים, במטרה לחזק את האיסוף למטרות ביטחון קיברנטי. (ה) מינוף כושר ההמצאה של האומה באמצעות כוח אדם יוצא דופן וחידושים טכנולוגיים מהירים.

שני מסמכי דוקטרינה מגדירים את עבודתו של צבא ארצות־הברית במרחב הקיברנטי. הראשון הוא Joint Publication 3-12, Cyberspace Operations המגדיר את המרחב הקיברנטי ואת יעדי צבא ארצות־הברית בפעילות בו ו/או באמצעותו להשגת מטרותיו.[22] המסמך השני המגדיר לוחמת מידע בצבא ארצות־הברית. במסמך זה מתייחס הצבא שוב להגדרות של המבצעים במרחב הקיברנטי (ובכך נותן שוב הקשר ברור להיותו של המרחב הקיברנטי ממד משמעותי בלוחמת המידע), וכן להגדרות של הגנת מידע (ובכך יוצר, בעינינו, זיקה בין היכולת לממש מבצעים במרחב הקיברנטי לבין היכולת להגן על המידע של עצמו).[23] שני המסמכים, הכתובים בסגנון צבאי מובהק, מהווים

תרגום של האסטרטגיה וההנחיות הכלליות של מסמכי משרד ההגנה וכוללים, בין השאר, שימוש במרחב הקיברנטי למטרות התקפיות כדי להשיג את יעדיו של צבא ארצות־הברית.

קית' אלכסנדר, המפקד הראשון של פיקוד הסייבר האמריקאי וראש הסוכנות לביטחון לאומי (NSA), פרסם בנאום שנשא ב־30 באוקטובר 2013 את תקציר האסטרטגיה של פיקוד הסייבר.[24] הוא מנה חמישה עקרונות שעליהם מתבססת האסטרטגיה של פיקוד הסייבר שבפיקודו. (א) כוח מאומן ומיומן בהתערבות בעת התקפת סייבר על ארגון חשוב. אלכסנדר ממחיש את הצורך בכוח כזה בתיאור של תקיפה אפשרית על המערכת הפיננסית האמריקאית בוול סטריט (המותקפת במתקפות DDoS רבות), במתאר דומה לתקיפה שבוצעה על חברת Aramco הסעודית ובמהלכה הותקפו כ־30,000 מחשבים. התסריט הדמיוני אך אפשרי הזה שימש את אלכסנדר ברבים מנאומיו כדי להסביר לשומעים ולשכנע אותם הן בחומרת האיום, והן בצורך הנוקב במימוש האסטרטגיה שגיבש בפיקוד הסייבר. (ב) חלוקת סמכויות ברורה ופיקוד ושליטה מוסכמים. אלכסנדר מחלק את העבודה כך: בתוך גבולות ארצות־הברית באחריות ה־FBI, ומחוץ לגבולות המדינה בשיתוף פעולה מודיעיני עם בעלי־ברית באחריות ה־NSA וה־Cyber Command. (ג) ארכיטקטורת רשתות במשרד ההגנה, שהיא בת־הגנה ולא מבנה של 15,000 רשתות שהתקיים במשרד ההגנה בעת ההיא. (ד) שיתוף בהערכת מודיעין בסייבר, הן בין הסוכנויות לבין עצמן והן בינן לבין המגזר הפרטי. שיתוף הפעולה צריך להיות על בסיס חקיקה, ולהתקיים בין גופי הממשל המטפלים בהגנה בסייבר (FBI, NSA, Homeland Security Department, Cyber Command) לבין ארגונים אזרחיים פרטיים כמו ספקי האינטרנט. בניסוח זה מבקש אלכסנדר לכסות שתי נקודות מהותיות – הן את סוגיית שיתוף הפעולה בין המגזר הממשלתי למגזר הפרטי והן את הסדרת העברת מידע בין המגזרים בחוק, בעידן שאחרי סנודן.[25] (ה) חלוקת סמכויות. כולם עובדים בהנחיית הנשיא ועל פי מדיניותו של משרד ההגנה, אבל יש צורך בקביעת סמכויות התנהלות בסיסיות, שלאורן ניתן לפעול.

בדבריו של אלכסנדר ניתן לראות את פירוש האסטרטגיה של משרד ההגנה בדרך של מימוש מעשי יותר. יחד עם זאת, ניכר שכוח ההתמודדות העיקרי עם ביטחון קיברנטי מצוי דווקא בארגונים שאינם מורשים לעבוד בתוך ארצות־הברית, ואילו ליבת האיום נמצאת דווקא שם. את האנומליה הזו מבקש אלכסנדר לפתור גם בדרך העברתם של פרטי מידע רלוונטיים לגופים שאינם ה־FBI לצורכי הגנה.[26]

דרך טובה לבדוק את האסטרטגיה היא להבין את החזון שיש לאחראים לגבי ההתנהלות במרחב הקיברנטי. מייקל רוג'רס, מחליפו של אלכסנדר, נשא דברים בסמינר סייבר והתייחס להתנהלותו של צבא ארצות־הברית במרחב הקיברנטי ב־2025.[27] הוא אמר שהשימוש בסייבר התקפי והגנתי כחלק מובנה יהיה טבעי ובלתי־נפרד ממכלול

הכלים של המפקד, והוא ינהל ויתמרן במרחב הקיברנטי כפי שהוא מתמרן כוחות יבשה, בצורה משולבת בתפיסה רחבה יותר של הפעלת כוח. רוג'רס מונה שלוש נקודות מהותיות כדי להגיע למצב הזה. הראשונה – ההבנה שפעילות בסייבר היא פעילות מבצעית לכל דבר, והיא כלולה באחריותו ובמרחב פעילותו של המפקד. מפקד חייב לרכוש ולהטמיע את היכולת ולהיות בעל ידע על יכולות היחידה, המבנה והחולשות הפוטנציאליות שלה. השנייה היא קיום רשת משותפת (joint network backbone) לכל כוחות משרד ההגנה, בכל מקום שהם יימצאו ובכל אמצעי שירצו, כולל סלולר. השלישית היא אנשים ושותפויות, שהם המפתח לעשייה הזו. בהקשר זה מתייחס רוג'רס לצורך בכוח אדם איכותי ואומר שהצבא לא יוכל להתחרות מבחינה כספית בהצעות של התעשייה האזרחית, והוא יצטרך להציע היבטים של תחושת מחויבות לאומית, להיות חלק ממשהו גדול ולאפשר לעשות באופן חוקי מה שהאנשים הללו יכולים לעשות מחוץ למערכת רק באופן לא חוקי.

באפריל 2015 פרסם משרד ההגנה של ארצות־הברית מסמך מעודכן על אסטרטגיית סייבר.[28] מסמך זה מציב חמישה יעדים לאסטרטגיית הסייבר: לבנות ולשמר מוכנות של האנשים והיכולות לטובת פעולה במרחב הקיברנטי, להגן על רשת המידע ועל מאגרי המידע של משרד ההגנה ולהתמודד עם איומים עליהם, להגן על ארצות־הברית ועל האינטרסים שלה מפני מתקפות סייבר הרסניות ומשמעותיות, לבנות ולשמר אפשרויות פעולה קיברנטיות ולתכנן שימוש בהן כדי לנהל עימותים ולשלוט בהם, וכן לבנות ולשמר בריתות ושותפויות בינלאומיות להגברת יכולת ההתמודדות עם איומי סייבר ולחיזוק היציבות. רוב המטרות המופיעות כאן הופיעו במסמכי משרד ההגנה גם קודם. קיימות שתי נקודות שבהן נראה שוני. הראשונה היא ההבנה והניסוח המפורש שאין יכולת אמיתית להגן על כל רשתות משרד ההגנה בצורה הרמטית, לסגור את כל נקודות החולשה והפגיעויות שיש בהן ולמנוע מתקפות מוצלחות. במצב כזה האסטרטגיה היא למפות, לזהות את המידע החיוני ואת הרשתות והמערכות החשובות ביותר, ולהגן עליהם. שוני קיים גם בניסוח המשימה הרביעית. משרד ההגנה הציב לעצמו יעד להפוך את הסייבר לכלי בעימותים שיאפשר לנשיא, כמפקד הכוחות המזוינים בארצות־הברית, אופציות פעולה גם במרחב הקיברנטי. בפירוט המשימה נכתב במפורש כי הכוונה היא לאפשר למפקדי הפיקודים שילוב של תכנון וביצוע קינטי וקיברנטי. אף שהדברים נאמרו על ידי מפקדי פיקוד הסייבר של צבא ארצות־הברית והם גם מופיעים בנוסחים שונים במסמכים, זהו ניסוח מפורש וחד בהגדרה לגבי היעד שאסטרטגיית הסייבר של הממשל האמריקאי צריכה להשיג. בשאר הסעיפים יש המשכיות לפעילות משרד ההגנה – ראייה של התשתיות האמריקאיות כיעד מובהק להגנה, משום שהן משרתות גם את משרד ההגנה, שיתוף פעולה עם מחלקות וסוכנויות ממשלתיות אחרות, שיתוף פעולה עם המגזר הפרטי, בניין כוח

טכנולוגי ואימוץ טכנולוגיות הגנה מתקדמות, הכשרת אנשים לרמה הגבוהה ביותר ושיתוף פעולה בינלאומי כמרכיב הכרחי ביכולת להגן בסייבר.

ווילאם לין (William J. Lynn III), איש ממשל ותיק ובכיר, מראה כיצד התמודדות סדורה עם אתגרי המרחב הקיברנטי נולדה בממשל האמריקאי כפועל יוצא של אירוע ספציפי, ומסביר את המורכבות בגיבוש אסטרטגיית ההתמודדות באי־התאמה מובהקת של מושגי העולם הקינטי לאופי העולם הקיברנטי.[29] מושגים כמו הרתעה בנוסח המלחמה הקרה או הגנה קשיחה על המרחב הקיברנטי האמריקאי אינם רלוונטיים. לין ממליץ על הרתעה על בסיס הגנה חזקה ואפקטיבית, שתביא את התוקפים הפוטנציאליים למסקנה כי הם יכלו את כוחותיהם לריק ולא ישיגו את יעדיהם, פיתוח אסטרטגיית הפחתת סיכונים מתוחכמת בפנטגון כתשובה יעילה יותר לאיומי החדרת רכיבים מפגעים בתוך חומרה וקושחה וגמישות מבצעית וטכנולוגית, המאפשרת התאמה מרבית לסביבה המשתנה. לין מתאר מערך הגנה משולב, שמורכב ממערך השומר על "השער הקיברנטי של הארגון" וממערך המחפש כל העת את הקוד המפגע שעבר את שער הארגון, ומצוי בתוך הרשת שלה. לין נדרש אף הוא לסוגיה הארגונית שמעסיקה מדינה המתארגנת להתמודדות עם אתגרי המרחב הקיברנטי, וטוען כי הכנסת משרד ההגנה לסוגיית ההגנה הקיברנטית בתוך ארצות־הברית, אף שהדבר אינו בסמכותו, היא משום היכולת המקצועית הגבוהה של אנשיו.

ל־FBI אחריות להגנה במרחב הקיברנטי בתוך ארצות־הברית. המטרה ששם לעצמו הארגון היא למנוע מתקפות על תשתיות, גופי ממשל, ארגונים, תעשייה פרטית ואזרחים בארצות־הברית. ה־FBI גיבש אסטרטגיה של פעילות מונעת על ידי טיפול בתשתיות של התוקפים, איסוף מודיעין ושיתוף פעולה בתוך ארצות־הברית ועם גורמים מחוץ לה. על בסיס האסטרטגיה הזו מממש הארגון פעולות מבוססות מודיעין, הקמת קבוצות מומחים הממוקדות באיום ספציפי ופיתוח מקצועי ייחודי של העובדים בתחום הסייבר. השיתוף בין הסוכנויות והמחלקות העוסקות בסוגיית הסייבר הוא נקודת מפתח גם בעיני ה־FBI. המימוש הוא במסגרת ה־NCIJTF (National Cyber Investigative Joint Task Force) ושותפויות נוספות, בתוך ארצות־הברית ובינלאומיות.[30]

בריטניה

ממשלת בריטניה הגדירה ב־2009 את האסטרטגיה של בריטניה במרחב הקיברנטי.[31] המסמך, אף שהוא נוטה להיות כללי מאוד (בטענה שפירוט יעניק מידע לתוקפים, ולכן הם נמנעים מפרסומו) מצליח להעביר את רוח האסטרטגיה של ממשלת בריטניה בעיקר בחלק העוסק במבנה ארגוני. הממשלה מצהירה על כוונתה להקים CSOC (Cyber Security Operational Center) לאומי, שבמסגרתו ייכללו כל הגופים שעוסקים בפעילות במרחב הקיברנטי. כמו כן מתכוונת ממשלת בריטניה להקים משרד לענייני

הגנת סייבר (OCS – Office of Cyber Security) בקבינט. במסגרת שני הגופים הללו מתכננת הממשלה את כלל הפעילות שלה בכל התחומים, תוך שמירה על עקרונות מתבקשים כמו חופש הפרט, חופש זרימת המידע, איזון בין החובה להבטיח את החופש הזה והצורך להגן על בריטניה ממתקפות קיברנטיות, שיתוף פעולה בינלאומי ופנים־מדינתי, מחקר ופיתוח, חינוך ושאר תחומים הרלוונטיים לעשייה במרחב הקיברנטי. המסמך מהווה מסגרת לעיסוק במרחב הקיברנטי בבריטניה, וברי לכול כי נדרשת תוכנית מפורטת בגופים השונים כדי לתרגמו לכלל עשייה.

בנובמבר 2011 פרסם ה־Cabinet Office מסמך העוסק באסטרטגיית הגנת הסייבר של בריטניה – הגנה על בריטניה וקידומה בעולם הדיגיטלי.[32] בתוכנית נקבעו ארבעה יעדים להתנהלותה של בריטניה במרחב הקיברנטי, בדגש על תחום ההגנה לשנת 2015: לחימה בפשעי סייבר במטרה להיות אחד המקומות הבטוחים ביותר בעולם למימוש סחר במרחב הסייבר, עמידות גבוהה יותר מול מתקפות סייבר והגנה טובה על האינטרס הבריטי במרחב הקיברנטי, סיוע בבניית מרחב קיברנטי פתוח, יציב ותוסס שישמש את הציבור הבריטי באופן בטוח, בניית מאגר בריטי שיכלול ידע, מיומנויות ויכולות הנדרשים להשגת יעדי ביטחון הסייבר הלאומיים. המסמך מפרט את החלקים הגלויים של התוכנית הממשלתית להשגת היעדים הללו, ובכלל זה מודעות אזרחים לאיומי סייבר וליכולות התגוננות, שיתוף פעולה של הממשלה עם המגזר העסקי הפרטי, שיפור האכיפה מול פשעי סייבר, שיתוף פעולה בינלאומי עם מדינות וארגונים, חינוך בכל הרמות, חיזוק יכולות של גופי ביטחון בהתמודדות עם איומים ברמה גבוהה, עזרה לצרכנים בקביעת פרמטרים לכלי הגנת סייבר יעילים, קביעת גורם מוסמך אחד להתמודדות עם תקיפות ומשברי סייבר, עידוד כוחות המשטרה המקומיים לתת מענה ברמה שלהם לתלונות אזרחים על תקיפות. להשגת היעדים הללו הקצתה ממשלת בריטניה בשנת 2011 סכום של 650 מיליון ליש"ט. בדצמבר 2014 פרסם ה־Cabinet Office דין וחשבון על יישום התוכנית מ־2011.[33] המסמך מתאר עשייה ממשלתית ענפה ומפורטת בכל אחת מארבע הסוגיות שהוצבו כיעדים ב־2011.

צרפת

ממשלת צרפת קבעה ב־2009 את האסטרטגיה הכללית שלה להתנהלות במרחב הקיברנטי.[34] ליבת האסטרטגיה היא הגנה על המידע, בהיבטי ביטחון העברת מידע (בעיקר מידע ממשלתי רגיש) ומניעת גניבת מידע. איום הייחוס המוגדר על ידי ממשלת צרפת הוא פעולות ריגול וגניבת מידע על ידי ממשלות זרות, תעמולה, הפצת אידאולוגיה והנחיות מבצעיות על ידי ארגוני טרור, ובעתיד גם תקיפת תשתיות מדינתיות הן על ידי גורמי טרור והן על ידי מדינות. ממשלת צרפת הגדירה שיתוף פעולה בינלאומי עם בעלות־ברית כמרכיב חיוני בהתמודדות עם איומים קיברנטיים, בשל אופיו של

הסייבר כ"חסר גבולות", וכן הגנה על מידע מדיני, ביטחוני, טכנולוגי, מסחרי ופיננסי שנוגע לריבונות הצרפתית והגנה על תקשורת רגישה של גופי מדינה באמצעות הצפנה, כזו שתהיה מספיק חזקה כדי שמרבית הגורמים לא יוכלו לפצח.

לתפיסתה של ממשלת צרפת, התאוששות מפגיעה קיברנטית בתשתיות היא מוגבלת, ולכן היא מעמידה את ההגנה על התשתיות כיעד חיוני, על בסיס חלוקה לקטגוריות הבאות: מגזרים חיוניים לחיי האוכלוסייה, מגזרים הקשורים בתפקוד שלטוני, הפעלת הכלכלה הצרפתית וקיום יכולות הגנה וביטחון לאומיים. ממשלת צרפת רואה באדמיניסטרציה הציבורית אחראית לביטחון המידע על האזרחים המצוי ברשותה, ואשר מוחלף בינה לבין האזרחים לצורך התנהלות שוטפת. בשנת 2010 פורסמו הנחיות להגברת ביטחון המידע הזה, וניתנה עדיפות ליישום ההנחיות. ממשלת צרפת רואה לעצמה חובה להתריע בפני אזרחים ומוסדות אזרחיים על איומי סייבר ולתת להם הנחיה להתגוננות. בטווח הארוך מתכננת הממשלה להטמיע את הערנות לביטחון קיברנטי דרך מערכת החינוך הצרפתית.

הדרך לממש את היעדים הללו היא באמצעות הצעדים הבאים: (א) ניטור, ניתוח, הבנה מלאה וחיזוי של פיתוחים טכנולוגיים, והדרך שבה הציבור יעשה בהם שימוש. (ב) ממשלת צרפת פיתחה מערכת לניטור תקיפות קיברנטיות (detection capability for attacks on information systems) הפועלת בעיקר ברשתות ממשלתיות, ציידה את רשות אבטחת המידע בחדר מצב (Operation-Room) לצורך גיבוש תמונת מצב לאומית וטיפול במקרה הצורך במצב חירום, וקבעה כי הסוכנות הצרפתית לביטחון מידע ורשתות (The French Network and Information Security-Agency (ANSSI) היא הרשות הלאומית האחראית להגנת מערכות מידע. הסוכנות נוסדה ביולי 2007, ועל בסיס צווים מ־2009 ו־2011 היא הרשות הלאומית להגנה וביטחון מערכות מידע. היא משויכת למזכיר הכללי להגנה וביטחון לאומי ונמצאת באחריות ראש הממשלה. (ג) שיפור מתמיד של יכולות טכנולוגיות, מדעיות, תעשייתיות ואנושיות בתחום הקיברנטי. (ד) הגנה על מערכות המידע של המדינה ועל הפעלת תשתיות לאומיות. בסעיף זה מפרטת ממשלת צרפת פעולות קונקרטיות כמו מערכות הצפנה למשרדים וגופים ממשלתיים, מערכת אימות־זהות המבוססת על כרטיסים חכמים. (ה) חיזוק החקיקה הצרפתית הרלוונטית לסוגיה הקיברנטית. (ו) פיתוח שיתוף פעולה בינלאומי בתחום. (ז) הפצת מידע. באחריות ANSSI לתת סיוע וייעוץ נקודתי למקבלי החלטות, כדי שיוכלו להגן על מערכות המידע החיוניות של הארגונים שלהם ועל מערכים טכנולוגיים, מדעיים, מסחריים ופיננסיים.

סין

האסטרטגיה שגובשה בסין לפעילות במרחב הקיברנטי שונה בתכלית השינוי במימוש שלה מזו שתוארה לעיל במדינות המערב (ארצות־הברית, בריטניה וצרפת). במאמרם על לוחמת הסייבר של סין מגיעים סיבוני וי.ר. למסקנה כי הסינים מימשו הלכה למעשה אסטרטגיה שרואה במרחב הקיברנטי ובמרחבים הקינטיים (יבשה, ים, אויר וחלל) חלק ממרחב אחוד, ומזהה את המרחב הקיברנטי כמקום שבו ניתן לפצות על חולשה שקיימת במרחב הקינטי ולאזן יחסי כוחות ביניהם לבין יריביהם המערביים, בעיקר ארצות־הברית.[35] כפי שניתן לראות בעיקר באסטרטגיה המתפתחת, בארצות־הברית קיים עיקרון דומה. גם שם רואים בפעילות קיברנטית חלק אינטגרלי מפעילות בשאר מישורי הפעולה האחרים, ואת הפעילות הקיברנטית כמשתלבת ומשלימה. יחידות הסייבר הסיניות, הצבאיות והלא־רשמיות, פועלות במבצעים תשתיתיים רחבים להשגת נגישות למערכי תקשורת ותשתיות, במגמה להשיג מידע ומימוש שליטה למטרות אפשריות של פגיעה בעת הצורך. המטרות העיקריות נמצאות בארצות־הברית, ואופי הפעילות שנותחה (פעילות שהתגלתה ודווחה באמצעים גלויים) הביאה את המחברים למסקנה שהסינים הפנימו חולשה צבאית ומדינתית בהתמודדות קינטית עם ארצות־הברית, הבינו את התלות המוחלטת של ארצות־הברית במערך הקיברנטי המתקדם שלה וזיהו אותו כפוטנציאל לפגיעה, שיביא בעת עימות לפיצוי כלשהו על חולשתם של הסינים במאזן היכולות הכולל שלהם מול האמריקאים. בפירוט ההתקפות הסיניות ניתן להתרשם כי היעדים הסיניים הם תשתיתיים, לדוגמה, תקיפת Google במטרה להשיג נגישות למערך הסיסמאות ולבקרת פיתוח הגרסאות של החברה, תקיפת חברת RSA לשם השגת נגישות למאגר ה־SecureID, שהיה מאפשר לסינים מימוש התקפות ביתר קלות על כל החברות המקבלות שירותים מ־RSA, וגל התקיפות בשנים 2011–2006 על יעדים מערביים, ובכלל זה מערכי ממשל, תשתיות נפט וגז, תשתיות תקשורת, תעשיות ביטחוניות, חברות מחשבים ואלקטרוניקה ומוסדות פיננסיים.

ארגונים בינלאומיים (OECD, ENISA, European Union)

ה־OECD (Organization for Economic Co-operation and Development) עוסק בסוגיית אבטחת מידע ובהיבטי ביטחון סייבר זה למעלה מעשרים שנה. ב־2012 פרסם הארגון דוח על אסטרטגיית ביטחון סייבר חדשה בחלק ממדינות הארגון (הדוח התבסס על נתונים מעשר מדינות שהסכימו להשתתף).[36] ליבת האסטרטגיה החדשה היא הגנה על החברות המפותחות התלויות במרחב הקיברנטי, וזאת מבלי לפגוע בחופש היוזמה ובמנועי הצמיחה שהאינטרנט מאפשר. האסטרטגיות שגובשו במדינות מעודדות שיתוף פעולה בין ממשלות ברמת המדיניות, ברמה האופרטיבית ובהבהרת התפקידים והאחריות של הגופים השונים, בחיזוק שיתוף הפעולה בין המגזר הפרטי

למגזר הממשלתי ובהדגשת הצורך לכבד ערכים כמו פרטיות, חופש הדיבור וזרימה חופשית של מידע. חלק מהאסטרטגיות מאמצות גישה גמישה וזריזה יותר בשל אופיו של התחום, ומדגישות את הממד הכלכלי כדומיננטי במדיניות ההגנה בסייבר, חלקן כוללות דיאלוג עם בעלי עניין בתחום הסייבר, הן לצורכי קביעת מדיניות והן למימוש המדיניות הזו. במסגרת האסטרטגיות החדשות יש השקעה רבה יותר במחקר ופיתוח, ניטור של תשתיות לאומיות וזיהוי תקיפות בזמן אמת, רתימת התעשייה הרלוונטית והמוטיבציה הכלכלית כמנועים ליצירת מערכות ביטחון סייבר, עידוד של שיתוף פעולה עם ספקיות אינטרנט ויצירת תרגילי ביטחון סייבר יזומים.

ארגון ENISA (European Network and Information Security Agency) פרסם אף הוא במאי 2012 דוח על מצב ביטחון הסייבר בחלק מהמדינות החברות בו – דוח שנסמך על איסוף נתונים לצורך חיבור מדריך מעשי לביטחון סייבר למדינות הארגון.[37] הארגון קובע שאין הגדרה מוסכמת לביטחון סייבר, לא באיחוד האירופי ולא מחוץ לו – עובדה המאיימת על שיתוף הפעולה הבינלאומי שנחיצותו מוסכמת על ידי כולם. בדוח מפורטים הנושאים שניתן למצוא ברוב האסטרטגיות לביטחון סייבר (נושאים מוכרים וטריוויאליים). הארגון קובע כי נכון לתאריך פרסום הדוח אין לאיחוד האירופי אסטרטגיית ביטחון סייבר, אבל הוא מתכוון לייצר עבודה עם קווים מנחים לאסטרטגיה כזו. הדוח ממליץ למדינות הארגון לייצר אסטרטגיה לאומית לביטחון סייבר.

האיחוד האירופי פרסם בפברואר 2013 (באמצעות ה־European Commission and High Representative of The European Union for Foreign Affairs and Security Policy) מסמך בנושא אסטרטגיית ביטחון סייבר למדינות האיחוד האירופי – מרחב קיברנטי פתוח ובטוח.[38] המסמך מונה את הערכים שלפיהם יש לבנות את האסטרטגיה, וקובע כי אותם ערכים שיש לאיחוד האירופי בעולם הקינטי תקפים גם בעולם הקיברנטי, כמו הגנה על זכויות יסוד, חופש ביטוי, הזכות למידע אישי ופרטי, גישה חופשית לכולם למידע ואינטרנט, ניהול אפקטיבי ודמוקרטי של הממד הקיברנטי על ידי בעלי עניין (לא ממשלתיים) ואחריות משותפת להשיג ולהבטיח ביטחון. הוועדה קובעת חמש עדיפויות לאסטרטגיה: השגת חוסן קיברנטי (cyber resilience), הפחתה משמעותית של פשעי סייבר, פיתוח מדיניות ויכולות הגנת סייבר הקשורות במדיניות הביטחון וההגנה הכללית, פיתוח התעשייה והמשאבים הטכנולוגיים הרלוונטיים להגנת הסייבר, בניית מדיניות קיברנטית בינלאומית קוהרנטית שבמסגרתה יקודמו הערכים של האיחוד האירופי. הוועדה קובעת שמימוש האסטרטגיה צריך להיעשות בעיקר על ידי הממשלות, ואין מקום להפעלה ריכוזית של מימוש האסטרטגיה הזו באיחוד. עם זאת, בשל האופי חוצה הגבולות של המרחב הקיברנטי והאיומים בסייבר, מוגדרת במסמך אחריות גם לגופי האיחוד האירופי במסגרת מימוש האסטרטגיה.

הגנה והרתעה

בדומה לעולה ממאמרם של אבן וסימן טוב, גם לדעתם של אורבוך וסיבוני הולכת ומתפוגגת האפקטיביות של מערכי ההגנה הקלאסיים, המבוססים על היכרות מקדימה של קוד מפגע, משום שהתוקפים למדו לעקוף את החתימה של מערכות האנטי־וירוס למיניהן, ולפיכך הם ממליצים על מערכות גילוי מבוססות אנומליה.[39] הטכניקה היא לימוד בשיטות שונות של ההתנהלות הנורמטיבית של הקוד המוכר כחיובי או דגימה מייצגת שלו, וכתיבת אלגוריתם המזהה את החריגה מהתנהלות הנורמטיבית הזו. ניתן להשתמש במערכות מבוססות אנומליה הן כמרכיב לזיהוי ומניעה בזמן אמת, בשערי הרשת המוגנת, והן כמרכיב לזיהוי קוד מפגע מורדם, שהוחדר לרשת והוער לפעילות במועד מאוחר יותר. האופן השני לשימוש במערכת מבוססת אנומליה מחייב מערכת המעבדת לוגים של מידע ונתונים על הנעשה במחשבים ובשרתים השונים ברשת המוגנת לפרקי זמן ארוכים, ומאפשרת מחקר של התופעות החריגות (SIEM - Security Information and Event Management). היקף החומר המטופל והנחקר הוא גדול מאוד (Big Data), ויש כלים ושיטות לטפל בו באופן שיאפשר את זיהוי האנומליות. נקודת התורפה של השיטה היא התרעות False Positive (התרעות שווא) רבות שמאיימות לעקר את האמינות והאפקטיביות של המערכת, והתרעות False Negative (התרעות אמת שהוחמצו) הנובעות מלימוד חלקי של השגרה או מעיבוד שגוי של הנתונים. נקודת העוצמה בטכנולוגיה זו היא היותה מנותקת ובלתי־תלויה בהיכרות ובחתימה מוקדמת של קוד מפגע כזה או אחר.

בן־ישראל וטבנסקי הציגו את האתגרים שמציב העידן הקיברנטי מול תפיסות הביטחון הקינטיות המקובלות.[40] היכולת לזהות את התוקף ולראות בפעילותו הקיברנטית אקט מלחמתי המאפשר תגובה על פי חוקי המלחמה בעייתית מאוד. היכולת להתגונן בעייתית אף היא, משום הקושי באבחנה בין תקיפה קיברנטית לתקלת מחשבים, ובשל הצורך להחזיק מערך הגנה יקר ומעודכן לאורך זמן. מושג ההרתעה בעייתי אף הוא, משום שהוא מותנה בזיהוי הגורם התוקף. זוהי פעולה קשה מאוד, בשל המבנה והתכונות של המרחב הקיברנטי העולמי, ובמקרה שזוהה מקור ההתקפה, הרי הסבת נזק נגדי למחשבים שמהם יצאה ההתקפה, ללא יכולת מוכחת לבדוק ולוודא את הנזק שהוסב למחשבים הללו, מפחיתה בצורה משמעותית את יכולת התרעה כמרכיב בבנייתה של תפיסת ביטחון קיברנטי.[41]

כהן מתאר בעבודתו[42] את האיום ככזה הנשקף לישראל ממדינות כמו סין, איראן ורוסיה, ובאופן פוטנציאלי גם מארגוני הטרור.[43] בדומה לאבן וסימן טוב, גם כהן מחלק את ההגנה לכזו הניתנת למושאי הגנה בקטגוריות השונות ולכזו המהווה הגנה מרחבית, המבוססת על לחימה בפשעי סייבר, על השגת מודיעין על ידי קהילת המודיעין ועל גוף מרכזי לניהול המערכה, שאותו הוא ממליץ להקים במסגרת צה"ל.[44]

התמודדות עם איומי חומרה

לדעת Pierluigi Paganini ההתמודדות עם איומי חומרה/קושחה אפשרית, ולו חלקית, על בסיס צעדים משבשים ומטעים, המונעים את הפעלת התקיפה.[45] יש לשקול טכנולוגיות "Power Resets" המונעת מרכיבים בעייתיים לחשב כמה זמן הם פעילים, כדי למנוע תקיפות מבוססות טיימר, או טכנולוגיית "Data Obfuscation" המבצעת הצפנה של מידע וערכים המוזנים לרכיבים בעייתיים כך שלא יוכלו לקבל קודים מיוחדים, או להיות מופעלים על בסיס זיהוי מידע או "Sequence Breaking" המבצעת שבירה/ערבול של רצף מסרים באופן אקראי, כך שיימנע מרכיבים בעייתיים לזהות תבניות מידע ולהפעיל תקיפה על בסיס תבניות אלה.

הרתעה

סוגיית ההרתעה בסייבר מאתגרת, לדעת אמיר לופוביץ, בעיקר משום ששלושת המרכיבים המרכזיים בהרתעה הידועה ממודל המלחמה הקרה אינם מתקיימים במרחב הקיברנטי בצורה דומה.[46] המחבר מבדיל בין הרתעה מתוך ענישה שתפקידה לגבות מהתוקף מחיר גבוה מהרווח שיש לו כתוצאה ממימוש ההתקפה, לבין הרתעה מתוך מניעה, שתפקידה לגרום לתוקף תחושה שממילא ההגנה של המגן חזקה מדי והוא צפוי להיכשל בתקיפתו, ולפיכך הוא יימנע מראש מביצועה. בהתרעה מתוך ענישה, המרכיב המרכזי של יכולת גביית מחיר מהתוקף או המאתגר אינו מובטח בעולם הקיברנטי, עקב הקושי לזהות את התוקף ומשום שלחלק מהתוקפים, בין אם הם יחידים ובין אם הם ארגונים/מדינות, אין בחלק מהמקרים מערך מחשבים ומידע מפותח דיו כדי לממש בו פגיעה מרתיעה. בהקשר זה מוצע במאמר להשתמש בהרתעה שאינה קיברנטית מפני מתקפת סייבר, ובכך ניתן להתגבר על המכשלה הנקודתית הזו. מרכיב שני הוא אמינות המגן. המגן חייב לממש את איומו להגיב כדי ליצור הרתעה. אם המגן חושש משרשרת תגובות הנגד שיבואו אחרי תגובתו, הוא עלול להימנע מפעולה ובכך תיפגע אמינותו. בנוסף, תגובה לא מידתית עלולה לגרור הקמת קול זעקה בינלאומי שיביא את המגן למתן את תגובתו, ובכך תיפגע אמינות ההרתעה שלו. המרכיב השלישי הוא היכולת להעביר את האיום באמצעות ערוץ תקשורת אמין ומוסכם בין היריבים. החולשה בנקודה זו היא הכשל המרכזי בגין חוסר היכולת לזהות את התוקף, בוודאי במועד מקדים לתקיפה, הרלוונטי למימוש הרתעה. הרתעה מתוך מניעה מחייבת מערך הגנתי אפקטיבי, שהתוקף יודע על קיומו ומבין את הקושי הקיים במימוש התקפה נגדו.

התקפה

בהקשר לתקיפה ראוי לבחון את הניתוח שמציע ראלף לנגנר לתקיפת ה־Stuxnet.[47] לנגנר מצביע על תקיפה במאפיינים הבאים: התקיפה הכילה שני חלקים. התקיפה בחלקה הראשון הייתה חשאית, ואופן מימושה נועד להשיג מטרה ממוקדת שאינה הרס המוני ומיידי של מערך הצנטריפוגות האיראני.[48] במהלך התקיפה בוצעה החלטה לעבור מטקטיקת פעולה זו לטקטיקה שנועדה להפיל כמות גדולה של צנטריפוגות, גם במחיר חשיפה של התקיפה, והתקיפה שונתה בהתאמה.[49] לנגנר מתאר את אפשרות השימוש שנעשה בקבלנים (Contractors) שהיו קשורים למערך בנתנז, כדי להביא את הנוזקה לתוך המחשבים הרלוונטיים.[50] בנוסף לנזק שתוכננה הנוזקה לגרום בנתנז, לנגנר מתאר במאמרו את ההתקפה ככזו שנועדה גם להביא מידע. העובדה ש־Stuxnet דילגה למערכים נוספים אפשרה, לדבריו, לתוקפים לבחון את המערכים הללו כאפשרות לקבלת מידע על קבלנים הקשורים לנתנז, ואולי אפילו קשר למתקני גרעין חשאיים של איראן.[51]

בניגוד לחידוש שרואה ראלף לנגנר באופן מימוש תקיפת Stuxnet, מביע ג'יימס לואיס ביקורת על הרואים בכלים Stuxnet ו־Flame בשורות חדשות או מחדשות בתחום הלוחמה הקיברנטית.[52] לואיס מנתח את ה"רעש" שנוצר בעקבות חשיפת הכלים הללו כחלק ממערכה פוליטית שמאחוריה עומדת רוסיה – מערכה שמטרתה צמצום היתרון של ארצות־הברית בטכנולוגיה קיברנטית. לואיס אינו רואה הבדל עקרוני בין כלי תקיפה שעיקר מטרתם ריגול ואיסוף מידע לכלי תקיפה שנועדו לחולל הרס. הפעולות הבסיסיות הנדרשות לריגול או להרס הן אותן פעולות של איסוף מודיעין ורכישת חזקה בתוך רשת מחשבים. התפיסה שניתן לבצע פעולה קיברנטית בעלת השלכה קינטית הרסנית אף היא אינה חדשה, לפי הניתוח של לואיס. המתקפות של רוסיה על אסטוניה וגיאורגיה הן דוגמה למימוש אסטרטגיה כזו, הגם שנעשתה באמצעות שלוחים (Proxy). על פי לואיס, השימוש ב־Stuxnet אינו מהווה עידן חדש מבחינה נוספת – הוא לא יוביל למתקפה קיברנטית מתוחכמת והרסנית על ארצות־הברית, בשל החשש שמתקפה שתגרום נזק קינטי של ממש תביא לתגובה אמריקאית קינטית עוצמתית. בכך תורם לואיס גם לדיון על ההרתעה, ובעצם גורס כי קיימת התרעה המשלבת את שני העולמות – הקיברנטי והקינטי – לתוך משוואת מאזן כוחות אחת.

התקפה במסגרת עימות גלוי

להבדיל מהתקיפה חשאית, ניתן לבחון מתקפה קיברנטית גלויה כחלק מעימות כוח גלוי, דוגמת הלחימה בין גיאורגיה לרוסיה ב־2008. בניתוח המתקפה הרוסית על גיאורגיה מצביעים Ronald J. Deibert, Rafal Rohozinski and Masashi Crete-Nishihata על אסטרטגיה רוסית לשימוש במרחב הקיברנטי לצורכי מלחמה על התודעה, הנרטיב,

המידע לציבור, המורל הלאומי ודעת הקהל, וכל זאת כחלק ממאבק קינטי א־סימטרי שהם ניהלו לטובת האינטרס הלאומי הרוסי על חבל ארץ שנוי במחלוקת.[53] השימוש במרחב הקיברנטי היה חלק מהמערכה תודעתית רחבה, שהייתה חלק מהמערכה הקינטית הכוללת לסילוק הריבונות הגיאורגית משטחי חבל אוסטיה. הרוסים, לדברי המחברים, הבינו את חשיבות המערכה התודעתית בעידן המידע כבר במלחמות בצ'צ'ניה, כאשר במלחמה הראשונה (1994) הם הפסידו במערכה על הנרטיב. את הלקחים ניתן לראות בכלל המאבקים שניהלו הרוסים מאז. במלחמה בגיאורגיה ניהלו הרוסים מערכה שכללה שיתוק המערכים הפיזיים (ניתוק סיבים אופטיים שדרכם עברה התעבורה הבינלאומית של גיאורגיה), שליטה בתעבורה הגיאורגית (ניתוב תעבורה דרך רוסיה עצמה), חסימה של שידורים גיאורגיים במטרה שלא לאפשר לראשי המדינה לפנות לציבור, שידור מסרי הסברה רוסיים באתרים גיאורגיים, ברחבי מדינות חבר העמים ולמדינות המערב, ולבסוף – שיתוק אתרים ושרתי אינטרנט גיאורגיים במתקפת DDoS מסיבית, שהביאה לכך שמשרד החוץ, משרד הנשיאות, שירותים שונים ובכללם המערך הבנקאי שותקו לפרקי זמן של שעות, ולא הצליחו להוות תשתית מתפקדת. הניסיונות של הגיאורגים להילחם במערכה הזו קצרו הצלחה חלקית בלבד. הרוסים לא היססו להרחיב את המתקפה הקיברנטית שלהם גם לאתרים מחוץ לגיאורגיה שניסו לסייע לממשלת גיאורגיה, כולל תקיפה של אתר אירוח (Hosting) אמריקאי שסיפק שירות לממשלה הגיאורגית. במסגרת מימוש האסטרטגיה רומזים המחברים כי נעשה שימוש בארגוני Proxy ובכללם ארגוני פשיעה רוסיים (אין בנמצא עדות למעורבות ישירה של ממשלת רוסיה במתקפות אלה), וכן, ככל הנראה, באזרחים תומכי רוסיה שמימשו התערבות קיברנטית על דעת עצמם.

תקיפה קיברנטית כחלק מתוכנית אופרטיבית במלחמה

מדינות מכינות עצמן למימוש פעילות התקפית במרחב הקיברנטי כחלק מובנה מהתוכניות הצבאיות האופרטיביות שלהן. הדוגמאות שהובאו כאן מלמדות ששלוש מעצמות לפחות (ארצות־הברית, רוסיה וסין) רואות בכך חלק מהאסטרטגיה של פעילותן במרחב הקיברנטי, וכפי שנכתב, סין מכינה, ככל הנראה, תשתית לפעילות כזו לעת חירום, ורוסיה מימשה את האסטרטגיה הזו עבור פרק לוחמת התודעה והמידע במלחמה עם גיאורגיה.

בהקשר זה ראוי להתעכב פעם נוספת על התפיסה האמריקאית. אמנם אין דוגמה של ממש שתעיד על מימוש האסטרטגיה הזו, אולם על פי מפקדי פיקוד הסייבר האמריקאים, אלכסנדר ורוג'רס, הפיקוד בונה את הכוח ודוחף לכך שפעילות קיברנטית תהיה חלק אינטגרלי בכל תוכנית אופרטיבית של פיקוד לוחם של צבא ארצות־הברית, בדיוק כמו תמרון יבשתי, ימי או הפעלת כוח אווירי. הפעילות הקיברנטית תהיה חלק

ממערך ההחלטות הפיקודיות־מבצעיות שיידרש לקבל מפקד הפיקוד, ולפיכך הוא נדרש להבין את הכוח שיש בידיו, את ההשלכות של הפעולות שיורה או יאשר לבצע, את היכולת של המטה הכללי לסייע לו ואת האופן שבו הפעילות הקיברנטית מסייעת לו בהשגת מטרות הלחימה. במקביל, מפקד אמריקאי יהיה חייב להבין את הסכנות הנשקפות לו מפעילות עוינת במרחב הקיברנטי, ואת הדרכים להתגונן מפני פעילות כזו. בצבר עדויות שמציגים אלכסנדר ורוג'רס הם מדברים על קבוצות קיברנטיות התקפיות שמתוכננות להיות במסגרת הפיקודים הלוחמים, ועל תפיסת שליטה ובקרה בהקשר של תמונת המצב הקיברנטית בפיקוד הלוחם, ובינו לבין פיקוד הסייבר.[54] חזונו של אדמירל רוג'רס הוא שהשימוש בסייבר – למטרות תקיפה ומגננה – יהיה חלק מובנה, בלתי־נפרד וטבעי ממכלול הכלים של המפקד, והוא ינהל ויתמרן אותו כמו שהוא מתמרן כוחות יבשה, בצורה משולבת ובתפיסה רחבה יותר של הפעלת כוח. זאת, תוך שימוש ברשת משותפת (joint-network backbone) לכל הכוחות.[55] בהזדמנות אחרת הסביר רוג'רס שיש לוודא פיתוח תפיסה מבצעית ומבנה פיקוד ושליטה, שיהפכו את המבצעים בסייבר למציאות מבצעית.[56]

השוואה בין מסמכי אסטרטגיה של מדינות שונות

ההשוואה בין מסמכי האסטרטגיה נעשתה מתוך הפרסומים הגלויים שנלמדו לצורך כתיבת מסמך זה.

	הגנה	התקפה	הרתעה	בניין כוח	ארגון ותהליכים	הסדרה משפטית	שת"פ בינלאומי
ישראל	הממשלה קיבלה המלצות על מיזם של המועצה למחקר ופיתוח שכותרתו "התמודדות עם האיום הקיברנטי".	אין אזכור ו/או התייחסות. מיוחסות לישראל יכולות תקיפה, וכן במשותף עם ארצות־הברית – תקיפת Stuxnet.	אין אזכור ו/או התייחסות.	קיימת התייחסות נרחבת בסיכום המיזם לבניין כוח טכנולוגי ואנושי.	קיים דיון גלוי לצד מספר החלטות ממשלה על חלוקת האחריות בין הארגונים בנושא הסייבר. הוקם המטה הקיברנטי והוחלט על הקמת רשות הגנה לאומית בסייבר. עוד הוחלט לאחרונה על הקמת זרוע סייבר בצה"ל.	אין אזכור ו/או התייחסות.	אין אזכור ו/או התייחסות.
ארצות־הברית	עיסוק אינטנסיבי ברמת ממשל	המרחב הקיברנטי נתפס כחלק והמשך של העולם הקינטי. קיימת תוכנית להטמעת יכולות של תקיפת סייבר בפיקודים הצבאיים, כחלק מכל תוכנית אופרטיבית, והצבת קבוצות תקיפה בפיקודים הללו. לארצות־הברית מיוחסת תקיפה במסגרת לחימה חשאית בגרעין האיראני (Stuxnet)	דיון רחב בסוגיה ־ האם ניתן לממש הרתעה בסייבר ללא עדויות למימוש ניסיונות להרתיע, למעט המקרה של התקיפה על צפון־קוריאה, בעקבות ההתקפה על Sony.	מהלך רחב לבניין כוח בהובלת משרד ההגנה ובהשתתפות משרדי ממשל וסוכנויות רלוונטיות. בניין הכוח כולל הפניית משאבים כספיים, הון אנושי, הכשרה, תו"ל וכלים.	ריבוי ארגונים הפועלים במרחב הסייבר האמריקאי עם תחומי חפיפה ביניהם. ניכר שהמבנה בהיבטי אחריות וסמכות טרם התייצב, אך קיים דיאלוג. תהליכים מצויים בשלבי הסדרה, הן בגופי הביטחון והצבא והן במגזר הממשלתי והאזרחי.	טרם מומשה. נמצאת בדיון במתח שבין ההגנה על זכות לפרטיות בעידן שאחרי סנודן לבין ההבנה שבלא נתונים על המגזר הפרטי/אזרחי, קשה יהיה להגן על הנכסים החיוניים של ארצות־הברית.	קיים כמרכיב משמעותי בתפיסה.

סין	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.
	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.
ארגונים בינלאומיים[57]	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.
צרפת	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.	אין מידע.

רוסיה[58]	אומנם: יש ערוץ קשר – אולי בעיקר מפני שהאמריקאים מעוניינים בכך.	מדינה	מדיניות הגנת הסייבר: מדיניות הגנת הסייבר הרשמית של רוסיה מתמקדת בעיקר בהגנה על תשתיות מידע קריטיות.	אומנם: יש ערוץ קשר – אולי בעיקר מפני שהאמריקאים מעוניינים בכך.	מדינת יחיד	אומנם: יש ערוץ קשר – אולי בעיקר מפני שהאמריקאים מעוניינים בכך.	מדינת פריפריה

הגנה

היעד המרכזי של אסטרטגיית הגנה לאומית בסייבר הוא לשמר את התפקוד הבסיסי של המדינה, שעלול להיפגע מתקיפה במרחב הקיברנטי. במילים אחרות: שימור הרציפות התפקודית של המדינה. יעד חשוב נוסף הוא לאפשר לגורמים הרלוונטיים במדינת ישראל להחליט ולממש פעולות במרחב הקיברנטי והקינטי נגד יריבים ואויבים, מתוך הכרה שניתן להגן על המרחב הקיברנטי מפני פעולות תגובה אפשריות. עם זאת, מימוש של כל אסטרטגיה לא יביא לתוצאה הרמטית של סיכול כל ניסיון תקיפה, מכל סוג ולכל מטרה, על כל מושא הגנה. לא ניתן להביא לתוצאות הרמטיות בהגנה, ולפיכך יהיו מתקפות במרחב הקיברנטי שיצליחו למרות הקווים המנחים לאסטרטגיית ההגנה שיוצעו כאן.

במסמך זה מוגדר סיכול התקפה במרחב הקיברנטי כמניעת השגת מטרתו של התוקף. המטרה אינה הגנה על המחשבים או הרשתות ואינה בהכרח סיכול ההתקפה. האבחנה הזו משמעותית משום שהיא עשויה לאפשר מרחב תמרון גדול יותר למגן, בבואו לתכנן אסטרטגיית הגנה ולבחור כלים עבורה. מוצע להבדיל באסטרטגיית ההגנה בין שלושה סוגי מתקפות: מתקפת עומק (APT), שהיא מתקפה מתוכננת לעומק מערך המחשבים של ארגון לפרק זמן ארוך יחסית, וכוללת מאמץ להסתרה. הסוג השני הוא מתקפה מהירה ושטחית, שהיא מתקפה שתוצאותיה נראות מייד ובדרך כלל יעדיה הם גרימת שינוי באתר, או מניעת גישה אליו ולשירותים שהוא מציע במרחב הקיברנטי (DDoS, Defacing). אף שהמתקפה הזו נראית שטחית ותוצאותיה לרוב מוגבלות בזמן ומשפיעות על תחום התודעה, הפעלה אינטנסיבית של הכלים הללו לאורך זמן על מגוון יעדים במדינה תשבש בצורה מהותית את שגרת החיים, והיא עלולה לגרום נזק גם בהיבטים שמעבר למורל. לבסוף קיימת מתקפת תשתית שהיא תקיפה על רכיבי חומרה או קושחה,[59] הן לצורכי השבתה (CNA) והן במטרה לאפשר נגישות עתידית למחשב/רשת.

בהקשר למתקפות עומק, מוצע להתבסס על שילוב בין כלים ויכולות שאינם מחייבים מידע והיכרות מוקדמים של רכיבי ושיטות התקיפה, יחד עם כלים ושיטות הגנה קיימים שאותם מוצע להמשיך לפתח. קו מנחה זה הכרחי אך אינו עומד לבדו. הגנת סייבר יעילה צריכה להתבסס על קווים מנחים נוספים ובהם שקיפות בדיווחים על תקיפות בין ארגונים, בניית הערכת מצב קיברנטית לאומית שוטפת ורחבה, בניית

גופי תגובה מהירה, שימוש בנתוני מחקר ולימוד על כלי תקיפה ועל קבוצות תקיפה, שיתוף עם ארגוני הגנה ומודיעין מסחריים, שיתוף פעולה בינלאומי היכן שניתן וכדאי, פיתוח איסוף מודיעיני מתמיד על אויבים ויריבים לצורך התרעה, גיבוש תוכנית לתגובה קיברנטית כחלק מממד הרתעה אפשרי ופיתוח יכולת התאוששות מתקיפה במקרים שהדבר ניתן, מתוך ההבנה שקו ההגנה לעולם ייפרץ, ולכן יש להתארגן לשיקום מהיר כתוצאה ממתקפות מוצלחות של האויב.

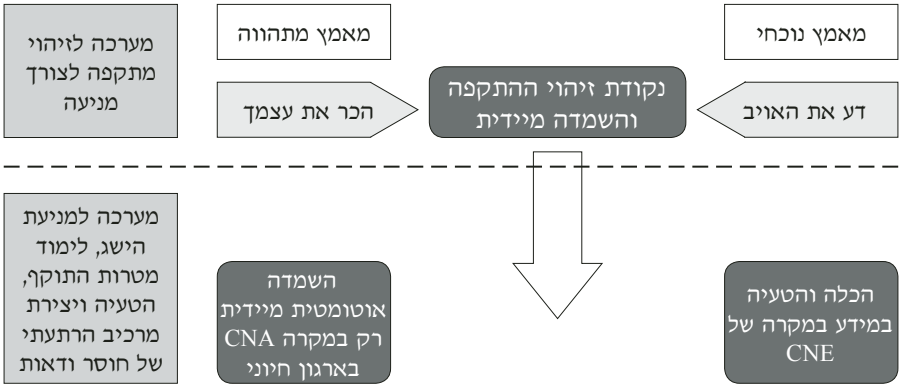
המענה למתקפת עומק (APT)

התמודדות עם סוג זה של תקיפות מבוססת על מספר הנחות: הראשונה היא שרוב הארגונים זקוקים לחיבור במאפיינים שונים למרחב הקיברנטי הציבורי, ולפיכך כל הרשתות מאוימות בתקיפה, כולל אלה המוכרזות כמנותקות לכאורה מהמרחב הקיברנטי החיצוני. השנייה היא שהתוקף יתקוף בנקודה הנוחה לו, קרי, הנקודה המוגנת פחות. נקודת התקיפה עלולה להיות גורם ב"שרשרת האספקה", כלומר, ארגון חיצוני העומד בקשר עם הגוף המוגן, אך אינו מוגן כמוהו. הנחה נוספת היא שהתוקף עלול לממש את התקיפה באמצעות כלים שנשתלו במוצרי המחשב מבעוד מועד, אפילו כבר בתהליך הייצור שלהם, ובהמשך התוקף יעדיף ליזום תקיפות השונות מאלה שזוהו ונחקרו, הן בבחירת כלי תקיפה והן במימוש שיטת התקיפה. לבסוף, יש להניח שלמגן לא יהיה המודיעין הנדרש על התקיפה – זהות התוקף, מיקומו הפיזי, המוטיבציה והמטרות שלו, כלי התקיפה והשיטה ומועד התקיפה.

בתכנון מערך ההגנה נדרש לתת מענה לנגזר מההנחות שפורטו לעיל, ולכן ככלל, על ההגנה להיות מתוכננת ברצף, מנקודות הקצה ברשת של הארגון המאובטח ועד לאחרון הארגונים הקשורים בדרך כלשהי למערך המחשבים שלו, כך שאופן ההגנה על ארגון רגיש העוסק בביטחון המדינה צריך להיות זהה לאופן ההגנה על רשת המחשבים של הארגונים שבאים איתו במגע קיברנטי. קו מנחה נוסף הוא גילוי התקיפה בנקודה המוקדמת ביותר האפשרית, ומערך לטיפול בהתקפה באופן מחושב, לומד ומגיב. זאת בשונה מעצירה מיידית ואוטומטית של ההתקפה. במערך הגילוי מוצע לשכלל את שיטות התנהלות ואת הכלים מבוססי מודיעין וניתוחי סטטיסטיקה הקיימים, ולשלב יכולת המבוססת על זיהוי תקיפה ללא חתימה מוקדמת, או כל מודיעין אחר.

כקו מנחה לטיפול מועדף בתקיפה מוצע לנקוט "הכלה" של התקיפה ככל שניתן, כשהגבול להכלה הוא הגעה לנקודה שבה התוקף עלול להשיג את מטרתו. ההכלה נועדה לאפשר לימוד של התקיפה, הכלים, המטרה ואם אפשר – גם את זיהוי התוקפים. במסגרת זו נדרש לבחון סיכול של התקיפה במגוון דרכים, ולאו דווקא השמדה מיידית של הכלי התוקף. גישה כזו רלוונטית בעיקר כשמטרת ההתקפה היא גניבת מידע,

וזאת, באופן שהתקיפה תהיה תחת שליטה ויבוצע מעקב מצד המגן מבלי שהתוקף יודע זאת. ראו בהקשר זה התרשים להלן.



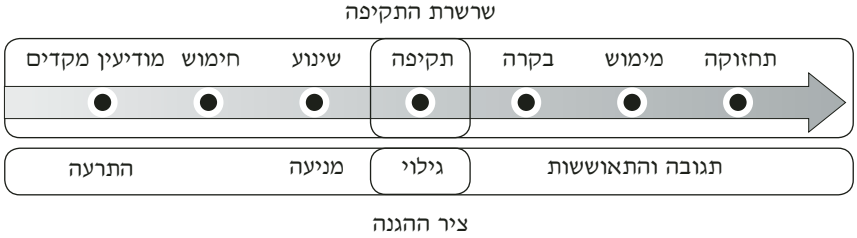
איור 3: תפיסת ההתמודדות עם תקיפות APT

חלקו העליון של התרשים לעיל, מעל לקו המקווקו, מתאר את מערך הגילוי. גילוי תקיפה הוא נקודה משמעותית בכל הנוגע לפעילות הקשורה למתקפת עומק במרחב הקיברנטי. התוקף ישקיע מאמצים ניכרים כדי שלא להתגלות מוקדם מדי, והמגן ישקיע כדי לגלות את המתקפה הזו מוקדם ככל האפשר. עצם הגילוי והזיהוי של התקיפה בנקודת זמן מוקדמת מאפשר יתרון של ממש למגן, אך אינו הכרחי. מתפתחת תפיסת הגנה הגורסת כי יש להניח שהתוקף הצליח במשימתו, ורשת הארגון מכילה תוכנה מזיקה. מה שנדרש הוא לאמץ דפוסי פעולה ויכולות טכנולוגיות המאפשרות למגן לשבש ולסכל את השגת מטרתו של התוקף בנקודות שונות, גם מבלי שזיהה את התקיפה בשלב מוקדם.[60]

היכולת הנפוצה כיום לגילוי וזיהוי תקיפה תלויה במידה רבה במידע מקדים, על משקל: "דע את האויב". המידע כולל היכרות עם קוד הכלי התוקף או חלק ממנו, ו/או היכרות עם דפוסי הפעולה של קבוצת תקיפה או של תוקף ספציפי. מידע זה הוא, לרוב, תוצר של ניתוח כלי תקיפה, קבוצות תקיפה ותוקפים בודדים המבוצע על ידי חברות הגנה ומודיעין במרחב הקיברנטי, ושל שיתוף מידע בין החברות הללו לארגונים המוגנים. ברמה גבוהה יותר מכיל מידע זה ניתוח סטטיסטי ואלגוריתמים התנהגותיים (behavioral algorithms) למציאת מאפיינים של תקיפות ללא אינדיקציה נקודתית לתקיפה.[61] זהו בסיס רחב וחזק, המבוסס על יכולות קיימות ומתפתחות למימוש מרכיב הגילוי הראשון במערך הגילוי המוצע כאן. בארגונים המהווים יעד להגנה בישראל ניתן וצריך לשכלל את המרכיב הזה על ידי הטמעה בתוכו של מידע

הנמצא בידי שירותי המודיעין של ישראל, וכמובן, מידע רב ורחב הנמצא בידי חברות הגנה ומודיעין מסחריות בכל העולם. המידע צריך להתעדכן קרוב ככל האפשר לזמן אמת, ולספק התרעה על כל איתור של פעילות חשודה.

המחשה גרפית של תפיסת ההגנה ניתן לראות גם בתרשים להלן. בתרשים זה מוצג תהליך הגנה המתייחס למרכיבים שונים בציר בשרשרת התקיפה. בהמשגה זו מחולק תהליך התקיפה לשבעה שלבים.[62] מול שלבים אלה ניתן להציב ארבעה מרכיבים בהגנה: התרעה מוקדמת, פעולות למניעת המתקפה, גילו המתקפה עם התרחשותה, תגובה למניעת נזקי המתקפה ולבסוף פעולות התאוששות במטרה לחזור לתפקוד מלא, אם נכשלו הפעולות למניעת נזקי המתקפה.



איור 4: ציר ההגנה מול שרשרת התקיפה

קו הגנה כזה זקוק למבנה תומך דוגמת CERT[63] ו־CSOC[64] ארגוני, ולתהליכי עבודה מתאימים. אופטימיזציה למרכיבים שונים של ההגנה ברמת הכלים, המודיעין, שיתוף הפעולה, השקיפות, זמן ואיכות התגובה ומקצועיות ה־CERT/CSOC הארגוני אינם מותרות או בחירה. האפקטיביות של קו הגנה זה אינה מובנת מאליה ואינה מובטחת. היא מותנית בעדכון ובשכלול מתמידים, משום שהמרדף התמידי שמתנהל אחרי כלי התקיפה הוא ממצב של נחיתות מובנית, ורק התנהלות מיטבית או קרובה לכך תקנה לקו ההגנה הזה רלוונטיות לאורך זמן, המצדיקה את ההשקעה בו.

כדי לוודא שניתן לזהות תקיפה מתוכננת וממוקדת שאין לגביה מידע מוקדם, יש להשתמש בטכנולוגיה שאינה מבוססת על היכרות מוקדמת ועל חתימה של כלי התקיפה או של התוקפים.[65] כבר ניתנה דוגמה לחשיבה מסוג זה בתיאור מוצר המבוסס על ניטור ובדיקה של נקודות היציאה ברשת הארגונית.[66] טכנולוגיה שאינה מבססת עצמה על הכרת התוקף, הכלים שלו והשיטות שלו מחייבת הכרה מעמיקה של התהליכים "החוקיים" במחשבי הארגון המוגן, ובדיקה של כל פקודה/תהליך מול שגרה ידועה מראש. בהנחה שקוד תקיפה יתקשה לדמות את הפעילות "החוקית", הוא יזוהה כקוד המבצע פעילות "לא חוקית", בלי קשר להיכרות מוקדמת של המגן עם הקוד התוקף. העוצמה של פתרון מסוג זה היא בניתוק תיאורטי של התלות בין יכולת הגילוי לבין

קיומו של מידע מקדים נקודתי או גנרי/מסקנתי. החלשה משמעותית של הקשר הזה מחלישה את אחד היתרונות המשמעותיים של התוקף – היכולת להפתיע עם כלי או יכולת חדשים, או באמצעות כלי או יכולת המבוססים על כלי תקיפה שזוהה ונחתם, אך בוצע בו שינוי מינורי שמאפשר לו לעקוף את מנגנוני ההגנה.[67]

הקווים המנחים לעיצוב שלב הגילוי הם, אם כן, הוספת מידע של קהילת המודיעין ושל חברות המודיעין המובילות באופן שוטף ועדכני למערך ההגנה המבוסס מודיעין, הוספת מרכיב גילוי שאינו מבוסס על מודיעין מוקדם (כמו הפתרונות שהבאנו כדוגמאות כאן), ושילוב של אלה לכלל מערך גילוי אחוד. זוהי פעולה שעשויה לשכלל ולשדרג את היעילות של מערך הגילוי הזה באופן שבו מרכיב אחד מזין את משנהו בנתונים המשכללים את יכולתו לגילוי וזיהוי תקיפה. קיומו של גוף ארגוני מקצועי האחראי לניהול מערך הגילוי ולקבלת ההחלטות הוא תנאי הכרחי להבאת הטכנולוגיה הזו לכלל אפקטיביות של ממש.

השלב הבא הוא ניהול הסיכול שימנע מהתוקף להשיג את מטרתו. זהו השלב המתואר בתרשים איור 3: תפיסת ההתמודדות עם תקיפות APT לעיל, מתחת לקו המקווקו. מעצם ההגדרה שנבחרה (סיכול מטרת התוקף ולא התקיפה עצמה), יש בשלב הזה פוטנציאל לשינוי המצב שבו עם הגילוי, ברירת המחדל היא ההחלטה לעצור את ההתקפה לאלתר. בשלב הזה מוצע להבדיל בין התקפה שמטרתה הרס (CNA) להתקפה שמטרתה ריגול וגניבת מידע (CNE), וכן בין ארגונים רגישים שתקיפתם היא בסבירות גבוהה רק למטרות הרס והשבתה כמו חברת החשמל או חברות מים, לבין ארגונים שהתקפה עליהם יכולה להיות גם למטרות השבתה והרס, אך גם למטרות ריגול וגניבת מידע. הקו המנחה הוא עצירה מיידית של התקפה עם גילויה, בכל ארגון רגיש שבו מטרתה המובהקת של ההתקפה היא הרס/השבתה ברמה גבוהה של ודאות. בשאר הארגונים ניתן להציע כקו מנחה את ההכלה לצורך לימוד התקיפה, לימוד הפן הטכנולוגי של הכלי, לימוד תחומי העניין של התוקף ואם אפשר – זיהוי של התוקף. כדי לצמצם את יכולתו של התוקף לגרום נזק או לגנוב מידע נדרשים מהלכים שמהותם שינוי מתמיד והטעיה של התוקף. לדוגמה, לאחר זיהוי ההתעניינות של התוקף, ניתן לבצע שינויי מיקום ברשת של המידע או של המערכות שעליהם נרצה להגן. שינויים כאלה יקשו מאוד על התוקף לממש את גניבת המידע שביקש לבצע.[68]

לאחר זיהוי תחומי העניין של התוקף ניתן לחשוב על כיווני פעולה נוספים, כגון הזנת התוקף במידע שגוי. דרך פעולה זו עשויה להוות סיכול ממשי של מטרת פעולת תקיפה.[69] יתרה מכך, מימוש כזה של הטעיה במידע עשוי להיות חלק מהרתעה. שתילת מרכיב חוסר ודאות ביחס לאמינות המידע הנגנב מהארגון עשויה להוות משקל משמעותי במשוואת הכדאיות לביצוע תקיפה. הקו המנחה להכלה ולשיבוש והטעיה עשוי להפוך את היוצרות ממצב שבו התוקף יוזם, לומד את חולשותיו של המגן ומבצע בחשאי

את תקיפתו ללא ידיעת המגן, למצב שבו המגן לומד את התקיפה, מנתח אותה ומגיב בצורה מתוחכמת בחשאי, ללא ידיעת התוקף.

מערך ההגנה המשולב רלוונטי לתקיפות עומק בתוכנה (APT) במרחב הקיברנטי. שני סוגים נוספים של תקיפות מחייבים מענה המשלים את אסטרטגיית ההגנה המוצעת: תקיפות מהירות ושטחיות יחסית, שתוצאותיהן נראות מייד ובדרך כלל נועדו לחולל שינוי או למנוע גישה לאתרים ולשירותים שהם מציעים במרחב הקיברנטי (DDoS, Defacing), ותקיפות באמצעות טיפול ברכיבי חומרה או קושחה בשלבי הייצור הסדרתי או על ידי בעלי יכולת מתאימה, לאחר שהמוצר נרכש.

המענה לתקיפות שטחיות ומהירות (DDoS, Defacing)

התקיפות השכיחות יותר ברשת הן אלה המאופיינות כמהירות ושטחיות יחסית ואינן דורשות מודיעין רב לתוקף, את המידע הנדרש להן ניתן להשיג במהירות, ולרוב אינן מצריכות תחכום בתקיפה או כלי תקיפה ייחודיים. בדרך כלל מדובר במתקפות מניעת שירות (DDoS-Distribute Denial of Service). גם הנזק הממשי שלהן (מניעת שירות של אתר או ארגון) מוגבל בזמן ובהיקף.[70] נדרש קו הגנה מפני המתקפות הללו לא רק בעטיה של ההשפעה המורלית והתדמיתית שהן יוצרות, אלא בעיקר משום שמתקפת DDoS, שמתוכננת כחלק מפעילות רחבה יותר, עלולה לגרום נזק ממשי. איום מהסוג הזה אינו מצוי רק בקטגוריה של השפעה על מורל ותחושת ריבונות ומשילות, אלא יכול להיחשב, כמו במקרה הגיאורגי, כמתקפת CNA של ממש, כאשר מטרתו של התוקף היא לשלול תקשורת והעברת מידע.[71] הקו המנחה להיערכות להגנה מפני מתקפות מניעת שירות או שינוי אתרים הוא התבססות הן על יכולות של ספקי השירות באינטרנט וספקי ענני מידע (בעיקרם – הרחבת רוחב פס לארגון בצורה משמעותית, ניטור ואיתור המתקפה וחסימתה), והן על ניטור מתמיד של ה־Data-Center בארגונים כדי להתמודד עם תקיפת האפליקציה שאמורה למנוע שירות.[72]

סיכון נוסף שיש להתמודד איתו במסגרת התקיפות האמורות נוגע לאפשרות לייצר כמות גדולה של תקיפות שטחיות. התקפת DDoS רחבת־היקף מניחה כי למרות שכל תקיפה כשלעצמה היא שטחית ובעלת פוטנציאל נזק מוגבל ומקומי, הרי סנכרון מספר רב של מתקפות כאלה עלול לייצר תוצאה חמורה. מוצע להתבסס על התפיסה שלפיה אתרים מהותיים להעברת מידע לציבור או סמלי שלטון וריבונות יוכלו לקבל רוחב פס המתגבר על החסימה, והם ינוקו במהירות מתקשורת עם כתובות המיוחסות לתקיפה, ובעת הצורך יועברו לאתרי אירוח חליפיים.

השימוש ב'ענן' על ידי ארגונים ביטחוניים וחיוניים

העבודה ב'ענן' נחלקת בין ענן חיצוני, ענן פנימי וענן היברידי (המשלב ענן פנימי וחיצוני על פי הצורך ומדיניות הארגון), וכן על בסיס השימוש בענן – כשירות תוכנה (Software as a Service – SaaS), כפלטפורמה (Platform as a Service – PaaS) וכתשתית (Infrastructure as a Service - IaaS).[73]

אמנם, אין חולק על היעילות והחיסכון לארגון העובד על ענן חיצוני, אולם סוגיית ההגנה על המידע של הארגון מטרידה. מעבר לתחושה הלא־נוחה הנובעת מהפקדת המידע של הארגון במקום חיצוני, ומעבר לסוגיות טכנולוגיות אובייקטיביות מטרידות (זמינות אפליקציות בזמן חירום, עמידות ספק הענן בפני עומסים), קיימת סוגיית ההגנה על המידע של הארגון בענן – איך ניתן להבטיח שמידע חיוני לארגון לא ייגנב (CNE), ואיך אפשר להבטיח שהמידע הארגוני לא יינזק (CNA)? הבעיה קיימת הן בארגונים החוששים מריגול תעשייתי, הן בארגונים פיננסיים שחייבים להגן על אמינות ודיסקרטיות והן בארגונים ממשלתיים וביטחוניים החוששים מפגיעה במידע ומגניבתו.[74]

השימוש בענן מציף סיכונים מעבר לסיכוני אבטחת מידע. סוגיית זמינות השירות היא קריטית עבור מגזרים מסוימים כמו המגזר הפיננסי. הסיכון כרוך לא רק בהקשר לזמינות הטכנולוגית של השירות, אלא גם להיבטים פוליטיים. לדוגמה: החלטה של מדינה שממוקם בה שירות הענן או חלק ממנו לחסום שירות זה (במקרה זה לישראל), בשל החלטה פוליטית מדינית. כאן עולה סיכון שעוצמתו גבוהה מאוד, אולם חובה לבחון את סבירות התרחשותו. ישראל, כמדינות רבות בעולם, תלויה בשירותים שמקורם במדינות אחרות. אחת הדוגמאות הבולטות היא השימוש במערכות מיקום גלובליות (GPS). מערכות ביטחוניות חיוניות רבות תלויות בשירותי מיקום אלה. גם כאן עוצמת הסיכון גבוהה, אולם ניסיון העבר מראה שההסתברות להתממשותו היא אפסית. לכן, בהיבט זה ניתן להקיש גזירה שווה בהקשר לשימוש בענן במגזרים אזרחיים חיוניים כגון המגזר הפיננסי. מומלץ למגזרים אלה לבצע תהליך ניהול סיכונים מוסדר ומקיף במעבר לשירותי ענן, ולהתייחס למיקום שרתי הענן גם בהקשרי מניעת השירות בשל שיקולים מדיניים, כך שמיקום השרתים יהיה במדינות בעלות תרבות פוליטית מערבית מתאימה.[75]

סוגיית השימוש בענן על ידי ארגוני ביטחון או ארגונים שמוגדרים כשירותים חיוניים במדינה נמצאת בראשית הדרך. ארגונים שמבוססים על מידע בלעדי, רגיש, מדויק, אמין ומוגן כמו בנקים, ואפילו ארגונים ביטחוניים כמו משרד ההגנה האמריקאי החלו לעשות שימוש חלקי וראשוני בענן, תחת הנחיות הגנה מפורטות.[76] ההתמודדות עם ביטחון המידע הארגוני בשימוש בענן מביאה את הספקיות לתת שירותי הגנה בענן במדרגות שונות[77] ואת הארגונים השונים לקבוע הנחיות, סטנדרטים ונהלים

לשימוש בענן. בצד אלה מתפתחים בתעשיית הסייבר מוצרים שנועדו להתמודד בצורה אפקטיבית עם האיומים הקיימים בשימוש בענן.[78]

בסוגיית השימוש בענן עבור הארגונים הביטחוניים והחיוניים בישראל, ההמלצה היא להמתין ככל האפשר ולא למהר להשתמש בענן חיצוני. הנושא נמצא בתחילת הדרך, בוודאי מבחינת ניתוח מימוש איומים על המידע המאוחסן בענן, ועל הדרכים היעילות להתגונן מפני האיומים הללו. אם יוחלט לאפשר לארגונים הללו כניסה לענן, הרי זו צריכה להיות כניסה מדודה ומדורגת, המודל חייב להיות היברידי (המשאיר את ליבת המידע והתהליכים ברשת הארגונית) ומלווה בהנחיות מפורטות ומחמירות לשימוש בענן.

המענה למתקפות על חומרה וקושחה

התקפה מבוססת חומרה[79] אפשרית בשני מאפיינים עיקריים: המאפיין הראשון הוא באמצעות החדרה של רכיב התקיפה בשלבי הייצור הסדרתי של הרכיב. לדוגמה, החדרה של יכולת "דלת אחורית", המאפשרת לתוקף לקבל גישה חשאית לתקשורת או לזיכרון של המכשיר, או החדרה של סוכן תוכנה (BOT) רדום שיוכל להיות מופעל באופן יזום על ידי התוקף, או לחלופין, עם התממשות תנאים שנקבעו מראש. לרוב, תקיפה בשלבי הייצור תבוצע על ידי מי שיש לו גישה לשלבים האלה, כגון מדינות או היצרן עצמו.[80] המאפיין השני של תקיפות הוא בציוד מסחרי רגיל, שמושתלות בתוכו יכולות שיאפשרו את הגישה הנדרשת לזיכרון או לתקשורת של המכשיר.[81]

תחום תקיפות החומרה הוא בעל פוטנציאל נזק רב מאוד. פוטנציאל הנזק נובע משלוש סיבות מרכזיות: א. לא ניתן להסיר את רכיבי התקיפה באמצעים קונוונציונליים (אנטי־וירוס, פִּרמוט). ב. הם יכולים לעקוף מנגנוני אבטחה (כמו סיסמאות, קובצי מערכת מוצפנים). ג. קושי עצום לאתר את רכיבי התקיפה שהוחדרו בתהליך הייצור.[82] הנזק הפוטנציאלי של תקיפות חומרה וקושחה הוא רב, וקיים קושי מהותי לאתר את התקיפות הללו ולטפל בהן.[83] היקף האיום וחומרתו מועצמים עקב העובדה שחלק ניכר מהחומרה למחשבים ומוצרי מחשב מיוצרים בסין, שנתפסת כמדינה שתוקפת במרחב הקיברנטי בכל דרך אפשרית.[84]

כפי שניתן להבין, ההתמודדות עם תקיפות על בסיס חומרה ו/או קושחה היא מורכבת ומטרידה גם את המעצמות. בדומה להצעה באשר להתמודדות עם תקיפות עומק, גם כאן מוצע כקו מנחה לאסטרטגיה שילוב של מספר שיטות. השיטה הראשונה היא שימוש בחומרה שנבנתה בישראל, במקום בטוח ומאושר. הפתרון הזה מנטרל חלקית את הבעיה, משום שבנייה עצמית של כל מערך הרכיבים הנדרשים בתהליך הייצור היא, ככל הנראה, מורכבת ויקרה ביותר, ולעתים אף בלתי־אפשרית מבחינה מעשית. לכן, שימוש בגישה זו אינו ישים בכל מקום ולכל צורך. מומלץ לממש אותה,

אם ניתן, במקומות הרגישים ביותר, שבהם ישראל זקוקה לרמה הגבוהה ביותר של ביטחון באבטחת המידע ותהליכי העבודה.

גישה שנייה מתמודדת עם תקיפה בעזרת בדיקה מעמיקה ככל האפשר של רכיבי החומרה. ניתן לבדוק לעומק את החומרה והקושחה בצורה של "הנדסה לאחור", שתגלה רכיבים או קוד שהוחדרו לאחר הייצור. גם פעולה זו יקרה ומעכבת ייצור והתקנה. "הנדסה לאחור" שתגלה רכיבים שהוחדרו בעת ייצור רכיבי המחשב היא קשה ויקרה עוד יותר. עם זאת, מוצע לבדוק אפשרות לבצע את ההנדסה לאחור במחשבים הקשורים במערך ייצור ובתהליכי עבודה רגישים, ואשר לא ניתן לייצר עבורם מערך מחשבים מבוסס חומרה בטוחה.

שונה במקצת המצב בתקיפות חומרה שהוחדרו במכשירים קיימים שיוצרו בייצור סדרתי. במקרה זה, אחת מגישות הטיפול האפשריות היא היכולת להשוות בין רכיבים במכשיר הסדרתי – בהנחה שניתן לקבוע כי זהו מכשיר תקין שלא טופל על ידי התוקף – לבין מכשיר שעלה החשש כי הוא טופל. השוואה זו אינה מיידית והיא מחייבת יכולות מקצועיות גבוהות.

לבסוף, בדומה למה שהוצע בתחום ההתמודדות עם תקיפות עומק, גם ההתמודדות עם תקיפת חומרה צריכה להיות מבוססת, כנראה, על הבנת הנזקים הפוטנציאליים של התקיפה. מוצע לנקוט צעדים משבשים ומטעים, המונעים את הפעלת התקיפה. במסגרת זו ראוי לבחון מימוש הצעות כמו "Power Resets" – טכניקה המונעת מרכיבים בעייתיים לחשב כמה זמן הם פעילים, כדי למנוע תקיפות מבוססות טיימר, "Data Obfuscation" המבצעת הצפנה של מידע וערכים המוזנים לרכיבים בעייתיים, כך שלא יוכלו לקבל קודים מיוחדים או להיות מופעלים על בסיס זיהוי מידע ו־"Sequence Breaking" המבצעת שבירה/ערבול של רצף מסרים באופן אקראי, כך שיימנע מרכיבים בעייתיים לזהות תבניות מידע ולהפעיל על בסיסם תקיפה.[85]

מומלץ לאמץ אסטרטגיה המורכבת ממגוון כיווני הפתרון שתוארו כאן. ניתן ולהשתמש בחומרה ובקושחה בטוחות המיוצרות בישראל באופן מאובטח, אבל הדבר אפשרי רק למושאי הגנה בודדים, שנראה כי קיימת מוטיבציה גבוהה לתקיפתם בדרך של תקיפת חומרה וקושחה. ניתן לבצע גם בדיקות חומרה פיזיות כדי לוודא שלא קיימים רכיבים שאינם אמורים להיות שם. ליבת ההגנה צריכה להיות מתוחכמת יותר, ולנסות לחולל שינויים במידע המוזרם לחלק מהרכיבים, כדי לעקר את בסיס הפעלת התקיפה. בנוסף ובשל הרגישות והמקצועיות הרבה הנדרשת בתחום זה, ראוי לשקול הקמה של מרכז לאומי לבדיקת חומרה וקושחה, שיוכל לספק מענה לכל הצרכים של הגורמים הרלוונטיים בישראל. מרכז זה יוכל להשתלב במעבדה הלאומית הקיימת כיום ב'רפאל' או במסגרת אחרת.

מניעת התקפה באמצעות הרתעה

אסטרטגיית ההגנה המוצעת אינה הרמטית, ויש להניח כי מתקפות יצליחו מעת לעת. הצלחת מתקפה קיברנטית מעלה לרוב שתי סוגיות באופן מיידי – שאלת התגובה (בדרך כלל לצורך הרתעה) ושאלת ההתאוששות מתקיפה. הנימוק הרציונלי הנפוץ למימוש תגובה למתקפה הוא הרצון להרתיע ולמנוע התקפות נוספות. תפיסת ההרתעה מבוססת על ההנחה שחשיבתו הרציונלית של התוקף תביא אותו לשקול את מחיר התקיפה שייגבה ממנו, מול הרווח מהתקפה מוצלחת. כל אימת שהמחיר יהיה גבוה מהרווח – לא תמומש התקפה, ובכך תיווצר למעשה הרתעה. תהליך כזה טרם הוכיח תקפות במרחב הקיברנטי. הסוגיה הראשונה המהווה מכשלה של ממש היא זיהוי ודאי של התוקף. זיהוי כזה אינו אפשרי במקרים רבים של תקיפה. הסוגיה השנייה היא היתרון שיש בנקודה הזו דווקא לגופים שהתשתית הקיברנטית שלהם אינה מפותחת. גופים ומדינות עם נחיתות קיברנטית תוקפים מדינות מפותחות בלי לחשוש מהתגובה הקיברנטית או הפיזית הצפויה,[86] וזאת משום שהיכולת להגיב בצורה שתכאיב לצד השני מוגבלת ממילא, כשהצד התוקף נחות מבחינה קיברנטית. בצד זאת, גם במקרים שבהם נראה על פניו כי ניתן לממש תגובה קיברנטית או פיזית למטרת הרתעה, לא בוצעה מתקפת תגובה כזו נגד תוקפים.[87]

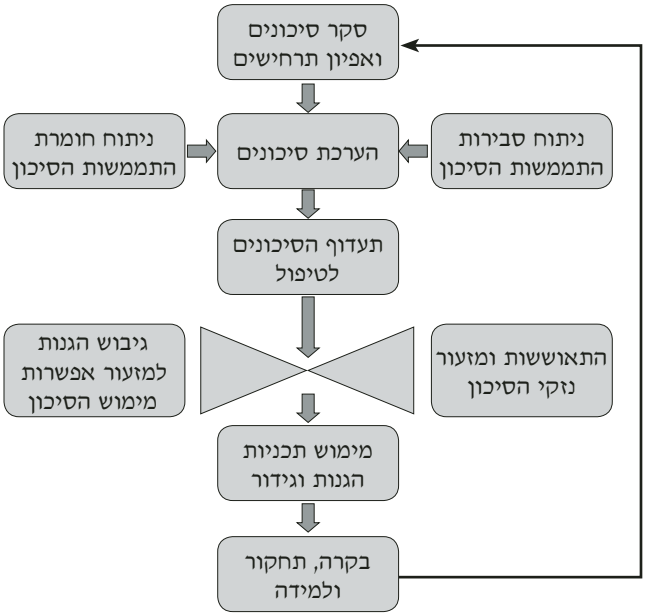
בצד הגדרה הקלאסית להרתעה, גם יכולת הגנה חזקה עשויה להוות מרכיב הרתעתי. הרתעה ניתן להשיג גם על בסיס יכולת הגנה חזקה מאוד, שתביא את התוקף לכלל הערכה כי לא כדאי לו להשקיע מאמץ בתקיפה, משום שסיכוייו לפרוץ את מערך ההגנה נמוכים מאוד.[88] בהמשך לרעיון ההרתעה הנובע מהגנה חזקה ניתן לחשוב, כפי שהוצע לעיל, על הרתעה הנובעת מתחושת חוסר הוודאות שתהיה לתוקף, אם המידע שיצליח לגנוב יהיה תמהיל של מידע אמיתי ומידע שגוי, ללא יכולת להבחין בין השניים.

התאוששות מתקיפה

"התאוששות מתקיפה" הוא מושג רחב העוסק בהכנות, בתהליכים, בכלים ובשיטות שמטרתם למזער את הנזק של תקיפה מוצלחת, ולחזור לתפקוד תקין במהירות. ניתן לתאר התאוששות מתקיפה במונחים טכנולוגיים כהחזרה של רשת המחשבים ותהליכי העבודה מבוססי המחשב בארגון לפעילות, אחרי שהושבתו עקב התקיפה. התאוששות טכנולוגית מבוססת לרוב על גיבוי מערכות ובסיסי מידע (לרוב תחת הכותרת של Disaster Recovery Plan – DRP). מערך גיבוי כזה מתוכנן בדרך כלל להתמודדות מהירה עם פגיעה פיזית (רעידת אדמה, הצפה, שריפה, פיצוץ), או עם תקלה בתפעול מערך המחשב שגורמת נזק בלתי־הפיך (מחיקת מידע בשוגג) במקום שבו נמצא מערך המחשבים המרכזי של הארגון. מערך גיבוי כזה עשוי להימצא רלוונטי להתאוששות גם מפני תקיפה קיברנטית הרסנית, ובלבד שהמתקפה לא פגעה גם במערכי הגיבוי.

מושג ההתאוששות מאירוע לקוח מתוך עולם ניהול הסיכונים. תחום עשייה זה הוא חלק מובנה בתכנון ההגנה בכלל ובמרחב הסייבר בפרט, והוא נועד לקבוע את תעדוף אמצעי ההגנה לנוכח מסגרת הסיכונים הכוללת. כלל הסיכונים מנותחים באמצעות סקר סיכונים, שבעקבותיו נקבע תעדוף לסיכונים שיינתן להם מענה הגנתי. לצד המענה ההגנתי לסיכונים אלה, נדרש להתייחס לצעדים שיש לנקוט כדי למזער את היקף הנזק ואת משכו, אם ההגנה לא תצליח והסיכון יתממש.

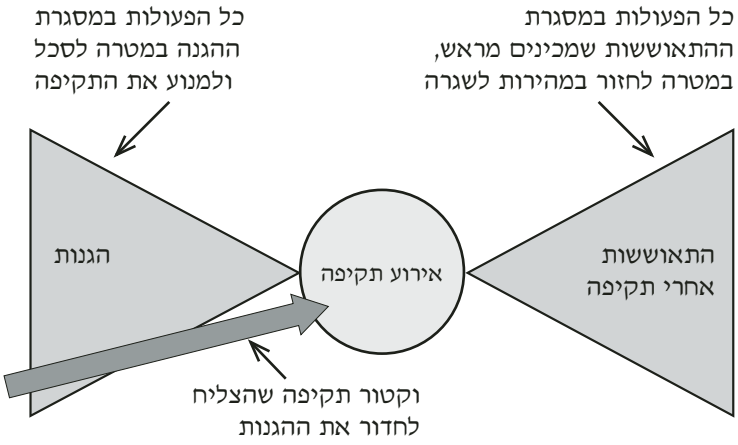
בהקשר התיאורטי, מושג ההתאוששות מתקיפה קשור לפיתוח הידע בתחום החוסן (resilience) המדינתי או הארגוני. חוסן זה משקף את היכולת של הארגון להתמודד עם מצבי קיצון צפויים או בלתי־צפויים, ולחזור לתפקד ברמה הקודמת לאירוע לפחות, ולעתים אף ברמה טובה יותר מאשר לפני התרחשות האירוע. כדי לאפשר שיפור מתמיד בחוסן הלאומי בתחום הסייבר, יש לשלב תהליכים אלה כחלק מובנה בתהליך ניהול הסיכונים, ולייצר כלים ושיטות שיאפשרו התאוששות מהירה ואפקטיבית מאירועי תקיפת סייבר. התרשים להלן מתאר את מסגרת תהליך ניהול הסיכונים הכולל, ואת ההתאוששות כחלק מובנה בו.



איור 5: המחשת תהליך ניהול סיכונים

הרחבה לתיאור היחס בין ההגנה על המרחב הקיברנטי לבין התאוששות מתקיפה ניתן לראות בתרשים המוצג להלן (איור 6). בחלקו השמאלי של התרשים ניתן לראות את

מערך ההגנות שהוקם כדי למנוע התרחשות של תקיפה. הגנות אלה הן רב־שכבתיות, שמטרתן להקשות על התוקף להגיע ולממש את התקיפה. וקטור התקיפה שמתואר משמאל הוא תהליך של התוקף המנסה לחדור את ההגנות כדי לבצע את התקיפה. מאחר שברור לכול כי כל הגנה, נחושה ומתוחכמת ככל שתהיה, עלולה להיפרץ על ידי תוקף נחוש ובעל יכולות מתקדמות, הרי ניתן להניח שבמוקדם או במאוחר התוקף יצליח להשיג את מטרתו. תהליך ההתאוששות נועד לתכנן מראש צעדים שיוכלו למזער את הנזק מן התקיפה, ולאפשר חזרה לתפקוד תקין במהירות האפשרית. בכך, התאוששות עשויה להיות גם מניעת ההישג המבוקש של התוקף. המודל המתואר בתרשים הוא אימוץ לתחום הסייבר של תפיסת ניהול סיכונים שפותחה בשנת 1979 והקרויה Bowtie, לאור דמיונה לקשר עניבת פרפר.[89]



איור 6: התאוששות מתקיפה כחלק מובנה בהגנה

התאוששות מתקיפה לא חייבת להיות רק בהיבט טכנולוגי. לדוגמה, תקיפה מוצלחת מבחינה טכנולוגית של מאגרי חברת 'סוני' לא הצליחה, בסופו של דבר, להביא להישג הנדרש (מניעת הקרנתו של סרט מסוים) על ידי צפון־קוריאה, שהייתה החשודה המרכזית בתקיפה, מפני שהממשל האמריקאי הצליח לשכנע את חברת 'סוני' להקרין את הסרט שהתוקף ביקש למנוע את הקרנתו. זוהי דוגמה מצוינת לתקיפה קיברנטית מוצלחת מבחינה טכנולוגית, המשלבת איום בהפעלת מרכיב קינטי בדמות אפשרות לפגיעה פיזית בצופים בבתי קולנוע שיקרינו את הסרט, ומניעת השגת היעד של התוקף בעזרת נחישות ומנהיגות.[90]

סוגיות משלימות בהגנה

מבנה ארגוני עם תרבות שיתוף ושקיפות

שתי סוגיות משלימות את האסטרטגיה שפורטה לעיל וראוי להתעכב עליהן – הסוגיה הארגונית והסוגיה של תרבות שקיפות ושיתוף פעולה. אסטרטגיית ההגנה שתוארה כאן לא יכולה להתממש בצורה מיטבית ללא יד מכוונת, המנחה בצורה אקטיבית את הגופים הרלוונטיים, או לכל הפחות את אלה המוגדרים בקטגוריות של ביטחון המדינה וחיוניים לתפקוד המדינה, וכל "שרשרת האספקה" שלהם. הנחיה אקטיבית פירושה קביעת גוף אחראי בכל ארגון מונחה (או ברמת מגזר) שחייב לקיים הגנה ברמה הנדרשת, וחייב לוודא שכל "שרשרת האספקה" שלו מקיימת הגנה באותה רמה. הוא יהיה חייב בדיווח על כל אירוע חריג, חייב לבצע החלפת מידע בשקיפות הן על תקיפה והן על כלי הגנה אפקטיביים שהוא מפעיל עם ארגונים מוגנים אחרים, וחייב בתיאום התגובה שלו למתקפה עם הגורם שייקבע כממונה על כך מטעם המדינה.[91]

בישראל קיימת חלוקת אחריות להגנת הסייבר. החלוקה היא שיקוף של האחריות הביטחונית הכוללת בישראל, בתוספת תיקונים ושינויים מהותיים שהתווספו עם השנים, ככורח שהולידו האופי והמאפיינים של הסייבר והמאבקים הבין־ארגוניים. למרות שחלוקה ארגונית אינה במוקד מסמך זה, נכון יהיה להסביר את התפתחות הפן הארגוני בישראל בתחום האחריות להגנה בסייבר.

החוק להסדרת הביטחון בגופים ציבוריים התשנ"ח-1998 קובע סמכויות ואחריות, בין השאר, לאבטחת מידע ולאבטחת מערכות מחשוב חיוניות של גופים ציבוריים שונים. בתוספות לחוק נקבע כי שירות הביטחון הכללי אחראי על אבטחת המידע של משרד ראש הממשלה, משרד הביטחון, מפעלי מערכת הביטחון, לשכת נשיא המדינה ומשרד החוץ. למרות הקביעה הזו הוחרגו חלק מהגופים. משרד הביטחון מונחה על ידי מלמ"ב, המוסד וצה"ל עצמאיים בהגנת הסייבר.[92] התוספות לחוק מגדירות שורה של גופים המהווים תשתיות חיוניות בישראל, ואשר מונחים על ידי שירות הביטחון הכללי בתחום אבטחת המידע ואבטחת מערכות מחשב.[93] ב־2002 החליטה הממשלה (החלטה 84ב' של ועדת השרים לענייני ביטחון) על הקמתם של שני גופים ייעודיים: ועדת היגוי עליונה, שתבחן באופן שוטף את זהות הגופים הציבוריים והפרטיים החיוניים לתפקודה של מדינת ישראל, ויחידה ממלכתית להגנה על המערכות הממוחשבות.[94] מטרת ועדת היגוי, בראשות ראש המועצה לביטחון לאומי, היא גיבוש צעדים להגנה על מערכות המחשב החיוניות של המדינה. הוועדה שימשה ועדת היגוי המנחה את היחידה הממלכתית לאבטחת תשתיות ממוחשבות בשירות הביטחון הכללי.[95]

בשנת 2011 הוחלט על הקמת מטה קיברנטי לאומי, "גוף מטה לראש הממשלה, לממשלה ולוועדותיה, אשר ממליץ על מדיניות לאומית ומקדם את יישומה בתחום הקיברנטי, בכפוף לכל דין ולהחלטות הממשלה".[96] בנוסף לתפקידיו כגוף מטה, הוטל

על המטה הקיברנטי הלאומי לפעול למימוש המלצותיו של יושב־ראש המועצה הלאומית למחקר ולפיתוח, יצחק בן־ישראל, שעיקרן – כמנוסח בהחלטת הממשלה – קידום ופיתוח תשתית הידע, המחקר והפיתוח הנוגעים בטכנולוגיה קיברנטית, וכן לפתח "כלים לחירום בתחום הקיברנטי", לפתח "מעטפת הגנה קיברנטית לאומית" ו"פתרונות להגנה מקומית" – כל זאת "מבלי לפגוע בסמכות שניתנה לגורם אחר על פי דין והחלטות הממשלה".[97] כמעט שלוש שנים לאחר מכן הטיל ראש הממשלה על ראש מטה הקיברנטי לפעול להקמת "רשות לאומית להגנה אופרטיבית בסייבר", שתפעל בצד המטה ותקבל אחריות וסמכות בסוגיית הגנת המרחב האזרחי מפני איומי הסייבר. הרשות תהיה גוף אופרטיבי.[98]

בשנת 2011 הטיל הרמטכ"ל אחריות לעיסוק בסייבר על שני גופים -על יחידת המודיעין 8200 בתחום ההתקפה, ועל מחלקת הגנה באגף התקשוב כאחראית על תחום ההגנה.[99] בראיון עם ראש אגף תקשוב הוא דיווח כי צה"ל הקים גוף מטה ייעודי, המשלב בין גורמים מחיל המודיעין לבין אנשי אגף התקשוב, שתפקידם לעסוק בהגנה מפני התקפות סייבר.[100] ב־15 יוני 2015 פורסם כי הרמטכ"ל החליט להקים זרוע סייבר בצה"ל שתעסוק בכל תחומי הפעילות הקיברנטית, והקמתה תארך כשנתיים.[101]

קיימים בישראל גופים נוספים שאין בהגדרתם אחריות מפורשת להגנה מפני התקפות בסייבר, אך עשייתם משיקה לתחום: אגף התקשוב הממשלתי במשרד האוצר (האחראי לאספקת שירותי גלישת אינטרנט בטוחים למשרדי הממשלה, ולהגנה על הרשתות הממשלתיות בחיבור שלהן לאינטרנט), היחידה למניעת פשיעה בסייבר של משטרת ישראל (פועלת במסגרת יחידת להב 433, ובין תפקידה חקירת פשיעה בסייבר ו"פעילות יזומה בנוגע לתרחישי איום מקוונים"),[102] והרשות למשפט, טכנולוגיה ומידע (הוקמה במשרד המשפטים ותפקידה "קידום המודעות של הפרט לנושאי פרטיות והגנת המידע האישי ברשת").[103] בהקשר להגנה מפני תקיפת סייבר, ניתן לחלק את ישראל למספר קבוצות (ראה גם התרשים להלן):

א. ארגוני הביטחון – צה"ל, ארגוני קהילת המודיעין, משטרת ישראל ודומיהם. אלה קובעים לעצמם את תפיסת ההגנה וממשים אותה בהתאם לצורכיהם המבצעיים ולסמכויות הפעולה שלהם.

ב. התעשייה הביטחונית – חברות ביטחוניות וארגונים בעלי רגישות ביטחונית. אלה מונחים על ידי הממונה על הביטחון במערכת הביטחון (מלמ"ב), הקובע את דרישות ההגנה בתחום הגנת הסייבר ופועל לוודא שדרישות אלה מתקיימות.

ג. תשתיות לאומיות חיוניות – מגזרים שפעילותם חיונית לתפקוד המדינה, לדוגמה: אספקת החשמל, מים, וכדומה. הם פועלים תחת הנחיה ובקרה של שירות הביטחון הכללי.

ד. משרדי הממשלה – ההגנה על רוב משרדי הממשלה (ורשויות ממשלתיות) נעשית בהנחיית אגף התקשוב הממשלתי, שלו יחידה הפועלת בתחום ביטחון הסייבר. משרד הביטחון מונחה מלמ"ב.

ה. המגזר האזרחי – שאר משתמשי הרשת האזרחיים הכולל: ארגונים, עסקים ופרטיים. זוהי הקבוצה הפגיעה ביותר, שכושר ההגנה שלה נקבע משיקולים עסקיים. כתוצאה מכך הם חשופים לתקיפה של גורמים עוינים, שייתכן כי יעדיפו לפעול מול ישויות בעלות הגנה ירודה. נדרש כי קבוצה זו תפעל תחת רגולציה מתאימה, שתיקבע על ידי הרשות הלאומית להגנה בסייבר שהוקמה לאחרונה.

איור 7: מצב האסדרה (רגולציה) הארגונית בישראל

המבנה הארגוני והגופים האחראיים או הנוגעים בהגנה בסייבר – בחלוקת אחריות וסמכות כזו או אחרת – מחייב אסדרה (רגולציה) מלאה. בהקשר זה ראו פרק הרגולציה להלן, המתייחס לביטחון המגזר האזרחי. מתיאור המעבר וההתפתחות של האחריות להתגוננות במרחב הקיברנטי נראה שלא ניתן משקל ראוי לאיומים, להשלכות הנובעות ממימוש אפשרי של האיומים ולצורך לגבש אסטרטגיה קוהרנטית להתגוננות במרחב הקיברנטי במובן הרחב, הכולל גם מודיעין, תקיפה ותגובה קינטית כאפשרות. כדי לממש אסטרטגיה כזו וכדי שהגנה תיעשה באופן אפקטיבי נדרשים תהליכי עבודה מתאימים, ומבנה ארגוני שהולם את תהליכי העבודה. היות שתהליכי העבודה טרם הוגדרו סופית והמבנה בישראל טרם התייצב, ומאחר שלא כל החלטות הממשלה בסוגיה הגיעו לכלל מימוש, כל שניתן לומר הוא כי לעת הזו נדרש להבטיח לפחות דיאלוג מקצועי עמוק, רחב ורציף בין כלל הארגונים הללו, בכל הדרגים, בדגש על דרגי עבודה. בין אם המבנה יתייצב לבסוף במתכונת של הקמת רשות להגנה בסייבר שתטפל בהגנה על כל המגזר האזרחי,[104] ובין אם במתכונת אחרת[105] – הכרחי שיתקיים דיאלוג שיוליד תהליך מובנה, המאפשר טיפול שיטתי מהיר באיומי תקיפה מרכזיים על ישראל.

בכל מתאר, ישראל זקוקה לגוף אחד שיש בו הערכת מצב כוללת לסטטוס ההתקפות הקיברנטיות על המדינה ועל ארגונים בתוכה. לגוף זה צריכה להיות מדיניות ביחס לתקיפות הללו, ועליו להוות כתובת כאחראי מטעם המדינה על ההנחיה בנושא התגוננות קיברנטית. עליו להיות גוף אופרטיבי, שבו מיוצרת תמונת הערכת מצב קיברנטית לאומית המבוססת על דיווחי ה־CERT/CSOC הארגוניים, על דיווחי ספקיות ישראליות ופרסומים גלויים, על דיווחי קהילת המודיעין ועל זרימת מידע מחברות הגנה ומודיעין מסחריות, ובו מתוכננת ההתגוננות מפני תקיפה רחבה על מגוון יעדים בישראל. גוף זה הוא שאמור לקבוע אסטרטגיה שכל הארגונים המונחים עובדים על פיה, לקבוע שורת כלים ומוצרים שכל הארגונים המונחים מחויבים להתקין לצורך מימוש האסטרטגיה, לקבוע שורת ארגוני הגנה ומודיעין מסחריים שהגופים ירכשו מהם מידע על איומים ברשת, להגדיר את סוגי המידע שיועבר מקהילת המודיעין לארגונים המונחים ולוודא עיגון העברת המידע בחוק. בנוסף נדרש לקבוע חובת דיווח רחבה לגוף המנחה הכוללת מידע על כל ניסיון תקיפה, על פיתוח שיטות התמודדות ועל ניסיונות מוצלחים עם כלים חדשים להגנה. שיתוף במידע בין הארגונים המונחים הוא הכרחי. הדיאלוג הרצוי הוא דיאלוג ישיר, כזה המתנהל ישירות בין ה־CERT/CSOC הארגוניים כל העת (בוודאי בין ארגונים המצויים באותו מגזר), תוך יידוע הרגולטור של המגזר ו/או מרכז CERT לאומי. המידע לשיתוף צריך להיות רחב ומגוון, החל מנתונים על ניסיונות תקיפה בזמן אמת, ממצאי ניתוח כלים שנמצאו בעת תקיפה, שיטות וכלי הגנה חדשים. דיווח על נזקי תקיפה יכול להימסר רק לרגולטור, אם קיים, או לגוף ההנחיה הלאומי ולמרכז ניהול ההגנה הקיברנטית הארצי, בשל הרגישות המסחרית שיש בדיווח כזה, וזאת מעבר לדיווח הנדרש מחברות ציבוריות וממשלתיות על פי החוק כיום. השקיפות ושיתוף הפעולה צריכים להיות מעוגנים בחוק, אך חשוב מזה – צריכים להיות חלק מחינוך על בסיס הטמעת ההבנה שרק שיתוף פעולה מבוסס שקיפות בדיווח יכול לסייע בצורה משמעותית במאבק האֵ־סימטרי של המגן מול התוקף במרחב הקיברנטי.

אף שכבר התקבלה החלטה להקים רשות לאומית להגנה בסייבר, הרי הקושי להפריד בין המרחב הפיזי למרחב הקיברנטי מעלה את הצורך לייצר מסגרת הגנה אחודה מפני איומים ביטחוניים. טענה זו מתבססת על העובדה שהתפוצה של איומים במרחב הסייבר ויכולת התוקפים לאתר חולשות ולפעול דרכן מחייבות התבוננות מקיפה על הביטחון הלאומי. החשיפה של המדינה לתקיפות סייבר אינה נובעת רק מחשיפה של מערכות המחשוב לאיומים דרך האינטרנט, אלא ממגוון רחב של פרצות. כך גוברת ההבנה שכדי להבין את המתרחש במרחב הסייבר, יש לייצר תמונת מצב אינטגרטיבית מקיפה על המתרחש במרחב הלאומי הקיברנטי והפיזי. התוקפים את ישראל אינם מפרידים בין המרחבים, אלא יוצרים מערכה משולבת בין מרחב הסייבר

והמרחב הפיזי, לכן על המגן להימנע מהפרדה מלאכותית בין ההגנה בשני המרחבים, העלולה לפגוע בו.[106] לאור זאת מוצע לממש את ניהול מערכת ההגנה הקיברנטית הביטחונית במסגרת שירות הביטחון הכללי. מניע נוסף להמלצה זו הוא שכל תקיפה רחבת־היקף או תקיפת עומק – הן לצורכי גניבת מידע וריגול והן לצורכי הרס – היא עניין ביטחוני, ולכן צריכה מערכת ההגנה להימצא באחריות גוף ביטחוני, וכן משום שהגנה מחייבת התבוננות ומחקר של מאגרי נתונים המצויים במרחב הקיברנטי בישראל, ולעתים מחייבת אף כניסה לפרטי מידע ותוכן. הגוף הביטחוני היחידי המורשה על פי חוק לממש פעילות כזו בקרב אזרחי ישראל הוא שירות הביטחון הכללי, זאת מלבד משטרת ישראל, האמונה על חקירה של פשיעה במרחב הסייבר.

הצעת המחליטים שאושרה על ידי ממשלת ישראל משאירה אמנם את כל הגופים הממשלתיים המיוחדים הפועלים בתחום ההגנה בסייבר על תילם, אך מנחה על יצירת גוף מרכזי (רשות) להנחיה ולניהול התגוננות בסייבר. במצב הנוכחי בישראל, כאשר קיים יותר מגוף אחד העוסק בנושא, יש לנהל דיאלוג רצוף, פתוח ושקוף בין גופי ההנחיה. לצד הדברים האלה יש לזכור שארגון הפעולה במרחב הסייבר מחייב הסדרה גם בהקשר לחלוקה בין המרחב הביטחוני לפלילי. חלק לא מבוטל מן האירועים מתרחש במרחב הפלילי, והגורמים האחראיים למרחב זה הם גורמי האכיפה השונים, ביניהם: משטרת ישראל, רשות המיסים, הרשות לניירות ערך וגורמים רלוונטיים אחרים. בתרשים להלן מתוארת ההמחשה של האחריות הארגונית המוצעת במרחב הסייבר הלאומי.

איור 8: אחריות מוצעת לפעולה במרחב הסייבר

הרשות הלאומית להגנה בסייבר תידרש להיות גורם הרגולציה המדינתי שיאפשר אסדרה של מרחב הסייבר האזרחי, הכולל את המגזר העסקי ואת שאר הגורמים הפועלים במרחב הזה. מוצע לייצר בידול בין המרחבים הללו, ובכך לאפשר לגורמים הביטחוניים להתמקד במרחב הביטחוני, ולרשויות האכיפה – להתמקד בפלילי. לצד זאת חובה לבנות תשתית לשיתוף פעולה בין־ארגוני כמתחייב במקרים שהאירוע חוצה מרחבים. לדוגמה, כשארגון פשע סייבר פועל גם למטרות פוליטיות ולמטרות טרור.[107] ראוי שמשטרת ישראל ושאר רשויות האכיפה יגבשו את האסטרטגיה לפעולה במרחב הפלילי כך שיוכלו להתמודד באופן יעיל עם הונאות סייבר, הונאות במסחר בניירות ערך, גניבות קניין רוחני, ריגול עסקי פלילי, פדופיליה ברשת, מכירה של חומרים אסורים ועוד.

רגולציה במרחב הסייבר הלאומי

מרחב הסייבר הלאומי כולל גם ארגוניים ועסקים שהפגיעה בהם עלולה לגרום נזק למשק, ואף לפגוע בביטחון הלאומי. פגיעות זו של הסביבה האזרחית מחייבת מענה מתאים. אחד הכלים למימוש מענה שיוכל לשפר את הגנת המרחב האזרחי הוא רגולציה בתחום ביטחון הסייבר של מרחב זה. עיקרי ההצעה לשיפור המצב שתואר לעיל נוגעים להכנסת תחום הגנת הסייבר כמרכיב מובנה בתהליכים סטטוטוריים קיימים, וזאת הן בשלבי ההקמה של מיזמים (אישורו בוועדות התכנון השונות) והן בתהליך התפעול שלהם (חוק רישוי עסקים).[108]

הקמה של כל מיזם במדינת ישראל מחייבת עמידה בתהליכי התכנון הסטטוטורי החל בישראל, והמיזם מחויב לקבל את אישורן של ועדות התכנון בהקשר למגוון נושאים, ביניהם: כיבוי אש, בריאות הציבור, הגנת הסביבה, חומרים מסוכנים, הגנת העורף ועוד. מוצע כי במסגרת זו יידרש כל מיזם להתייחס גם לנושא הגנת הסייבר הרלוונטית לו. זאת, באמצעות תסקיר/דוח עמידות סייבר. מסמך זה יהווה הכלי הסטטוטורי העיקרי לצורך איתור ובחינת חשיפתו של המיזם לאפשרות של התקפות סייבר, ולגיבוש תהליכי הגנה מפני חשיפות אלו. לצד מיזמים חדשים, מוצע שימוש גם בתהליך רישוי העסקים המחייב חידוש עתי, כדי לוודא שפעולת המיזם לאורך שנים עומדת בקריטריונים מתחייבים בתחומים שונים, כולל בתחום האבטחה מפני תקיפת סייבר. בדרך זו יהיה כלי בקרה חוקי נוסף בידי הרגולטור.

מבחינה סטטוטורית, תכולת התסקיר צריכה להיות גורפת ועליה לחול על כל הבקשות, אלא אם ניתן לכך פטור מהגורם המוסמך. אולם מבחינה מעשית, נדרש לקבוע אמות מידה שיגדירו את המיזמים והפרויקטים שלגביהם תתקיים חובת הגשת התסקיר. אמות מידה אלו יוכלו להתייחס למספר מרכיבים כמו גודלו של המיזם, המגזר שאליו הוא משתייך, לדוגמה: מיזם הפועל בתחום האנרגיה, המזון, התרופות,

התחבורה וכדומה. משהוחלט כי על גוף להגיש מסמך עמידות סייבר, יופעל התהליך לאור אבני הדרך הבאות: הנחיות – גורם הרגולציה יהיה אחראי להכין הנחיות לביצוע המסמך האמור. הכנה – המסמך יוכן באחריותו ובמימונו של היזם, תוך שימוש ביועצים מוסמכים. בדיקה – הבדיקה תהיה באחריות הרגולטור, תוך שימוש ביועצים חיצוניים שיוכשרו ויוסמכו לבדיקה של תסקירים. אישור – בחינה ואישור המענה ייעשו על ידי הרגולטור הרלוונטי, שגם יקבע את המשך הנחיית הארגון או העסק.

שתי חלופות קיימות באשר לזהות הרגולטור לתחום הסייבר: הראשונה – בנייה של יכולות רגולציה מגזריות. בגישה זו הרגולטור של כל גורם במשק יהיה מהמגזר הרלוונטי. כך, לדוגמה: הרגולציה בתחום הגנת סייבר במערכת הבריאות תיקבע על ידי משרד הבריאות, הרגולציה על תאגידי מים תקבע על ידי משרד התשתיות וכן הלאה. החלופה השנייה היא רגולציה באמצעות רגולטור מרכזי, שיתבסס על המטה הקיברנטי ורשות ההגנה הלאומית שתוקם. בחינה של שתי החלופות מראה כי בשל המורכבות הטכנולוגית של אמצעי ההגנה והצורך לשמר סף אבטחה אחוד במדינה, לצד החשש שרגולציה מגזרית עלולה לייצר "מגדל בבל" של הוראות אבטחה במגזרים השונים, נראה שהדרך היעילה ביותר למימוש תפיסת ההגנה המוצעת לתחום בצורה זו היא קביעת מסגרת מקצועית אחודה להגנה במגזר האזרחי. זאת בדומה לרגולטורים מרכזיים אחרים כגון רשות כיבוי האש, פיקוד העורף, אחסנת חומרים מסוכנים ועוד.

מקצועיות עובדים, אחראי ההגנה (CISO) ואחריות מנהלים בעסקים

כדי להפעיל בצורה יעילה וממצה מערכת הגנה רב־שכבתית כמו זו המוצעת כאן נדרשים עובדים מקצועיים, בעיקר בעלי ידע וכישורים טכנולוגיים ברמה גבוהה מאוד. כל "החוכמה" שתוטמע במערכות צריכה להיות פרי הניתוח וההבנה המקצועית של העובדים המאיישים את עמדות הניטור והניתוח הפורנזי (במקומות שהוא קיים). עובדים כאלה זקוקים כל העת להכשרה, לרענון מקצועי, להתעדכנות, לשיח מקצועי חוצה ארגונים, להשתתפות בכנסים והשתלמויות ומעל לכול – לאימון. מיומנות נרכשת בצורה חלקית בעבודה שוטפת. תהליך סדור ורחב של למידה מטעויות, הטמעת ידע שנרכש במקומות אחרים ומיומנות רחבה יותר נרכשים בתרגול ובאימון. מוצע לוודא שכל העובדים במערך ההגנה של הארגון, המגזר והמדינה יזכו ללמידה מתמדת בכל שיטה אפשרית ומעל לכול יקבלו אימון תקופתי, עם תובנות מעודכנות ותפיסות עבודה משוכללות יותר. קיימות בישראל חברות שמדריכות ומאמנות עובדים במערכי הגנה קיברנטיים לזהות ולהגיב נכון (מבחינה מקצועית ולפי מדיניות הארגון) להתרעות. ההחלטות של העובדים הללו עשויות לקבוע את הנתיב שבו תטופל התרעה. החלטה זו עלולה להיות הרת־גורל לארגון המותקף, ולפיכך ההשקעה הכרחית.

אחראי ההגנה הקיברנטית בארגון, ה־CISO (Chief Information Security Officer), הוא מקבל ההחלטות המקצועי העליון בארגון, והממליץ למנהל הארגון על נקיטת הצעדים הדרושים במהלכי הגנה החורגים מרמת הטיפול השוטף בהתרעות. אין ספק כי בעל התפקיד הזה חייב להיות ברמה מקצועית גבוהה. הוא חייב להיות בעל כישורי ניהול ומנהיגות הנובעים מקצב העבודה ומקצב השינויים בתחום, מניהול עובדים ייחודיים ברמה מקצועית גבוהה מאוד ומלחץ במקרים של תקיפות רציניות, ונדרשים אורך רוח וקור רוח נוכח התרעות שווא ו"רעש" שמערכות ההגנה מייצרות. יחד עם זאת וחשוב מכל אלה, אחראי ההגנה הקיברנטי בארגון חייב להיות משימתי ולחשוב כל העת על נקודות התורפה של ארגונו ועל הדרכים לטפל בהן. אחראי כזה צריך לעסוק במהות (מאיזו פרצה בלתי־מזוהה ובאיזה דרך יצירתית תגיע התקיפה) ופחות בסוגיות של נראות ההגנה, היצמדות לנהלים וחשיבה על יכולתו להוכיח שפעל באופן סביר כשתתגלה התקיפה. אחראי כזה צריך, לדוגמה, ליזום בדיקות PT (Penetration Test) שוטפות על ידי צוות פנימי, אם קיים כזה, ובעיקר על ידי צוותים חיצוניים משתנים, כדי להביא תוקפים עם חשיבה ייחודית לחשוף בפניו את חולשות מערך ה־IT של ארגונו. הוא צריך לאמן את עצמו ואת אנשיו להתנהלות במצבים שבהם התקפה התגלתה בתוך הרשת הארגונית, ונדרשים קור הרוח, המקצועיות והסבלנות כדי להגיב באופן מתוחכם ומוצלח לסיכול מטרת התוקף, ולאו דווקא לסיכול המתקפה. אחראי הגנה קיברנטי בעל רוח כזו עשוי להיות ההבדל בין תקיפה שהצליחה לזו שסוכלה.[109]

מנהלי הארגונים צריכים לראות בהשקעה בהגנה קיברנטית חלק מובנה מתשתית הארגון שלהם, ויכולת מהותית־מקצועית שבלעדיה הארגון לא יכול להתקיים. ההגנה הקיברנטית על הארגון היא אחריותו של מנהל הארגון לא פחות מרווחים, ייזום עסקאות חדשות ומציאת דרכים להגדיל את החברה. הסוגיה של ההגנה על המידע ותמיכת מחשב בתהליכי העבודה בארגון צריכה להיות חלק מהמהות, ולא עניין לניהול טכנולוגי טקטי של מנהל IT או Cyber Security כזה או אחר. אחד הקשיים הגדולים של מנהלי חברות וארגונים הוא המשאבים שמערך הגנה קיברנטי דורש, וההשקעה בהם בעייתית. הדבר דומה להשקעה בתקציב הביטחון. בהרצאה שנשא מר דוד ברודט בכנס השנתי של המכון למחקרי ביטחון לאומי (INSS), הוא ניסה להסביר את הקושי במדידת התועלת בהשקעה בתקציב הביטחון בכך שהתקציב הזה נועד "למנוע אירוע [כדי] שלא יקרה בפועל בעתיד" ואשר "ההסתברות [שיתרחש] אינה ידועה לנו".[110] באופן דומה, השקעה בהגנה קיברנטית אמורה לטפל במניעת אירוע או השלכותיו כדי שלא יקרו בעתיד, ואשר כלל לא ברור שאכן עומד להתרחש אירוע כזה. ההשקעה הזו אינה נושאת רווח ישיר ומיידי ואפילו לא רווח עתידי. היא רק עשויה לחסוך "אסון" אפשרי לארגון, שכלל לא בטוח שיתרגש עליו. למרות הקושי המובן הזה, מנהלים צריכים להשקיע בהגנה קיברנטית מתוך כוונה למנוע מתקיפה עתידית להשיג את

מטרתה. המטרה הזו אינה מובנת מאליה או ברורה באופן אינטואיטיבי לכל המנהלים. לעיתים קיימת תחושה כי גם מנהלים פועלים כדי לצאת ידי חובה ולהראות כי התנהלו באופן סביר, לכשתתגלה התקיפה שתזיק לארגון. התנהלות מנהלים בתחום ההגנה הקיברנטית שאינה מכוונת במלואה למניעת השגת מטרת התוקף מקרינה על שאר העובדים בתחום, והיא עלולה, בסבירות גבוהה, לגרום לכישלון ההגנה הקיברנטית.

סיכום פרק ההגנה

הדיון בעקרונות המוצעים לאסטרטגיית הגנה קיברנטית לישראל נפתח בתיאור מערך הגנה משולב מפני תקיפות עומק (APT). סוג תקיפה זה הוא המטריד ביותר את מערכי ההגנה בעולם, הוא מאתגר ומתחדש ועלול לגרום נזק כבד לארגון שאותו הוא תוקף, אם יצליח. לתחושתנו, הטכנולוגיה המתפתחת בעולם ההגנה הקיברנטי מציעה אפשרויות חדשות יצירתיות להגנה, וניתן בניהול נכון להביא לכלל "היפוך יוצרות" שבמסגרתו המגן מנטר, מנתח ומגיב בצורה מתוחכמת לתקיפה ומונע את השגת יעדיה, לעיתים אף מבלי שהתוקף מודע לכך. אף שחלק חשוב במערך ההגנה המשולב שהוצע הוא היכולת לזהות מתקפה ללא מודיעין מוקדם, מומלץ להמשיך לנסות להשיג מודיעין מקדים מכל סוג ומקור. מודיעין עשוי לסייע במידה ניכרת בהתמודדות עם מתקפות מכל סוג. קיים מודיעין למתקפות ספציפיות שנועדו, בין השאר, להפגנת עמדה אידאולוגית מוצהרת וגלויה.[111] מודיעין אחר הוא תשתיתי יותר ותוצריו הם מחקר של כלי תקיפה, אפיון של קבוצות תקיפה ו/או אפיון של שיטות תקיפה.[112] המודיעין הזה, וכך גם מודיעין ממקורות אחרים, עשוי להועיל ולהביא לכלל התמודדות אפקטיבית וקלה יותר עם תקיפות. מוצע לשלב אותו כמרכיב במערך ההגנה, להשקיע ולפתח אותו כל העת, משום שבמשחק בין התוקף למגן הוא עשוי להוות בנקודה מסוימת בסיס ליכולת לאתר ולסכל מתקפה. ניתן להמליץ על מימוש הגנה משולבת ומדורגת מפני תקיפות חומרה/קושחה, והגנה המבוססת על שיטות וכלים קיימים מפני תקיפות מהירות ושטחיות. ההצעה היא לממש את כלל יכולות ההגנה הללו כהנחיה ברמת הארגונים במדינה, לפי מפתח חשיבות וחיוניות.

למימוש ההגנה הזו בארגון נדרש, בנוסף ליכולת הטכנולוגית המשולבת, גם גוף ארגוני שכל עיסוקו הוא הגנה קיברנטית על הארגון (CERT/CSOC ארגוני). כדי לממש את האסטרטגיה הזו ברמת המדינה נדרש גוף שעוסק בהנחיה אקטיבית למימוש האסטרטגיה, מרכז תמונת מצב קיברנטית מדינתית ומנהל מדיניות תגובה לכל מתקפה על הארגונים המוגנים ברמה הלאומית. רצוי שיהיה גוף אחד כזה, היות שבמצב הנוכחי בישראל קיים יותר מגוף אחד שהממשלה הטילה עליו אחריות בסוגיה, ולכן נדרש דיאלוג מתמיד בכל הרמות בין גופי ההנחיה השונים. מעבר להסדרת המבנה הארגוני

המדינתי, יש לפעול להטמעת תרבות של דיווח ושקיפות מרבית בנוגע לתקיפות, לשיטות הגנה, לכלי הגנה ולממצאים רלוונטיים מחקירות.

נדרש לוודא רמה מקצועית גבוהה ככל שניתן בקרב עובדי מערך ההגנה הקיברנטי בכל הארגונים ובכל הרמות, להמריץ התמקצעות של מנהלי ההגנה הקיברנטית בארגון ולחפש כל העת את החולשות והפרצות במערך המחשבים, הרשתות והמידע הארגוני במטרה לתת להם מענה, לעודד מנהלים לראות בסוגיית הביטחון הקיברנטי תחום אחריות מהותי שלהם ולהשקיע את הדרוש לצורך מימוש הגנה קיברנטית אפקטיבית.

התקפה

להתקפה במרחב הקיברנטי מניעים שונים, מבצעים שונים ומטרות שונות. פירטנו את שלושת הסוגים הידועים של מטרות ההתקפה (CNA, CNE, CNI). את ההתקפות הללו מבצעים גורמים שונים, מדינות, קבוצות לא־מדינתיות ויחידים, חלק מהתקיפות נעשות על ידי שכירי תקיפה (בעיקר כשמדינה לא מעוניינת לקשור עצמה לתקיפה).[113] המניעים לכל סוגי התקיפות יכולים להיות אידאולוגיים, אתגר טכנולוגי, פשע (לרוב גניבת כסף), מסחריים או טכנולוגיים (גניבת סודות מסחריים, פטנטים, מידע מוגן זכויות יוצרים), ריגול (גניבת סודות מדינה), עימות כוחני, מימוש מדיניות.

עבור מדינה, התקפה במרחב הקיברנטי היא חלק מתוכנית להשגת אינטרסים. לא נמצאה עדות לכך שהתקפה קיברנטית לבדה הביאה למימוש אינטרס זה או אחר של מדינה כלשהי. עם זאת, ראוי לציין כי אין כמעט עדויות מפורשות לתקיפה קיברנטית שביצעה מדינה וקיבלה אחריות לכך, ובכך אפשרה מדידה של ההישג שהתקיפה הקיברנטית השיגה.

נבדיל בין שלושה מצבי תקיפה – גלוי, עמום וחשאי. במצב גלוי התקיפה מאותרת וידועה, קיימת קבלת אחריות רשמית או יכולת הוכחה משפטית לאחריות של מדינה/ארגון לתקיפה. במצב "עמום" התקיפה מאותרת וידועה, אין קבלת אחריות רשמית, אף על פי שניתן לעיתים לנחש או להניח מי עומד מאחורי התקיפה. שאיפת התוקף היא שחקירה, אם תמומש, לא תצליח להביא הוכחה משפטית לאחריותה של המדינה לתקיפה. במצב "חשאי" התקיפה מוסתרת כך שהמותקף (ובשאיפה – אף אחד חוץ מהתוקף) אינו יודע על התקיפה. מרגע שהתקיפה אותרה והיא ידועה למותקף או לגורמים אחרים (בין אם פורסמה ברבים ובין אם לאו), היא תימצא בסטטוס של "עמימות", לעיתים אפילו ללא השערה מובהקת לגבי זהות מדינה אחת אחראית.

מאחר שאנו רואים במרחב הקיברנטי המשך ישיר וחלק בלתי־נפרד מהפעילות בעולם הקינטי, הרי יעדי התקיפה הקיברנטית של מדינה רחבים כמרחב האינטרסים שלה, ומהווים חלק ממגוון הפעולות שהיא נוקטת להשגת יעדיה. תקיפה קיברנטית תוכל להעצים ולמנף אפקטים קינטיים, ובכך לתרום לקיצור משך המערכה או למובהקות התוצאה שלה. ברי שהתקפה קיברנטית אינה מחליפה את המערכה הכוללת מאחר שבעתיד הנראה לעין, השגת יעדי מערכה רק על ידי פעולה קיברנטית אינה ריאלית.

התקפה קיברנטית במצב גלוי ובמצב עמום

כדי לגבש קווים מנחים בנושא ההתקפה באסטרטגיית הסייבר של ישראל, יש להבין כיצד תחום התקיפה נתפס ומיושם על ידי מדינות בעולם. לשם כך ניתן להתמקד בכמה נקודות בתפיסה האמריקאית כפי שהיא באה לידי ביטוי בשיח בארצות־הברית, ובכמה מסקנות אפשריות מהמערכה הקיברנטית שהייתה חלק מהמלחמה בין רוסיה לגיאורגיה ב־2008. התקפה קיברנטית של מדינה כחלק מעימות גלוי ומוצהר נועדה לסייע בהשגת המטרה או לחדד את מובהקות התוצאה, והיא צריכה להיות חלק מתוכנית כוללת צבאית, מדינית, כלכלית, תודעתית־מורלית, או שילוב שלהן.

הבחינה המיוחסת לממשל אובמה בארצות־הברית לגבי היכולת של תקיפה קיברנטית לפתור את סוגיית תקיפות חיל האוויר הסורי על אזרחים במלחמת האזרחים בסוריה ללא פעילות צבאית נלווית אינה מפתיעה במסקנות שלה – לא ניתן לממש סוג כזה של הישג רק באמצעות תקיפה קיברנטית.[114] מכאן שהמחשבה כי ניתן להשיג מטרת מדינה באמצעות תקיפה קיברנטית בלבד אינה מעשית בשלב זה, ככל הנראה.

התקפה קיברנטית כחלק מעימות גלוי ומוצהר יכולה להיות במאפייני CNA, CNE או CNI, והיא יכולה להיות גלויה, עמומה או חשאית. מהשיח הגלוי בארצות־הברית ניתן ללמוד כי מתקפה קיברנטית על ארצות־הברית עלולה לשמש עילה לתקיפה נגדית במרחב הקיברנטי, ויכולה לשמש גם בסיס לתגובה קינטית מצד ארצות־הברית. האמריקאים רואים בסייבר מרחב פעילות כשאר ארבעת המרחבים, ולכן אינם מגבילים עצמם לפעילות רק במרחב הקיברנטי. מעורבות אמריקאית בעימות כלשהו יכולה לבוא לידי ביטוי גם בפעילות אמריקאית במרחב הקיברנטי. ברור כי לצורך ביסוס אסטרטגיה מסוג זה יש לעסוק בבניין כוח מקדים, שתכליתו בניית יכולת תקיפה במרחב הקיברנטי.[115]

לפיכך, משרד ההגנה (Department of Defense - DoD) בארצות־הברית נערך באופן שיטתי לממש פעילות התקפית במרחב הקיברנטי כחלק המובנה בתפיסת הלחימה האמריקאית. מהדברים שנכתבו בפרק סקר הספרות ניתן לראות שארצות־הברית חותרת להגיע למצב שבו השימוש בסייבר התקפי והגנתי יהיה חלק מובנה ממכלול הכלים של המפקד, והוא ינהל ויתמרן אותו כמו שהוא מתמרן כוחות יבשה, בצורה משולבת ובתפיסה רחבה יותר של הפעלת כוח.[116] הקמת זרוע הסייבר המתוכננת בצה"ל מבהירה אף היא את ההבנה שיש לשלב יכולות סייבר התקפיות בארגז הכלים של המפקד הישראלי, ובתוכניות האופרטיביות של צה"ל.

לפי שעה, אין עדויות לשימוש בלחימה קיברנטית על ידי ארצות־הברית כחלק מעימות מערכתי כולל. נהפוך הוא, העדויות הן על הימנעות משימוש בפעילות תקיפה קיברנטית, כפי שתואר במקרה הסורי לעיל, וכפי שמשתקף מניתוח ההימנעות האמריקאית מתקיפה קיברנטית שאמורה הייתה למוטט את כוחו הכלכלי של סדאם חוסיין ערב

המתקפה ב־2003, ולמנוע ממנו יכולת לממן את הלחימה ולשלם לכוחות המזוינים שלו. אירוע מסוג זה (בהנחה שהתרחש באופן הזה) משקף הרתעה עצמית הקיימת בארצות־הברית לגבי שימוש בהתקפה קיברנטית כחלק מלחימה. עיקרו של החשש הוא מהשלכות עקיפות על גורמים שאינם היעד להתקפה, וכן מאי־עמידה בדרישות הדין הבינלאומי ובעיקר בעקרון המידתיות.[117]

דוגמה למימוש תקיפה קיברנטית בעת עימות גלוי יכולה לשמש מתקפת הסייבר שבוצעה על גיאורגיה במהלך המלחמה בינה לבין רוסיה באוגוסט 2008. ליבת התקיפות היו פעולות DDoS ו־Defacing. התקיפות כוונו לאתרי חדשות וגופים ממשלתיים גיאורגיים, בוצעו בגלים של מספר שעות, ובשילוב של פעולות קינטיות ואלקטרוניות לשיתוק מערך התקשורת בגיאורגיה הן היו אפקטיביות. התקשורת של ממשלת גיאורגיה עם אזרחיה ועם העולם שובשה בצורה מהותית. הבנק המרכזי בגיאורגיה הפסיק את המסחר המוניטרי האלקטרוני בעקבות התקיפות הללו. ניכר כי מממשי התקיפות היו ממוקדי מטרה (שיבוש מהותי של התקשורת הגיאורגית) וידעו מה הם עושים (לתקיפה של אוגוסט קדמו תקיפות ביולי על אותם אתרים). הגיאורגים הבינו כי הם מצויים תחת מתקפה קיברנטית וניסו להתגונן. הם חסמו כניסת תקשורת אינטרנט מרוסיה כדי למנוע תקיפות ותעמולה. ממשלת גיאורגיה ניסתה לקבל שירותים מחברות תשתית במדינות שונות וגם התשתית הזו הותקפה, כולל תשתית אמריקאית. התקיפות מיוחסות לגופים שאינם רשמיים, לגופי פשע או לגופי תקיפת סייבר להשכרה (התוקפים מימשו את רוב התקיפות מאתרים באירופה ובארצות־הברית). יחד עם זאת, העיתוי של ביצוע המתקפה הקיברנטית (ב־8 באוגוסט, עם כניסת הכוחות הרוסיים לגיאורגיה) מעלה את המחשבה על קשר אפשרי בין הממסד הרוסי לקבוצות התוקפים, אולם קשר כזה לא ניתן להוכחה. גם בהיעדר קשר כזה, וגם אם נאמין כי מדובר במעורבות אזרחים אכפתיים ממניעים אידאולוגיים, התופעה שבה גורמים לא־רשמיים יכולים להתערב בעימות צבאי בקלות ובאפקטיביות היא מרשימה.[118]

בדומה לאסטרטגיה במספר מדינות, בדגש על ארצות־הברית, ראוי שהאסטרטגיה הלאומית של מדינת ישראל בתחום הסייבר תכלול שילוב מאמצי סייבר התקפיים בכל המערכות הרלוונטיות, במשולב עם מאמצים קינטיים. במסגרת זו נדרש להפנים את הדין הבינלאומי שיחול על המרחב הקיברנטי. ההנחה היא שדיני המלחמה המקובלים יחולו גם על מרחב הסייבר, והעוסקים בסייבר התקפי יידרשו לעמוד בדרישות אלה.[119]

התקפה כאמצעי להעברת מסר

עימות גלוי בין שני צדדים אינו מחייב עימות קינטי ישיר ביניהם. "דיאלוג" בין שני צדדים מתקיים בצורות שונות, וכלים קיברנטיים יכולים לשמש "שפה" בפני עצמה בעימות. פעילות כזו היא תוגדר כמתקפה לצורכי השפעה (CNI). דוגמה אפשרית ניתן

לראות בתקיפה שבוצעה באוגוסט 2012 על חברת Aramco הסעודית ועל חברת RasGas מקטאר. בתקיפה על Aramco הושמד מידע בכ 30,000 מחשבים של החברה. בכירים בממשל האמריקני התבטאו בזמנו שאיראן אחראית למתקפה זו.[120] ניתן להעריך שזו באה כדי להעביר מסר הרתעתי לארצות הברית בהקשר למשטר הסנקציות על איראן.

דוגמה אפשרית נוספת היא העימות בין ארצות־הברית לצפון־קוריאה. במסגרת עימות זה תקפה צפון־קוריאה את הרשת של חברת 'סוני' כחלק ממערכה שנועדה למנוע הקרנת סרט עלילתי על מנהיג צפון־קוריאה. לתקיפה נלוו איומים בתקיפת טרור על רשתות בתי קולנוע, במטרה למנוע את הקרנת הסרט. התגובה של חברת 'סוני', שנכנעה בתחילה ללחץ ורק לאחר מכן התירה את הקרנת הסרט, והתגובה של הממשל האמריקאי שביקש מ'סוני' לא להיכנע, ושכנראה עומד מאחורי התגובה של התקיפה הקיברנטית שבמהלכה נותקה צפון־קוריאה מהאינטרנט – סיימו את הפרשיה.[121] המהלכים הללו מאפשרים לנתח את הפרשיה הזו כ"דו־שיח" בין מדינתי בשפה קיברנטית, שהוא חלק ממערכה כוללת, רחבה יותר.

מהמתואר לעיל ניתן לנסח כמה מסקנות ולהשתמש בהן כקווים מנחים לגיבוש אסטרטגיה בנושא ההתקפה:

א. יכולת התקפית קיברנטית אינה עומדת בפני עצמה. היא צריכה להיות חלק מתוכנית כוללת כדי להשפיע בעימות גלוי כולל.

ב. ניתן לממש תקיפה קיברנטית אפקטיבית למטרה ממוקדת (לדוגמה – שיבוש התקשורת של הממשלה במקרה הגיאורגי) גם באמצעות תקיפה שטחית, מהירה ורחבה של יעדים שאינם "יעדי זהב" (מטרות צבאיות, תשתיות מדינה), אם הדבר משתלב בתוכנית כוללת.

ג. תקיפה אפקטיבית לא חייבת להיות תקיפת עומק מתוחכמת. במקרה דנן, תקיפות DDoS ו־Defacing השיגו את יעדן. גם יעד שאינו "עתיר סייבר" ומבוסס טכנולוגיה יכול להיפגע בצורה משמעותית מתקיפה. (יתרה מכך – קיימת טענה כי דווקא מדינה שאינה מפותחת מבחינה טכנולוגית תיפגע במידה רבה יותר מתקיפה קיברנטית, משום שיש לה גם פחות יכולות הגנה).[122]

ד. ניתן לממש תקיפות קיברנטיות אפקטיביות באמצעות שליחים (Proxy) מבלי לקבל אחריות, כחלק ממלחמה גלויה שהפן הקינטי שלה מוכרז כאחריות מדינה. למתקפה קיברנטית נדרשים בניין כוח, הכרת היעד ותכנון מוקדם.

ה. ניתן להסיק שתקיפה קיברנטית יכולה להוות נדבך ב"שיח" בין מדינות, כשמטרת התקיפה היא להעביר מסר (לרוב – מרתיע).

התקפה כחלק ממערכה חשאית

מערכה חשאית היא מאבק באמצעים נסתרים, ששימוש בהם והאחריות לתוצאות – אם הם מתגלים – ניתנים להכחשה. מדינה מנהלת מערכה חשאית במטרה להשיג אינטרסים או לשמור עליהם. בניהול מדיניות בסוגיות מרכזיות ומורכבות, מדינות יכולות לפעול במסגרת מערכה גלויה וגם באמצעות מערכה חשאית, שמסייעת לניהול הפן הגלוי ותורמת להשגת המטרה (לדוגמה, גניבת מידע/ריגול).

באופן טבעי, אין בנמצא דוגמאות מוכחות למערכה קיברנטית חשאית, בעיקר משום שאין קבלת אחריות על מתקפות כאלה גם לאחר שנחשפו. לצורך המחשת מתקפה חשאית וגיבוש המלצה לאסטרטגיה בתחום ניתן לעשות שימוש בניתוח המקרה הידוע ביותר של לחימה קיברנטית חשאית – מקרה התקיפה של אתר הגרעין האיראני בנתנז באמצעות Stuxnet.[123]

כפי שהוזכר בסקירת הספרות שלעיל, הניתוח שמציע ראלף לנגנר מצביע על תקיפה שכללה שני חלקים. התקיפה בחלקה הראשון הייתה חשאית, ואופן מימושה נועד להשיג מטרה ממוקדת שאינה הרס המוני ומיידי של מערך הצנטריפוגות.[124] במהלך התקיפה בוצעה החלטה לעבור מטקטיקת הפעולה הזו לטקטיקה שנועדה להפיל כמות גדולה של צנטריפוגות, גם במחיר של חשיפת התקיפה, ובהתאמה שונתה התקיפה.[125] לנגנר מתאר את האפשרות לשימוש שנעשה בקבלנים (Contractors) שהיו קשורים למערך בנתנז, כדי להביא את הנוזקה לתוך המחשבים הרלוונטיים.[126]

בנוסף לנזק שתוכננה הנוזקה לממש בנתנז, לנגנר מתאר במאמרו את ההתקפה ככזו שנועדה גם להביא מידע. העובדה ש־Stuxnet דילגה למערכים נוספים אפשרה, לדבריו, לתוקפים לבחון את המערכים הללו כאפשרות לקבלת מידע על קבלנים הקשורים לנתנז, ואולי אפילו קשר למתקני גרעין חשאיים של איראן.[127]

מאפייני התקיפה החשאית, כפי שנותחו על ידי לנגנר, כוללים מציאת נקודות התורפה במערך הנתקף כדי לעקוף מנגנוני הגנה ולחדור למחשבים הרלוונטיים (ניצול שרשרת האספקה כדוגמה המנותחת אצלו). על פי הניתוח שלנגנר מציע, היעד של תקיפה למטרות הרס קובע את אופייה (דוגמת ההבדלים בין הגרסה הראשונה של Stuxnet לגרסה השנייה), וכן ניתן לנצל תקיפה למטרת הרס גם לצורך איסוף מידע. שינוי מטרה במהלך תקיפה חשאית הוא מהלך אפשרי שיכול לגרור שינוי כלי התקיפה וטקטיקת התקיפה, כפי שלנגנר מספר על השינוי במטרה של Stuxnet. גם לאחר הגילוי, יש להימנע מאפשרות של הוכחת קשר (ברמת הוכחה משפטית) לתוקף. במקרה דנן התקיפה מיוחסת לארצות־הברית, ולעיתים לפעילות משותפת לארצות־הברית ולישראל, אך ללא הוכחה ממשית שמאפשרת קישור חד־משמעי של התקיפה למדינות הללו.

סיכום פרק ההתקפה

ההתקפה הקיברנטית ככלי בשימוש המדינה היא חלק ממערכה רחבה יותר, והיא אינה עומדת בפני עצמה. יכולת התקפית קיברנטית היא דרך נוספת שבה המדינה פועלת להשגת יעדיה ולשמירה על האינטרסים שלה. ההמלצה המרכזית היא להטמיע את ההתקפה הקיברנטית בכל התוכניות ברמות השונות ככלי המסייע, כחלק מתוכנית רחבה יותר, להשגת המטרה. ניתן לסכם את סוגיית התקיפה כולה בטבלה הבאה:

	עימות גלוי	עימות חשאי
סוג התקיפה	גלויה או עמומה (כולל שימוש ב־Proxy) כל סוגי התקיפות רלוונטיות – קצרה ושטחית, עומק, חומרה/קושחה שהוכנו מבעוד מועד.	חשאית, ולאחר גילוי – עמומה. סוגי התקיפות הרלוונטיות ־עומק, חומרה/קושחה.
סוג היעד	ייעודי (צבאי/ממשלתי) או אזרחי.	ייעודי (צבאי/ממשלתי) או אזרחי.
הישג נדרש מהתקיפה	איסוף / השפעה (כולל להעברת מסרים) / הרס.	איסוף והרס.
מעמד התקיפה	חלק ממערכה.	חלק ממערכה.
מאפיינים	תוצאות גלויות מיידיות (לתקיפות השפעה והרס), אפשרות להגעה לעימות קיברנטי גלוי בזמן אמת, תגובה יכולה להיות במישור הקינטי, יכולה לשמש "שפה נוספת להעברת מסרים" בין יריבים.	התוצאות תלויות בתכנון התקיפה ולא תמיד מופיעות מייד במלוא העוצמה.

תובנות והמלצות

הדיון על גיבוש אסטרטגיה לפעולה במרחב הקיברנטי לישראל אינו שונה במהותו מדיון על אסטרטגיה מדינתית בכל תחום אחר. יש לדעת מהו ההישג הנדרש ונדרשת תוכנית שתתווה את הדרך להגיע להישג זה. דיון לקביעת אסטרטגיה הוא תמיד מאתגר ומורכב, ובמדינת ישראל לעתים מורכב שבעתיים, לנוכח הנטייה להתנהל ממקרה למקרה ולקבע את התגובה הנקודתית כאסטרטגיה. אבל בכל הנוגע לדיון על המרחב הקיברנטי, יש כמה אתגרים מורכבים נוספים. ראשית, כללי המשחק בשדה הקיברנטי טרם גובשו במערכת היחסים הבינלאומית. לפיכך, כל מדינה משתדלת לשמור את האסטרטגיה שלה, בפרט זו העוסקת בהתקפה, מאחורי מעטה חשאיות ותוך יכולת הכחשה. אתגר נוסף הוא היותה של ליבת העיסוק במרחב הקיברנטי טכנולוגית. היכולת הטכנולוגית היא שמאפשרת לגבש תוכנית אסטרטגית ולהשיג את יעדי המדינה. הטכנולוגיה הזו נמצאת כל העת בפיתוח ובמסע קידום מכירות אגרסיבי, ורק חלקה הקטן נמצא בסטטוס של טכנולוגיה מוכחת. דווקא הטכנולוגיה החדשנית, שנועדה לתת מענה לפערים ביכולת ההגנה במרחב הקיברנטי, טרם הוכיחה בשלות מלאה. לפיכך יש לבסס את האסטרטגיה המוצעת על תפיסה וכיוונים טכנולוגיים הנראים מבטיחים, גם אם טרם הבשילו לכלל פתרונות מוכחים. לבסוף, כמו בכל תחום חדש, מתפתח, עתיר משאבים, מרכזי ומבטיח, מתקיימים מאבקים ארגוניים על אחריות, על סמכות ובעיקר על שליטה במשאבים. הנטייה לעסוק בסוגיה הארגונית ברמת המדינה מובנת, אך כתהליך היא בבחינת "רתימת העגלה לפני הסוסים". התהליך הנכון הוא לקבוע יעדים, תוכנית, טקטיקת מימוש ותרבות שבה נתנהל במרחב הקיברנטי, ורק אז להתאים את המבנה הארגוני לתוכנית ולתהליכי העבודה למימוש התוכנית. בהיעדר סדר דברים נכון, נדרש היה להתייחס למציאות הארגונית בישראל – שעליה החליטה הממשלה – כאל אילוץ, ולנסות להמליץ איך כדאי לפעול במסגרת זו.

בניית האסטרטגיה בתחום הקיברנטי לכל מדינה מתחילה בהגנה. הדבר נובע מכך שעיקר האתגר והפער מצויים כיום ביכולתה של המדינה להגן על נכסיה ועל אזרחיה מנזק המתחיל בפעולה קיברנטית, אך החשש האמיתי ממנו נובע מהשלכותיו הקינטיות. מדינות חוששות מאובדן סודות, מפעילות ריגול שתשאב מידע רב האגור כיום במערכות מחשב מדינתיות. החשש מריגול אינו חדש (הגם שהמרחב הקיברנטי מעצים אותו מאוד). תחום חדש, לא מובן עד סופו ולכן מפחיד, הוא האפשרות שהמדינה

תיפגע בתחומים מהותיים לקיומה. מדינות חוזרות חדשות לבקרים על החשש מפעולה קיברנטית שתכליתה שיתוק מערכת האנרגיה במדינה, מפגיעה קיברנטית שתביא לקריסת המערכת המוניטרית או מפגיעה ביכולות צבאיות בעת מבחן, כתוצאה מפעילות קיברנטית מקדימה. החששות הללו, בתוספת היתרון המובנה ששמור לתוקף ואיכות ההתקפות העולה כל העת, הביאו לצורך לוודא שקיים פתרון אפקטיבי לאתגר ההגנה במרחב הקיברנטי ברמת התפיסה ושיטת הפעולה, וברמת הטכנולוגיה.

עיקרי ההמלצות

מדינת ישראל נדרשת לממש פעילות במרחב הקיברנטי, הן פעילות הגנתית והן פעילות התקפית. מטרת האסטרטגיה שאנו מציעים היא לאפשר את הפעילות הזו באופן שתשיג את יעדיה בעת שתידרש לכך, ותגן על נכסי המדינה ברמת ביטחון גבוהה יחסית לאורך זמן. במסמך זה נותחו מרכיבים שונים וניתנות המלצות באשר לכיווני פעולה בהיבטי ההגנה וההתקפה של מדינת ישראל במרחב הסייבר. לסיכום ההמלצות הללו, נראה כי נכון להדגיש מזווית נוספת כמה מהמרכיבים היסודיים של יסודות האסטרטגיה הלאומית, שעליהם בנויים כיווני הפעולה המומלצים.

המלצות בתחום ההגנה

• שימוש בטכנולוגיה בהגנה

ראוי לעשות שימוש במערך טכנולוגי המשלב מתודולוגיות שונות וכלי הגנה התואמים את המתודולוגיות הללו. מוצע לנצל את היתרון היחסי של התעשייה הישראלית בתחום ולבחון בחיוב, ביתר קלות ובהתמדה שילוב והטמעת כלי הגנה חדשים במערך ההגנה הארגוני. ראוי לקיים דיאלוג מתמיד עם מספר רב של ארגונים בתעשייה הרלוונטית בישראל ובעולם, לבחינה מתמדת וסדורה של מוצרים.

• בחירת התגובה הנכונה בהגנה

מומלץ לגבש גישה המבוססת על הגנה אקטיבית, החל ממניעת תקיפה מיידית, דרך שיבוש טכנולוגי שימנע מהתוקף להגיע ליעדו וכלה בהכלת התקיפה ומימוש הטעיה, שלא תאפשר לתוקף להשיג את מטרתו ולא תאפשר לו להבין שהתגלה עד למועד מאוחר מאוד.

• שיתוף פעולה בינלאומי ופנים־מדינתי

מומלץ לממש ולהעמיק את שיתוף פעולה בכל הרמות למטרות הגנה בסייבר עם מדינות עמיתות, ובתוך המדינה – בין המערך הממשלתי למגזר הפרטי. בנוסף מוצע שישראל תרחיב את פעילותה בפורומים בינלאומיים רלוונטיים.

בתחום ההתקפה

מוצע להכניס את המתקפה הקיברנטית כחלק מובנה בתוכניות להשגת יעדי המדינה ושמירה על האינטרסים שלה. יש לפעול למימוש מתקפה קיברנטית רק לאור הגדרת הישג נדרש.

באשר לשילוב בין התקפה להגנה, מוצע לשלב תוקפים במערך המרכזי המגן על ישראל לצורך תכנון ותפעול שוטף של מערך ההגנה.

בתחום הארגון

• שילוביות המרחב הקיברנטי והמרחב הקינטי

מוצע להתייחס למרחב הקיברנטי כאל חלק מהחיים הפיזיים והממשיים במרחב הקינטי, ולא לראות בו מרחב העומד בפני עצמו, ולממש את החשיבה הזו בהחלטות רלוונטיות כמו המבנה הארגוני ברמת המדינה בסוגיה הקיברנטית, או בסוגיית שיטות פעולה נבחרות במרחב הקיברנטי.

• האנשים ורוח המשימה

מומלץ לקבע הכשרת מקצועית מתמשכת לבעלי תפקידים בתחום הקיברנטי (גם האוטו־דידקטיים) במסגרת לימודי מדעי המחשב מותאמים, וכן אימון ותרגול בנושא באופן מתמיד. מומלץ גם להכשיר את מנהלי הגופים הקיברנטיים לבחירת התמהיל הנכון לקבוצה שבאחריותם, וליצירת רוח המשימתיות הדרושה.

• הקשר בין ארגוני מדינה לתעשייה הקיברנטית בישראל

מומלץ לארגונים הלאומיים בישראל העוסקים במרחב הקיברנטי להיות מעורים ולהכיר את כיווני החשיבה והפיתוח החדשים, לפחות אלה הקיימים בתעשייה הקיברנטית בישראל.

מומלץ לבצע העברה דו־כיוונית של מידע בצורה זהירה ומבוקרת בין ארגונים ממלכתיים לארגונים אזרחיים מהשוק הציבורי/פרטי בישראל. יש לעגן על בסיס חקיקה קשר דו־כיווני כזה מבלי לפגוע בביטחון המדינה ומקורותיה המודיעיניים, ומבלי לפגוע בצורה מהותית בזכויות צנעת הפרט.

• מבנה ארגוני

מומלץ שיהיה גוף אחד האחראי לניהול המערכה על ההגנה הקיברנטית הלאומית כולה. בכל מגזר ובכל ארגון ממשלתי או גוף העובד עם הארגונים הממשלתיים, יש לוודא קיומו של גוף ארגוני אחראי על הפעילות הקיברנטית. גוף כזה יונחה על ידי הגוף המדינתי המרכזי, וידווח על כל אירוע או חידוש בתחום. בשל היותו של המרחב הקיברנטי חלק מהתנהלות מערכה קינטית, ומשום שהגנה במרחב הקיברנטי היא

בעלת אופי ביטחוני בעיקרה, מומלץ להתבסס על גוף ביטחוני כאחראי מטעם המדינה על ההגנה הקיברנטית.

• בזכות "ההתנהלות הלא־רשמית" הישראלית

ראוי יהיה להתייחס לשיטת התנהלות ישראלית הלא־רשמית, שמוצאת את מקומה גם בהתנהלות במרחב הקיברנטי. ההיכרות במסגרת רשתות חברתיות רחבות, ההתנהלות החברתית, הרצון לסייע, הרצון לקחת חלק בפעילות בעלת גוון לאומי, הרצון להיות ב"מרכז העניינים" ולהוכיח רלוונטיות אישית ומקצועית – כל אלה מובילים בישראל להתגייסות אנשים רבים כל אימת שנדרש, בין אם כעזרה לחברים ובין אם לצורך לאומי, ובוודאי במצב המשלב בין שתי הסיבות. הפעילות על הבסיס הלא־רשמי הזה מתרחשת כמעט תמיד, וניתן לסמוך על כך שתתרחש באחוז גבוה מאוד מהמקרים שבהם היא נדרשת. בהיותה וולונטרית, מבוססת רצון טוב ומעוגנת בתרבות בישראל, היא חזקה יותר ולעתים איכותית יותר משיתוף פעולה הנובע ממחויבות מבנית, חוקית או נוהלית. היא יוצרת שיתופי פעולה אד הוק, ציוות של אנשים איכותיים מאוד מבחינה מקצועית ממקומות שונים, צינורות העברת מידע מהירים ופתוחים, פתרון מהיר לבעיות והתגברות על אתגרים שבהתנהלות רגילה היו אורכים זמן רב, ואף ספק אם היו נפתרים. לעתים, ההבדל בישראל הוא בין התנהלות ופתרונות יצירתיים, מהירים ואמיתיים, בדרך לא־רשמית ותוך הישענות על פרשנות לחוק ולכללים, לבין התנהלות בעצלתיים, גרירת רגליים ואף היעדר פתרון – כל זאת באופן מבוסס חוק, נוהל ואחריות ארגונית מנוסחים היטב.

מוצע לגבש חוקים, נהלים, הגדרות אחריות ארגוניות ומבניות, תרשימי זרימה ונוהלי עבודה, אך לא לדרוס את הפעילות הלא־רשמית. רצוי לאפשר לפעילות הזו להימשך לצד כל החוקים והנהלים, ולא להסס להשתמש בה בעתות בעיה ומצוקה, גם בהיעדר הלימה מלאה לכללים, לתרשים הארגוני ולאחריות הרשמית.

סיכום

קיימת שורת נושאים "לא בשלים" בעשייה הקיברנטית, שאף אם זכו להתייחסות במסמך זה, הרי התייחסות זו חסרה. נושאים אלה מושלכים על העשייה הקיברנטית מתוך מערכת מושגים וכללי ההתנהלות המוגדרים והמוסכמים בעולם הקינטי המוכר. ניכר שהנושאים הללו מצויים בתהליך הגדרה מחדש, שתאפשר התאמה אמיתית שלהם לעולם הקיברנטי. בנושאים אלה מצויות סוגיות משפטיות כגון: כיצד מוכיחים אחריות משפטית לנזק שנגרם מפעולה קיברנטית, או סוגיות ערכיות־מוסריות – האם נכון לממש תקיפה קיברנטית שלא ניתן "לתחום" אותה רק ליעד המוגדר שלה, ויש חשש שתזלוג ליעדים אזרחיים אחרים/נוספים ותפגע במערכות אזרחיות ותסכן חיים? לצד אלה קיימות סוגיות אזרחיות הנוגעות לשאלת אופן ההגנה על זכות האזרח לפרטיות, בעוד הרשויות זקוקות למידע כדי להגן עליו.

בנושא גישות הרתעה עולה השאלה: האם ניתן להרתיע מדינה, ארגונים או יחידים מביצוע פעולה קיברנטית עוינת למדינה, או לגורמים פרטיים ואזרחים בה? האם ההרתעה צריכה להיות קיברנטית בלבד, או שניתן לממש הרתעה בכלים קינטיים נגד פעולה קיברנטית? נושא ההתאוששות מתקיפה (או חוסן הסייבר הלאומי) נוגע לטקטיקות התאוששות, ולשאלות: האם ניתן לגזור גזירה שווה בין התאוששות מאסונות טבע כגון רעידת אדמה, שריפות, או אירועים מעשה ידי אדם, לבין מקרה של התאוששות מתקיפה קיברנטית? מה צריך להיות חלקה של המדינה בהתאוששות כזו? נושאים אלה זכו להתייחסות במסמך, אך בהיותם "לא בשלים", לפחות בחלקם, לא תמיד ניתן לספק המלצה ברורה לגבי ההתנהלות המוצעת לישראל בסוגיות הללו, וברי כי יש להמתין להמשך הבשלה, התנסות וחשיבה, בטרם ניתן יהיה לקבוע מסמרות למדיניות בתחומים הללו.

נקודה נוספת הראויה להתייחסות בהקשר זה נוגעת לשקיפות הנדרשת לארגון, למגזר ולמדינה במערכת ההתגוננות הקיברנטית. ארגונים נוטים באופן טבעי להסתיר נקודות חולשה או סוגיות שלדעתם עלולות להזיק להם. בשל כך קיימת נטייה של ארגונים לא לדווח, בוודאי לא בפירוט הנדרש, על תקיפה קיברנטית שחוו. בעיקר אמורים הדברים לגבי ארגונים שרמת האמינות שהציבור מייחס להם היא נכס מרכזי ועיקרי עבורם, ובלעדיו הם עלולים לעמוד בסכנת קריסה וסגירה. דוגמה מובהקת אך לא יחידה היא המערכת הבנקאית. היותו של חשבון הבנק עניין שבין הבנק ללקוח בלבד

היא הבסיס לאמון שנותן הלקוח בבנק, והסיבה לכך שהוא מוכן להפקיד את הנכסים הכספיים שלו בבנק. חשיפה שגורם זר חדר למערכת וביצע בה פעולות – מבלי שהבנק הגיב במועד ומבלי שהצליח להגן על המידע – עלולה להביא את הלקוחות לתחושה שכספיהם אינם בטוחים, ומכאן למצב שקריסת הבנק, ולעיתים המערכת הבנקאית כולה, עלולה להתברר כסיכון אמיתי ומוחשי. גם אם החשש מובן, היכולת להתגונן באופן אפקטיבי מחייבת שיתוף מידע בנקודה מוקדמת, ובצורה שקופה וחושפנית לגבי פרטי התקיפה והנזקים שגרמה. במגזרים רגישים כמו המערכת המוניטרית, ייתכן כי הדיווח והשקיפות צריכים להיות מוגבלים לבעלי התפקידים הרלוונטיים, לרגולטור ולגופים האחראיים על ההגנה במרחב הקיברנטי בישראל, ולאו דווקא לכלל הציבור. כך או כך, ברור כי דיווח ושקיפות הם הכרחיים, ויש לעמוד על מימוש העיקרון הזה כבסיס להגנה איכותית במרחב הקיברנטי.

בצד תהליך גיבוש האסטרטגיה במרחב הקיברנטי, נדרש להתייחס לכלים תומכים הכרחיים למימוש האסטרטגיה הזו, וביניהם: בניית יתרון יחסי טכנולוגי ושמירה עליו לאורך זמן, קיומו של תהליך עבודה מוסדר ומוסכם ודיאלוג מקצועי חיובי ושוטף בין כל הגופים הלאומיים העוסקים בהגנה ובהתקפה במרחב הקיברנטי, ובינם לבין מושאי ההגנה, שיתוף פעולה מקצועי בין הגופים הממשלתיים לבין גורמים חיצוניים כמו תעשיית הסייבר האזרחית בישראל, גופי ממשל של מדינות בעלות־ברית בכפוף לאינטרסים לאומיים ותעשיית סייבר בעולם על פי הצורך, ולבסוף – התאמת החוק הישראלי לפי הנדרש עבור הגנה אפקטיבית, תוך ליווי משפטי ברמה גבוהה בתחום המשפט הבינלאומי.

קיימות שתי נקודות שבהן יש לישראל ייחודיות, ונדמה שכדאי לשמר את הייחודיות הזו. נקודה אחת, ידועה ומהווה יתרון יחסי לישראל זה תקופה ארוכה, היא היותנו חברה בעלת כושר המצאה ויוזמה, בעיקר בכל הנוגע לתעשיית ההיי־טק, שעליה מבוסס המרחב הקיברנטי. רב מספרן של חברות ההזנק הישראליות המפתחות מוצרים עבור המרחב הקיברנטי, הרעיונות מרשימים וברובם מהווים מענה מקורי ובעל פוטנציאל לפתרונות מפתיעים וייחודיים לסוגיות שונות במרחב הקיברנטי. לישראל צורך אמיתי בשימור היתרון היחסי הזה ובהרחבתו, בעיקר באמצעות המשך הכשרה פורמלית של אוכלוסייה טכנולוגית בעלת כישורים, וכן באמצעות המשך השקעה פרטית וציבורית בשוק ההיי־טק הישראלי. הנקודה השנייה היא היכולת של החברה בישראל לייצר פתרונות אד הוק לאתגרים שונים. בשל היותה של רשתיות חברתית בסיס לפעילות בישראל ניתן לחבר יכולות, מוצרים ושיטות פעולה בזמן קצר ובאופן לא־רשמי לכלל פתרון אמיתי לאתגר בתחום הקיברנטי. ההוויה הזו, הנראית לעתים ככאוס, מאפשרת יתרון של תגובה מהירה, עקיפת מכשלות בירוקרטיות והתגברות על היעדר הגדרות משפטיות או עודף הגדרות סמכות ומאבקים ארגוניים. בצד הצורך לממש התנהלות

תקינה, ממוסדת ומבוססת עקרונות משפטיים וחוקיים, יש להקפיד שלא לבטל את היתרון הזה, המובנה בתרבות הישראלית.

כדי לרתום את כל בעלי העניין לפעולה מסונכרנת וסינרגטית, רצוי שחלק נכבד מהאסטרטגיה שתגובש תהיה גלויה לציבור, ותאפשר לו לגזור ממנה את מה שרלוונטי עבורו. מובן גם שלמסמך כזה צריכים להיות חלקים מסווגים שיעסקו בנושאים שהשתיקה יפה להם, ושיסייעו לתאם ולסנכרן ככל הניתן בין כלל ארגוני הביטחון הפועלים בישראל. זהו אתגר משמעותי ובר־השגה, שיוכל לקבע את מעמדה של ישראל כמובילה בתחום פעילות הסייבר בעולם.

נספח

מילון מונחים

מונח	המשמעות
כללי	
אסטרטגיה	מרכיבים יסודיים בתוכנית להשגת יעדי המדינה, תוך רתימת המשאבים הלאומיים כדי להגיע הישגים בפעולה במרחב הסייבר. המונחים מערכה וטקטיקה, המופיעים לרוב בהמשך לאסטרטגיה, מפרטים את דרכי הפעולה הקונקרטיות (כל מרחב ברמתו), את השיטה ואת האמצעים למימוש האסטרטגיה לפעולה במרחב הסייבר.
מרחב קיברנטי מרחב הסייבר – Cyberspace	המתחם הפיזי והלא־פיזי שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה.
התקפה קיברנטית	חדירה לא־חוקית, לרוב סמויה, למחשב, לרשת מחשבים או לכל כלי המחובר לרשת מבוקרת על ידי מחשב לצרכים שונים. התקפות מחולקות לפי מטרתן, לפי סוג/שיטת ההתקפה, ולעתים לפי כלי התקיפה.
הגנה קיברנטית	מניעת השגת יעדו של התוקף במרחב הקיברנטי. אין הכוונה בהכרח למניעת הגעה למחשבים או לרשת.
מטרות התקפה קיברנטית	
CNE- Computer Network Exploit	התקפה למטרות מיצוי המידע על המחשב/רשת והמידע האגור במחשב/רשת.
CNA - Computer Network Attack	התקפה למטרות הרס. הביטוי להרס יהיה בעולם הקינטי (לדוגמה – מחיקת מידע הכרחי, כיבוי חשמל, הפסקת הזרמת מים, שיבוש מערכות נשק).
CNI- Computer Network Influence	התקפה לצורכי השפעה פסיכולוגית, פגיעה במורל, השפעה על תודעה.
סוגי התקפות עיקריות	
מניעת שירות – DDoS – Distributed Denial of Service	הצפת אתר נותן שירות בכמות רבה מאוד של פניות סרק, באופן שחוסם אותו וגורם לקריסתו, ובכך נמנע שירות ממשתמשים.
השחתה/שינוי חזות – Defacing	שינוי חזות של אתר ושתילת מסרים המשרתים את המסר של התוקף.

מונח	המשמעות
התקפת עומק מתוחכמת / איום מתקדם מתמשך – APT – Advanced Persistent Threat	תקיפה, לרוב חשאית ומתוחכמת, לצורך שהות ממושכת ככל הניתן בעומק מערך או רשת המחשבים, לרוב לצורכי איסוף מידע וריגול, ולעתים כשלב בדרך למתקפה למטרות הרס.
כלים ושיטות תקיפה	
נוֹזֶקָה/קוד זדוני – Malware, Malicious Software	תוכנה/קוד שנעשה בהם שימוש על ידי משתמש לא־מורשה/לא־חוקי במחשב, לכל מטרה.
תקיפת "יום אפס" Zero-Day Attack	תקיפה המנצלת חולשה/פרצת תוכנה הידועה לתוקף ואינה ידועה למתגונן, לחברות המודיעין וההגנה וליצרנית התוכנה.
סוס טרויאני – Trojan horse	קוד/תוכנת מחשב מזיקה המנסה לחדור למחשב בהסוואה של תוכנה תמימה (השם שאול מהסיפור המיתולוגי על הסוס במלחמת טרויה).
דלת אחורית – Back Door	קוד המאפשר הרשאות לתוקף להיכנס למחשב הנתקף מרחוק.
רוֹבּוֹרֶשֶׁת – Botnet	רשת של סוכני תוכנה המותקנים במחשב (בדרך כלל ללא ידיעת בעל המחשב) לצורך ניצול המשאבים של המחשבים ברשת למימוש משותף של משימה, על בסיס מערך תוכנות חוקי המותקן בהם. בהקשר של תקיפה קיברנטית – המונח מתייחס להשתלטות מרחוק, לא־חוקית וסמויה על מחשב, ושעבודו למימוש משימות שהתוקף הגדיר.
דִיוּג – Phishing	ניסיון לא־חוקי להשיג מידע ממחשב, כמו שם משתמש (Username), סיסמה (Password) או פרטים מזהים אחרים על אנשים. בדרך כלל, הניסיון יתבסס על תקשורת דואר אלקטרוני (Email), מסרים מיידיים (Instant Massaging) או רשתות חברתיות (Facebook לדוגמה), והפניית המשתמש לאתר הנראה כאמין ולעתים מוכר.
התקפות חומרה/קושחה – Hardware/Firmware	התקפות המבוססות על שינויים בחומרה (בדרך כלל, כבר בשלב הייצור) או שינויים בתוכנה הנמצאת ברכיבי החומרה לצורכי תפעול ראשוני/בסיסי של המחשב.
סוגי הגנה קיברנטית	
הגנה מבוססת מידע/ מודיעין מקדים	הגנה מפני התקפה קיברנטית שבה קוד התקיפה מוכר ומזוהה ו/או יעד ומועד התקיפה ידוע. לדוגמה, תוכנות זדוניות (Malware) ידועות וחתומות, קרי, קוד תקיפה מוכר שמזוהה כולו או חלקו על ידי מערכות הגנה (כלי Anti-Virus מבוססים לרוב על היכרות מוקדמת כזו). דוגמה נוספת היא הגנה מפני מתקפת מניעת שירות, שניתנת לגביה התרעה גלויה מבחינת יעד ומועד.
הגנה שאינה תלויה במידע/ מודיעין מקדים	שימוש בטכנולוגיה שאינה תלויה באיסוף מידע על קודי תקיפה או על כוונות תקיפה, אלא מתבססת על היכרות מיטבית של הסביבה המוגנת.
כלים להגנה קיברנטית	

מונח	המשמעות
SIEM – Security Information and Event Management	המונח SIEM מורכב מחיבור של שני מונחים: SIM – Security Information Management שהוא ביטחון מידע המבוסס על אגירת נתונים ושמירת לוגים של פעילות מחשב, ניתוח מעמיק שלהם והבנה מקצועית של אירועים שהתרחשו. SEM – Security Event Management שהוא ניהול אירועי ביטחון מידע המתייחס ליכולת לנטר, להבין ולהגיב בזמן אמת או קרוב מאוד לזמן אמת לאירועי תקיפה קיברנטית על רשת מחשבים.
computer forensic science	ענף במסגרת חקירה מדעית דיגיטלית, שמתייחס לעדויות חוקיות (לעיתים לצורך הצגה בבית משפט) שנמצאו במחשב או באמצעי אחסון דיגיטליים. המטרה היא לבחון מדיה דיגיטלית בחקירה מדעית לצורך זיהוי, שימור, שחזור, ניתוח והצגת עובדות על המדיה הדיגיטלית הנחקרת.
Anti-Virus	תוכנה שנועדה לאתר וירוסי מחשב ולהגן על המחשב מפני פעילותם.

הערות

1 במונח "אסטרטגיה לפעולה בסייבר" הכוונה למרכיבים יסודיים בתוכנית להשגת יעדי המדינה, תוך רתימת המשאבים הלאומיים במטרה להגיע להישגים בפעולה במרחב הסייבר. המונחים "מערכה" ו"טקטיקה", המופיעים לרוב בהמשך לאסטרטגיה, מפרטים את דרכי הפעולה הקונקרטיות (כל מרחב ברמתו), את השיטה ואת האמצעים למימוש האסטרטגיה לפעולה במרחב הסייבר.

2 החלטת ממשלת ישראל מספר 3611, מיום 7 באוגוסט 2011. http://www.pmo.gov.il/secretary/govdecisions/2011/pages/des3611.aspx

3 נתי כהן, "הממד החמישי", **מערכות** 452, דצמבר 2013, עמ' 10, http://maarachot.idf.il/PDF/FILES/4/113334.pdf

4 ראו: קווי היסוד למדיניות הממשלה, כפי שמופיעים באתר הכנסת. ניתן לסכם אותם תחת ההגדרה הכללית של ביטחון ורווחה כלכלית, http://www.knesset.gov.il/docs/heb/coalition2013_3.pdf

5 יצחק בן־ישראל וליאור טבנסקי, "מבט בינתחומי על אתגרי הביטחון בעידן המידע", **צבא ואסטרטגיה**, גיליון 3, כרך 3, דצמבר 2011, http://heb.inss.org.il/index.aspx?id=4354&articleid=1126

6 שמואל אבן ודוד סימן טוב, **לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**, מזכר 109, יוני 2011, המכון למחקרי ביטחון לאומי, תל אביב, http://heb.inss.org.il/index.aspx?id=4354&articleid=1043

7 Tyrone C. Marshall Jr., "Cybercom Commander Calls Cybersecurity Order First Step," *DoD News*, February 13, 2013.
William J. Lynn III, "Defending a New Domain, The Pentagon's Cyber strategy," *Foreign Affairs*, September/October 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain
Claudette Roulo, "Alexander: Laws, Policies Lag Behind Changes in Cyber Threats," *DoD News*, February 27, 2014.

8 לדוגמה: ניתוח למתקפת "Red October":
Kaspersky Security Bulletin, "Kaspersky Lab Global Research and Analysis Team", 2013, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
וגם דוגמה לאפיון מגמות בתקיפה וניתוח מבוסס איסוף רחב:
Symantec, 2014 "Internet Security Threat Report," Volume 19, http://www.symantec.com/en/uk/security_response/publications/threatreport.jsp?inid=il_ghp_hero3_istr-2014-V19

9 Michael Porter, "What is Strategy?" *Harvard Business Review*, November 1996, https://hbr.org/1996/11/what-is-strategy

10 ראו לדוגמה: הדיון בנושא הסדרה חוקית של פעילות ה־NSA בתוך ארצות־הברית בהיבטי הגנה, כפי שמשתקף בדבריו של קית' אלכסנדר, מפקד פיקוד הסייבר וראש ה־NSA בעדותו בפני ועדת הכוחות המזוינים של הסנאט ב־12 במארס 2013 (עדות משותפת עם C. Robert Kehler, מפקד הפיקוד האסטרטגי של צבא ארצות־הברית). אלכסנדר מודע לקונפליקט בין הגנת הסייבר והזכות

לפרטיות, חושב שניתן לממש את שניהם בו־זמנית ומבקש לקבל נתונים ללא תוכן מספקיות האינטרנט ולתת להם מידע מסווג על מאפייני הפוגענים, כדי שימצאו אותם וידווחו בזמן אמת.
Hearing to receive testimony on U.S. strategic command and U.S. cyber command interview of the defense authorization request for fiscal year 2014 and the future years defense program, pp 8-10,
http://www.armed-services.senate.gov/imo/media/doc/13-09%20-%203-12-13.pdf

11 הגדרת המושג התקפת עומק ניתנת במילון המונחים בנספח לעבודה זו.

12 החלוקה בפועל בישראל תואמת בחלקה את המוצע כאן. הדיון במושאי ההגנה במרחב הקיברנטי בישראל ממוקד בסוגיות של מבנה וחלוקה בין־ארגונית בהיבטי סמכות, אחריות ומשאבים. לפירוט מושאי ההגנה במרחב הקיברנטי בישראל, ראו:
רועי גולדשטיין, **המרחב הקיברנטי וההגנה על תשתיות חיוניות**, הכנסת – מרכז המחקר והמידע, 12 במאי 2013. המסמך נכתב לקראת דיון בוועדת המדע והטכנולוגיה של הכנסת בנושא "קידום ישראל כמובילה בתחום הסייבר", עמ' 6-7, וכן הערת שוליים 19, שם,
www.knesset.gov.il/committees/heb/material/data/mada2013-05-13.doc

13 להלן ניסוח החלטת ממשלת ישראל מיום 7 באוגוסט 2011 על הקמת המטה הקיברנטי הלאומי, ובמרכזו הסוגיה הארגונית:
" לאור זאת, בהמשך להחלטת ועדת שרים לענייני ביטחון לאומי מספר ב/84 מיום 11.12.2002 (להלן־החלטה ב/84) ומבלי לפגוע בסמכות שניתנה לגורם אחר על־פי כל דין והחלטות ממשלה:
להקים מטה קיברנטי לאומי (להלן – המטה) במשרד ראש הממשלה, כמפורט בנספח א' להלן.
להסדיר את האחריות לטיפול בתחום הקיברנטי, כמפורט בנספח ב' להלן.
לקדם את יכולת ההגנה על המרחב הקיברנטי בישראל ולקדם מחקר ופיתוח בתחום הקיברנטי וחישוב העל, כמפורט בנספח א'.
התקציב למימוש החלטה זו יסוכם על ידי ראש הממשלה, בהתייעצות עם שר האוצר, ויוגש לאישור הממשלה בתוך חודשיים מיום קבלת החלטה זו.
על אף האמור בהחלטה זו, ולמען הסר ספק, מובהר בזאת כי החלטה זו לא תחול על הגופים המיוחדים, עליהם יחולו הסדרים מיוחדים, כפי שייקבעו בהסכמה ביניהם ובין המטה בתוך 120 יום מיום הקמתו."
מתוך אתר משרד ראש הממשלה,
http://www.pmo.gov.il/secretary/govdecisions/2011/pages/des3611.aspx

14 דוח המועצה למחקר ופיתוח לשנים 2010-2011, פרק ראשון, סעיף א', עמ' 10,
http://most.gov.il/Molmop/Reports/Documents/AnnualReport2010-11.pdf

15 שם, פרק שני, סעיף א', עמ' 39-40.

16 הודעת מזכיר הממשלה על הכרזת ראש הממשלה מיום 21 בספטמבר 2014,
http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokerashot210914.aspx
והודעת מזכיר הממשלה על החלטת הממשלה בסוגיית 'הצעת המחליטים', מיום 15 בפברואר 2015, http://www.pmo.gov.il/mediacenter/secretaryannouncements/pages/govmes150215 aspx#three

17 שמואל אבן ודוד סימן טוב, **לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**, מזכר 109, יוני 2011, המכון למחקרי ביטחון לאומי, תל אביב, עמ' 70-73,
http://heb.inss.org.il/index.aspx?id=4354&articleid=1043

18 שם, עמ' 70.

19 גבי סיבוני, "דרושה מדיניות לאומית – בניין כוח לאומי בסייבר", **הארץ**, מוסף מיוחד, ינואר 2014.

20 Department of Defense Strategy for Operating in Cyberspace, July 2011.

21 שם, עמ' 5-10.

22 "Cyberspace Operations" US Army Joint Publication 3-12(R), February 5, 2013,

http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

23 "Cyberspace Operations", Joint Publication 3-13 ®, Information Operations, Chapter II, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

24 Cheryl Pelleri, "Alexander: Defending Against Cyberattacks Requires Collaboration," U.S.A. Department of Defense, October 30, 2013.

25 אחרי התפוצצות פרשיית סנודן עסק השיח הציבורי בארצות־הברית בהפרת זכויות הפרטיות על ידי ה־NSA, מטעמי הגנה וביטחון. באווירה זו התקשה גנרל אלכסנדר לשכנע לאפשר לגופים כמו ה־NSA וה־Cyber Command לקבל פרטי מידע הנוגעים לאזרחי ארצות־הברית, למרות שהדבר חיוני להגנתם.

26 Cheryl Pelleri, "Alexander: Defending Against Cyberattacks Requires Collaboration" U.S.A Department of Defense News, October 30, 2013.

27 Cheryl Pellerin, "Cybercom Chief: Cyberspace Operations Key to Future Warfare," U.S.A Department of Defense, June 16, 2014.

28 The Department of Defense Cyber Strategy," The Department of Defense, April 2015, " http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

29 William J. Lynn III, "Defending a New Domain," The Pentagon's Cyber Strategy, *Foreign Affairs*, September/October 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

30 The Federal Bureau of Investigation, "Ten Years after: The FBI since 9/11 – Cyber," http://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/cyber-1

31 Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space, Presented to Parliament by the Prime Minister, by Command of Her Majesty, June 2009, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf

32 *The UK Cyber Security Strategy - Protecting and promoting the UK in a digital world*, Cabinet Office, November 2011.

33 *The UK Cyber Security Strategy Report on Progress and Forward Plans*, Cabinet Office, December 2014.

34 *Information Systems Defence and Security – France's Strategy*, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/France_Cyber_Security_Strategy.pdf

35 גבי סיבוני וי.ר., "מה עומד מאחורי לוחמת הסייבר של סין", **צבא ואסטרטגיה**, כרך 4, גיליון 2, ספטמבר 2012, http://heb.inss.org.il/index.aspx?id=4354&articleid=1185

36 "Cybersecurity Policy Making at a Turning Point", Analyzing a new generation of national cybersecurity strategies for the Internet economy, and Non-governmental stakeholders and Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies Contributions from BIAC, CSISAC and ITAC, OECD, 2012, http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

37 *National Cyber Security Strategies*, ENISA – European Union Agency for Network and Information Security, May 8, 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

38 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,

European Commission High Representative of the European Union for Foreign Affairs and Security Policy, Brussels, February 7, 2013, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

39 אמיר אורבוך וגבי סיבוני, "כישלון שיטות הגנת הסייבר הקלאסיות – מה הלאה?", **צבא ואסטרטגיה**, כרך 5, גיליון 1, אפריל 2013, עמ' 37–48, http://media.wix.com/ugd/d48d94_9186fa75ca504ff2bf61ff3a0f60f40d.pdf

40 יצחק בן־ישראל, ליאור טבנסקי, "מבט בינתחומי על אתגרי הביטחון בעידן המידע", **צבא ואסטרטגיה**, כרך 3, גיליון 3, דצמבר 2011, http://heb.inss.org.il/index.aspx?id=4354&articleid=1126

41 שם.

42 נתי כהן, "אופן היערכותה והתארגנותה של מדינת ישראל למתקפת סייבר נרחבת", המכללה לביטחון לאומי מחזור מ' והמחלקה למדעי המדינה באוניברסיטת חיפה, מאי 2013.
וגם:
נתי כהן, "הממד החמישי", **מערכות**, גיליון 452, דצמבר 2013, http://maarachot.idf.il/72194-he/Maarachot.aspx

43 שם, עמ' 15.

44 שם, עמ' 15–16.

45 Pierluigi Paganini, *Hardware attacks, backdoors and electronic component qualification*, InfoSec Institute, October 11, 2013, http://resources.infosecinstitute.com/hardware-attacks-backdoors-and-electronic-component-qualification/

46 אמיר לופוביץ, "לוחמה קיברנטית והרתעה: מגמות ואתגרים במחקר", **צבא ואסטרטגיה**, כרך 3, גיליון 3, דצמבר 2011, עמ' 41–52.

47 Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy*, November 19, 2013, http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin

48 על פי הניתוח שלנגנר מציע, מטרת התוקפים הייתה לגרום לאיראנים אי־אמון ביכולתם לתפעל את מערך הבקרה על הצנטריפוגות, ולא לגרום לנזק המוני לצנטריפוגות עצמן. בהתאם, התקיפה תוכננה לייצר נזק מתמשך ולא נזק מיידי רב, שיאותת לאיראנים כי הבעיה אינה בידע הטכנולוגי שלהם אלא בתקיפה קיברנטית. במילותיו של לנגנר (שם, עמ' 7):
"If catastrophic damage had been caused by Stuxnet that would have been by accident rather than on purpose. The attackers were in a position where they could have broken the victim's neck, but they chose continuous periodical choking instead. Stuxnet is a low-yield weapon with the overall intention of reducing the lifetime of Iran's centrifuges and making the Iranians' fancy control systems appear beyond their understanding."

49 במילותיו של לנגנר (שם עמ' 5, 7):
"The results of the overpressure attack are unknown. Whatever they were, the attackers decided to try something different in 2009. This new Stuxnet variant was almost entirely different from the old one. For one thing, it was much simpler and much less stealthy than its predecessor. It also attacked a completely different component of the Natanz facility: the centrifuge drive system that controls rotor speeds." …… "At some point the attacks should have been recognizable by plant floor staff just by the old eardrum……It's another sign that the makers of this second Stuxnet variant had decided to accept the risk that the attack would be detected by operators."

50 שם, עמ' 9.

51 שם, עמ' 9.

52 ג'יימס א. לואיס, "להגנת וירוס הסטקסנט", **צבא ואסטרטגיה**, כרך 4, גיליון 3, דצמבר 2012,
http://www.inss.org.il/uploadImages/systemFiles/%D7%9C%D7%95%D7%90%D7%99%D7%A1%D7%98%D7%A7%D7%A1%D7%A0%D7%98.pdf

53 Ronald J. Deibert, Rafal Rohozinski and Masashi Crete-Nishihata, "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war," *Security Dialogue*, Vol. 43, No. 1, February 2012,
http://sdi.sagepub.com/search/results?fulltext=cyclones+in+cyberspace&submit=yes&journal_set=spsdi&src=selected&andorexactfulltext=and&x=0&y=0

54 Cheryl Pellerin, "Cybercom Builds Teams for Offense, Defense in Cyberspace," *DoD News*, March 12, 2013,
וגם: Hearing to receive testimony on US strategic command and US cyber command in review of the defense authorization request for fiscal year 2014 and the future years defense program, March 12, 2013,
http://www.armed-services.senate.gov/imo/media/doc/13-09%20-%203-12-13.pdf

55 דברי רוג'רס מיום 12 ביוני 2014 (cyber-seminar hosted by the Association of the U.S. Army's Institute of Land Warfare).

56 דברי רוג'רס מיום 28 במאי 2014 (2014 Cyber Summit)
http://www.defense.gov/news/newsarticle.aspx?id=122384

57 OECD והאיחוד האירופי.

58 ההשוואה לגבי רוסיה נסמכת על ממצאים בפועל מהתנהלות המיוחסת לרוסיה במרחב הקיברנטי.

59 קושחה (באנגלית firmware) היא תוכנה המשובצת בהתקן חומרה ומטפלת בתפקוד הרכיב. מבחינת גמישותה לשינויים, קושחה היא מצב ביניים בין תוכנה (שקל מאוד לשנותה) לבין חומרה, שלא ניתן לשנותה. ברוב המקרים הקושחה של רכיב אלקטרוני שמורה על זיכרון ROM. לעתים הקושחה שמורה על זיכרון הבזק (flash), ואז היא ניתנת לעדכון על ידי משתמש הקצה. סיבות נפוצות לעדכון קושחה הן תיקון באגים או הוספת תכולות לרכיב. ההגדרה לקוחה מתוך מילון מורפיקס.

60 ראו כדוגמאות את מוצרי חברת enSilo, הבוחנים רק את נקודת היציאה של הרשת הארגונית ומטפלים רק בנקודה הזו במידע חשוד, ואת מוצרי חברת Secure Islands המוודאים כי הקבצים ברשת מוגנים ברמה גבוהה על בסיס מדיניות ההגנה של החברה, וללא קשר למקורם או למהות השימוש בהם.
רפאל קאהאן, כלכליסט, 25 במארס 2015, בעקבות תצוגת החברות בכנס CyberTec,
ואתרי החברות enSilo ו־Secure Islands בהתאמה:
https://www.ensilo.com/, http://www.secureislands.com/product/technology/

61 קיימים מוצרים מסחריים, ראו כדוגמה אפשרית התיאור באתר חברת VERINT,
http://www.verint.com/solutions/communications-cyber-intelligence/solutions/cyber-security/index

62 Giora Engel, Deconstructing the Cyber Kill Chain, *LightCyber*, November 26, 2014,
http://lightcyber.com/deconstructing-the-cyber-kill-chain

63 Computer Emergency Response Team / Computer Emergency Readiness Team / Cyber Event Readiness Team

64 Cyber-Security Operation Center.

65 תיאור לפתרון עקרוני מבוסס אנומליה ניתן למצוא במאמרם של אמיר אורבוך וגבי סיבוני, "כישלון שיטות הגנת הסייבר הקלאסיות – מה הלאה?", **צבא ואסטרטגיה**, כרך 5, גיליון 1, אפריל 2013,
http://media.wix.com/ugd/d48d94_9186fa75ca504ff2bf61ff3a0f60f40d.pdf

66 ראו ההפניה לאתר חברת enSilo, https://www.ensilo.com

67 ראו כדוגמה את הפתרון שמציעה חברת Nyotron, באתר החברה: http://www.nyotron.com
דוגמה נוספת היא הפתרון שמציעה חברת Light cyber, באתר החברה: http://lightcyber.com/products/
ודוגמה לפתרון מבוסס מידע על אפיון המשתמש הבודד שמציעה חברת Bio Catch באתר החברה:
http://www.biocatch.com/#!products/c5rw

68 ראו כדוגמה את דבריו של קית' אלכסנדר ב־the 4th Annual Cybersecurity Summit מיום ה־25 בספטמבר 2013: "we can break down each system we see being scanned by an adversary and put it in a new place. You can jump networks, you can jump databases, and you can jump your phone system, [making] it very difficult for adversaries to exploit them."
http://www.defense.gov/news/newsarticle.aspx?id=120854

69 החשיבה על טיפול במידע או תוצר הנגנבים ממחשב או מרשת מבוסס על סיפור הפגיעה בקו הגז הסיבירי. עיקרו של הסיפור הוא הבנה של ה־CIA שהסובייטים גונבים תכנון של רכיב בקרה ממחשבי חברה קנדית לטובת שימוש ברכיב דומה שהם יבנו. המידע בתוכניות שובש מבעוד מועד וגרם לפיצוץ בקו הגז הסבירי. בין אם הסיפור נכון ובין אם לאו, הוא מעלה את האפשרות שמניפולציה במידע גנוב לא תאפשר לגונב שימוש מוצלח במידע שגנב. התוצאה לא חייבת להיות קינטית וגלויה כפי שמתואר בסיפור הנ"ל. את פירוט הסיפור ניתן לראות במאמר ב־The Economist, תחת הכותרת: "War in The Fifth Domain", מה־1 ביולי 2010, המבוסס על ספר של Thomas Care Reed, שכיהן בממשלי פורד וקרטר כ־Secretary of the Air Force ובממשל רייגן כיועץ.
http://www.economist.com/node/16478792

70 ניתוח ממצה של הסוגים העיקריים של מתקפות מסוג DDoS ניתן לראות באתר של חברת Arbor Networks, http://www.arbornetworks.com/ddos-attacks

71 Ronald J. Deibert, Rafal Rohozinski and Masashi Crete-Nishihata, "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war," *Security Dialogue 2012*, Vol. 43, No. 1, February 2012, http://sdi.sagepub.com/search/results?fulltext=cyclones+in+cyberspace&submit=yes&journal_set=spsdi&src=selected&andorexactfulltext=and&x=0&y=0

72 ראו כדוגמאות את הניתוחים הבאים:
Sean Leach, "Four ways to defend against DDoS attacks." *Network World*, September 17, 2013,
http://www.networkworld.com/article/2170051/tech-primers/four-ways-to-defend-against-ddos-attacks.html,
George V. Hulme, "7 essentials for defending against DDoS attacks," *CSO*, January 14, 2013,
http://www.csoonline.com/article/2133613/malware-cybercrime/7-essentials-for-defending-against-ddos-attacks.html

73 Benedikt Martens and Frank Teuteberg, "Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model," University of Osnabrueck, Association for Information Systems AIS Electronic Library, May 2011,
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.231.6718&rep=rep1&type=pdf

74 "מעבר ניסיוני של בנק הפועלים לענן של אמזון", **TechTime**, 18 בספטמבר 2014,
http://techtime.co.il/2014/09/18/aws/
"בנק ישראל מסדיר את השימוש בענן", **Israel Defense**, 3 בפברואר 2015,
http://www.nrg.co.il/online/1/ART2/625/607.html
"ארה"ב: "ספקים מסחריים של שירותי ענן בשירות משרד ההגנה"", **iHLS**, 15 בדצמבר 2014,
http://i-hls.com/he/2014/12/commercial-vendors-invited-u-s-dod-data-centers

75 טיוטת הוראת המפקח על הבנקים בישראל בנושא ניהול סיכונים בסביבת ענן, 10 בספטמבר 2014,

http://www.boi.org.il/he/BankingSupervision/DraftsFromTheSupervisorOfBanks/DocLib/10861.pdf

76 "משרד ההגנה האמריקני עושה שימוש בענן אמזון", **iHLS**, 27 באוגוסט 2014, http://i-hls.com/he/2014/08/amazon-expands-cloud-services-u-s-military

77 ראו כדוגמה מערכי ההגנה בענן שמציעות Microsoft (עבור Azure), http://azure.microsoft.com/en-us/support/trust-center/security ושל הענן של חברת Amazon, http://aws.amazon.com

78 לדוגמה טכנולוגיה שפותחה על ידי חברת BIOCATCH המיועד ועל פי הכתוב באתר החברה מטרתה בעיקר הגנה בענן, http://www.biocatch.com

79 מתקפות חומרה הן מתקפות המבוססות על טיפול ברכיבי חומרה (Hardware) – הרכיבים הפיזיים במחשב, ו/או קושחה (Firmware) – התוכנה הצרובה על הרכיבים הפיזיים הללו.

80 החשש הזה, בין אם מוצדק ובין אם לאו, בא לידי ביטוי בדוגמה הבאה: ציוד מחשוב מתוצרת החברות Lenovo, Huawei ו ZTE הסיניות אינו מורשה לרכש על ידי ה־CIA, בשל החשש מהחדרה של רכיבי תקיפה כבר בשלב הייצור. ראה:
James Sanders, "Corporate espionage or fearmongering? The facts about hardware-level backdoors," IT Security, August 7, 2013
http://www.techrepublic.com/blog/it-security/corporate-espionage-or-fearmongering-the-facts-about-hardware-level-backdoors

81 לדוגמה תקיפה על בסיס קושחה שהודגמה ב־Black Hat security conference in Las Vegas על ידי Jonathan Brossard, מומחה סייבר. התקיפה שמכונה Rakshasa הדגימה החדרת "דלת אחורית" לתוך זיכרון לא נדיף (BIOS), ואת הקושי הגדול בניקוי התקיפה הזו ובחסימתה.
Sebastian Anthony, "Rakshasa: The hardware backdoor that China could embed in every computer," *EXTREME TECH*, August 1, 2012,
http://www.extremetech.com/computing/133773-rakshasa-the-hardware-backdoor-that-china-could-embed-in-every-computer

82 Sebastian Anthony, "Rakshasa: The hardware backdoor that China could embed in every computer," *EXTREME TECH*, August 1, 2012,
http://www.extremetech.com/computing/133773-rakshasa-the-hardware-backdoor-that-china-could-embed-in-every-computer

83 ראו מאמרו של Sebastian Anthony על התקיפה המכונה "Rakshasa".

84 Pierluigi Paganini, "Hardware attacks, backdoors and electronic component qualification," InfoSec Institute, October 11, 2013,
http://resources.infosecinstitute.com/hardware-attacks-backdoors-and-electronic-component-qualification/
William J. Lynn III, "Defending a New Domain, The Pentagon Cyber Strategy," *Foreign Affairs*, September/October, 2010,
http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain
וגם:
שחר סמוכה, "עולם תחת מתקפה: מלחמות הסייבר קופצות גרם מדרגות", **גלובס**, 12 בינואר 2012, http://www.globes.co.il/news/article.aspx?did=1000714597

85 Pierluigi Paganini, "Hardware attacks, backdoors and electronic component qualification," InfoSec Institute, October 11th, 2013,
http://resources.infosecinstitute.com/hardware-attacks-backdoors-and-electronic-component-qualification/

86 גבי סיבוני ודודי סימן טוב, "סחיטה קיברנטית – צפון קוריאה נגד ארצות הברית", **מבט על**, גליון 646, דצמבר 2014, http://heb.inss.org.il/index.aspx?id=4354&articleid=8424
וגם:
גבי סיבוני וסמי קורננפלד, "תקיפת סייבר איראנית ב'צוק איתן'", **מבט על**, גליון 598, אוגוסט 2014, http://heb.inss.org.il/index.aspx?id=4354&articleid=7583

87 ראו כדוגמה את ההתקפות הקיברנטיות על ארצות־הברית המיוחסות לאיראן, שלא זכו לתגובה גלויה כלשהי לצורכי הרתעה:
Elliot Jager, "Iranian Hackers Penetrated US Navy Marine Corps Internet for Four Months," *NEWSMAX*, February 18, 2014, http://www.newsmax.com/Newsfront/Iran-hackers-cyberattack-Navy/2014/02/18/id/553238
וגם:
Julian E. Barnes and Siobhan Gorman, "U.S. Says Iran Hacked Navy Computers" *Wall Street Journal*, September 27, 2013, http://online.wsj.com/news/articles/SB10001424052702304526204579101602356751772

88 אמיר לופוביץ, "לוחמה קיברנטית והרתעה: מגמות ואתגרים במחקר", **צבא ואסטרטגיה**, כרך 3, גיליון 3, דצמבר 2011, http://heb.inss.org.il/uploadimages/Import/(FILE)1325967373.pdf

89 Steve Lewis and Kris Smith, "Lessons Learned from Real World Application of the Bow-tie Method," Prepared for Presentation at American Institute of Chemical Engineers, 6th Global Congress on Process Safety, San Antonio, Texas, March 22-24, 2010.

90 הנשיא אובמה הגיב להתקפלות של 'סוני' בתחילת הדרך וקבע כי זו טעות, ועודד את החברה להקרין את הסרט למרות האיומים והתקיפה. הנשיא הבטיח תגובה פרופורציונלית של ארצות־הברית (צפון־קוריאה ספגה מתקפות ששיתקו את תעבורת האינטרנט שלה, וכן אושרה בארצות־הברית הטלת סנקציות על צפון־קוריאה כתוצאה מהתקיפה על 'סוני').
David E. Sanger, Michael S. Schmidt and Nicole Perlroth, "Obama Vows a Response to Cyberattack on Sony," *The New York Times*, December 19, 2014, http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html?_r=0

91 בסוף ספטמבר 2014 קיבלה הממשלה החלטה להקים רשות לאומית בסייבר. ב־15 בפברואר 2015 אישרה הממשלה 'הצעת מחליטים' מפורטת להקמת הרשות, ראו באתר משרד ראש הממשלה, הודעת מזכיר הממשלה מיום ה־15 בפברואר 2015,
http://www.pmo.gov.il/mediacenter/secretaryannouncements/pages/govmes150215.aspx#three

92 רועי גולדשטיין, "המרחב הקיברנטי וההגנה על תשתיות חיוניות", הכנסת – מרכז המחקר והמידע, 12 במאי 2013, www.knesset.gov.il/committees/heb/material/data/mada2013-05-13.doc

93 שם, עמ' 7.

94 גיל ברעם, "טכנולוגיית הלוחמה הקיברנטית ובנין הכוח בישראל", **צבא ואסטרטגיה**, כרך 5, גיליון 1, אפריל 2013, עמ' 24,
http://www.inss.org.il/uploadImages/systemFiles/Armey%20-%205.1.pdf

95 מתוך אתר המועצה לביטחון לאומי – פעילות המטה ללוחמה בטרור: הגנה על מערכות משובצות מחשב, http://147.237.72.17/NSCWeb/Templates/CounterTerrorismActivities.aspx

96 החלטת ממשלה מספר 3611 מיום 7 באוגוסט 2011,
http://www.pmo.gov.il/secretary/govdecisions/2011/pages/des3611.aspx

97 החלטת ממשלה מספר 3611 מיום 7 באוגוסט 2011.

98 ראו הודעת דובר ראש־הממשלה מיום 21 בספטמבר 2014,
http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokerashot210914.aspx

99 מתוך אתר אגף התקשוב – מחלקת הגנה בסייבר,

http://www.tikshuv.idf.il/1090-he/tikshuv.aspx#.VGD4r8IUHIU

100 ראיון עם קצין תקשוב ראשי, אייל זלינגר, **הארץ**, 4 במארס 2013. http://www.haaretz.co.il/news/politics/1.1946156

101 הודעת דובר צה"ל: "הרמטכ"ל הורה על הקמת זרוע סייבר", 15 ביוני 2015, http://www.idf.il/1133-22318-he/Dover.aspx

102 מתוך אתר משטרת ישראל: http://www.police.gov.il/contentPage.aspx?pid=308&mid=9

103 מתוך אתר משרד המשפטים: http://index.justice.gov.il/Units/ilita/news/Pages/NewsSekonimVeDarkiHetmodedot.aspx

104 בהתאם להחלטת ממשלת ישראל שפורסמה ב־21 בספטמבר 2014, http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokerashot210914.aspx

105 לתיאור המחלוקות בנושא החלוקה הארגונית של האחריות להגנה בסייבר בישראל, ראו: ברק רביד, "השב"כ ומטה הסייבר נאבקים מי ילחם בהתקפות מחשבים, נתניהו נמנע מהחלטה". **הארץ**, 14 ספטמבר 2014, http://www.haaretz.co.il/news/politics/.premium-1.2432606

106 גבי סיבוני, דרושה תפיסה אינטגרטיבית, **הארץ**, מוסף סייבר, מארס 2015.

107 המקבילה במרחב הקינטי היא, לדוגמה: גורמי פשיעה בדרום־ישראל המבריחים אמצעי לחימה מחצי־האי סיני לתוך ישראל, כך שנוצר שילוב שבין אירוע פלילי לאירוע בטחוני.

108 גבי סיבוני, "הגנת נכסים ותשתיות קריטיות מפני תקיפה קיברנטית – הממד הסטטוטורי", **צבא ואסטרטגיה**, כרך 3, גיליון 1, מאי 2011.

109 Matt Comyns, Tim Cook, Jesse Reich, "Global Leadership – New Threats New Leadership Requirements: Rethinking the Role and the Capabilities of the Chief Information Security Officer,", Russell Reynolds Associate, October 29, 2014 http://www.russellreynolds.com/content/rethinking-capabilities-of-chief-information-security-officer

וגם:

"המפקח על הבנקים, ניהול בנקאי תקין, ניהול הגנת סייבר", הוראה 361, מארס 2015. http://www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/361.pdf

110 הרצאת דוד ברודט במסגרת פאנל בנושא "תקציב הביטחון – בנפרד או חלק מהעוגה הכללית", הכנס השנתי של המכון למחקרי ביטחון לאומי, תל־אביב, 16 בפברואר 2015, https://www.youtube.com/watch?v=JqmGOCTxeds

111 אור הירשאוגה, "קבוצת האקרים יוזמת מתקפה על ישראל ביום רביעי הקרוב", **הארץ**, 9 בספטמבר 2013, http://www.themarker.com/technation/1.2116064

112 Kaspersky Security Bulletin, Kaspersky Lab Global Research and Analysis Team, 2013, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf

113 שם.

חלק מהתקיפות המתוחכמות נעשות בעזרת "שכירי חרב" – קבוצות ה"משכירות" שירותי תקיפה, חלקן מתוחכמות ועל בסיס כלי תקיפה שנבנו במיוחד.

114 DAVID E. SANGER, "Syria War Stirs New U.S. Debate on Cyber-attacks," *The New-York Times*, Middle-East. February 24, 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?_r=0

הכותב קובע כי התכנון שהיה לאמריקאים ב־2011 לממש תקיפת סייבר לשיתוק חיל האוויר הסורי כדי למנוע תקיפות על אזרחים לא אושר על ידי הנשיא, משום שהיה צורך לממש גם תקיפות פיזיות להשגת המטרה.

115 בעקרונות הפעולה של ארצות־הברית במרחב הקיברנטי, כפי שפורסמו על ידי משרד ההגנה,

העיקרון הראשון הוא התייחסות למרחב הקיברנטי כתחום פעילות מבצעי המחייב את משרד ההגנה להתאמן ולהצטייד, כך שיוכל להפיק את מלוא היתרונות הפוטנציאליים במרחב הקיברנטי. ראה:

"Department of Defense Strategy for Operating in Cyberspace," July 2011, pp 5-6, http://www.defense.gov/news/d20110714cyber.pdf

116 ראו דבריו של אדמירל רוג'רס במאמר הבא:

Cheryl Pellerin, "Cybercom Chief: Cyberspace Operations Key to Future Warfare," *DoD News*, June 16, 2014,

"In the year 2025, I believe … Army commanders will maneuver offensive and defensive capability much today as they maneuver ground forces," Rogers said, adding that command and control, key terrain, commander's intent, synchronization with the broader commander's intent, and a broader commander's operational concept of operations will be cornerstones of Army cyber operations by then"

117 John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *The New-York Times*, August 1 2009, http://www.nytimes.com/2009/08/02/us/politics/02cyber.html?_r=0

118 Ronald J. Deibert, Rafal Rohozinski and Masashi Crete-Nishihata, "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war," *Security Dialogue 2012*, Vol. 43, No. 1, February 2012, http://sdi.sagepub.com/search/results?fulltext=cyclones+in+cyberspace&submit=yes&journal_set=spsdi&src=selected&andorexactfulltext=and&x=0&y=0

119 Michael N. Schmitt, "The Law of Cyber Targeting," *Tallinn Paper No. 7*, 2015, https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_07_2015.pdf

120 גבי סיבוני וסמי קרוננפלד, "לוחמת הסייבר של איראן", **צבא ואסטרטגיה**, כרך 4, גליון 3, דצמבר 2013, http://media.wix.com/ugd/d48d94_1f8bd495a0554e44967b99e25e931eae.pdf

121 גבי סיבוני ודודי סימן טוב, "סחיטה קיברנטית – צפון קוריאה נגד ארצות הברית", **מבט על**, גליון 646, דצמבר 2014, http://heb.inss.org.il/index.aspx?id=4354&articleid=8424

"ההאקרים שתקפו את סוני: נבצע פיגועים בארה"ב", אתר **וואלה**, 17 בדצמבר 2014, http://news.walla.co.il/item/2811400

Nicole Perlroth and David Sanger, "North Korea Loses Its Link to the Internet," *The New-York Times*, December 22, 2014, http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html?_r=0

122 Ellada Gamreklidze, "Cyber security in developing countries, a digital divide issue," *Journal of International Communication*, Vol. 20, No. 2, 2014, http://dx.doi.org/10.1080/13216597.2014.954593

123 Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy*, November 19, 2013, http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/

124 על פי הניתוח שלנגנר מציע, מטרת התוקפים הייתה לגרום לאיראנים אי־אמון ביכולתם לתפעל את מערך הבקרה על הצנטריפוגות, ולא לגרום נזק הרסני חמור לצנטריפוגות עצמן. בהתאם, התקיפה תוכננה לייצר נזק מתמשך ולא נזק מיידי רחב, שיאותת לאיראנים כי הבעיה אינה בידע הטכנולוגי שלהם אלא בתקיפה קיברנטית. במילותיו של לנגנר (שם, עמ' 7):

"If catastrophic damage had been caused by Stuxnet that would have been by accident rather than on purpose. The attackers were in a position where they could have broken the

victim's neck, but they chose continuous periodical choking instead. Stuxnet is a low-yield weapon with the overall intention of reducing the lifetime of Iran's centrifuges and making the Iranians' fancy control systems appear beyond their understanding."

125 במילותיו של לנגנר (שם עמ' 5, 7):

"The results of the overpressure attack are unknown. Whatever they were, the attackers decided to try something different in 2009. This new Stuxnet variant was almost entirely different from the old one. For one thing, it was much simpler and much less stealthy than its predecessor. It also attacked a completely different component of the Natanz facility: the centrifuge drive system that controls rotor speeds." …… "At some point the attacks should have been recognizable by plant floor staff just by the old eardrum……It's another sign that the makers of this second Stuxnet variant had decided to accept the risk that the attack would be detected by operators."

126 שם, עמ' 9.

127 שם, עמ' 9.

INSS Memoranda, May 2014–Present

No. 149, October 2015, Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy* [Hebrew].

No. 148, September 2015, Meir Elran and Gabi Sheffer, eds., *Military Service in Israel: Challenges and Ramifications* [Hebrew].

No. 147, June 2015, Zvi Magen and Tatyana Karasova, eds., *Russian and Israeli Outlooks on Current Developments in the Middle East.*

No. 146, April 2015, Shmuel Even, *The Cost of Defense in Israel: Defense Expenditures and Recommendations for Drafting the Defense Budget* [Hebrew].

No. 145, December 2014, Yoav Zacks and Liran Antebi, eds., *The Use of Unmanned Military Vehicles in 2033: National Policy Recommendations Based on Technology Forecasting Expert Assessments* [Hebrew].

No. 144, November 2014, Oded Eran, Dan Vardi, and Itamar Cohen, *Political Feasibility of Israeli Natural Gas Exports to Turkey*.

No. 143, November 2014, Azriel Bermant, *The Russian and Iranian Missile Threats: Implications for NATO Missile Defense*.

No. 142, September 2014, Emily B. Landau and Anat Kurz, eds., *The Interim Deal on the Iranian Nuclear Program: Toward a Comprehensive Solution?*

No. 141, September 2014, Emily B. Landau and Anat Kurz, eds., *The Interim Deal on the Iranian Nuclear Program: Toward a Comprehensive Solution?* [Hebrew].

No. 140, July 2014, Oded Eran, Dan Vardi, and Itamar Cohen, *Exporting Israeli Natural Gas to Turkey: Is it Politically Possible?* [Hebrew].

No. 139, July 2014, Arik Rudnitzky, *Arab Citizens of Israel at the Start of the Twenty-First Century* [Hebrew].

No. 138, June 2014, Pnina Sharvit Baruch and Anat Kurz, eds., *Law and National Security: Selected Issues*.

No. 137, May 2014, Emily B. Landau and Azriel Bermant, eds., *The Nuclear Nonproliferation Regime at a Crossroads*.

No. 136, May 2014, Emily B. Landau and Anat Kurz, eds., *Arms Control and National Security: New Horizons* [Hebrew].