**אוניברסיטת חיפה – המחלקה למדעי המדינה**

**המכללה לביטחון לאומי**

**מחזור מ"ז**

**אסטרטגיה בעידן הסייבר– מטלת סיום קורס**

**ההרתעה הישראלית בסייבר**

**מרצים:**פרופ' אביתר מתניה

**מדריך מלווה:**אבי אלמוג

**מגישים:**

בר צ'צ'ק (ת"ז: 028923951)

רם ארז (ת"ז: 028602365)

אודי שילה (ת"ז: 038951570)

**אפריל 2020**

**מבוא**

עבודה זו מתמקדת בחיבור בין שני מושגי יסוד בביטחון הלאומי בעת הנוכחית: הרתעה וסייבר, בהקשר הישראלי. במיוחד מעניינות אותנו השאלות הבאות: האם ניתן להשתמש במרכיבי ההרתעה המוכרים מהעולם הקינטי לעולם הסייבר? מהם היחסים בין שני המושגים? והאם ניתן ליצור קישור (לינקג') בין הרתעה בעולם 'הקינטי' לעולם הסייבר?

כדי לענות על שאלות אלה, יעסוק, בקצרה, חלקה הראשון של עבודה זו במרכיבי ההרתעה. לאחר מכן, נבחן את ההבדלים שאנו מזהים בין ה'קינטי' לבין מרחב הסייבר בהקשר ההרתעה ומשם ביחסים שבין הרתעה בסייבר להרתעה בעולם הקינטי ונסכם בתובנות ובהמלצות. המקרה הישראלי משמש אותנו כבסיס להתייחסות, אם כי אנו מתייחסים גם לנעשה במדינות אחרות, בדגש על ארה"ב.

**הרתעה ומרכיביה**

במטרה להבין טוב יותר את פוטנציאל הקשר בין סייבר לבין הרתעה ובהמשך גם למה הכוונה בהרתעה בסייבר, נתחיל במושג ההרתעה ומרכיביו בעולם הקינטי, כלומר בעולם בו בתגובה על כישלון ההרתעה, מדינות פועלות, לרוב, תוך הפעלת כוח צבאי או כלכלי (סנקציות לדוגמא). באופן זה, נוכל לעמוד בהמשך על הדמיון והשוני בין שני העולמות, הקינטי והסייבר, ולבחון את הקישוריות ביניהם.

מושג ההרתעה זכה לתהילת עולם בעידן הגרעיני, שכן עד אותו עידן, ההרתעה הקונבנציונאלית כשלה פעם אחר פעם ואילו בעידן הגרעיני, מיוחסת לו הצלחה במניעת מלחמות כוללות בין יריבים גרעיניים. הרתעה, אם כן, היא "היכולת למנוע פעולה על יריב באמצעות איום אמין לתגמול בלתי נסבל ו/או אמונה של היריב, כי מחיר הפעולה יעלה על תועלות אפשריות" (DoD 2020: 64)[[1]](#footnote-1). בהקשר זה, אפיינו בידץ ואדמסקי **שני מימדים להרתעה**: הרתעה באמצעות **שלילה** והרתעה באמצעות **ענישה** (בידץ ואדמסקי, 2014: 11). הראשונה, גורמת ליריב להימנע מפעולה בשל הצפי כי פעולתו תיכשל והוא לא יצליח לגרום לנזק המיוחל ומכאן שלא ישיג את יעדיו. במקרה השני, היריב חושש מהתגובה הצפויה.

אם לסכם את תנאי המינימום לקיום הרתעה אפקטיבית: 1) נדרשת יכולת הגנה אפקטיבית ו/או יכולת גרימת נזק בלתי נסבל; 2) היריב צריך להיות מודע ליכולות אלה, הוא צריך להתייחס אליהן כאמינות (לרבות האיום הגלום בהן) והוא צריך להיות מסוגל לשקול שיקולי רווח והפסד. 3) חייבת להתקיים תקשורת בין הצדדים, מילולית ושאינה מילולית, כדי להשפיע על שיקולי היריב. בסופו של דבר, ההרתעה מתבססת על פחד – פחד מתגובה או פחד מכישלון המאמצים והפחד הוא זה שמניא את היריב מלפעול.

**דמיון ושוני בין העולם הקינטי לעולם הסייבר בהקשרי הרתעה**

גם בעולם הסייבר יש עניין רב להניא את היריב מלפעול, כלומר להרתיע אותו. אלא שבשונה מהעולם הקינטי, עולים במרחב הסייבר מספר קשיים מהותיים:

ראשית, חיכוך מתמשך: אפלגייט (Applegate 2012) עמד על כך שמרחב הסייבר מתאפיין בעימותים המתמשכים המתחוללים בו - כך, שבמרחב הסייבר מתקיים חיכוך יום יומי, כמעט בלתי פוסק[[2]](#footnote-2).

שנית, שלא כמו בעולם הקינטי, שבו ההרתעה מתוחמת בעיקר למדינות ולארגונים בעלי יכולות צבאיות מדינתיות, הרי שבעולם הסייבר, מגוון השחקנים, ומספר השחקנים שהינם בעלי יכולת להזיק ושאותם צריך להרתיע הוא גדול יותר. החל ממעצמות, עבור דרך מדינות אחרות, ארגונים תת מדינתיים אך גם שחקנים לא מדינתיים ולעתים אף פרטים[[3]](#footnote-3). מדינה אשר אינה ערוכה כראוי, עלולה לספוג פגיעה בתשתיות לאומיות אפילו מהאקר הבודד, תיאורטית, מכל מקום בעולם, והיא תתקשה להרתיע אותו. בנוסף, סוגי ההתקפה בסייבר רבים ומגוונים. ישראל לדוגמא, הינה יעד למבצעי CNA וגם, ואולי בעיקר ל-CNE (מידע ומודיעין) ויתכן אף ל-CNI (השפעה)[[4]](#footnote-4). גם **עוצמת הפגיעה** מפעילות סייבר התקפית היא מגוונת מאוד, החל מנזקים כמעט אגביים ועד לנזקים העשויים לאיים על הביטחון הלאומי (נפילת רשת החשמל, בתי חולים, תחבורה, מערכות שלטוניות ועוד) של ישראל או של כל מדינה אחרת.

שלישית, בשונה מהעולם הקינטי, בתמרון בסייבר מתקיים מרחב הכחשה רחב. כל עוד מדינה אינה נוטלת אחריות, הצד המותקף יתקשה לדעת מידית מי תקף אותו, ואפילו ייתכן שלא יידע שהוא נתקף בזמן אמת. עלול לחלוף משך זמן ארוך, עד שהשחקן המותקף ידע ברמת סמך גבוהה מי תקף אותו וכיצד. אנונימיות התקיפה מקשה על הרתעה אמינה, שכן לא ברור על מי יש לאיים בגמול במקרה זה. הדבר גם מקשה מאוד על מימוש מתקפת נגד בפרק זמן רלבנטי (Applegate 2012). מקרה מעניין בהקשר זה, היא הייחוס המהיר והפומבי שביצעה ארה"ב של תקיפת חברת סוני לצפון קוריאה, באופן שלפי הערכת חוקרים חשפה שיטות ואמצעים שסייעו למדינות אחרות לפתח כלפיהן חסינות (Borghard & Lonergan 2017), אך ניתן לשער שנועדה לבסס בדיוק את יכולת הייחוס המהירה ובכך לבסס הרתעה.

כמו כן, בשונה מהעולם הקינטי, יכולות התקיפה של מדינות בתחום הסייבר הן סודיות, שכן הן מתבססות על תורפות במערכים של היריב. כפי שהגדרנו בחלק הקודם, כדי לבסס הרתעה היריב צריך להיות מודע לכך שלמרתיע יש יכולות מסוימות. אולם בהקשר זה, אם הוא יידע, או יהיה מודע להן, הוא יוכל להתגונן מפניהן (בשונה מתקיפה קינטית) ואפקט ההרתעה ייחלש. בקשר לפרדוקס זה ציינו בורגארד ולונרגן, כי:

"…a coercing state must ensure that the target believes its self-declared attribution. This could present a problem for the coercing state if, in order to demonstrate that it was the one sending a signal, it had to reveal capabilities and accesses that it may prefer to keep private." (ibid.)

הקושי בזיהוי התוקף תוך פרק זמן קצר, לצד העובדה שהחיכוך במרחב הסייבר מתקיים כל העת ואל מול מגוון שחקנים, עשוי להביא שחקנים מדינתיים להידמות או לעשות שימוש בגופים ובתוקפים עצמאיים, דבר שיקשה עוד יותר על ניהול המתח שבין ספיגה לתגובה, ובין פעולה לשימור וחיזוק ההרתעה לבין חשיפת יכולות. צפון קוריאה לדוגמא, עושה שימוש נרחב בתקיפות במרחב הסייבר לטובת עקיפת הסנקציות הכלכליות כנגדה, תוך שימוש ומימון קבוצת האקרים מקומית ושכירת פושעי סייבר בצפון קוריאה וברחבי העולם[[5]](#footnote-5).

כמו כן, ובהמשך לנקודה הקודמת, בשונה מהעולם הקינטי, יכולת סייבר התקפית רגישה מאוד לשינויים ביכולות ובהיערכות של היריב. כלומר, בניית יכולת התקפית ליום פקודה, עלולה להתגלות כבלתי רלוונטית, אם היריב ביצע במהלך הזמן עדכון תוכנה, או שדרוג. כלומר, יש אי ודאות אינהרנטית באשר ליכולת לגרום נזק בלתי נסבל ליריב באמצעי סייבר. נקודה זו גם מדגישה את התלות הגבוהה במודיעין לצורך תקיפה מוצלחת. בעוד שבעולם הקינטי, ניתן ליצור נזק רב גם ללא מודיעין, במיוחד כנגד ריכוזי אוכלוסייה. בכך מוטלים בספק שני מרכיבים מרכזיים בהרתעה – האחד יכולת גרימת נזק בלתי נסבל והשני אמינות האיום.

אם כן, מתקיים קושי מהותי לבסס הרתעה בסייבר. ניתן לציין שלוש דרכים להתגבר על כך: ראשית, מרכיב השלילה בהרתעה מרכזי יותר מאשר בעולם הקינטי. כפי שנראה בהמשך, אכן, מדינות משקיעות רבות במרכיבי ההגנה[[6]](#footnote-6). שנית, מדינות פועלות לביסוס תקדימים לתקיפות בסייבר כדי להוכיח יכולת לגרום נזק במרחב זה. בולטת בהקשר יכולתן של ארה"ב, רוסיה וסין (ביכולות ובתו"ל). שלישית, מדינות פועלות לביסוס מערך הגנה לאומי רובוסטי בסייבר, המסייע למקד את ההרתעה מול שחקנים מדינתיים מתקדמים ומותיר תוקפים בודדים וארגונים קטנים מחוץ למגרש המשחקים. על רקע זה, חשוב לחדד למה הכוונה בדיון על הרתעה בעולם הסייבר ובכך יעסוק החלק הבא.

**לקראת הרתעה בסייבר**

כדי לבסס הרתעה בסייבר יש לשאול את השאלות הבאות: מפני מה רוצים להרתיע? מה רוצים למנוע? על מי רוצים להגן? כיצד עושים זאת? מי היריב שאותו צריך להרתיע? באלו ממדים? באלו כלים?

ההתפתחות הטכנולוגית המאפיינת את מרחב הסייבר הביאה לכך שמדובר במרחב בעל חשיבות אסטרטגית עצומה. פגיעה במרחב הסייבר עשויה להוות "איום מוחשי לאינטרסים רבים של הביטחון הלאומי ובכלל זה פגיעה בתהליכים חיוניים, שירותים, תשתיות, פגיעה בחיי אדם או כישלון שיטתי בעל השלכות ברמה הלאומית" (Matania, Yoffe, Mashkautsan 2016) . כך שהרתעה בסייבר נועדה להרתיע מפני שימוש במרחב הסייבר כדי לפגוע באינטרסים הלאומיים ובביטחון הלאומי של המדינה. בהקשר זה, נכתב במסמך אסטרטגיית הסייבר האמריקנית מ-2018, כי:

"The United States seeks to use all instruments of national power to deter adversaries from conducting malicious cyberspace activity that would threaten U.S. national interests, our allies, or our partners. The Department will prioritize securing sensitive DoD information and deterring malicious cyber activities that constitute a use of force against the United States, our allies, or our partners." (Cyber Strategy 2018: 4)

בישראל, במסמך האסטרטגיה להגנת הסייבר, מוזכרת סוגיית ההרתעה באופן מצומצם למדי. המונח "הרתעה" עצמו מופיע יחד עם המונח "אכיפה" כרכיב אחד ב"מערכה כנגד תוקפים"[[7]](#footnote-7), המהווה תת-מערכה במסגרת שכבת ההגנה הלאומית, שמהותה: "ניהול מערכה מדינתית נגד איומים חמורים, אשר עומדים מאחוריהם תוקפים נחושים ובעלי משאבים, המהווים סיכון ממשי לביטחון המדינה, תוך שילוב בין מאמצים מגננתיים להכלת תקיפות והשלכותיהן **ובין מאמצים אקטיביים להתמודדות עם מקורות האיום**." (עמ' 8, הדגשה הוספה).

"שכבת ההגנה", אם כן, הינה מרכיב באסטרטגיית ההגנה בסייבר המסור תחת אחריותה של המדינה היות והוא מתמקד ברכיב האנושי מאחורי תקיפות הסייבר באמצעות יכולות ההגנה המבצעיות של המדינה (Matania, Yoffe, Mashkautsan 2016). במקרה הישראלי, ובשונה מהזווית האמריקנית כמעצמה גלובלית, המיקוד הוא הגנה על הנכסים הלאומיים. היות וגבולות המדינה במרחב הסייבר אינם חופפים לגבולות הפיזיים (Applegate 2012), ואין משטרים או אמנות שמגדירים את 'חוקי המלחמה', והיות ואין הגדרה מוסכמת וברורה מה נכלל בנכסים עליהם תגן מדינה ובגין פגיעה בהם היא עשויה להגיב בחומרה (לאומיים, ציבוריים או פרטיים), למעשה, בהקשר הנדון, מתקיימת **עמימות** אשר משרתת את ההרתעה ומותירה מרחבי   
אי-וודאות, שגם התוקף צריך לקחת אותם בחשבון. ביחס לשאלה כיצד עושים זאת, הנושא מטופל בהמשך.

**יחסים בין הרתעה בעולם הקינטי להרתעה בעולם הסייבר**

ב-5 במאי 2019, במהלך אחד מסבבי הלחימה בין ישראל לחמאס, תקפה ישראל מבנה ממנו ביצע חמאס פעילות סייבר נגדה. בפרסום דובר צה"ל (ערוץ 20, 5 במאי 2019) נאמר כי:

"סוכל ניסיון של חמאס לשימוש בממד הסייבר לצרכי פגיעה ביעדים ישראלים. ארגון הטרור חמאס ניסה לבסס יכולות התקפיות בסייבר ופעל מרצועת עזה בניסיונות לפגוע במרחב הסייבר הישראלי. כלל הפעולות והניסיונות, התגלו וסוכלו מבעוד מועד והתשתית לא הצליחה לממש את תכניותיה, לרבות ניסיון כושל בימים האחרונים. בהמשך לפעילות הסיכול הטכנולוגי, מטוסי קרב של צה"ל תקפו הלילה מבנה ממנו פעל מערך הסייבר של חמאס".

לכאורה מדובר בביטוי מובהק לתפיסת ההרתעה של ישראל בהקשרי הסייבר: החוסן והאפקטיביות של הגנת הסייבר בישראל והסיכול של כוונות הפגיעה של החמאס בסייבר מהווה דוגמא של הרתעה באמצעות שלילה. תקיפת המבנה ממנו בוצעה פעילות סייבר התקפית נגד ישראל מהווה דוגמא להרתעה באמצעות ענישה, הגם שלפעילות כזו ישנם גם היבטים של שלילה (בהנחה שהתקיפה פגעה ביכולות של מערך הסייבר של חמאס). הממד התקשורתי שנלווה לסיכול ההגנתי ולתקיפה הקינטית, ובכלל זה הפרסום של דובר צה"ל, הינו חלק חשוב מהאיתות של ישראל לחמאס, שכלל גם את התקיפה הקינטית, על מנת לוודא שהמסר הרצוי, יגיע ליריב - ויובן. בנוסף, התקיפה הכתה גלים ברחבי העולם, לאור היותה דוגמא חריגה, ראשונה מסוגה, של תקיפה קינטית בתגובה לפעילות סייבר עוינת (Chesney 2019)[[8]](#footnote-8).

דוגמא הופכית, לתגובה בעולם הסייבר על פעולה בעולם הקינטי, ניתן לראות בפעולתה של ארה"ב כנגד איראן, לאחר שזו האחרונה הפילה מטוס ביון מתקדם ללא טייס ביוני 2019. על פי הפרסום, פיקוד הסייבר של צבא ארה"ב תקף את מערכות הפיקוד והשליטה הממוחשבות של משמרות המהפכה באיראן והוציא מכלל פעולה מאגר מידע 'קריטי', שמנע מהארגון לתכנן תקיפה נוספת של מכליות נפט במפרץ. ארה"ב לא נטלה אחריות באופן רשמי על הפעולה, אך בעקבות פעולת הסייבר, הנשיא טראמפ ביטל מתקפה קינטית שתוכננה (Barnes, NYT ,August 28, 2019).

שתי דוגמאות אלה ממחישות עד כמה הקשר בין העולם הקינטי ועולם הסייבר יכול להיות הדוק. נטייה 'טבעית' היא להגיב 'באותו מטבע' ('Tit for Tat'), נטייה אשר מועצמת על ידי היבטים ארגוניים: הגוף האחראי טיפל בתקיפה נגד המרתיע ומכאן שהוא גם ידחוף להיות האחראי על התגובה ואולי גורמים אחרים במערכת כלל לא יעורבו תחילה. אך אם פורצים ערוצים צרים אלה, כמו בדוגמאות שהוצגו לעיל, מרחב ההרתעה גדל, הכלים העומדים בידי מקבל ההחלטות נותנים בידיו גמישות, ואולי חשוב מכל – היריבים לומדים את מרחב 'מגרש המשחקים' החדש ומייצרים במעשיהם את כללי המשחק בו, לרבות הקישוריות בין העולמות. בהקשר זה, מציין מסמך אסטרטגיית הסייבר האמריקנית, כי במקרה שבו כשלה ההרתעה בסייבר, לרשות ארה"ב עומדת כל קשת היכולות הצבאיות שלה לטובת תגובה (US Cyber Strategy 2018). במרומז, ניתן לראות במשפט זה אף קישור לתגובה גרעינית, כתלות כמובן לחומרת התקיפה נגד ארה"ב והשלכותיה.

נקודה נוספת ביחס לקישוריות בין העולמות, ועל רקע ההבדלים שהוצגו קודם לכן בין העולמות בהקשרי הרתעה, מתקיים קושי מהותי, בוודאי בשלב זה, לפתח יכולות סייבר לטובת הרתעה, שהן חלופיות ליכולת התקפיות קינטיות. יתר על כן, גם יכולות סייבר כשלעצמן, אין בהן די כדי לייצר הרתעה מספקת. בהקשר זה ציינו שני חוקרים, כי:

"…cyber power alone has limited effectiveness as a tool of coercion, although it has significant utility when coupled with other elements of national power." (Borghard & Lonergan 2017).

משמעות הדבר היא, שעלות הביטחון רק גדלה, אם מבקשים להחזיק גם כלי התקפה בסייבר, כי היא מצטרפת לפיתוח יכולות התקפה קינטיות מתקדמות.

**הרתעה וסייבר- המקרה הישראלי**

**אם כן, כיצד נכון עבור מדינת ישראל לייצר הרתעה בממד הסייבר?** לכאורה, תפיסת ההרתעה של ישראל בעולם הקינטי, או לפחות הפרקטיקה שלה מתאימה לממד הסייבר של היום, בוודאי אל מול יריבים זירתיים, מדינתיים ותת מדינתיים. מושג ההרתעה שונה בין ארה"ב וישראל, בארה"ב מקורו של המושג הוא במלחמה הקרה ובגרעין בעיקר. בראיה האמריקאית, במידה וארה"ב הפעילה כוח, או שכוח הופעל מולה, הרי שההרתעה אינה קיימת. בישראל לעומת זאת, הפעלת הכוח מתחזקת את ההרתעה. התפיסה הישראלית, לפיה השימוש בכוח על ידי היריב הוא בלתי נמנע (ביידץ ואדמסקי 2014: 11), מתאים לממד הסייבר, שכן מדובר בממד בו אנחנו צפויים לאיומים רציפים ומגוונים. ההתמודדות ארוכת השנים והחיכוך היום יומי של ישראל עם יריבים תת מדינתיים והיברידיים, התפיסות הידע והכלים שפיתחה מולם, רלבנטיים גם להתמודדות מולם בממד הסייבר.

הדגש בתפיסת ההפעלה של הגנת הסייבר הישראלית הוא **הגנתי בעיקרו** (אדמסקי 2017: 118). כלומר, ההרתעה הישראלית בסייבר מתבססת בעיקר על בסיס שלילה (הגנה). מבין שלוש השכבות המרכיבות את תפיסת ההפעלה של אסטרטגיית הסייבר בישראל, שתיים הינן בעלות ממד הגנתי לחלוטין (עמידות משקית, חוסן מערכתי) ורק השכבה השלישית (הגנה לאומית) הינה בעלת מרכיבים של התקפה או ענישה, ואלו מסורים למוסדות המדינה בלבד (האסטרטגיה הישראלית להגנת הסייבר). הדגש הרב על הרובוסטיות ההגנתית של מדינת ישראל, באסטרטגיית ההגנה בסייבר אכן מכסה חלק גדול מהאיומים והאתגרים, הן בהיבט של מגוון היריבים והן בהיבט של סוגי התקיפה (CNA, CNE), ומשרת את היכולת להרתיע על בסיס שלילה. אולם, ובהנחה ש"קו ההגנה תמיד ייפרץ", והיות וחלק מהאיומים בסייבר הינם בעלי השלכות על הביטחון הלאומי, נדרשים בנוסף **ממדים של התקפה: הן בהרתעה באמצעות שלילה והן בהרתעה באמצעות ענישה**.

תנאי הכרחי למיסוד משטר הרתעה הוא היכולת להעביר מסרים ואיומים אמינים ליריבים הזירתיים-רציונאליים של ישראל. בהיבט זה ישנה מורכבות בעולם הסייבר. התקיפות בסייבר הינן לרוב אנונימיות, בוודאי יחסית לתקיפות באמצעות אמצעים קינטיים. פעמים רבות לא ברור מי היריב שביצע את הפגיעה, היריב עשוי להיות מעצמה, יריב מדינתי, יריב תת מדינתי או אפילו גורם פלילי כזה או אחר. בנוסף, למרכיב הזמן חשיבות רבה. גילוי הפגיעה ומי שעומד מאחורי הפגיעה עלול להימשך זמן מה, דבר שמקשה על מימוש תגובה והעברת מסר בעיתוי רלבנטי. חשאיות זו אינה רק נחלתו של היריב, גם יכולות התקיפה בסייבר של ישראל, כמו גם של מדינות אחרות הינן חשאיות. חשאיות זו מקשה על העברת איומים ומסרים ברורים, שהם תנאי הכרחי לבניית הרתעה אפקטיבית. כך לדוגמא, יש להבהיר ליריב כי תקיפה בסייבר אינה לגיטימית, ואינה פחותה במשמעותה מאשר תקיפה קינטית והדבר מחייב העברת מסרים, גלויים וחשאיים, ליריבים.

ישנה חשיבות גדולה לחיזוק וחיסון מערכות ההגנה הישראליות בסייבר. ככל שאלו יהיו אפקטיביות יותר, יתכן ונוכל לפגוע במוטיבציה של השחקנים, בוודאי אלו התת-מדינתיים, אשר צריכים למקד את מאמצי בניין הכוח שלהם, להשקיע מאמצים רבים, ואם לא אזי לפחות למנוע את הצלחת התקיפות. ואכן, אסטרטגיית ההגנה בסייבר של ישראל מדגישה מאוד את החשיבות שבבניית שכבות ומערכות הגנה רובוסטיות במרחבים שונים במדינת ישראל, ללא תלות באירועים ובהקשר לאירועים (שכבת ה"עמידות המשקית" ושכבת ה"חוסן המערכתי"). על מנת לאפשר הרתעה המבוססת על שלילה, יש לשקף את אותה רובוסטיות כלפי חוץ. כאן, מתקיים, כרגיל המתח בין חשיפת היכולות לטובת ההרתעה, לבין חשיפתם ליריב, שעשוי להשקיע מאמצים בלאתר את חולשותיהן. זהו מתח המתקיים גם בזירות פעולה צבאיות נוספות של מדינת ישראל, והוא אינו שונה במהותו מחשיפת יכולות "כיפת ברזל" לדוגמא.

על מנת להפוך את ההתרעה מתוך שלילה לאפקטיבית יותר יש להוסיף למרכיבים ההגנתיים מרכיב של **שלילת יכולות באופן אקטיבי והתקפי**, אל **מול ציוד, משאבים והון אנושי של היריב ובשטחו.** בתקציר אסטרטגיית הסייבר של משרד ההגנה האמריקאי, שעודכן ב-2018 (DoD, Cyber Strategy 2018). משתמשים במונח "Defending Forward", שמשמעותו בהקשר הנדון כאן, להגן על הנכסים בסייבר מחוץ לשטחה של המדינה, קרי "בשטח" היריב (Kreps & [Schneider](https://warontherocks.com/author/jacquelyn-schneider/) 2018).

כמו כן, וכפי שהובהר בדוגמא של תקיפת מתקן הסייבר של חמאס בעזה, **ההרתעה באמצעות ענישה** אינה צריכה להישאר בעולם הסייבר (תקיפה בסייבר כתגובה על תקיפה בסייבר), למרות שזו בהחלט אפשרית. יציאה מעולם הסייבר, וסנקציה בעולם הקינטי, בעולם הכלכלי, בעולם האזרחי או בעולם המדיני עשויה להיות אפקטיבית לטובת ההרתעה, ולאפשר העברת מסר אמין ואיום ברור. לאמור משנה חשיבות לאור עוצמת הפגיעה הפוטנציאלית בביטחון הלאומי במרחב הסייבר. אחד מהמאפיינים של ממד הסייבר הוא שגם שחקנים תת מדינתיים או מדינתיים עשויים לגרום לנזקים משמעותיים מאוד לתשתיות קריטיות (Chesney 2019)[[9]](#footnote-9). במקרה כזה, תגובה לאיום כזה או למימושו אינה צריכה להיוותר בעולם הסייבר. כך לדוגמא פורסם ביוני 2018 שארה"ב שוקלת להגיב **בתקיפה גרעינית** במקרה של פגיעה נרחבת ברשת החשמל או המים שלה (Kreps & [Schneider](https://warontherocks.com/author/jacquelyn-schneider/) 2018).

**אל מול המעצמות,**נהיר שישראל אינה יכולה לכונן "משטר הרתעה" בילטרלי מול מעצמות כמו רוסיה, סין או אפילו צפון קוריאה, מדינות שמולן מנופי הלחץ הישראלים מצומצמים לחלוטין עד לא קיימים, או לחלופין, המחיר של התנגשות בסייבר או כל התנגשות אחרת הוא יקר. על מנת לייצר הרתעה מול שחקנים כאלו בתווך הסייבר נכון לייצר **שיתוף פעולה עמוק**, הדוק וגלוי בחלקו, עם ארה"ב. ארה"ב רואה בסין וברוסיה שחקנים יריבים הנמצאים בתחרות אסטרטגית עם ארה"ב ועלולים להוות בטווח הארוך סיכון אסטרטגי לאומה כמו גם לבעלות בריתה ושותפותיה (DoD, Cyber Strategy 2018). שותפות גלויה בחלקה בהקשר זה של ישראל עם ארה"ב עשויה להוות משקל נגד מסוים לא-סימטריות שבין ישראל לפעילות מעצמתית בתחום הסייבר.[[10]](#footnote-10)

יש לציין כי ארה"ב עצמה שינתה ופיתחה את האסטרטגיה שלה בסייבר. כישלון האסטרטגיה שנוסחה ב-2015 ובעיקר כישלון ההתנהלות של ממשל אובאמה אל מול התקיפות הרוסיות בסייבר, נתפסו כשגויות על ידי אנשי משרד ההגנה בעצמם. גם כאשר הוכנו תכניות לתגובה ולהרתעה, הן לא מומשו בפועל (Isikoff 2018). לא זו בלבד שהאמריקאים לא הרתיעו את הרוסים מהמשך פעילות הסייבר ההתקפית בארה"ב, ארה"ב הורתעה למעשה על ידי רוסיה ועל ידי עצמה. החשש העיקרי בממשל אובאמה היה שתגובה משמעותית של ארה"ב בסייבר, תייצר אסקלציה בסייבר ובתחומים נוספים (Healey 2018). בשל כך, נוסחה ב-2018 אסטרטגיה חדשה בסייבר, הפעם תחת הנשיא טראמפ. אסטרטגיה זו כללה גם פרק נפרד שכותרתו "להתחרות ולהרתיע בממד הסייבר" ("Compete and Deter in the Cyberspace"), כשבפרק זה ההרתעה כוללת שימוש בכלל כלי העוצמה הלאומית ("All Range of Military Capabilities") תוך דגש על האחריות ושיתוף הפעולה עם "בעלי בריתה ושותפיה" (DoD, Cyber Strategy 2018)[[11]](#footnote-11). כמו כן מדגיש הנייר את העובדה שמדובר למעשה בתחרות יום-יומית. האמריקנים כוללים באסטרטגיית הסייבר שלהם ובהרתעה במרחב זה את כל סוגי התקיפה של היריבים (CNA, CNE, CNI) . כך שניתן לומר שבהיבטים אלו ישנם קווי דמיון בין תפיסת ההרתעה האמריקאית בסייבר לתפיסה ההרתעה הישראלית, תוך המיקוד המתבקש ביריבים המעצמתיים, שישראל תתקשה לייצר מולם הרתעה. הדגש באסטרטגיה האמריקאית בסייבר על האחריות ועל שיתוף הפעולה של ארה"ב עם בעלי בריתה ושותפיה בעולם, עשוי לייצר עבור ישראל מנוף הרתעתי, לפחות במידה מסוימת ובמקרים ספציפיים אל מול אתגרים מעצמתיים בעולם הסייבר.

**תובנות והמלצות**

לאור הניתוח לעיל, אנו מציעים מספר תובנות והמלצות ראשוניות, העשויות לשמש בהמשך פיתוח מרכיב ההרתעה באסטרטגיית הסייבר הישראלית:

**ראשית, מושג ההרתעה הינו רלוונטי לעולם הסייבר**, למרות הקשיים המהותיים הכרוכים בהשאלת המושג ולמרות השוני העמוק בין שני העולמות שנותחו כאן, הקינטי והסייבר. מעבר לדיון האינטלקטואלי בסוגיה, ישראל, כמו גם מדינות אחרות, פועלות הלכה למעשה לבסס הרתעה גם בעולם הסייבר. כיום, משקלו היחסי של מרכיב ההרתעה באסטרטגיית הסייבר הישראלית הינו מצומצם, לפחות בגרסה הגלויה. כאמור, לדעתנו, יש מקום להמשך פיתוח מרכיב זה בתפיסה הכוללת ולשילובו בה.

**שנית, דווקא בעולם 'אנרכי' כמו עולם הסייבר, שבו אין שום הסדרה, פוטנציאל התרומה של מושג ההרתעה גבוה** ומכאן גם נובעת חשיבות העיסוק בנושא. יתר על כן, למרות שעולם הסייבר פתוח לכל שחקן, לכאורה, עדיין פוטנציאל האיומים המשמעותיים, בהקשר זה, נותר מיכולות מדינתיות מתקדמות ולא מהאקרים בודדים. לכן, עקרונית, תמיד מושא ההרתעה קיים, גם אם לא קל לזהותו. נכון להמשיך למקד את הדיון בהרתעה בשחקנים מדינתיים ותת מדינתיים מתקדמים אזוריים.

**שלישית, לא ניתן לבסס את ההרתעה הישראלית בסייבר על מרכיב השלילה בלבד**, אלא נדרש בנוסף להבטיח יכולת מניעה פרו אקטיבית ויכולת ענישה, כלומר יכולת גרימת נזק כגמול. לשם כך, נדרש לפתח כלים ייעודיים במיוחד בתחום המודיעין ו'הזיהוי הפלילי' כדי להבין מה נעשה ועל ידי מי, ובקבועי זמן קצרים ככל הניתן. יכולות אלה יאפשרו להבין מי תקף אותנו, באילו כלים ובאיזה אופן (ישיר או עקיף) ולהגיב בזמן קצר (במגוון כלים) לתקיפות של היריב בסייבר. יכולות אלו יאפשרו גם לשלול יכולות מהיריב עוד טרם תקיפה ספציפית או אף בשלב בניין הכוח שלו.

**רביעית, יש מקום להרחיב, תפיסתית וכן מבצעית, את הקישוריות בסוגיית ההרתעה בעולם הסייבר לבין העולם הקינטי**, **מעין 'הרחבת תחום ההרתעה'.** כלומר, אין הכרח שפעולת תקיפה בסייבר תוגבל למענה בסייבר, ומנגד, אין מניעה שפעולה בעולם הקינטי תיענה בעולם הסייבר. פעולות בכיוון זה צפויות להגדיל את פוטנציאל ההרתעה ואת הגמישות של מקבלי ההחלטות. **לא נכון לייצר הבחנה בין הרתעה בעולם הקינטי לבין הרתעה בעולם הסייבר.**

**חמישית, מתקיים תהליך למידה בין הצדדים**, בו כל צד לומד את האחר, מהם הערכים היקרים ביותר עבורו ואלו פעולות הוא מוכן לנקוט כדי להגן עליהם, וכיצד הוא עשוי לפעול אם הם יפגעו. כך גם כל צד לומר על הקישוריות בין העולמות, אם יוצרים אותה. תהליך זה עשוי לייצר כללי משחק חדשים בין השחקנים, שישקף מי מהם היטיב להבין את הדינאמיקה והיטיב להגיב לה. מנגד, תהליך למידה שלילי, עלול להביא להסלמה ולערעור היציבות. יש חשיבות בהכרה כי מתקיים תהליך למידה, וכי גם השחקנים האחרים שותפים בו ותובנותיהם משפיעות גם עלינו על אפקטיביות הפעולות שלנו בסייבר. לכן, חשוב להיות מודע לקיום תהליך הלמידה, להשקיע מאמצים בהבנת תהליך הלמידה של היריבים, ארגונית ותהליכית, ולבסוף גם לשלב את ממדי הלמידה כמרכיב בתהליכי עיצוב המדיניות והפעולות שלנו.

**שישית, המשך בנייה וחיזוק של החיבור עם ארה"ב** בהיבטי הסייבר. ההתפתחות באסטרטגיית הסייבר של ארה"ב, הממוקדת במעצמות, ואשר נותנת משקל להרתעה ולקשרים עם בעלות ברית ושותפות עשויה לאפשר, לפחות במידה מסוימת מענה לפער ההרתעתי של ישראל בהתמודדות עם מעצמות במרחב הסייבר. פיתוח כושר התקפי הינו חשוב בהקשר האזורי, אך אינו נכון מול האיום המעצמתי, שם נכון שישראל תמשיך לחזק את הרובוסטיות ההגנתית שלה ובהעברת מסרים לחיבור שלה בנושא זה עם ארה"ב. בוודאי, שאין תוחלת להשקיע ולקדם יכולת התקפית נגד מעצמות. לפיכך חיזוק החיבור עם ארה"ב בהיבטים אלו הינו חשוב ואף קריטי.

**לסיכום**  
בהחלטת ממשלת ישראל מיום ה-15 בפברואר 2015 הוגדרה הגנת הסייבר כ-

"מכלול הפעולות למניעה, לנטרול, לחקירה ולהתמודדות עם איומים, תקיפות וחדירות מרחב הסייבר הארגוני והמדינתי ולצמצום השפעתם והנזק הנגרם מהם, וז**את בטרם התרחשותם**, במהלכם ואחריהם."[[12]](#footnote-12)

לפיכך, אנחנו רואים בגיבוש והרחבת תפיסת ההרתעה ישראלית גם לממד הסייבר, וכן בגיבוש יכולות ותו"ל בהקשר הזה **כמרכיב משמעותי ומרכזי במניעת איומים ותקיפות סייבר** כנגד מדינת ישראל. להבנתנו ההרתעה הינה חלק חשוב, מניעתי במהותו, **בשכבת ה"ההגנה הלאומית" באסטרטגיית הישראלית להגנת הסייבר**. שכן, ההרתעה בסייבר, בדומה לשאר המאמצים בשכבה זו, מתבססת על הפעלת כלים וסמכויות המסורים למדינה בלבד, לטובת התמודדות עם איומים על האינטרסים ועל הביטחון הלאומי ולטובת התמודדות עם התוקפים והשחקנים המדינתיים והתת-מדינתיים שמפעילים אותם.

95

עבודה טובה מאוד ומעניינת. הרצף הלוגי והטיעונים ברורים ומבוססים היטב והסגנון רהוט וקולח.

**ביבליוגרפיה**

בידץ, יוסי ואדמסקי, דמיטרי (דימה) (2014). "התפתחות הגישה הישראלית להרתעה: דיון ביקורתי בהיבטיה התיאורטיים והפרקטיים", **עשתונות, במה למחשבות ורעיונות**, גיליון מספר 8, המכללה לביטחון לאומי - מרכז המחקר תשע"ה.

מערך הסייבר הלאומי (2015). **האסטרטגיה הישראלית להגנת הסייבר**. משרד הראש הממשלה.

סיבוני, גבי, ואסף עופר (2015).**קווים מנחים לאסטרטגיה לאומית במרחב הסייבר**, INSS–המכון למחקרי ביטחון לאומי.

ערוץ 20 (2019). **הודעת דובר צה"ל**. 5 במאי<https://www.20il.co.il/%d7%93%d7%95%d7%91%d7%a8-%d7%a6%d7%94%d7%9c-%d7%a1%d7%99%d7%9b%d7%9c%d7%a0%d7%95-%d7%a4%d7%a2%d7%99%d7%9c%d7%95%d7%aa-%d7%a1%d7%99%d7%99%d7%91%d7%a8-%d7%a9%d7%9c-%d7%97%d7%9e%d7%90%d7%a1/>

Adamsky, Dmitry (Dima) (2017). "The Israeli Odyssey toward its National Cyber Security Strategy", **The Washington Quarterly** 40:2, pp. 113-127.

Applegate S., (2012). "The Principle of Maneuver in Cyber Operations", **4th International Conference on Cyber Conflict**, NATO(Tallinn). <https://www.researchgate.net/publication/236020494_The_Principle_of_Maneuver_in_Cyber_Operations/>

Barnes, Julian E. (2019). "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers," **New York Times**, August 28. <https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html>

Borghard, Erica D., Lonergan, Shawn W., (2017). "The Logic of Coercion in Cyberspace", **Security Studies**26: 3, pp. 452-481.

Borghard, Erica D., [SchneiderJacquelyn](https://warontherocks.com/author/jacquelyn-schneider/) (2019). "Israel Responded to a Hamas Cyberattack with an Airstrike. That’s Not Such a Big Deal", **The Washington Post**, May 9th.  
<https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/?outputType=amp>

Chesney, Robert (2019). "Crossing a Cyber Rubicon? Overreactions to the IDF’s Strike on the Hamas Cyber Facility", **Lawfare**, May 6th.  
<https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility>

Cropsey, Set (2019). "Hamas Cyber Attack and Israel’s Armed Response", **The Hudson Institute**, May 9th.   
<https://www.hudson.org/research/15016-hamas-cyber-attack-and-israel-s-armed-response>

Department of Defense (DoD) (2015).**Cyber Strategy 2015**  
<https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf>

Department of Defense (DoD) (2018).**Cyber Strategy 2018 - Summery**  
<https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF>

Department of Defense (DoD) (2020).**Dictionary of Military and Associated Terms**. <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>

Healey Jason (2018). "Not the Cyber Deterrence the United States Wants," **Council on Foreign Relations**, Jun. 11th.  
<https://www.cfr.org/blog/not-cyber-deterrence-united-states-wants>  
  
Kollars, Nina, [SchneiderJacquelyn](https://warontherocks.com/author/jacquelyn-schneider/) (2018). "Defending Forward: The 2018 Cyber Strategy Is Here", **War on the Rocks**, Sep. 20th.  
<https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/>

Ikeda, Scott (2019). "What Does Israel’s Missile Strike on Hamas Hackers Mean for Military Cyber Response?",**CPO Magazine**, May 14th.  
<https://www.cpomagazine.com/cyber-security/what-does-israels-missile-strike-on-hamas-hackers-mean-for-military-cyber-response/>

Isikoff, Michael (2018). "Obama Cyber Chief Confirms 'Stand Down' Order Against Russian Cyberattacks in Summer 2016**", Yahoo! News**, Jun 20th.  
<https://www.yahoo.com/news/obama-cyber-chief-confirms-stand-order-russian-cyberattacks-summer-2016-204935758.html>  
  
Matania Eviatar, "Cyber Generates New Possibilities", **Israel Globes** (Israel Business Arena), Dec 2016.

Matania Eviatar, Yoffe Lior and Mashkautsan Michael, "A Three-Layer Framework for a Comprehensive National Cyber-Security Strategy", **Georgetown Journal of International Affairs** XVII, No. 3 (2016): 77-84.  
  
Kreps, Sara, [Schneider](https://warontherocks.com/author/jacquelyn-schneider/),[Jacquelyn](https://warontherocks.com/author/jacquelyn-schneider/) (2018). "Should the U.S. Try to Deter Cyberattacks by Promising Nuclear Retaliation?",**The Washington Post**, Jan 29th.  
<https://www.washingtonpost.com/news/monkey-cage/wp/2018/01/29/should-the-u-s-try-to-deter-cyberattacks-by-promising-nuclear-retaliation/>

Sanger, David E., Perlroth, Nicole (2020). "U.S. Accuses North Korea of Cyberattacks, a Sign That Deterrence Is Failing", **The New York Times**, Apr 15th.

<https://www.nytimes.com/2020/04/15/world/asia/north-korea-cyber.html>

1. תרגום חופשי מאנגלית. [↑](#footnote-ref-1)
2. תקציר מסמך האסטרטגיה בסייבר של משרד ההגנה האמריקאי מ-2018 מכנה זאת "Day to Day Competition" (DoD, Cyber Strategy 2018). [↑](#footnote-ref-2)
3. ראו לעניין זה סעיף הרקע במסמך "האסטרטגיה הישראלית להגנת הסייבר" (עמ' 12) [↑](#footnote-ref-3)
4. CNA –Computer Network Attack . CNE–Computer Network Exploiting, CNI–Computer Network Influnce [↑](#footnote-ref-4)
5. ראו לעניין זה פרסום ב-New York Times מה-15 באפריל 2020 שכותרתו "U.S. Accuses North Korea of Cyberattacks, a Sign That Deterrence Is Failing [↑](#footnote-ref-5)
6. "כך לדוגמא, בריטניה מתמקדת ביכולותיה ההגנתיות", תרגום חופשי מאנגלית מתוך:  
   Matania Eviatar, "Cyber Generates New Possibilities", Israel Globes (Israel Business Arena), Dec 2016 [↑](#footnote-ref-6)
7. עמוד 20 במסמך "האסטרטגיה הישראלית להגנת הסייבר" [↑](#footnote-ref-7)
8. על פי Chesney אירוע זה הינו הפעם הראשונה מאז ומעולם בה ניטלה אחריות פומבית על תקיפה כזו ועל ההקשר הסייברי שקדם לה. [↑](#footnote-ref-8)
9. " A cyberattack can have devastating effects in the real world, so disruptive as to cripple a nation and put its citizens in physical danger", (Chesney 2019) [↑](#footnote-ref-9)
10. כך לדוגמא, תקיפות הסייבר המשתקות של רוסיה באסטוניה ב-2007 הביאו להתערבות של נאט"ו ולסיוע לאסטוניה בתחומי הסייבר, (Ikeda 2019). [↑](#footnote-ref-10)
11. Chesney (2019), מפריד בין "הגנה בסייבר" לבין "הרתעה בסייבר". כאשר "הגנה בסייבר" הינה כל מאמצי ההגנה הפאסיביים ואילו הרתעה עוסקת באיומים בהפעלת כוח בסייבר ובאמצעים אחרים, בתגובה לפעילות סייבר. כאמור, עלפי המודל של אדמסקי (2017) מדובר בהרתעה על בסיס שלילה והתרעה על בסיס ענישה. [↑](#footnote-ref-11)
12. מתוך החלטת ממשלת ישראל מס' 2444 מיום 15 בפברואר 2015. ההדגשה אינה מופיעה במקור. [↑](#footnote-ref-12)