לוחמה קיברנטית והרתעה: מגמות ואתגרים במחקר

אמיר לופוביץ

מבוא

בשנים האחרונות מספר הולך וגדל של חוקרים הרחיבו את הדיון באסטרטגיית ההרתעה כדי לבחון התמודדות עם מגוון של איומים "חדשים". בשונה מתקופת המלחמה הקרה שבה התמקד המחקר בהרתעה בין מדינות, בין מעצמות ובהרתעה גרעינית, אנו רואים בשנים האחרונות – ובייחוד מאז פיגועי ה־11 בספטמבר 2011 – מחקרים רבים הבוחנים את אסטרטגיית ההרתעה כלפי איומים נוספים, כמו טרור, מדינות סוררות וכלפי הרתעה בסכסוכים אתניים. למחקרים אלה יש כמה מאפיינים משותפים: הם מתבססים ברובם על ניסיון לבחון את רלוונטיות התנאים להצלחת הרתעה כפי שפותחו בהקשר של המלחמה הקרה, והם שמים דגש חזק למדי על המלצות מדיניות (policy oriented), ובעיקר על המלצות הנוגעות להתמודדות עם האתגרים הניצבים לפני ארצות־הברית.[1] מאפיינים מחקריים אלה בולטים מאוד גם בדרך שבה התפתח הדיון בקשר שבין הרתעה לבין לוחמה קיברנטית.[2] כך, רבים מהמחקרים העוסקים באסטרטגיית ההרתעה ולוחמה קיברנטית, יוצאים מנקודת המבט האמריקנית ובוחנים את האפשרות של ארצות־הברית ליישם אסטרטגיה של הרתעה כדי למנוע התקפות קיברנטיות עליה, או את הדרך שבה ארצות־הברית יכולה להשתמש בלוחמה הקיברנטית כדי להרתיע מגוון של איומים אותם היא מבקשת למנוע.[3]

ממחקרים אלו עולה, כי האפשרות להרתיע התקפות של לוחמה קיברנטית היא מוגבלת בכל אחד מהממדים הדרושים להפעלה מוצלחת של אסטרטגיה זו: הימצאות היכולת (אמצעי נשק), אמינות האיום והאפשרות להעביר את המסר המאיים למאתגר הפוטנציאלי.[4] עם זאת, יש כמה גורמים העשויים בתנאים מסוימים לשמש בסיס להרתעה מוצלחת גם של לוחמה קיברנטית. במאמר זה אסקור את ספרות המחקר ואציע כיוונים להמשך המחקר בסוגיות האמורות.

ד"ר אמיר לופוביץ' הוא מרצה בחוג למדע המדינה, אוניברסיטת תל־אביב

בחלק הראשון של המאמר מוצגים התנאים להצלחת אסטרטגיית ההרתעה. בחלק השני נסקרים הטיעונים המרכזיים שהוצגו בנוגע לקשיים להפעיל הרתעה מוצלחת נגד לוחמה קיברנטית לגבי כל אחד מן התנאים הללו. החלק השלישי עוסק בכמה גורמים העשויים לחזק את ההרתעה כנגד לוחמה קיברנטית, ובמספר יתרונות וחסרונות שלהם. בחלק האחרון אצביע על החשיבות להמשיך את הדיון בקשרים שבין הרתעה ולוחמה קיברנטית, ואציע כיוונים אפשריים למחקר ולחשיבה בנושא.

התנאים להצלחת הרתעה

שחקנים יכולים לנסות לגרום ליריבם להימנע מפעולה לא רצויה במגוון דרכים. האסטרטגיה של הרתעה על־ידי איום בענישה (deterrence by punishment) היא אחת הנחקרות ביותר שבהן. סוג זה של הרתעה זכה למספר רב של ההגדרות,[5] כשביניהן הגדרתם של גורג׳ וסמוק זכתה לשימוש נרחב. לטענתם, הרתעה היא היכולת לשכנע יריב (פוטנציאלי) כי המחיר שהוא ישלם עקב ביצוע הפעולה הלא רצויה יעלה על כל רווח אפשרי.[6] סוג זה של הרתעה שונה מ**הרתעה על־ידי** מניעה (deterrence by denial),[7] המבוססת על הניסיון לשכנע תוקפן אפשרי שעליו להימנע מהפעולה מאחר שלא יצליח להשיג את מטרותיו.[8] המושג של הרתעה גם שונה מהמושג אכיפה (compellence), המבוסס על שימוש באיומים כדי לגרום ליריב לבצע פעולה, בעוד הדגש בהרתעה הוא כאמור לגרום ליריב להימנע מביצוע הפעולה הלא רצויה.[9]

סוגיה מרכזית שעסקו בה חוקרים שבחנו את אסטרטגיית ההרתעה על־ידי איום היא התנאים שבהם היא עשויה להצליח, כלומר לגרום ליריב פוטנציאלי להימנע מאתגור המגן. המחקר, שהתפתח ברובו בתקופת המלחמה הקרה ועסק בהרתעה בין מעצמות־העל, עמד על שלושה תנאים מרכזיים: יכולות המגן, אמינות האיום והעברת המסר של האיום למאתגר.

תנאי ראשון בכדי שהרתעה על־ידי איום בענישה תפעל, הוא שהמגן יוכל לגבות מחיר מהשחקן המאתגר. לא מפתיע אפוא שמחקרי ההרתעה התפתחו מאוד בעידן הגרעיני מאחר שנשק זה מאפשר להבהיר היטב את המחיר של מלחמה עתידית. הנשק הגרעיני נתן למנהיגים "כדור בדולח", שאפשר להם לראות את תוצאות המלחמה הגדולה הבאה, ולכן לנקוט משנה זהירות בהתנהגותם.[10] עם זאת חשוב להדגיש, כי אין מדובר רק ביכולת לא קונבנציונליות, וגם אמצעים קונבנציונליים עשויים לשמש לגביית מחיר ממאתגר.[11] יתרה מכך, חלק חשוב מממד היכולת הוא אמצעי העברה שיש בידי המגן, למשל מטוסים, טילים ואפילו כבישים או כלי רכב העשויים להיות חלק מנדבך היכולת בהקשר של הרתעה.

תנאי שני להצלחת הרתעה הוא אמינות האיום. כדי שאיום ההרתעה יהיה אפקטיבי, השחקן המגן צריך להיות נכון להשתמש באמצעים שברשותו. חוקרים

הציגו מגוון גורמים העשויים להגביל נכונות זאת, למשל דעת קהל פנימית או בינלאומית, או אפילו יכולת ההרתעה של היריב עצמו (השחקן המאתגר).[12] המשותף לגורמים אלה הוא, שהם מעלים, כל אחד בדרכו, את המחיר של הפעולה ומקטינים את האמינות של השחקן להוציא לפועל את האיום אם יידרש לכך.[13]

התנאי השלישי הוא העברת המסרים למאתגר בדבר שני התנאים הקודמים — היכולות והכוונות. כלומר, על המאתגר להיות מודע לאמצעים שיש בידי השחקן המגן ולנכונותו להשתמש בהם. יש הטוענים שתנאי זה הוא החשוב ביותר, כפי שרמזו לכך חוקרים שפיתחו את הגישות הפסיכולוגיות להרתעה. לטענתם, לתפיסות ולעיוותי תפיסה של מקבלי החלטות יש השפעה ישירה על הצלחת הרתעה.[14] במובן זה, מה שחשוב זה לא היכולות של השחקן המגן וכוונותיו, אלא כיצד אלו נתפסים בעיני המאתגר הפוטנציאלי.

לבסוף, אסטרטגיית ההרתעה עשויה לשמש למניעת סוגים שונים של איומים. לכן קשה לדון באופן אחיד בתנאים להצלחת הרתעה, שכן אלו צריכים להיות מותאמים לא רק לשחקן המאתגר, אלא גם לסוג הפעולה שמנסים להניא אותו מלבצע. למשל, בעוד נשק גרעיני עשוי להיות אפקטיבי בהרתעה מפני מתקפה כוללת ("הרתעה כללית"), מידת יעילותו תהיה נמוכה יותר כלפי איומים מוגבלים יותר.[15]

הרתעה ולוחמה קיברנטית – הקשיים בהרתעה

חלק גדול מן המחקרים שבחנו את אסטרטגיית ההרתעה בהקשר של לוחמה קיברנטית, ביקשו ליישם את התיאוריות של המלחמה הקרה בכל הנוגע להצלחת ההרתעה. חוקרים בחנו את התנאים המרכזיים להצלחת הרתעה שהוצעו בספרות (ונידונו בחלק הקודם): יכולת המגן, אמינות האיום ותקשורת, כלומר האפשרות להעביר אל המאתגר את המסר בדבר היכולות ואמינות האיום. מרבית החוקרים סבורים על סמך בחינת התנאים האלה, שאסטרטגיית ההרתעה צפויה להיכשל לנוכח האיומים שיוצרת לוחמה קיברנטית.[16]

היכולת

קושי מרכזי בהרתעת לוחמה קיברנטית נובע מכך שסוג לוחמה זה מאפשר גם לשחקנים חלשים להעתיק את העימות למרחב שבו יוכלו למקסם את רווחיהם ובמידת סיכון נמוכה. למעשה, ככל ששחקן מפותח יותר מבחינה טכנולוגית, כך הוא פגיע יותר להתקפות של לוחמה קיברנטית.[17] גורם זה מקטין את אפשרות התגמול, ולכן את היכולת לבסס איום הרתעה אמין. כך למשל, קשה מאוד להרתיע שחקנים, ובייחוד יחידים, שאין ברשותם מערכות מידע משל עצמם הניתנות לאיום בפגיעה בהן.[18] בעיה זו באה לידי ביטוי גם בהתמודדות עם מדינות שמידת

ההתבססות שלהן על מערכות מידע היא נמוכה. במצבים כאלה האפשרות של איום אפקטיבי באמצעים של לוחמה קיברנטית בלבד היא מוגבלת.

האמינות

בעיה שנייה בהרתעת איומי לוחמה קיברנטית היא אמינות המגן. לפגיעות המגן עשויה להיות השפעה המגבילה את נכונותו להפעיל את יכולותיו עקב חששו כי תגמול עלול להוביל להסלמה. הבעיה של המגן היא, שהסלמה כזאת עלולה להיות מסוכנת לו יותר מאשר למאתגר, ועל כן עלול לגדול חוסר האמון של המאתגר בנכונותו של המגן לפעול.[19] הבעיה אף מועצמת מכך, שעל־פי־רוב לצד החלש השוקל שימוש בלוחמה קיברנטית יש חסמי כניסה נמוכים (low entry costs).[20] במילים אחרות, העלויות של מאתגר פוטנציאלי לעשות שימוש באמצעים של לוחמה קיברנטית הם במקרים רבים נמוכות, מה שמגדיל עוד את הקשיים בהצגת האיום ההרתעתי הנדרש כדי למנוע פעולה כזאת.

גם דעת קהל פנימית ובינלאומית עשויה להגביל את אמינות איום התגמול עקב המאפיינים של הלוחמה הקיברנטית. במצבים שיהיה קשה לבסס את זיהוי מקור הפגיעה (כפי שיתואר בהמשך),[21] יהיו מגבלות גם על היכולת להפעיל תגמול שיגרום נזק.[22] מגבלות אלה יכולות להיחשב בעיני מאתגר פוטנציאלי למערערות את אמינותה של ההרתעה. וכך תוקפן פוטנציאלי, המעריך כי קטנים הסיכויים שהמגן יממש את איומיו בגלל נזק שעשוי להיגרם לו עקב כך, תוקפן כזה יהיה נכון להסתכן ולפעול.

העברת האיום

הבעיה השלישית נובעת מהקושי של המגן להעביר למאתגר את המסר בדבר יכולותיו ובדבר אמינות התגובה שלו. מלבד הבעיות הבסיסיות בנוגע לכל אחד מן ההיבטים הללו, שתוארו לעיל, מאתגרים יכולים להיות לא רק אנונימיים אלא אפילו יחידים, שפעמים רבות אין להם כתובת פיזית הניתנת לזיהוי.[23] כך למשל, לטענת ליביקי, עד היום לא לגמרי ברור מה המקור להתקפה על שרתי האינטרנט של אסטוניה בשנת 2007, והאם הייתה זו פעולה מכוונת מלמעלה של ממשלת רוסיה, כפי שטענו גורמים אחדים שבדקו את הנושא.[24] מקור הפגיעה יכול להיות מדינה אחרת, ארגונים או יחידים הפועלים בתוך מדינה אחרת, וכן ארגונים או יחידים הפועלים בתוך גבולות המדינה שאותה רוצים לתקוף. למעשה, מצב זה מבטא את הטשטוש הקיים בין פשיעה, טרור ולוחמה.

יתרה מכך, לצורך הרתעה לא מספיק זיהוי בדיעבד של הגורם המאתגר, אלא נחוץ זיהוי שלו מבעוד מועד, בטרם התקפה, כדי שיהיה אפשר להפנות אליו את האיום המרתיע. זוהי סוגיה מרכזית, שכן הרתעה מבוססת כאמור על כך

שהמאתגר הפוטנציאלי יהיה מודע מראש ליכולתו של המגן ולנכונותו להפעיל את האמצעים שבידו. ואולם אם המגן מתקשה לזהות את מקור הפגיעה לאחר התרחשותה, קל וחומר שיתקשה בכך בטרם פגיעה. יתרה מכך, גם הפתרון של הצגת איומים כלליים שנועדו להקיף טווח רחב למדי של שחקנים שהמגן מעריך כמי שעלולים לנסות ולפגוע בו הוא מוגבל. זאת מכיוון שההרתעה יעילה יותר במקרה שהאיום, גם אם אינו מפורש לגמרי, מופנה לשחקן ספציפי ולא לשורה אנונימית ולא מוגדרת של שחקנים או סוגי שחקנים העלולים לנסות ולאתגרו.[25]

קושי אחר הקשור ישירות להעברת המסרים למאתגר נוגע לשאלת האמצעים להעברת מסרי האיומים לתוקף הפוטנציאלי.[26] קושי זה מתעצם משום ריבוי השחקנים היכולים ליצור איומים. שלא כמו בתקופת המלחמה הקרה, שבה מספר היריבים (שהיו מדינתיים) היה מוגבל ויכולותיהם היו ברורות למדי, בעידן המידע יש ריבוי של תוקפים אפשריים, מה שמקטין את האפשרות להציג הרתעה יציבה ואמינה.[27] במילים אחרות, בתקופת המלחמה הקרה — ובעימותים בין־מדינתיים מסורתיים בכלל — היריב היה ידוע, ולכן היה ברור מיהו הנמען של המסר ההרתעתי. מנגד, ריבוי האיומים של הלוחמה הקיברנטית וגיוונם יוצר זירה מורכבת יותר לפעולה, שבה לא ברור לגמרי כיצד יש להעביר את המסר המרתיע.

הרתעה ולוחמה קיברנטית – לעתים ההרתעה אפשרית

למרות הקשיים שצוינו, אין לפסול לגמרי את האפשרות שהרתעה כנגד לוחמה קיברנטית עשויה בתנאים מסוימים להצליח, חלקית לפחות. למשל, חוקרים הדגישו כי האיום בתגמול אינו חייב להיות מוגבל לחלל הקיברנטי, אלא יכול להיעשות באמצעים מסורתיים יותר. כך אם מדינה מאיימת לפעול באמצעים של לוחמה קיברנטית, האיום ההרתעתי כלפיה יכול להתבסס על קשת רחבה של אמצעים המצויים ברשותה של המדינה המבקשת להתגונן. איומים כלכליים, פוליטיים, דיפלומטיים או צבאיים עשויים להיות יעילים בהרתעת מדינה הרוצה להפעיל לוחמה קיברנטית נגד מדינה אחרת. בדומה, גם עם איומים שמציבים יחידים או ארגוני טרור המבקשים להפעיל לוחמה קיברנטית, יכולות מדינות – כפי שהציעו חוקרים (ואף כמה מקבלי החלטות) – להתמודד בעזרת אמצעי הרתעה שאינם מן המרחב הקיברנטי. למשל, איומים באמצעות מערכת המשפט (הפנימית והבינלאומית), ובאמצעות ארגונים לביטחון פנים, זאת למשל בשילוב עם איומים צבאיים מסורתיים.[28] באופן זה, אם יש שחקנים המעריכים שישיגו רווחים מהסטת העימות לחלל הקיברנטי, שבו הם נהנים מיתרונות, השחקנים העלולים להיפגע יכולים לפעול בזירות הנוחות להם ולא להגביל את עצמם לתגובה במרחב הקיברנטי בלבד.

אמצעי אחר הוא הרתעה על־ידי מניעה. היתרון הטמון באסטרטגיה זו הוא אפשרות ביסוסה על אמצעים הגנתיים, וכך לא רק להניא יריב מפעולה, אלא גם לתת פתרון במקרה שהמאתגר החליט לתקוף. יתרה מכך, לדברי מורגן, התבססות על אמצעים הגנתיים מגוונים, שיסייעו לביסוס הרתעה על־ידי מניעה, יוכלו לסייע לזהות את התוקפן ולחזק את היכולת להפעיל תגובת־נגד, מה שעשוי לחזק גם את ההרתעה באמצעות ענישה.[29] עם זאת, הפעלת אסטרטגיה זו כרוכה בהתגברות על בעיות דומות לאלו הקשורות להפעלה מוצלחת של הרתעה על־ידי איום. בשני המקרים, מחיר הכניסה הנמוך שנדרשים מאתגרים לשלם כדי להפעיל לוחמה קיברנטית נותר קושי מרכזי. עוד מציע מורגן, כי הרתעה סדרתית (serial deterrence)[30] יכולה גם היא להיות מועילה להתמודדות עם איומים של לוחמה קיברנטית. לטענתו:

> attacks are very likely to turn out to be manageable cyber repeated serial deterrence, primarily through applications of harmful responses over an extended period, to induce either eventually permanent suspensions of the most temporary or bothersome attacks or of attacks by the most obnoxious opponents.[31]

בעוד שזוהי דרך מקורית להתמודד עם איומים במרחב הקיברנטי, ויש בה ניסיון מעניין להשתמש במושגים קיימים בדרך חדשנית, אין היא אינה חפה מאתגרים. ראשית, לא ברור שהיריב יכול להיות מושפע לאורך זמן מאותם ניסיונות, שכן אלו עלולים ללמד את המאתגר כי ההרתעה שמפעיל המגן אינה עובדת (ועל כן הוא נדרש לאותן פעולות חוזרות).[32]

בעיה נוספת הקשורה לאסטרטגיה המבוססת על הרתעה סדרתית היא חשיפת האמצעים שבידי המגן. הבעיה של חשיפת היכולת באה אומנם לידי ביטוי בכל אחת מצורות ההרתעה במרחב הקיברנטי (הרתעה על־ידי איום, הרתעה על־ידי מניעה); ואולם עקב אופיים של האמצעים שמשתמשים בהם במרחב זה, הבעיה חריפה במיוחד בכל הקשור לניסיונות הרתעה לאורך זמן, כמו הדרישות המתחייבות מאסטרטגיה של הרתעה סדרתית.[33] במצב זה, חשיפת היכולות ההתקפיות כפועל יוצא של התקיפות החוזרות ונשנות עשויה לשמש מקור לידע או השראה בעבור המאתגר.[34] מורגן עצמו התייחס לסוגיה זו וטען, כי חשיפת היכולות עלולה לא רק להעניק השראה ליריבים ומוטיבציה להשגת יכולות דומות, אלא גם עלולה לאפשר ליריב להתכונן לאיום העתידי ולפגוע ביעילותו של האיום הזה.[35]

כיוונים לחשיבה ולמחקר נוסף

אומנם כמה חוקרים כבר החלו להציע כיווני מחקר מגוונים לבחינת הרתעה במרחב הקיברנטי, אך אני מבקש להצביע כאן על שני כיוונים מרכזיים שבהם אפשר להרחיב עוד את הספרות בנושא. ראשית, יש מקום למקד יותר את המחקר העוסק באיומים במרחב הקיברנטי. נראה שקיים פער הולך וגדל בין הפרקטיקות בזירה הבינלאומיות וסוגי האיומים בה לבין הדרך שהמחקר בתחום בוחן את אסטרטגיית ההרתעה. פער זה קיים בתחומי מחקר נוספים של הרתעה, אך הוא בולט במיוחד בנוגע למרחב הקיברנטי, המכיל מגוון רחב של סוגי אינטראקציות בין סוגים שונים ומגוונים של שחקנים המאיימים בדרכים שונות. לכן יש להרחיב את הדיון בסוגי השחקנים והאיומים שהם יוצרים, ובדרכים להרתעת כל אחד מהם. זאת ועוד, בדומה למחקר הרחב בנוגע לאסטרטגיית ההרתעה, קיימת נטייה להתמקד בהרתעה של מדינות כלפי סוגים שונים של שחקנים (ארגוני טרור, מדינות סוררות וכו'),[36] בעוד חלק חשוב שאינו זוכה לתשומת לב מספקת נוגע להרתעה של אותם שחקנים את המדינות שאותן הם מבקשים לאתגר. בעיות אלה של הרתעה קיימות גם בלוחמה קיברנטית, ומעצימות את הקשיים של מדינות המתמודדות בזירה מורכבת בהרבה ממה שידעו בעבר.

בדומה, המחקר העוסק בלוחמה קיברנטית נוטה לעסוק בהיבטים קלאסיים של ביטחון, בעוד זירת האיומים מורכבת ומגוונת.[37] למשל, מדינות מוטרדות מאוד מכוחם העולה של שחקנים כלכליים (למשל גוגל), או אידיאולוגיים (למשל יחידים או קבוצות חברתיות המבקשים לקדם רפורמות שלטוניות), המשתמשים במרחב הקיברנטי. בלי להיכנס לשאלה, האם ההגדרות הקיימות ללוחמה קיברנטית מכילות את האינטראקציות עם שחקנים אלה, עשויה להיות תרומה חשובה לניתוח יחסים אלה באמצעות התיאוריות של ההרתעה. לדוגמה, אפשר לחקור באמצעות הכלים והמושגים של אסטרטגיית ההרתעה את האינטראקציות בין גוגל לבין סין בנוגע לאיומים המרומזים או הישירים שהציגו שחקנים אלה זה לזה בסוגית הצנזורה על התוצאות המוצגות במנוע החיפוש. בנוסף, פירוק המחקר של הרתעה ולוחמה קיברנטית לסוגים שונים של איומים (cyberwar, cybercrime, cyber-terror, internetwar) ולסוגי השחקנים המפעילים אותם (מדינות, יחידים, ארגונים כלכליים) עשוי להיות לא רק מדויק יותר ופורה, אלא גם להצביע על התנאים לקיום סיכויים רבים יותר להצלחתה של אסטרטגיית ההרתעה של כל אחד מן השחקנים המעורבים כלפי יריבו.

שנית, אני סבור כי יש להמשיך ולבחון בגישה ביקורתית ומקורית את הספרות האסטרטגית המסורתית בנושאי הרתעה. הדבר כבר נעשה במידה לא מבוטלת בכמה מן המאמרים שפורסמו בנושא, אך יש מקום להמשיך ולבחון מושגים נוספים לגבי אסטרטגיית ההרתעה, כמו "הרתעה מידית",[38] "הרתעה כללית" ו"הרתעה

מורחבת".[39] יש לנסות להבין את המשמעות והרלוונטיות של יישום פרקטיקות כאלה במרחב הקיברנטי.

בדומה אפשר להשתמש במושגים כמו "עמימות". מושג זה עשוי לשמש מסגרת חשיבה להתמודדות עם הדילמה הכרוכה מחד גיסא בצורך בחשיפת היכולות,[40] ומאידך גיסא החשש שהיריב יוכל לנצל חשיפה זו להגדיל את עוצמתו ואת חסינותו מפני איומי ההרתעה. שימוש בתובנות שפותחו בהקשרים שונים עשוי להיות בסיס מעניין לפיתוח רעיונות של עמימות במרחב הקיברנטי, לא רק לגבי הכוונות והנכונות להפעיל את האיומים, אלא בכלל ביחס לשאלת קיומן של היכולות. באור זה אפשר למשל לנתח את המאמצים שעושות מדינות בשנים האחרונות בתחום הלוחמה הקיברנטית. לא רק שאמצעים אלה שמפתחות מדינות עשויים לחזק את אסטרטגיית ההרתעה שלהן כלפי איומים אלה, אלא שעצם הבולטות שזכו לה מאמצים אלה יכולה לשמש ככלי הרתעתי. כך הגם שלהקמת פיקוד אסטרטגי לניהול לוחמה קיברנטית של ארצות־הברית יש מגוון מטרות ותפקידים,[41] עצם אזכורו והבולטות שקיבל מאפשרים לא רק את שיפור היכולת, אלא גם מדגימים את הנכונות להשקיע משאבים בצמצום האיומים והנזקים. ייתכן שהבלטת הרצון להשקיע באמצעים מעין אלו, וחשיפה של היקף התקציבים, המשאבים וכוח האדם המופנה לנושא — גם בלי פירוט מדויק של האמצעים הנרכשים ויכולותיהם — יוכלו לסייע בהגדלת אמינות המסר ההרתעתי נגד איומים במרחב הקיברנטי, במיוחד כלפי איומים הכרוכים ברמות גבוהות של אלימות מצדן של מדינות אחרות. במילים אחרות, חשיפה חלקית של היכולות תוך שמירה על ערפול ועמימות לגבי מהותן, מאפשרת לצמצם את אותן השפעות מזיקות שתוארו לעיל, אך גם להעביר מסר תקיף. עם זאת, אפשר לצפות כי סף הכניסה הנמוך לפעולה במרחב הקיברנטי, במיוחד כשמדובר בעימותים א־סימטריים, ימשיך להציב אתגר לביסוס אסטרטגיה של הרתעה המבקשת למנוע איומים במרחב הזה.

סיכום

המחקר העוסק בהרתעה של לוחמה קיברנטית דן בעיקר בקשיים הטמונים בהרתעת יריבים מלעשות שימוש באסטרטגיה זו. הגם שבתנאים מסוימים הרתעה עשויה להתקיים, בכל זאת הקשיים הנוגעים ליכולת המגן, לנכונות שלו להשתמש באמצעים אלה וליכולתו להעביר את המסר המרתיע למאתגר הפוטנציאלי מגבילים מאוד את האפשרות להפעיל הרתעה מוצלחת. עם זאת, בשל היתרונות הגלומים באסטרטגיית ההרתעה בהקטנת היקפי אלימות בסכסוכים, חשוב לנסות ולפתח עוד את המחקר העוסק בקשרים בין הרתעה לבין לוחמה קיברנטית. במאמר זה ביקשתי להצביע על שני כיוונים מרכזיים להמשך החשיבה והפיתוח של רעיונות אלה. ואולם, וכפי שטוען כאמור מורגן, יש לנהוג זהירות בתובנות

הקיימות, שכן נדרש עוד ידע אמפירי על מהותה של הלוחמה הקיברנטית, הן על הנזק שהיא גורמת, והן על הדרך שאפשר להשתמש בה.

הערות

1 Lupovici Amir, "The Emerging Fourth Wave of Deterrence Theory–Toward a New Research Agenda," *International Studies Quarterly* 54, no. 1 (2010): 705-732.

2 בלוחמה קיברנטית הכוונה היא לסוג מסוים של לוחמת מידע, הגם שלעתים המושג לוחמת מידע משמש כמושג חליפי למושג לוחמה קיברנטית. סוג לוחמה זה מבוסס על הניסיונות השונים למנוע, לשבש, לנצל או להשמיד את מערכות המידע של האויב, תוך הגנה על מערכות המידע של המגן מפני איומים דומים. ראו: Harknett J. Richard, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (1996), pp. 93-97; Wheatley F. Gary and Hayes, E. Richard, Infor*mation Warfare and Deterrence*. (Washington DC: National Defense University Press, 1996), pp. v-vi, 5-6; Molander, C. Roger, Riddile, S. Andrew, and Wilson, A. Petter (1996). "Strategic Information Warfare: A New Face of War," *Parameters* 26 No. 3 (1996), pp. 83, 86-90. לסקירה מקיפה של מושגים מרכזיים על לוחמה במרחב הקיברנטי ראו: טבנסקי ליאור, "לחימה במרחב הקיברנטי: מושגי יסוד". **צבא ואסטרטגיה**, כרך 3, גיליון 1 (2011). עמ' 65–80.

3 על הנטייה הכללית של המחקר העוסק בלוחמת מידע וביטחון לבחון שאלות מדיניות, ולהמעיט בשילוב היבטים תיאורטיים כלליים יותר, ראו: Eriksson Johan and Giacomello Giampiero, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?" *International Political Science Review* 27, no. 3 (2006), pp. 221-244.

4 במאמר זה אשתמש במונחים הרווחים לתיאור השחקנים הנוגעים לאסטרטגיית ההרתעה: השחקן המגן, השחקן המבקש להפעיל את אסטרטגיית ההרתעה כדי למנוע פעולה שאינה רצויה לו; והשחקן המאתגר, השחקן המבקש לפעול נגד המגן. השימוש במושגים החלופיים, השחקן המרתיע או השחקן המורתע, כפי שנעשה לעתים, הוא בעייתי, שכן הוא מרמז על הצלחת האסטרטגיה.

5 לסקירה מצוינת של הגדרות המושג הרתעה על־ידי איום ראו: Morgan, M. Patrick, *Deterrence Now* (NY: Cambridge University Press, 2003), pp 1-2.

6 George Alexander and Smoke Richard. *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), p. 11.

7 חשוב להבהיר כי אסטרטגיה של הרתעה על־ידי מניעה גם שונה מאסטרטגיה של הגנה. אף שקיימת חפיפה ביניהן, הרי הגנה מבקשת לספק פתרון למקרה שאסטרטגיית ההרתעה תיכשל, ואילו הרתעה על־ידי מניעה מבקשת למנוע את הפעולה על־ידי כך שהמאתגר יבין שאין ביכולתו לבצע את הפעולה עקב יכולותיו של המגן.

8 להבחנה זו ראו: Snyder Glenn, *Deterrence and Defense* (Princeton: Princeton University Press, 1961). עם זאת, הרתעה על־ידי איום והרתעה על־ידי מניעה עשויות עקרונית לחזק זו את זו. אם מאתגר פוטנציאלי יידע לא רק שסיכויו להצליח נמוכים, אלא שגם ייגבה ממנו מחיר יקר, גדלים הסיכויים שהוא יימנע מפעולה.

9 Schelling Thomas, *Arms and Influence* (New Haven: Yale University Press, 1966), p. 69.

10 Carnesale Albert, Doty Paul, Hoffmann Stanley, Huntington, P. Samuel, Nye, Jr. S. Joseph, and Sagan D. Scott, *Living with Nuclear Weapons*. (Cambridge: Harvard University Press, 1983).

11 לדיון בהרתעה קונבנציונלית ראו למשל Shimshoni Jonathan, *Israel and Conventional Deterrence: Border Warfare from 1953 to 1970* (Ithaca: Cornell University Press, 1988); Mearsheimer J. John, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983).

12 כך למשל נטען, שהתפתחות נורמות בינלאומיות הקוראות לאיסור השימוש בנשק גרעיני ודעת קהל בינלאומית התומכת בכך, מחלישות את אסטרטגיית ההרתעה הגרעינית מאחר שהן מעלות את מחיר מימוש האיום של המגן Paul T.V., "Nuclear Taboo and War Initiation in Regional Conflicts," *Journal of Conflict Resolution* 39, no. 4 (1995), pp. 699-700, 711.

13 חוקרים דנו בשאלה כיצד להגדיל את אמינות האיום, ואף הציעו אמצעים לכך, למשל "מסרים יקרים" (costly signals) Fearon James, "Domestic Political Audiences and the Escalation of International Disputes," *American Political Science Review* 88, no. 3 (1994), pp. 577–592. עם זאת, היו חוקרים שהטילו ספק באפקטיביות של חלק מן האמצעים האלה. לדיון בנושא ראו למשל Huth, Paul, "Reputations and Deterrence: A theoretical and Empirical Assessment," *Security Studies* 7, no. 1 (1997), pp. 72-99.

14 Morgan, *Deterrence Now*, pp. 15-16.

15 לסקירה מצוינת המדגימה היטב את הסוגים השונים של ההרתעה הישראלית ראו: בר־יוסף אורי, "50 שנות הרתעה ישראלית: לקחי העבר ומסקנות לעתיד". **מערכות**, גיליון 366–367, 1999, עמ' 12–29.

16 Harknett, Ibid, pp. 93-107; Berkowitz D. Bruce, "Warfare in the Information Age," In Athena's Camp: Preparing for Conflict in the Information Age. eds. John Arquilla and David F. Ronfeldt (Santa Monica, CA: RAND Corporation, 1997), pp. 183-184; Goldman O. Emily, "Introduction: Security in the Information Technology Age," In *National Security in the Information Age,* ed. Emily O. Goldman (London: Taylor & Francis, 2004), p. 3; Arquilla, John, "Thinking About New Security Paradigms," in National Security in the Information Age, ed. Emily O. Goldman (New York: Routledge, 2004), pp. 210-213. למסקנות דומות מגיע מורגן, הטוען כי היבטים שונים הנוגעים לפרקטיקות של ההרתעה מתקופת המלחמה הקרה ומבוססים הן על אסטרטגיה זו והן על גורמים תומכים כמו אמצעי בקרת נשק, רלוונטיים פחות להרתעה במרחב הקיברנטי. עם זאת, אין הוא פוסל על הסף את האפשרות של שימוש בסוגים שונים של אסטרטגיית ההרתעה להתמודדות עם איומים אלה Morgan, M. Patrick, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," in *Proceedings of a Workshop on Deterring Cyberattacks*, eds. John D. Steinbruner et al., (Washington: The National Academies Press, 2010) pp. 55-76. נוכח מגבלות היכולת לבסס הרתעה כנגד לוחמה קיברנטית הוצע – במיוחד בעבור ארצות־הברית, שבה עוסק כאמור רובו של הדיון המחקרי – לנקוט אמצעים חלופיים לאסטרטגיה זו, למשל שימוש באמצעים הגנתיים. Adams James, Wheatley and Hayes, Ibid, p. 9; "Virtual Defense," *Foreign Affairs* 80 (2001), pp. 107-112.

17 Harknett, Ibid, pp. 96-97, 103-104; Wheatley and Hayes, Ibid, p. 9; Berkowitz, Ibid, pp. 183-184; Libicki C. Martin, *Conquest in Cyberspace* (Cambridge, UK: Cambridge University Press, 2007), p. 272. על הפגיעות של חברות (societies) למתקפות אלקטרוניות ראו: Deibert Ron, "Circuits of Power: Security in the Internet Environment," in *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, eds. J.P. Singh and James N. Rosenau (NY: Suny Press, 2002), p. 115. על נקודות הרגישות לאיומים חיצוניים ופנימיים של מערכות

מידע, ראו: Libicki C. Martin, *Cyber Deterrence and Cyber War* (Santa Monica, CA: RAND Corporation, 2009), pp. 13-23. Available at: www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.
עם זאת, חשוב לציין כי לטענת ליביקי היקף האיום שיוצרת לוחמה קיברנטית בתקופה הנוכחית אינו ברור או ודאי. לטענתו, סוגיית היקף הנזק שעשויה לוחמה קיברנטית לגרום היא מרכזית ועומדת בבסיס הוויכוח בדבר חשיבות אסטרטגיית ההרתעה כלפי סוג לוחמה זה Libicki, *Cyber Deterrence and Cyber War*, p. 36.
מסיבות דומות, הנוגעות למיעוט המידע הקיים וחדשנות הנושא, ממליץ מורגן להיזהר ממסקנות חפוזות בנוגע לאפשרויות ההרתעה של איומים במרחב הקיברנטי, Morgan, "Applicability of Traditional Deterrence Concepts", pp. 61-62.

18 Libicki, *Cyber Deterrence and Cyber War*, p. 26.

19 Harknett, Ibid, p. 104.

20 Molander et al., Ibid, p. 87.

21 על הקשיים בזיהוי מקורן של התקפות של לוחמה קיברנטית ראו גם: Libicki, *Cyber Deterrence and Cyber War*, pp. 44-45.

22 על דעת הקהל הפנימית והבינלאומית המגבילות את אפשרות השימוש בכוח, ובכך משפיעות על ההרתעה של השחקן המגן, ראו למשל:, Jervis Robert, "Deterrence, Rogue States, and the Bush Administration," in Complex Deterrence, eds. T.V. Paul, Patrick Morgan, and James Wirtz (Chicago: University of Chicago Press), p. 153.

23 Hayes and Wheatley, Ibid, p. 9; Harknett, Ibid, p. 104; Berkowitz, 1997, pp. 183-184; Cordesman Anthony, and Cordesman, Justin, *Cyberthreats, Information Warfare, and Critical Infrastructure Protection: Defending the US Homeland*. (Westport: Praeger: 2001), p. 7; Arquilla, Ibid, pp. 210-211.

24 Libicki, *Cyber Deterrence and Cyber War*, pp. 1-3.

25 הסיבה לכך היא שהאיום המרתיע צריך להיות מותאם כאמור לסוג האיום ולסוג הגורם המפעיל אותו. לכן נטען כי קיימת חשיבות לבסס את ההרתעה על איום ממוקד כלפי מאתגר מסוים. למשל, הרתעה כלפי שחקן מדינתי הנהנה מריבונית בטריטוריה מסוימת ואשר יש לו "מטרות ערך", שונה מהרתעה כלפי שחקן שאינו מדינתי, המחייבת אפוא שימוש בסוגים שונים של איומים. סוגיה זו זוכה בשנים האחרונות לדיון נרחב בהקשר של הרתעה "תפורה" (tailored deterrence), בעיקר בהקשר של הרתעת טרור. לדיון במושג ראו: Lantis S. Jeffrey, "Strategic Culture and Tailored Deterrence: Bridging the Gap between Theory and Practice". *Contemporary Security Policy* 30, no. 3 (2009), pp. 469-471. לדיון במושג ביחס ללוחמה קיברנטית ראו: Kugler, L. Richard, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), pp. 331-333.

26 Harknett, Ibid, pp. 98-100.

27 לדיון נוסף בהשפעת המהפכה בענייני צבא Libicki, *Conquest in Cyberspace* p. 272. (RMA) על הרתעה ועל היכולת להרתיע ראו: Morgan, *Deterrence Now*, pp. 219-224.

28 ראו, Hayes and Wheatley, Ibid, pp. 13, 19-20 Kugler, Ibid, p. 328. וכן ראו ב־ Cordesman and Cordesman, 2002, p. 7.

29 Morgan, "Applicability of Traditional Deterrence Concepts", p. 59.

30 במושג דומה – הרתעה מצטברת (cumulative deterrence) – השתמש דורון אלמוג בנוגע לדרך להרתיע איומים של טרור שלא במרחב הקיברנטי, Almog Doron, "Cumulative Deterrence and the War on Terrorism," *Parameters* 34, no. 4

(2004-2005): pp. 4-19.

31 Morgan, "Applicability of Traditional Deterrence Concepts", p. 59.

32 Lupovici, Ibid, p. 722.

33 כך למשל עשוי המאתגר ללמוד על אמצעי הגנה (או לקבל השראה לאמצעים כאלה) מהאמצעים שמשתמש בהם השחקן המבקש להפעיל הרתעה על־ידי מניעה, וכך הוא עלול להגביל את היכולת להרתיע באמצעות אסטרטגיה זאת.

34 ביקורת דומה הועלתה לאחר הדיווחים על וירוס סטקסנט (Stuxnet), שעל פי הפרסומים שיבש את פיתוח הגרעין באיראן. החשש שהציגו מומחים לאבטחת מידע הוא, כי תקיפה קיברנטית זו תשמש לא רק השראה למה שאפשר לעשות באמצעות סוג לוחמה זה, אלא שחלקים מהקוד של הווירוס עצמו נחשפו ועלולים לסייע לשחקנים שונים לפגוע בתשתיות רגישות. ראו למשל: "Experts Fear Hackers Can Launch Stuxnet-Like Attacks on Power Plants, Prison Gates", *The Globe and Mail*, October 24, 2011.

35 Morgan, "Applicability of Traditional Deterrence Concepts", p. 63.

36 לאזכור של סוגיה זו בהקשר של לוחמת מידע ראו למשל: Goldman, 2004, p. 3.

37 לדיון במגוון איומים אלה ראו: טבנסקי 2011, ובעיקר עמ' 70, 75–77.

38 הבחנה בסיסית רווחת במחקר ההרתעה מבדילה בין הרתעה כללית, המבוססת על הניסיון למנוע מהיריב לשקול אפשרות של תקיפה (למשל כפי שבא לידי ביטוי בהרתעה גרעינית), לבין הרתעה מידית, הנוגעת למצב שבו שחקן מבקש לעשות פעולה (למשל מזיז כוחות) ובעזרת שימוש באיומים המגן מניא אותו מפעולה זאת. דיון חשוב ומעניין בהקשר זה יכול לעסוק במשמעות של כל אחת מצורות ההרתעה הללו במרחב הקיברנטי.

39 ליביקי, למשל, החל לבחון הרתעה מורחבת במרחב הקיברנטי, Libicki, *Cyber Deterrence and Cyber War,* pp. 104-106. ואפשר למקד ולפתח עוד את הדיון בסוגיות התיאורטיות שנידונו בנוגע לאסטרטגיה זו. לדיון במושג הרתעה מורחבת ראו למשל: Huth Paul, *Extended Deterrence and the Prevention of War* (New Haven: Yale University Press, 1988), pp. 15-27.

40 כאמור, הספרות בנושאי ההרתעה מדגישה את הצורך בהעברת המסר המאיים לצד היריב, ובכלל זה את המחיר שהוא יידרש לשלם. לכן מסרים לגבי יכולות המגן או חשיפת האמצעים שבידו הוזכרו כגורמים חשובים בהקשר הזה.

41 "ארצות־הברית מקימה פיקוד צבאי למלחמה בהאקרים", *Ynet*, 24 ביוני 2009, http://www.ynet.co.il/articles/0,7340,L-3736253,00.html