הגנת סייבר באמצעות אסטרטגיות של "צמצום מידע אסימטרי"[1]

גיא פיליפ גולדשטיין

"אם אתה יודע את האויב ויודע את עצמך, אל לך לחשוש גם לא ממאה קרבות. אם אתה יודע את עצמך אך לא את אויבך, אזי כל ניצחון שלך יִלָווה בתבוסה. אם אינך יודע לא את האויב ולא את עצמך, תובס בכל קרב".
סאן צו, אמנות המלחמה[2]

מאמר זה מתמודד עם שתי בעיות מרכזיות בהגנת סייבר: סוגיית ייחוס התקיפה (מי התוקף) וסוגיית סף ההחלטה (האם הפגיעה מצדיקה מלחמה כוללת). המאמר פותח בתרחיש של משחק מלחמה, ומציע מסגרת אנליטית המבוססת על "מדריך טאלין" לשרטוט מקרים של מלחמה ואזורי משבר. בהמשך מציע המאמר דרכים להתמודד עם משברי סייבר, וזאת באמצעות שתי אסטרטגיות של "צמצום מידע אסימטרי": טיפול בסוגיית הסף בעזרת הבנה טובה יותר של ההשפעות הגלויות והמדומות על מדינות מרושתות הפועלות כמערכת המתגוננות מפני מתקפות סייבר, תוך התבססות על הרעיון של קולונל ג'ון וורדן; טיפול בבעיית הייחוס, המחייב מצוינות בשיטות הליבון וההבהרה, וכן חקירה כופה הזוכה בתמיכה בין־לאומית – בהשראת מושג הכפייה (compellence) של תומאס שלינג. השליטה הגוברת של העולם הדיגיטלי בחברות המודרניות עשויה להפוך אסטרטגיות אלו לחלק מאבני היסוד של דוקטרינה חדשה להשגת יציבות צבאית ופוליטית במאה ה־21.

מילות מפתח: נשק הסייבר; הגנת הסייבר; הרתעה; דוקטרינה; אכיפה; מדריך טאלין

גיא פיליפ גולדשטיין הוא סופר; מחבר רב המכר **בבל שעת אפס**, הוצאת שוקן, 2010.

מבוא – תרחיש אזורי

השעה 09:00 במדינה X. הכספומטים בבירת המדינה הפסיקו לעבוד. חלק מהלקוחות המקוונים של שלושה מהבנקים הגדולים במדינה לא מצליחים ליצור גישה לחשבונות הבנק שלהם. בחלק מהמקרים, נתוני החשבונות המקוונים נמחקו. טלפונים סלולריים כמעט שלא מתַפקדים. דומה שמדובר במתקפה מסוג חדש, שההשפעות שלה דומות למתקפות הסייבר של שנת 2007 באסטוניה, אולם מבחינה טכנית, הפעם הן לא נראות כמתקפות מפוזרות למניעת שירות: לא זוהתה כמות גדולה של כתובות IP המכבידות על השרתים. אין פתרונות מיידיים לתיקון התקלה ולא ברור כמה זמן היא תימשך. החרדה ברחובות מדינת X גואה במהירות. האם ניתן יהיה לשחזר את הנתונים? האם זהו גל ראשון המבשר על מתקפות נוספות?

מדינת X אינה לבדה. שבוע לאחר מכן, חברת אבטחת תוכנה ידועה ממדינה B זיהתה תוכנה זדונית חדשה: GlobalWorm. למרות שאופן פעולתה אינו ידוע ברגע הגילוי, נראה ש־GlobalWorm הדביקה מערכות רבות במדינות שונות. בהודעת התרעה שמוציאה חברת אבטחת התוכנה, היא מקשרת את המתקפה נגד מדינה X ל־GlobalWorm. מדינות נוספות שנפגעו מ־GlobalWorm חוות קשיים, וביניהן מדינות ידידות של מדינה X וגם אויבות שלה, אולם מדינה X חווה את ההשפעות החמורות ביותר.

מי אחראי למתקפות על מדינה X באמצעות GlobalWorm? מהו סוג האיום ש־GlobalWorm מציב בפני מדינה X? כיצד עליה להגיב? התשובה לשאלה השלישית תלויה בשתי השאלות הראשונות.

כאילו המצב לא סבוך דיו, מתברר שלחברת אבטחת התוכנה, שבידיה המידע הרב ביותר על GlobalWorm, יש קשרים הדוקים עם המערכת הצבאית של מדינה B, שאינה ידידה קרובה של מדינה X. כאשר המועצה לביטחון לאומי של מדינה X מתכנסת, השאלות מתלהטות: האם זו מכה נוספת מכיוונה של מדינה Y – האויב המוצהר של מדינה X? האין זה נכון שמדינה Y הגדילה את השקעותיה בנשק סייבר? או שמא המתקפה מגיעה ממדינה Z, שקשריה עם מדינה X התערערו בצורה דרמטית במהלך חמש השנים האחרונות?

ראש מדינת X מנסח את שלוש השאלות המרכזיות שעומדות על הפרק:

1. האם תוכלו להוכיח לי שמדינה Y ומדינה Z לא קשורות לעניין?
2. כמה זמן עומד לרשותי לפני שיהיה עליי להגיב?
3. כיצד אוכל להגיב אם איני יודע את התשובות לשאלה הראשונה והשנייה ?

ראש המודיעין של מדינה X מאשר כי בשלב זה אין אינדיקציה ברורה שמדינה Y או מדינה Z עומדות מאחורי המתקפות, למרות שלא ניתן לשלול זאת. במקביל, הוא לא שולל את האפשרות שמדובר במניפולציה של מדינה B.

המתקפות אמנם זעזעו את אוכלוסיית המדינה, אולם לא הסלימו במהלך שמונה השעות האחרונות. לא ניתן לומר כיצד האיום עתיד להתפתח – אם הוא בכלל ימשיך להתפתח. מה שברור הוא שחלה פגיעה בעוצמתה של מדינה X. ללא נקיטת צעדים כלשהם לבירור הנושא, לשיקום העוצמה ולתגמול על הפגיעה, מעמדה של מדינה X כמעצמת סייבר יאותגר, דבר שאין להקל בו ראש. הסברה המקובלת בעידן הנוכחי היא שפעולות מלחמתיות גדולות יתחילו במרחב הסייבר, כך שהשליטה במרחב זה היא מבחן לעוצמה הצבאית הכוללת.

שר החוץ של מדינה X מקבל את רשות הדיבור. לדבריו, למדינה A, אחת מהידידות הקרובות ביותר של מדינה X בזירה הבין־לאומית, אין אינדיקציה ברורה על מקור ההדבקה ב־GlobalWorm. עם זאת, מכיוון שמדינה A רואה בכך בעיה עולמית, היא לא תתיר למדינה X להגיב ללא הוכחה ודאית מיהו התוקף. מעבר לכך, מדינה A טוענת שהתגובה צריכה להיות מתואמת היטב, למקרה שהיא תביא לעוד פעולות תגמול בסייבר, שכן גם מדינה X וגם מדינה A אינן יודעות כיצד GlobalWorm עובד. המצב שונה מתרחישים שבהם מדינה X היא הצד התוקף. מדינה X אינה שולטת בנתונים וגם לא בסביבה, ומהלך שגוי שלה עלול להתגלות כמסוכן עבורה, ואולי אף עבור שאר המדינות. ניתן לדמיין אינספור מניפולציות, והלא ידוע רב על הידוע.

מצב זה של בלבול אסטרטגי הוא אולי מה שהתוקף כיוון אליו כשתכנן את המתקפה. מדינה X עדיין אינה יודעת על מה ועם מי מתנהל השיג והשיח. ההצעה הברורה היחידה מגיעה ממדינה B: באמצעות חברת אבטחת התוכנה שלה, היא מציעה מומחיות ייחודית ב־GlobalWorm. מן הסתם יהיה לכך מחיר. בנוסף, מדינה A ומדינה B הן מדינות מתחרות בזירה הבין־לאומית. מדינה A עשויה להתנגד לכך שמדינה B תגיש סיוע למדינה X. היחסים בין מדינה A למדינה X עלולים אז להיפגע.

בתרחיש שתואר לעיל לא ניתן להסתמך על תגובה בכלים קונבנציונאליים או אסטרטגיים. למעשה, מדינה X ניצבת בפני שיתוק אסטרטגי. תיאוריית ההרתעה המושלמת קובעת כי האסטרטגיה האופטימלית היא "תגובה בעוצמה זהה" (response in kind)[3]. אסטרטגיה כזו תוכיח שהצד המותקף מחזיק באיום אמין לגמול על התקפה עליו. במקרה המדובר, יהיה בכך איתות שמדינה X אינה מחפשת בהכרח להסלים את המצב. פול הות' (Huth) תיאר מצב זה כסגנון משא ומתן "קשוח אך גמיש".[4] תגובה הנמנעת מהסלמה חריפה, ובמקום זאת מציגה עמדה קשוחה, מאפשרת לרמוז על אופציות מבלי ליישם אותן: זוהי העֶמדה המועדפת ביותר על פוליטיקאים, כמו גם על אנשי המערכת הפיננסית. זהו מצב אופטימלי גם כשמדובר בתהליכי החלטה בתחום הסייבר. אולם במצב הנוכחי שבו נתונה מדינה X, "תגובה בעוצמה זהה" אינה אפשרית. ראשית, ישנו מכשול

מרכזי: מדינה X אינה יודעת כלפי מי להגיב ונתקלת למעשה בבעיית הייחוס.[5] אבל גם אם הייתה יודעת בוודאות מי התוקף, אזי עומד בפניה מכשול גדול נוסף: היא לא בהכרח יודעת כיצד להגיב.

הבה נניח לרגע שמדינה X הוכיחה שמדינה Y היא הצד התוקף. מכיוון שנפרצו כספומטים של בנקים, חשבונות בנק מקוונים וכמה רשתות סלולריות, מדינה X מבקשת להגיב בעוצמה זהה. הבה נניח עוד שמדינה Y לא הקשיחה מראש את אבטחת הסייבר סביב מה שהיא יודעת שיהיו יעדי התגובה של מדינה X. נותר עדיין ספק גדול באשר לשאלה האם מדינה X תהיה מסוגלת לגרום לפגיעה במדינה Y לפחות באותה רמה כמו זו שהיא עצמה ספגה. אם היא תנסה לגרום נזק דומה אך תיכשל בכך, אמינות האיום שלה תיפָגע עוד יותר; אם היא תגרום לנזק גדול מדי, היא עלולה לעורר השלכות לא צפויות ולהכניס את העימות לסחרור. במצב הנוכחי של היכולות הטכניות, קשה לחזות במדויק את ההשפעות של נשק הסייבר, וקושי זה גובר עוד כאשר מדובר בשימוש מאולתר בנשק זה במטרה להשיג תגמול מהיר.

מדינה X ניצבת בפני בעיה נוספת: סוגיית הסף.[6] אין לה פתרון בדרך של תגובה בעוצמה זהה, כלומר אין לה יכולת לאיים בצורה אמינה בתגמול. דוקטרינה הדוגלת ב"תגמול מאסיבי" בסייבר עשויה להיות נתונה לאותה ביקורת כמו זו של וויל קאופמן על החלטה NSC-162/2 של נשיא ארצות הברית אייזנהאואר משנת 1954,[7] בתוספת אזהרה שהמונח "מאסיבי" קשה להגדרה, אלא אם מדובר בפגיעה מאסיבית וודאית באזרחים. מנגד, היעדר תגמול פוגע בבירור בעקרון ה"תגובה בעוצמה זהה", ועשוי להזמין תקיפה נוספת.

בשלב זה אין אופציות תגמול טובות למדינה X. אם המתקפות הגיעו לסף נזק מסוים ומדינה X תחוש מאוימת ממצבה הגיאופוליטי המשתנה, היא עשויה לרצות לרמוז לשכנותיה שיהיו השלכות למתקפה עליה. היא גם עשויה לנסות להוציא לפועל "תגובה בעוצמה זהה" שאינה מושלמת, בכך שתשים את הדגש על האיום האמין והקביל ביותר שיש לה – איום שאינו בתחום הסייבר אלא בתחום הקינטי, כמו הפגנת כוח אווירית או קרקעית. אם הייחוס לא יהיה ודאי, יהיו לכך השלכות דיפלומטיות נגדיות שיחזרו כמו בומרנג במקרה שמתקפות הסייבר יימשכו, וסופן שיעלו את הסיכון לפגיעה באמינותה של מדינה X (לאור העובדה שחשפה את היכולות הקונבנציונאליות שלה). מצד שני, אם מתקפות הסייבר לא גבו מחיר גבוה מדי, ומקורן נותר מעורפל, אזי ייתכן שמדינה X תרצה להפיג את המתח ולהפחית את הסיכון, ואז תוכל לייחס את הקשיים שנוצרו לבעיות טכניות או לגורמים שאינם מדינתיים. מדינה X תוכל אז להסכים לקבל סיוע ממדינה B דרך חברת אבטחת התוכנה שלה. כמובן שיהיה לכך מחיר, כפי שכבר צוין קודם לכן.

אסטרטגיה ראשונה של "צמצום מידע אסימטרי": הבהרת שאלת הסף בעזרת תהליך ומסגרת להערכת מתקפות סייבר

מסגרת ההערכה

למדינה X יכולה להיות דרך פעולה טובה יותר. כדי לתכנן את התגובה הטובה ביותר, עליה להבין אילו סוגי מתקפות עומדים בפניה. במיוחד עליה לפתור שתי בעיות שכבר הוזכרו: ייחוס וסף. הייחוס חייב להיות מקושר בצורה ישירה יותר לסוגיית "ההכחשה הסבירה" (plausible deniability), שכן מה שמוטל בכף הן ההשלכות הפוליטיות והדיפלומטיות של היעדר ייחוס. הגדרת הסף היא בעיה מורכבת אפילו יותר: ישנו קושי מובנה בהגדרה של "סף פשוט וניתן לזיהוי" במתקפות סייבר.[8] פעולות המתקרבות אל הסף ניתן לחלק לשתיים: כאלו שיש להן השפעה ישירה על המדינה (כמו שיבוש של ענף תעשייה ואובדן חיים), והכנות צבאיות (כמו תזוזת צבא ופעולות איסוף מידע) הקודמות לפעולות אלו שיש להן השפעה ישירה.

האם הצבת מלכודות לוגיות ברשת האלקטרונית של היריב מהווה פעולת מלחמה? האם יש מקבילה בלוחמת סייבר לתזוזת צבאות וריכוזם על הגבול? לשאלות אלו אין מענה פשוט, במיוחד משום שהן מתייחסות לנושאים כמו סוגיית הסף לפעולת תגמול על פי "עקומת האמינות"[9].

"מדריך טאלין" הוא נקודת מוצא לתשובות לשאלות אלו, אולם נכון להיום אינו מציע מענה מוסמך להן.[10] מבחינה כללית והיסטורית, אלו הן סוגיות המצויות בליבת ההתנהלות האסטרטגית של מדינות, שנענות כל אחת לגופה מתוך ראיית המציאות, אולם מבלי שגובש להן מענה רשמי ומקיף. אסטרטגיית הסייבר מחייבת מאמץ נוסף להמשגת התשובה. למרות שיהיה בכך משום חריגה ממסגרתו של מאמר זה, ניתן לציין בו כמה מראי דרך ראשוניים.

נקודת המוצא, המוזכרת בספרות העוסקת בלימודי לוחמת הסייבר וכן ב"מדריך טאלין", היא ההשפעה הישירה.[11] זוהי גישה שצבאות רבים בעולם יכולים להבין, החל מחיל האוויר של ארצות הברית, שהוא עדיין חסיד של מבצעים מבוססי־תוצאה המקשרים בין פעולות, תוצאות ויעדים.[12] כפי שמודגש ב"מדריך טאלין", לגישה כזאת יש גם תקדימים משפטיים, במיוחד סביב המונח "היקף ותוצאות".[13] יחד עם זאת, נותרת בעינה השאלה אילו תוצאות פירושן חציית קו אדום מבחינת הצד המתגונן? קל יותר להתחיל מִמה שנתפס כקביל או כנסבל, ולאחר מכן להבהיר מה לא יהיה קביל לעולם ויגרור תגובה צבאית אוטומטית, כאשר בין שני אלה שוכן השטח האפור של המשברים.

לדוגמה, ריגול הוא בגדר הנסבל (אם כי לא רשמית). הוא נהנה מסובלנות בין־לאומית, מכיוון שהוא "שלוחה של משטרים המקיימים פיקוח", דבר שמאפשר

שיתוף פעולה פונקציונלי.[14] דומה שחלק מסובלנות זו התפשט גם לכמה מ"יישומי הסייבר" של הריגול.[15]

מה שלא יהיה קביל לחלוטין ואף יצית תגובה צבאית אוטומטית, הוא מספר גבוה של קורבנות בקרב אוכלוסייה שאינה לוחמת. מקרה כזה יתורגם ככלל להפרה של דיני העימות החמוש בנוגע ל־*jus ad bellum* (צדקת המלחמה), כפי שנוסחו באמנת ז'נבה משנת 1949 ואושררו ב"מדריך טאלין".[16] מה שלא יהיה קביל לחלוטין מבחינה אסטרטגית, וייחשב כמלחמה, גם הוא ברור ממבט ראשון: הרס חלקי או מלא של מקומות מקלט (sanctuary). הדבר מתייחס גם לכל ניסיון משמעותי לפגוע בצורה הרסנית במוסדות המגנים על מקומות אלה. מכיוון שהמדינה מחזיקה במונופול על הפעלת אלימות בקנה מידה רחב,[17] פירוש הדבר הוא להגן הן על היכולת לממש אלימות בהיקף גדול והן על מרכז קבלת ההחלטות המפקח על השימוש באלימות. במונחים מעשיים, הגנה על מקום מקלט פירושו, בראש ובראשונה, הגנה על חיי האזרחים. מלחמה הופכת לבלתי נמנעת כאשר אומה סופגת אבידות כבדות.

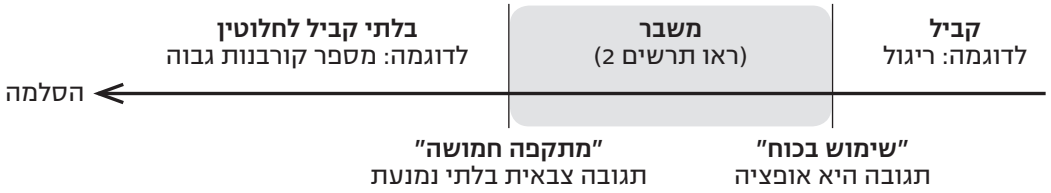
כשמדובר בהפעלת אלימות בקנה מידה גדול, ישנן כמה סוגי יכולות ומערכות שאין לפגוע בהן: בראש ובראשונה יכולת המכה השנייה של המדינה, אולם גם מערכות אחרות שכל תפקוד כושל שלהן עשוי לפגוע באופן משמעותי ביכולת להגן על מקומות המקלט. באלו נכללים מערכות התקשורת ברשת והחיישנים הספציפיים הדרושים להפעלת מערכות אלו, וכן מערכות תקשורת פנים־ממשלתיות החיוניות לראש המדינה ולצוותו לצורך פיקוד ושליטה ולשם תקשורת בין ראשי מדינות. תנאים אלה זכו להסכמת שתי המעצמות הגדולות במהלך המלחמה הקרה. ההסכם לאמצעים שיש לנקוט בעת תאונות (Accident Measures Agreement) וההסכם למודרניזציה של "הקו החם" (Hotline Modernization Agreement) משנת 1971 הגנו על תקשורת לוויינית החיונית להעברת מסרים בין ארצות הברית לברית המועצות בעתות משבר, כמו גם על מתקני התקשורת למערכות התרעה נגד טילים.[18]

ניסיונות לפעול נגד כוחות חירום ונגד אמצעים רפואיים שנועדו להגביל את מספר האבידות מהווים גם הם קו אדום. סוגיה זו זכתה להסכמתם של דיפלומטים רוסיים ואמריקאיים ב־2011 ונכללה גם ב"מדריך טאלין", וזאת במטרה להחיל את החוקים הקיימים של דיני העימות החמוש על ההתנהלות בתחום הסייבר.[19] המדובר באמצעים ובמערכות תקשורת לפיקוד ושליטה של כוחות חירום ורפואה, וכן לתקשורת עם ראש המדינה. חשוב לציין עוד שהגנה על מערכות התקשורת פירושה גם הגנה על נתונים מפני השחתה: אם לא ניתן להגן על הנתונים, המשמעות המעשית היא חבלה במערכות התקשורת המשמשות להעברת הוראות.

כאשר מדובר בהגנה כלכלית על מקום המקלט, יש לשאול את השאלה: באיזה שלב הופך הנזק הכלכלי לחמור כל כך, עד שמלחמה היא בלתי נמנעת? לפי ספרות מדע המדינה, קשיים כלכליים יכולים להביא לשינוי פוליטי: מיתון יכול להוביל להחלפת מפלגת השלטון במדינות דמוקרטיות,[20] ותקופות שפל יכולות להביא לשינוי משטר דרך עליית תנועות קיצוניות, כפי שאירע בתקופה שבין שתי מלחמות העולם.[21] אם תסיסה כלכלית כזו מקורה בחבלת סייבר, היא מהווה "פעולה כופה" שנועדה להרוס את שלמותה של המדינה.[22] תוצאה "פוליטית" זו עשויה להצטרף להגבלת משאבים שתוטל על צבאה של אותה מדינה כתוצאה מהקשיים הכלכליים. צמצום משמעותי במוכנות הצבאית הוא נקודת סף בפני עצמה. תרחישים אחרים עשויים להיות מניפולציה ישירה על מנגנוני הפיקוח הפוליטיים של המדינה (למשל, השחתה של מערכות הצבעה אלקטרוניות וסחיטה אלקטרונית המונית של נבחרי ציבור). אם רוב פוליטי יכול ליפול בעקבות חבלת סייבר, דינה של חבלה כזו הוא כדין ניסיון משמעותי לפגיעה בשלמות המדינה, ולכן כדין חציית קו אדום. אלו הן פעולות הפוגעות בצורה כה חמורה, עד שניתן לסווגן בקלות כ"בלתי קבילות לחלוטין". מתקפות שגורמות לתוצאות כאלו נחשבות ב"מדריך טאלין" ל"מתקפות חמושות".[23] בנקודת סף זאת, תגובה צבאית היא ודאית.

אם זהות התוקף ידועה, זהו חלק מ"שפת האלימות" המקובלת בין מדינות, וניתן להחיל עליה את כלליה של "שפה" זו. המדינות ייכנסו אז למשחק הסלמה – מתגובה קונבנציונלית ועד תגמול בעל פוטנציאל אסטרטגי. נשק הסייבר יהפוך אז לנשק נלווה לשאר מערכות הנשק,[24] אף שמדינות יכולות להגיב בעוצמה זהה עם נשק שאינו סייבר. הדבר יוסיף ממד של הבהרה ודגש לשיח זה. (ראו תרשים 1)

תרשים 1: מסגרת לקבלת החלטות בעלת סובלנות להשפעות



אם התוצאות ניתנות לזיהוי ומשפיעות על נכסים או על אוכלוסייה אזרחית, ואם זהות התוקף ידועה, אזי ניתן להגדיר את הפעולה כטרור. האקרים המאפשרים מתקפות כאלו, ללא ייחוס לאומי הניתן לזיהוי, פועלים כ"לוחמים בלתי חוקיים"[25] או כ"לוחמים חסרי זכויות".[26] הם אזרחים המעורבים ישירות בעימות חמוש, תוך הפרה של דיני המלחמה. מכיוון שלא ניתן לקשר אותם למדינה המחויבת לאמנת ז'נבה, ברגע שהמתקפה שלהם גורמת לנזק "בלתי קביל לחלוטין", הם מאיימים למעשה על כל המטרות האזרחיות. התגובה למתקפת טרור כזו חייבת להוביל

למאסר ההאקרים, או לכל הפחות להענשת המדינה המארחת אותם. זאת, בהתאם לתקדים המשפטי שנקבע בעקבות המתקפה על אפגניסטן לאחר אירועי 11 בספטמבר 2001, ובמיוחד לאור החלטות 1368 ו־1372 של מועצת הביטחון של האו"ם מ־2001.[27] כמו במקרה של טרור גרעיני הנעדר ייחוס, גם כאן, איסוף מודיעין הוא המפתח לפעולת תגמול.[28]

בין ה"קביל" ל"בלתי קביל לחלוטין" משתרע שטח אפור של משברים. הנזק במקרים הנכללים בשטח זה ברור דיו כדי שאותם מקרים יוגדרו כ"שימוש בכוח", אך עוצמתו אינה חמורה מספיק כדי להגדיר אותו בוודאות כ"מתקפה חמושה".[29] כפי שמציין בית המשפט הבין־לאומי לצדק, המצוטט ב"מדריך טאלין": "[...] לא כל שימוש בכוח עולה לדרגת מתקפה חמושה".[30] המשבר יכול להישאר נסתר מעיני הציבור – אופציית ברירת מחדל שנועדה למנוע התערבות ידיים רבות מדי בעולם חסר החוקים של מרחב הסייבר – אם כי הוא יהיה עדיין אמיתי. לאי־הוודאות במקרה זה יש סיבות רבות. התוצאות של מקרה "בלתי קביל לחלוטין" אולי טרם התממשו, אולם ניתן להתייחס אליהן כאל ודאיות: אם הבעיות בבנקאות המקוונת מתפשטות ונמשכות מספר שבועות, האם הדבר לא יוביל לפאניקה פיננסית? האם ההתאוששות תהיה פשוטה? כך גם לגבי מקרה של פריצת רֶשת החשמל, אף שביום השני לאירוע יהיה עדיין קשה לומר דברים ברורים.

לא רק שקשה להעריך את התוצאות הישירות, אלא שגם קשה להעריך מה המשמעות של פעולות צבאיות של האויב במרחב הסייבר, קרי של "תזוזת צבאות וירטואלית". זוהי נקודה קריטית, מכיוון שעל פי כללי המלחמה, כפי שנוסחו לראשונה על ידי סאן צו, ההפתעה היא המפתח לניצחון:[31] הלוחם הטוב יותר הוא זה שאינו יוצר דפוסים קבועים או תקדימים, ושצעדיו קשים לניבוי.

חובה להתמודד עם מצב זה של "שטח אפור" ולמפות אותו. ניתן להיעזר לצורך זה בקטגוריות ההסלמה שתיאר הרמן קאהן בספרו *On Escalation*.[32] מהי עוצמת המתקפה, מבחינת הסבירות שהיא תגיע לדרגה של "בלתי קבילה לחלוטין"? כמה מרכיבים שונים של המדינה כמערכת מותקפים? מהם ההתפתחות והקצב של המתקפה, במיוחד לאור העובדה שהאצה חדה בהם עלולה להיות סימן לפעולות צבאיות פיזיות העומדות על הפרק? הסיווג שמציע הרמן קאהן מאפשר לעשות הבחנה פשוטה בין:

1. מה שאינו קביל, אולם מבטא ריסון עצמי בהסלמה: המתקפה מוגבלת בעוצמתה ולא ניתן להגדירה כמאיימת על מי שאינם לוחמים. היא מוגבלת בהיקפה בכך שרק סוג אחד של מטרות מותקף; היא מוגבלת בממד הזמן שלה בכך שהתרחשה רק פעם אחת או פעמים ספורות בלבד, או שיש לה "תאריך תפוגה". מתקפות כאלו ניתן לסווג כמתקפות "מוגבלות".

2. מה שאינו קביל וניתן להגדירו כבעל פוטנציאל להסלמה: העוצמה או ההיקף של המתקפה נראים כנטולי ריסון עצמי ועלולים להסלים, או שיש חזרה והאצה שלהם לאורך זמן, ללא תאריך סיום ברור. מתקפות כאלו ניתן לסווג כמתקפות "מסלימות".

לדוגמה, אם GlobalWorm היה מכוון במודע לשנות את התפקוד של תוכנה או של ציוד ספציפיים בלבד, או אם התוכנה או הציוד שנפגעו מ־GlobalWorm היו רק לשימוש צבאי או לשימוש כפול, ולא הייתה זליגה למערכות נשק אחרות או לתשתית אזרחית, או אם השינוי שחל לא הוביל לנזק נלווה משמעותי בקרב כוח אדם אזרחי או בחיי אזרחים, או אם ל־GlobalWorm היה תאריך תפוגה ידוע (לדוגמה, כתוצאה מאישורים דיגיטליים שהגנו עליו ואשר נועדו לפוג במועד מסוים), אזי מתקפת GlobalWorm נגד מדינה X הייתה מוגדרת כמתקפה "מוגבלת". אולם נראה שאין זה כך במקרה של מדינה X: תוצאות המתקפה עליה אינן מוגבלות לציוד מסוים אלא הולכות ומסלימות, וכמו כן קשה לזהות מה יהיו ההשלכות המשניות שלה, למשל של היעדר פעילות בנקאית מקוונת במשך 48 שעות.

כדי לפשט את העניין, ניתן לצרף יחדיו תוצאות "מזוהות"[33] (שניתן לזהותן ולהבין היטב את כל ההשלכות המיידיות שלהן) אך "מסלימות", עם תוצאות שהן "קשות לזיהוי" (שלא ניתן להבין באופן מלא מה יהיו כל ההשלכות המיידיות שלהן). שני סוגי התוצאות מציגים סיכון גבוה להפתעה, לשיפוט שגוי ולהסלמה, כמפורט בתרשים 2.

תרשים 2 – מסגרת החלטות ל"משברים"

		אפיון התוצאות	
		מזוהות ומוגבלות	קשות לזיהוי / מזוהות ומסלימות
אפיון הזהות	ידוע	מִבצעים מיוחדים/ מכה מוגבלת. יריית אזהרה.	מתקפות נגד מערכות נשק טקטי. מתקפות בעצימות נמוכה נגד אזרחים.
	לא ידוע	מבצעים חשאיים. פעולת ריגול (שלא נחשפה).	מתקפת חבלה. טרור בעצימות נמוכה. פעולת איסוף מידע.

תהליך ההערכה

הקטגוריה של תוצאות "קשות לזיהוי" הינה בעייתית במיוחד. קשה להשיג דרגה מספיקה של חיזוי לתוצאות אלו: לא מדובר בנזקים "סבירים לחיזוי", אם להשתמש בביטוי שמופיע ב"מדריך טאלין";[34] לא די בהסתמכות על צפייה בתוצאות, מקיפה ככל שתהיה, תוך התמקדות במודיעין, או בניתוח צורת הפעולה של התוכנה הזדונית בסביבת התוכנה שלה; גם לא ניתן להגיע, בעזרת צעדים חיוניים אך בלתי מספקים אלה, להערכת ההשלכות על "מדינה הנתפסת כמערכת" – אם להשתמש במונחים של קולונל ג'ון וורדן.[35] הערכה כזו היא תוצאה של בניית מודלים, הדמיה וניתוח מערכות, כולל רכיבים חברתיים וכלכליים. המטרה של ניתוח כזה היא להעריך את הנזק הפוליטי הצפוי למדינה המותקפת. בהקשר הגנתי, הצעד הבא יוביל באופן טבעי לניתוח, באמצעות תהליך של הִנדוס לאחור, של "מבצעים מבוססי תוצאה". המטרה היא לא להשיג את הדיוק הדרוש לשימוש התקפי ב"מבצעים מבוססי תוצאה", שהיה קשה למדי להשגה עד היום, עם כלי התוכנה הנוכחיים;[36] המטרה היא להטמיע, כחלק מהשימוש ההגנתי, צורה של לוחמת סייבר שנקודת הסף שלה מוכרת מבחינה בין־לאומית ושתקשר את פעולות הסייבר עם יעדים רצויים ועם תוצאות ישירות. הדבר גם ישמש למתַן תוקף חוקי לכל סוגי התגובות, לרבות פעולות קינטיות או דיפלומטיות. או אז, הקטגוריה של "פשוט, בולט וניתן לזיהוי" תהפוך לקטגוריה של "מדויק ביותר".

כדי שאפשר יהיה לתת אמון בצורת לוחמה זו, חיוני שמעצמות הסייבר המובילות יצהירו עליה. השתתפות מדינות נוספות בגיבושה, על פי אותו הגיון מרכזי משותף, תבטיח שהיא גם תוכר על ידי גורמים רבים, ובאופן כזה גם תהפוך לשיטה הבולטת והמקובלת. כדי להיות גם אמינה, יהיה עליה לשקף את ההשפעה האמיתית שיש לה על עקומת האמינות של המדינה. לשם כך, יהיה צורך לפעול על פי המתווה של קולונל ג'ון וורדן ולפתח מסלול של מחקר והדמיות, שמטרתו להבין את מהותה של "המדינה המרושתת כמערכת". במסגרת זו ניתן יהיה לבחון ב"טווחי סייבר" וירטואליים לא רק את האינטרנט, אלא גם רכיבי משנה של המדינה.

ארגונים ומערכות תשתית שונים לוקחים כיום חלק בהפצת "נתוני ענק" (big data) – החל מפרויקטים של נתונים פתוחים במגזרים ציבוריים, דרך ממשקיAPI בתהליכים פנימיים של תאגידים ותעשיות,[37] וכלה בשימוש חברתי ופוליטי, כפי שהוא מתבטא ברשתות חברתיות. כל אלה מסייעים בפיתוח מודל בסיסי משופר ומדויק יותר של "המדינה המרושתת כמערכת". מודלים דינמיים אלה של מידע יכולים להיבדק אז מול הדמיות של מקרי אלימות. במקרה זה, הדייקנות פחות חשובה מאשר הערכות אמינות ומוסכמות. התפתחות זאת תהיה כרוכה במאמץ מתמשך, שכן מרחב הסייבר מתפתח ללא הרף.

הבנה של נקודת הסף אינה פותרת את הבעיה המרכזית השנייה בתחום המידע, והיא שאלת הייחוס. בעיה זו מחייבת מאמץ ייחודי המעֵבר מודיעין, כפייה ודיפלומטיה.

אסטרטגיה שנייה של "צמצום מידע אסימטרי": הבהרת שאלת הייחוס בעזרת "כפייה משותפת"

מכיוון שמרחב הסייבר נשען על שלושה יסודות – חומרה, תוכנה,[38] ו"תודעת רשת" (brainware) – על המודיעין לחקור ולפתח השערות לגבי כל אחד משלושת היסודות האלה. מערך הייחוס צריך להיות מורכב מאוסף של סימנים אופייניים שונים, כמו דפוסי תעבורת IP, סגנונות קידוד ושיטות פעולה. יש לכלול גם מודיעין אנושי "קלאסי" על ההאקרים עצמם ועל נותני החסות הפוליטיים שלהם. פעולות חקירה אלו צריכות להשתמש בשיטות העבודה הטובות ביותר בתחום ליבון הנתונים, תוך שימת דגש על שיטות דדוקטיביות המיושמות במודיעין, כפי שמציע יצחק בן־ישראל.[39] לפי אחת המתודולוגיות של עבודת המודיעין,[40] השערות ייחוס יכולות להיות מוצגות בקבוצות שונות (כגון, "השערה 1: מדינה Y היא התוקפת"; "השערה 2: מדינה Z היא התוקפת"). לאחר מכן ניתן להעמיד נתונים אמפיריים המפריכים כל השערה בכל קבוצה. צבירת נתונים מול השערת הייחוס תהיה השלב הראשון בניסיון לענות על השאלה איזו מדינה היא החשודה העיקרית בתקיפה.[41] הדבר יחייב לזהות מראש את המודלים הרבים של ההכנות הדרושות לפתיחה במתקפת סייבר מאסיבית על ידי מדינה כלשהי ולעשות הדמיה שלהם. מודלים אלה יכללו, כמובן, גם מאמצים נוספים להסתרה ולהקשחת ההגנה. במצב אידיאלי ניתן יהיה לערוך בשלב זה מבחני דדוקציה A/B, בצורה של ניסויים מבוקרים ב"נאשמים" אפשריים, כדי לאשר או להפריך השערות ייחוס. לדוגמה, ניתן לעשות שימוש באחת מהאסטרטגיות ששימשו את הדמות הבדיונית ג'ורג' סמיילי: הדמיה של השפעות בלתי צפויות של תוכנה זדונית עשויה לחשוף את מקורה האמיתי, וזאת בשל חוסר נוחות ומבוכה פתאומיים שהיא גורמת.[42] איתור חוסר נוחות כזה יכול לסייע לקביעת הייחוס.

חתירה אל האמת היא קריטית ליצירת הגנה וחיונית לשכנוע בעלות ברית שאין כוונה לתמרן אותן. אם מדינות אלו ישוכנעו בכנות הדברים, הן יוכלו להיות "עדי אופי" בפני דעת הקהל העולמית ולספק קונצנזוס דיפלומטי רחב יותר לאופציות התגמול. חתירה אל האמת גם תבטיח שהדרג הפוליטי של המדינה המתגוננת לא יטעה טעות חמורה בייחוס המתקפה, ושלממשלתה יהיה ביטחון מלא בהחלטותיה. בשלב זה תימצא הממשלה במקום נוח יותר לבחון אמצעים לא פומביים ולא מענישים, אם אלה הם אכן האמצעים הנדרשים. כמו בכל עבודת

ריגול נגדי, ייתכן שטוב יותר לשמור לזמן מה את האויב באשליה שתחבולותיו טרם נחשפו.

במרחב הסייבר, כמו בכל תחום מידע אחר דוגמת המודיעין ה"מסורתי",[43] אמת היא כוח. האמצעים והשיטות לביסוס אמת שלכאורה אינה ניתנת להפרכה הם המפתח לכוח, ולכן המפתח להשפעה. יבוא יום שזירת הדיפלומטיה בסייבר תִדמה לזירת האינטרנט האזרחי הרגיל, שבו כמה ממנועי החיפוש הגדולים ביותר או ספקי תוכן (כמו ויקיפדיה) מתחרים על מקומם כבעלי הרלוונטיות הגבוהה ביותר. היכולת להפריד ולבודד את האות הנכון היא התכונה החשובה ביותר של כל מערכת מידע.

מן הסתם, קשה לשתף מספר רב של מדינות בנתונים ובטכניקות של קביעת הייחוס שצוינו לעיל, כפי שמקובל לרוב בשיתוף פעולה מודיעיני. בעולם ההופך בהדרגה לרב־קוטבי, אם לא תימצא דרך לטפל בהבהרת סוגיית הייחוס או לנהל אותה במשותף, הדבר עשוי להוביל לשיתוק יכולת ההגנה או לחילופין לירידה באמינות ההרתעה. ייתכן שניתן למצוא שיטה כזו באמצעות מבחן דדוקטיבי רחב היקף ופומבי, במיוחד לאור העובדה שדדוקציה היא שיטה מעולה להבהרת האמת בניתוחים מודיעיניים.[44]

ריצ'רד קלארק ורוברט נֶייק מדגישים בספרם *Cyberwar* את "עקרון ה־רֶסְנִיסְט": נטל החקירה צריך להיות מועבר מהחוקרים אל המדינה שממנה שוגרה המתקפה.[45] אם המדינה החשודה תסרב לשתף פעולה, היא תיחשב לאחראית. במקרה כזה, גוף בין־לאומי, שקלארק ונייק מכנים "צוות בין־לאומי לציות וזיהוי פלילי בסייבר", יהיה רשאי להציע סנקציות סייבר, החל מהשבתת ספקי שירותי אינטרנט מסוימים ועד חסימת אותה מדינה בפני מרחב הסייבר.[46] הישענות על גישה זו והרחבתה מאפשרות לטפל באופן ממשי בכמה מקרים של לוחמת סייבר, שהם בעלי פוטנציאל להיות חמורים במיוחד, ולשקם מחדש את הרתעת הסייבר. בנוסף לקביעת עצם הייחוס באמצעות "עקרון הארסניסט", גישה כזו יכולה לייחס מעשית את המתקפה לתוקף מסוים. במונחים דיפלומטיים, היא יכולה למנוע מהתוקף את השימוש ב"הכחשה סבירה". ביסוס הייחוס הוא חקירה מודיעינית לא פחות משהוא תהליך דיפלומטי, שבֵּן יש לפעול לשכנע בו מדינות נוספות.

אמינותה של האמת מושגת טוב יותר כאשר משקיפים (או בוחנים) חיצוניים מאשרים את השערת הייחוס. תהליך חברתי זה קיים מאז "כלל שני העדים" במשפטי בגידה בימי אנגליה האליזבתנית,[47] דרך הכלל של הופר בנוגע ל"עדות בו־זמנית",[48] ועד לשיטות הסטטיסטיקה המודרניות, שבהן עולה הביטחון בתחזיות ככל שגדֵל מספר התצפיות. מבחן ברמה הציבורית מחייב שמדינות ותושביהן יהפכו לתצפיתנים.

תהליך דיפלומטי יבטיח תיאום טוב יותר, ולכן יחזק את מצור הסייבר שיש להטיל כדי ללחוץ על מדינות חשודות. חוזק המצור חיוני כדי שהאיום יהיה אמין. אם ניתן יהיה להתגבר עליו, כפי שמעצמות המערב הצליחו לעשות במהלך משבר ברלין ב־1948 כנגד המצור שהטילה ברית המועצות על העיר, אזי המדינה המאיימת תיכשל במאמציה[49]. אם לא ניתן יהיה להתגבר על המצור, אזי המדינה המאוימת תיאלץ לבחור בין הסלמה ובין נסיגה, וכאשר הסיכון לעצמה יהיה גבוה מדי, יש סיכוי סביר שהיא תבחר לסגת, כפי שברית המועצות עשתה במהלך משבר הטילים בקובה ב־1962. בנוסף לכך, קידום תהליך הייחוס – תחילה עם ידידות קרובות ולאחר מכן עם קבוצה גדולה יותר של מדינות – יוביל ליצירת רצון טוב, להתקרבות וליתר הבנה כלפי המדינה המתגוננת. מצב זה נותן למדינה המתגוננת שוליים פוליטיים לתמרון, אם תבקש לפעול להטלת סנקציות דיפלומטיות, כלכליות או צבאיות נוספות מעבר למרחב הסייבר ולמצור הסייבר. הדבר יתרום לאמינות נוספת לְמה שביסודה היא אסטרטגיה כופה, או כפי שתיאר זאת שֶלינג: "איום המיועד להניע את האויב לפעולה כלשהי".[50] מדינות חשודות ייאלצו לשתף פעולה, אחרת הן ימשיכו לסבול לא רק ממצור הסייבר, אלא גם מבידוד. מדינות שיהיו מעוניינות להוכיח את רצונן הטוב יעדיפו לשתף פעולה ולו כביכול, ואולי אפילו יחלקו את המודיעין שלהן הנוגע לסוגיית הייחוס, כמחווה נוספת של רצון טוב. מדינות שלא ישתפו פעולה יַחשפו בכך את כוונותיהן האמיתיות.

קל יותר לכפות שיתוף פעולה אם המדינות המעורבות לא צריכות להתבזות. ניתן להשתמש באבטחת סייבר במודל לבריאות הציבור של רָטְרֵי והִילי ובמטאפורה של צוותי החקירה של ארגון הבריאות העולמי (WHO) הפועלים בעת מגפות:[51] ממשלות אינן חייבות להיות מואשמות ישירות, שכן הן אינן האחראיות למגפה; במקרה שלנו האשמה מוסטת אל עבר התוכנה הזדונית או אל עבר ההאקרים הזדוניים שמאחוריה. ניתן לנצל את העובדה של היעדר ייחוס ברור של המתקפה למדינה מסוימת, כדי לאפשר לקואליציה של המדינות המתגוננות לבקש את שיתוף הפעולה של המדינות החשודות. כשם שאזורים שלמים מוכנסים להסגר בעת מגפות, כך יכולה להתבצע גם חסימת הסייבר. במצב זה, המחיר של אי־שיתוף פעולה יוטל על הצד התוקף, ומחיר זה יעלה ככל שמדינות אחרות ישתפו פעולה והמדינה התוקפת תידחק לבידוד הולך וגובר. מנגד, מחיר שיתוף הפעולה מצד המדינה התוקפת יהיה נמוך יותר, שכן הוא לא יהיה כרוך באובדן כבוד, גם אם הוא יכלול עדיין איום ממשי – עצם המחיר שהתוקפן אמור לשלם על ביצוע הפעולה: חשיפה ונטרול של יכולות התקיפה שלו (שרתים, קודים, האקרים) כאשר יחליט לבסוף לשתף פעולה. שיתוף פעולה מתמשך מצד המדינה התוקפת, והמודיעין הנוסף שיתלווה אליו, יסייעו לשמר מצב זה.

מדינות שהתחמקו משיתוף פעולה ייאלצו לחזור ולשתף פעולה, וההשקעה שלהן ביכולות ההתחמקות תרד לטמיון. עם זאת, שיתוף הפעולה שלהן לא יהיה כרוך בהכרח בנזק לעצמן בדעת הקהל – דבר ההופך את "החזרה לשיתוף פעולה" לאפשרות סבירה, ולפיכך לבעלת פוטנציאל להשגת יציבות. במצב כזה, המשימה הקשה של ייחוס פומבי ורשמי של המתקפה לגורם ספציפי – דבר המחייב רמת ודאות גבוהה מאד – הופכת למיותרת.

אסטרטגיות ותנאים לכפייה משותפת

כדי שאסטרטגיה זו תצליח, עליה למנף את המאמצים להגיע לייחוס המתקפה. איכות המודיעין היא קריטית למימושה של גישת כפייה זו. ראשי המדינות נמצאים בלב העימות האסטרטגי. דרך התנהלותם ואופן העברת המסרים המאיימים ישפיעו על אמינות פעולת התגמול שלהם. ראש המדינה המתגוננת, בסיוע קואליציה של מדינות ידידותיות, כמוהו כחוקר משטרה המטיח בפני החשודים: "תנו לנו גישה למידע, שתפו עמנו פעולה, או שנשאיר אתכם במעצר". מדובר במיקוח, בדיוק כפי שנעשה בעבודת המשטרה.[52] ככל שהמודיעין טוב יותר, כך תכנון החקירה והתהליך יהיו יעילים יותר: "המידע עשוי להיות מקור הכוח החשוב ביותר" בחקירות.[53] כשנעשה בו שימוש בתהליך החקירה, הוא ממחיש את ההתמצאות הרבה של החוקר. בכך הוא מבסס את אמינותו ואת העובדה שלא ניתן להוליך אותו שולל, והנחקר יהסס למסור לו מידע שגוי. במקביל, החוקר מוכיח שהוא יכול להיות בן־שיח בעל ידע. עסקת שיתוף פעולה תהיה, במקרה זה, עסקה יציבה.

במקרה שלנו, "החוקר" יכול ליזום מבחנים כדי לבדוק באמצעותם את תגובת המדינות החשודות. מבחנים כאלה יכולים לעשות הדמיה של תוצאות בלתי צפויות למדינה המתגוננת. המדינה המתגוננת, מצדה, יכולה לזרוע ספק במדינה התוקפת באמצעות מניפולציה נגדית, המשדרת למדינה התוקפת מסר, לפיו נשק הסייבר אינו כלי אמין ועלול לגרום להסלמה לא רצויה לתוקף.

המדינה המתגוננת יכולה לזכות ביתר קלות באהדה ובתמיכה חיצוניות ככל שהתוכנה הזדונית פוגעת באינטרסים פנימיים חיוניים שלה. הסולידריות שיפגינו כלפיה מדינות אחרות תעמיק ככל שמקורה של התוכנה הזדונית לא יהיה מזוהה, כך שכל מדינה עלולה להפוך ליעד למתקפה שלה. התהליך הדיפלומטי שילווה את הכפייה יסייע בהפניית המתקפה של התוקף כלפי עצמו, כפי שקורה בג'ודו. ככל שמתקפת הסייבר חמורה יותר, כך תתחזק הסולידריות בין המדינה המתגוננת ובין ידידותיה ויתהדק מצור הסייבר על המדינות החשודות. באופן כזה, היוזמה תעבור לידיו של המתגונן, והוא אף יוכל לשלוט בקצב ההסלמה.

אסטרטגיית כפייה זו לפתרון בעיית הייחוס היא בת־ביצוע, שכן מאחורי כל מתקפה מתוחכמת חייבת לעמוד מדינת לאום, ומאחורי כל מתקפה של גורמים

לא מדינתיים עומדת בהכרח מדינה מפותחת. לארגוני טרור הממוקמים ב"מדינות כושלות" אין כרגע יכולת טכנית ליזום מתקפות סייבר מתוחכמות ואסטרטגיות. לדוגמה, "סטוקסנט" היה קוד שנכתב על ידי מהנדסי IT מוכשרים ביותר. הוא עשה שימוש באישורים דיגיטליים שנגנבו משתי חברות טיוואניות חוקיות,[54] ונבדק על מודל סייבר מלא, שכָּלל הדמיות של צנטריפוגות P-1.[55] כל אלה מחייבים מימון רב לגיוס ולשימור המומחים, גישה ממשית למאגר מומחים רב־תחומיים (במיוחד אם יש צורך במודלים של סייבר), וכן השקעה קבועה בהכשרה ובפיתוח, שֶּׁאין מרחב הסייבר משתדרג ללא הפסקה. אין גם לשכוח בהקשר זה את הצורך בשירותים חשאיים שיחדרו לתוכנות חסויות או ישיגו גישה אליהן. מדובר ביכולות שנכון להיום אינן מצויות באזורים לא מפותחים של העולם.

כאמור, מאחורי כל ארגון אד־הוק הפותח במתקפת סייבר מתוחכמת ניצבת מדינת חסות מפותחת ומתקדמת. מדינות מתקדמות תלויות יותר מתמיד במרחב הסייבר לצורך גישה לנתונים, פיתוחם ועיבודם. חלק גדול מהתקשורת העסקית ועיבוד הנתונים עובר ל"ענן", כלומר לשרתים הממוקמים לרוב במדינות זרות. לאור זאת, ההשפעה המשתקת שיש לחסימת הסייבר עשויה להיות חריפה במיוחד במדינות מפותחות.

אסטרטגיית הכפייה המשותפת תפעל אם בעלות בריתה של המדינה המתגוננת ייאלצו או יומרצו גם הן לפעול. יש ליצור תיאום מתמשך, הסכמה על נורמות ושיתוף תהליכים כתנאים מוקדמים לכך, עוד לפני פרוץ המשבר. רמות שיתוף הפעולה יהיו פועל יוצא של מעגלי הקִרבה בין המדינות משתפות הפעולה – מהידידות הקרובות ביותר ועד לרחוקות ביותר – כך שמרחב הסייבר ישקף את מערכת היחסים והסכמי שיתוף הפעולה הקיימים ביניהן זה מכבר.[56] בנוסף, כדי להוסיף אמינות לתהליך, ניתן להגביר את שיתוף הפעולה בתוך המעגלים ובין מעגלים סמוכים. התוויית הכיוון הצפוי חשובה כדי לגבש שיתוף פעולה בין־לאומי. חשובים עוד יותר הם הקשרים בין הצדדים, שצריכים לקבל תרגום מעשי בשטח. לדוגמה, מדינות ידידותיות יכולות לעשות שימוש בתוכנות הנמצאות בשימוש אצל מדינות ידידותיות אחרות. שימוש משותף באותה תוכנה או באותם תקנים יגביר את הסיכון של המדינה התוקפת להיתקל בתוצאות בלתי צפויות. שימוש כזה גם מעביר מסר חזק שהתקפה על מדינה מסוימת כמוה כהתקפה על כל ידידותיה. שימוש משותף באותה תוכנה במרחב הסייבר עשוי למלא תפקיד דומה לזה שמילא הכוח הצבאי האמריקאי בברלין במהלך המלחמה הקרה[57]: הוא ייצור מעורבות אוטומטית ולא יותיר ספק בכך שתהליך הכפייה מופעל במשותף בידי קואליציה של מדינות ידידות.

על המדינות המתגוננות לייצר יכולות סייבר עודפות כדי שיוכלו לספוג את המכה הראשונה. יכולות מִחשוב ותקשורת עודפות יפחיתו באופן זמני צווארי

בקבוק. ניתן לנטרל באופן חלקי מניפולציה סמנטית בעזרת שמירה של נתונים חיוניים במאגר נתונים "לכתיבה בלבד", וזאת כדי לאפשר שחזור "ערכי אמת" לפני מתקפה.

אמצעי הגנה הם לרוב בלתי מספיקים. כל עוד לא מתמודדים עם נחישותו של האויב ללמוד טכניקות מתקפה חדשות, הוא ימשיך ללמוד ולאמץ כאלו, כשהוא מחקה את דינמיקת האבולוציה של "המַלפה האדומה" הקיימת בטבע.[58] ללא התמודדות כזו לא ניתן להשיג הרתעה. כדי להשיגה יש להתמודד ישירות עם רצון התוקף ללמוד שיטות תקיפה חדשות מבלי לחלוק אותן עם אחרים; כמו כן, יש לקבוע מחיר לאויב על שאיפותיו אלו. בכל מקרה, חיוני שתימצא בידי המותקף יכולת לספוג את המכה הראשונה. מודלים להרתעה קונבנציונלית יוצאים מתוך הנחה שחולשה של המותקף מזמינה מתקפות עליו.[59] במצב של חולשה, מכה ראשונה עלולה להיות כה קשה, עד שלמדינה המותקפת לא יהיה זמן לתגובה ראויה ולגיבוש קואליציה של ידידות.

המצב האידיאלי הוא שתהליך הייחוס ייקבע בעזרת צוות מפקחים בין־לאומי. דבר זה יבטיח את שמירת "הצל הארוך של העתיד":[60] במצב כזה, האמת תצא לאור, סוגיית הייחוס תובהר סופית והתוקף לא יוכל לברוח מאחריות.

לסיכום, ברגע שנקבע הייחוס וניתן לזהות ולהעריך את תוצאות התקיפה במסגרת עקומת האמינות של המדינה המתגוננת, האסימטריה פוסקת לפעול לטובת הצד התוקף. "שפת הפעולה הצבאית" שבה לפעול לטובת הצד המתגונן, שיכול אז לאיים בצורה אמינה בתגמול. לאחר זיהוי ראוי של תוצאות ההתקפה, המתגונן יכול ליזום תגובה הולמת אפילו בעזרת אמצעים שאינם סייבר – דיפלומטיים, כלכליים, קינטיים או אסטרטגיים. יכולת זו מעניקה משקל רב יותר לצד המתגונן, וכל האופציות הופכות אז לזמינות עבורו. איומים בתגובה שאינה בתחום הסייבר יכולים להיות עדיפים, אם יתברר שתגובה כזו היא בלתי פגיעה למתקפות סייבר. יכולת העמידה שלה תהפוך אותה אז לבת מימוש. חריגה מתגובה באמצעות סייבר בלבד מהווה איתות של הצד המתגונן כי ביכולתו לעבור למתקפות שיש להן תוצאות חומריות ממשיות. התוקף ייאלץ אז לבחור בין נסיגה להסלמה, וייקלע למצב קשה, במיוחד כאשר יעמוד מול כפייה רבתי. כאמור, כפי שהיה בעת משבר הטילים בקובה, במצב כזה התוקפן המבקש לחרוג מהסטטוס קוו יעדיף לסגת מאשר להסלים את המצב.

סיכום: לקראת דוקטרינה צבאית ומדינית חדשה לעידן הדיגיטלי

הצורך ליצור שוויון בתוצאות השימוש בנשק הסייבר ובנשק שאינו סייבר, והצורך להחליף את אמצעי התגמול מאמצעי סייבר לכאלה שאינם סייבר, מצביעים

על החשיבות הרבה שיש להגדרה מחודשת של הפעולות הנעשות במסגרת לוחמת הסייבר, יחסית לשאר מערכות הנשק. בהמשך לדברי אדוארד לוטוואק,[61] אסטרטגיית סייבר המתבססת על כוח אחד (one force) עשויה להיות בלתי יעילה, בדומה למה שלוטוואק מכנה בביטול "לא־אסטרטגיה", דהיינו, אסטרטגיה המבוססת על כוח אחד בלבד וטוענת לאוטונומיה אסטרטגית, כמו "אסטרטגיה ימית", "אסטרטגיה אווירית" ו"אסטרטגיה גרעינית".

מרכזי הכובד של אסטרטגיות הלחימה התפתחו תמיד בד בבד עם השינויים הטכנולוגיים באמצעי הלחימה. כך, מרכזי הכובד במלחמה הקרה היו שונים מאלה של מלחמת הבזק של גוּדֶריאן, או של וָאוּבָּאן ומבצרי הענק שלו; האסטרטג ג'וליאן קוֹרְבֶּט קבע ששליטה ימית ניתן להשיג לא על ידי כיבוש שטחים ימיים – שאינם אפשריים בהחזקה – אלא על ידי הבטחת יכולת המעבר בימים.[62] ככל שהעימותים עוברים לעולם הדיגיטלי או אל ה"לוגוס" הדיגיטלי,[63] עתידים להתפתח מרכזי כובד חדשים.

ככל שהקריטיות של המרחב הסמנטי גבוהה יותר מאשר הבסיס הפיזי, פוחתת חשיבותם היחסית של קווי התקשורת המסורתיים: האינטרנט נבנה כדי שאפשר יהיה לשגר מידע גם בהיעדר תשתית פיזית. החשוב מכל הוא לוודא את נתוני האמת – מיהם התוקפים? מה הם תוקפים? – לדעת למי לייחס את המתקפה ולהכיר ולזהות את תוצאותיה. אלה הם מרכַזי כובד קוגניטיביים. במונחים אסטרטגיים, זוהי עליונותו של הידע: להפעיל פיקוח ולגונן על המדינה ועל מערכות המשנה שלה מפני מניפולציות במידע. במילים אחרות, האמת היא הגורם החשוב ביותר בעולם המידע.

חשיבות עולם המידע הדיגיטלי יחסית לשאר המרכיבים של "האומה המרושתת הפועלת כמערכת" עשויה לשנות עדיפויות אסטרטגיות. שינויים נוספים בתעשייה עשויים לשנות עוד את סדר העדיפויות החדש. ככל שהתוכנה ממשיכה "לאכול את העולם",[64] וחשיבותם של נתונים ושל יישומים מבוססי־נתונים עולה, כך שמירה על ה"לוגוס" הדיגיטלי עשויה להפוך לחשובה לא פחות מאשר שמירה על הנכסים הפיזיים. בחלק מהתחומים החיוניים זוהי המציאות כבר כיום: עושר נמדד ועובר ידיים באמצעות ביטים אלקטרוניים המייצגים ערכים כספיים. בעוד שעל פי הגדרתו של לוטוואק, לוחמת סייבר נחשבת ללא־אסטרטגיה, יש אפשרות – קטנה ורחוקה ככל שתהיה – שהאסטרטגיה של ה"לוגוס" הדיגיטלי תהפוך לאוטונומית, כלומר תייצג הן את המטרה והן את האמצעים. מערכות מידע, החל מהדנ"א ועד לשפה המדוברת, חיוניות לניהול כל אורגניזם, כך שעליונותו של ה"לוגוס" הדיגיטלי אינה אמורה להפתיע איש.

תהליך זה מסמן שינוי עמוק בתפקיד המדינה המגֵנה על האומה. המדינה חייבת לשמור על המונופול שיש לה להפעיל אלימות בקנה מידה גדול, אלימות

אותה ניתן להגדיר כהגנה על נכסים פיזיים מפני השחתה באמצעות כוח קינטי. יהיה עליה גם להגן על מהימנות הנתונים שמשמשים את המערכות האסטרטגיות האזרחיות והצבאיות, וברמה גבוהה יותר – לשמר את מהימנותו של המידע האסטרטגי עצמו, וזאת כדי לאפשר המשך המודעות למצב של "אומה הפועלת כמערכת". המדינה תהיה אז קו ההגנה האחרון של האמת.

כל האפשרויות האלו נידונו להתממש בשל התגברות יכולות המחשוב והאחסון של טכנולוגיות המידע. לשם דוגמה, כוח המחשוב של מחשבי העל המובילים עתיד להתחזק פי עשר בשלישית פלופס לפחות במהלך עשר השנים הבאות.[65] לאור העלייה בסדרי הגודל של עוצמת המחשוב, אין לשלול גם שינויים גדולים ביכולת ההדמיה והלמידה של המחשבים.[66] אפשר שהמגבלות הקיימות כיום בניתוחי "מבצעים מבוססי תוצאות" ו"מדינה הפועלת כמערכת" הן זמניות, כמו הקשיים שהיו בזמנם בתחום הבינה המלאכותית: הבינה המלאכותית הוגדרה במשך עשורים כשדה מחקר בעייתי,[67] אך כיום היא נחשבת לתחום מבטיח.[68] לאור זאת, היכולות המתפתחות של ניתוח והדמיה של "מבצעים מבוססי תוצאות" עשויות לגרום לשינויים גם בשיקולים של מעצמות גדולות.

עלייה ביכולת ההדמיה פירושה שיפור יכולת החיזוי: בדרך זו מתאפשר מבט ארוך טווח וצפוי יותר על המתרחש. ככל שהמידע על היכולת ה"אמיתית" של כל צד מדויק יותר, כך פוחת הסיכון למלחמה. גם זָגָארה[69] וגם אקסלרוד[70] מראים, כל אחד בנפרד, שככל שתהליך זה הולך ומתפתח, כך גובר הסיכוי לגיבוש אסטרטגיות שיתופיות (או אסטרטגיות של סטטוס קוו).[71] שימוש מוצלח באסטרטגיית כפייה משותפת יביא גם הוא בטווח הארוך להעדפת הסטטוס קוו: אם אין תועלת במעבר מצד לצד והכפייה המשותפת צפויה להביא להגברת שיתוף הפעולה, אזי אין טעם בתשלום הכרוך במעבר כזה, והדבר מעלה אוטומטית את ערכה היחסי של אופציית הסטטוס קוו (כלומר המשך שיתוף הפעולה). כפי שמניחה תיאוריית "ההרתעה המושלמת", העלייה בערכה של אופציית הסטטוס קוו יחסית לכל אסטרטגיה אחרת של מעבר מצד לצד, היא אחד הגורמים החשובים ביותר להשגת יציבות.[72]

על רקע דברים אלה ניתן להוסיף, כי הגישות העוסקות בהדמיות של "מדינה הפועלת כמערכת" ושל "כפייה משותפת" מצביעות על כך שכניסתה המואצת של הציביליזציה האנושית למעמקי ה"לוגוס" הדיגיטלי עשויה להפוך לגורם נוסף שיביא לשלום וליציבות. אסטרטגיות אלו של "צמצום מידע אסימטרי" יכולות לשמש כאבני בניין מרכזיות למסגרת דוקטרינרית חדשה לקבוצות חברתיות בעידן ה"לוגוס" הדיגיטלי. מסגרת דוקטרינרית זאת תמשיך לקדם שלום ויציבות, תוך שילוב הדוקטרינות העכשוויות של הרתעה קונבנציונלית והרתעה גרעינית. היא גם תכיר ביתרון של מערכות המידע הדיגיטליות בנושאים אזרחיים וצבאיים, ולבסוף תוביל להגדרה מדויקת יותר של מושג העימות.

הדוקטרינה של "השמדה הדדית מובטחת" הפכה את המלחמות בין מתחרים לעמיתים בזירה הבין־לאומית לתרגיל עקר ב"משחק־סכום־שלילי", וזאת במידה רבה בשל היכולות להנחית מכה שנייה. דוקטרינה של שיתוף פעולה דיגיטלי כפוי, המלווה בביטול כל יתרון אסימטרי בתחום המידע שיש למדינה הקוראת תגר, עשויה לסייע בבלימת הסלמתם של משברים בין־לאומיים ב"ציביליזציה הדיגיטלית" של המאה ה־21.

הערות

1 ניתן לראות מאמר זה כהשלמה לסוגיות אי־היציבות במרחב הסייבר שפורטו במאמר: Guy-Philippe Goldstein, "Cyber Weapons and International Stability", *Military and Strategic Affairs*, Vol. 5, No. 2, 2013, pp. 121-139.

2 Sun Tzu, *The Art of War*, (transl. Lionel Giles), 1910, Ch. 3, http://www.gutenberg.org/cache/epub/132/pg132.html

3 Frank C. Zagare, D. Marc Kilgour, *Perfect Deterrence*, Cambridge: Cambridge Studies in International Relations, 2000, pp. 296-301.

4 Paul K. Huth, *Extended Deterrence and the Prevention of War*, New Haven: Yale University Press, 1988, cited in: Zagare, Kilgour, *Perfect Deterrence*, pp. 296-301.

5 לפירוט נוסף של הסוגיה ראו לדוגמה: Goldstein, "Cyber Weapons and International Stability".

6 שם.

7 William W. Kaufmann, *The Requirements of Deterrence*, Princeton: Center of International Studies, Princeton University Press, 1954; Fred Kaplan, *The Wizards of Armageddon*, Stanford: Stanford University Press, 1983, pp. 193-200.

8 ראו דיון בנושא זה אצל: Goldstein, "Cyber Weapons and International Stability". גולדשטיין מפנה להגדרות של תומס שלינג ל"קו אדום":
Thomas C. Schelling, *Arms and Influence*, Yale University Press, 1966, p. 137.

9 ראו דיון אצל גולדשטיין, שם, המפנה לרעיון של "עקומת האמינות" בתוך:
Carey B. Joynt, Percey E. Corbett, *Theory and Reality in World Politics*, Pittsburgh: University of Pittsburgh Press, 1978, pp. 94-95.

10 Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, 2013, p. 88: "The international Group of Experts achieved no consensus as to whether non-destructive but severe cyber operations satisfy the intensity criterion"; Ibid. pp. 82-83, comments #14 and #15.

11 דוגמה לדיון על לוחמת סייבר בהקשר של "לוחמה מבוססת השפעה" ראו:
Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends", in: Christian Czosseck and Kenneth Geers (eds.), *The Virtual Battlefield: Perspective on Cyber Warfare*, Amsterdam: IOS Press, 2009.
"מדריך טאלין" מציין בצורה מפורשת עוד יותר כי "פעולת סייבר מהווה שימוש בכוח כאשר ניתן להשוות את ההיקף וההשפעה שלה לפעולה שאינה סייבר שעושה שימוש בכוח" (כלל מספר 11); ולאחר מכן: "מתקפת סייבר היא פעולת סייבר, בין אם לצרכי הגנה או התקפה, שיש סיכוי סביר שתגרום לפגיעה או למוות לאנשים, או לנזק או להרס של אובייקטים" (כלל מספר 30). הדיון מדגיש בהקשר זה כי: "אין לראות

'פעולות אלימות' כמוגבלות לפעולות של כוח קינטי. הדבר מוסדר היטב בדיני העימות החמוש. בהקשר זה יש לציין שמתקפות כימיות, ביולוגיות או רדיולוגיות חסרות בדרך כלל השפעה קינטית על המטרה, אולם יש הסכמה כוללת שהן מהוות מתקפות על פי החוק". מה שחשוב הוא ההשפעה הישירה על אוכלוסייה אזרחית או על רכוש, ואין זה משַנה באיזו דרך – קינטית או אחרת.

12 Col. Paul M. Carpenter and Col. William F. Andrews, "Effects-Based Operations – Combat proven", *Joint Force Quarterly* 52, 1st Quarter (2009), pp. 78-81.

13 קבוצת המומחים הבין־לאומיים של "מדריך טאלין" מציינת את הרעיון של "היקף ותוצאה", שהוצג בפסק הדין של בית הדין הבין־לאומי לצדק בעניין ניקרגואה: "Nicaragua judgement: Military and Paramilitary Activities in and against Nicaragua (Nicar. V. US), 1986 I.C.J.14 (27 June); Schmitt, *Tallinn Manual*, p. 45.

14 Christopher D. Baker, "Tolerance of International Espionage: A Functional Approach", *American University International Law Review*, Vol. 19, Issue 5 (2003), pp. 1091-1113.

15 "The lack of an international prohibition of espionage leaves decision makers with the usually acceptable liability of merely violating the target nation's domestic espionage law": Thomas C. Wingfield, "Legal Aspects of Offensive Information Operations in Space", *USAF Academy Journal of Legal Studies*, 121, 1999, p. 140; Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica: Rand Corporation, 2009, pp. 23-24.
הדיון על כלל 10 ("איסור על איום או שימוש בכוח") ב"מדריך טאלין" (מהדורת 2013) מציין: "[...] לא כל התערבות ב[מערכות] סייבר מפרה אוטומטית את החוק הבין־לאומי האוסר על התערבות [...] כפי שציין בית הדין בניקרגואה, 'התערבות' מנוגדת לחוק כאשר היא עושה שימוש בשיטות של כפייה. יוצא מכך שריגול סייבר וניצול של סייבר, הנעדרים מרכיב של כפייה, אינם מפרים כשלעצמם את עקרון אי־ההתערבות".

16 Schmitt (ed.), *Tallinn Manual*, Part I, Section 2: Self-Defence, and Rule 32, "Prohibition on attacking civilians".

17 Charles Tilly, "War Making and State Making as Organized Crime", in: Peter Evans, Dietrich Rueschemeyer and Theda Skocpol (eds.), *Bringing the State Back*, Cambridge: Cambridge University Press, 1985; Antonio Giustozzi, *The Art of Coercion: Armed Force in the Context of State Building*, CSRC Seminar, 2008.

18 Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War Between the United States of America and the Union of Soviet Socialist Republics, http://www.state.gov/t/isn/4692.htm; Agreement Between the United States of America and the Union of Soviet Socialist Republics on Measures to Improve the USA-USSR Direct Communications Link, http://www.state.gov/t/isn/4787.htm, Cited in: Laura Grego, *A History of Anti-Satellite Programs*, UCS Global Security Programs, 2012.

19 Karl Frederick Rauscher, Andrey Korotkov, "Russia-US Bilateral on Critical Infrastructure Protection", in: *Working toward Rules for Governing Cyber Conflict*, East-West Institute, 2011; Schmitt, (ed.), *Tallinn Manual*, "3/The law of armed conflict generally" (in particular "Rule 20"), "4/Conduct of hostilities" (in particular "Rule 29 – Civilians" and Section 3: "Attacks against persons").

20 Michael S. Lewis-Beck, Mary Stegmaier, "Economic Determinants of Electoral Outcomes", *Annual Review of Political Science*, Vol. 3 (2000), pp. 183-219.

21 Alan de Bromhead, Barry Eichengreen and Kevin Hjortshøj O'Rourke, *Right Wing Political Extremism in the Great Depression*, Discussion Papers in Economic and Social History, Number 95, University of Oxford, 2012.

22 "מדריך טאלין" מגדיר כלא חוקית פעולת סייבר המנסה לפגוע בעצמאות הפוליטית של מדינה כלשהי (כלל 10).

23 "מדריך טאלין", כלל 11, עמ' 51.

24 Martin C. Libicki, "Cyberspace is not a Warfighting Domain", *I/S: A Journal of Law and Policy for the Information Society*, 8, no. 2 (2012), p. 330.

25 ראו "מקרה קווירין" מ־1942, העוסק במחבלים גרמניים, עם דגש מיוחד על מחבלים שלא ענדו סמלים לאומיים: "[...] מרגל שחוצה את הגבול בזמן מלחמה בצורה חשאית וללא מדים, מתוך כוונה לאסוף מידע צבאי ולהעבירו לאויב, או לוחם של האויב החוצה את הגבול באופן חשאי וללא מדים, במטרה לפגוע בחיים או ברכוש, הם דוגמאות ללוחמים שבאופן כללי אינם זכאים למעמד של אסירי מלחמה, אלא של מי שהפרו את דיני המלחמה, והם יועמדו למשפט וייענשו בבתי דין צבאיים". U.S. Supreme Court, EX PARTE QUIRIN, 317 U.S. 1 (1942). יש לציין שלוחמים בלתי חוקיים זכאים בכל זאת "ליחס הומאני, ובמקרה של משפט לא תימָנע מהם הזכות למשפט סדיר והוגן על פי האמנה הנוכחית": Geneva Convention Relative to the Protection of Civilian Persons in Time of War, August 12, 1949 (GCIV).

26 על "לוחמים חסרי זכויות" ראו "מדריך טאלין" 2013, עמ' 100, הערה 17.

27 Ben Smith, Arabella Torp, "The Legal Basis for the Invasion of Afghanistan", *House of Commons, International Affairs and Defence Section*, February 26, 2010, pp. 4-5.

28 Ashton B. Carter, Michael M. May, William J. Perry, *The Day After – Action in the 24 Hours following a Nuclear Blast in an American City*, Report based on Workshop, The Preventive Defense Project, Harvard and Stanford Universities, 2007, in particular: "6. Retaliation and Deterrence", pp.15-17.

29 כלל 11 ב"מדריך טאלין", 2013.

30 כלל 13, הערה 5 ב"מדריך טאלין" 2013, עמ' 55, המצטט את פסק דין ניקרגואה, פסקה 191.

31 "All warfare is based on deception", Sun Tzu, *The Art of War*, p. 66.

32 Herman Kahn, *On Escalation*, London: Pall Mall Press Ltd., 1965.

33 לזיהוי התוצאה יש לצרף ניתוח טכני של התוכנה הזדונית עצמה. דבר זה עשוי לארוך זמן רב. לדוגמה, הווירוס "סטקסנט" זוהה על ידי וירוס "בלוקדה" ביוני 2010, אך נותח לעומק רק בנובמבר 2010. ראו: Nicolas Falliere, Liam O. Murchu, Eric Chien, *W32. Stuxnet Dossier*, Symantec, 2010. מכאן הדרישה לחילופי התרעות מידע עדכניות, שיזרמו מכל מרכזי הפעילות האזרחיים והצבאיים לנקודת איסוף אחת בתחום הסייבר, שתהיה מסוגלת לפרש תקריות סייבר וליצור תמונה שלמה לשימושם של מוסדות הביטחון של המדינה.

34 ראו כלל 30, הערה 5, ב"מדריך טאלין" 2013, עמ' 106.

35 John A. Warden III, "The Enemy as a System", *Airpower Journal*, Vol. 9, Issue 1, 1995.

36 General James N. Mattis, USMC, "USJFCOM Commander's Guidance for Effects Based Operations", *Joint Force Quarterly,* No. 51, 2008; Paul M. Carpenter, William F. Andrews, "Effects-Based Operations Combat Proven", *Joint Force Quarterly*, No. 52, 2009: (ביקורת של קציני חיל האוויר האמריקאי על USJFCOM).

37 Robin Vasan, "Business Process API-ification: the LEGO promise fulfilled",

GigaOm, October 6, 2012, http://gigaom.com/2012/10/06/business-process-api-ification-the-lego-promise-fulfilled/; Mark Boyd, "Getting C-Level Buy-In: Demonstrating the Business Value of APIs", *ProgrammableWeb*, September 11, 2013, http://blog.programmableweb.com/2013/09/11/getting-c-level-buy-in-demonstrating-the-business-value-of-apis/

38 לדיון במרכיבים המרכזיים של מרחב הסייבר ראו: Goldstein, "Cyber Weapons and International Stability".

39 Isaac Ben-Israel, *Philosophie du renseignement*, Paris : Editions de l'Eclat, 2004.

40 שם.

41 דוגמה זו שואבת השראה ישירה מניתוח מלחמת יום הכיפורים, כפי שהובא ב: Ben-Israel, *Philosophie du renseignement*.

42 כדי לגלות את הזהות של "ג'רלד", החפרפרת שעבדה עבור ברית המועצות, שולח סמיילי הודעה לראש ה"סירקוס", המאלצת את "ג'רלד" לבקש פגישת חירום עם איש הקשר הסובייטי שלו בדירת מבטחים, שמיקומה היה ידוע זה מכבר לסמיילי. זה המבחן שאִפשר לסמיילי לפרוץ לדירת המבטחים ולזהות את "ג'רלד": John Le Carré, *Tinker Tailor Soldier Spy*, London: Hodder & Stoughton, 1974.

43 לדיון המשווה בין העולם "הדיגיטלי" המגדיר את מרחב הסייבר לבין עולם "המידע החסוי" שמגדיר את תחום המודיעין המסורתי ראו: Goldstein "Cyber Weapons and International Stability".

44 Ben-Israel, *Philosophie du renseignement*.

45 Richard Clarke and Robert K. Knake, *Cyberwar*, New York City: HarperCollins Publishers, 2010, pp. 249-254.

46 שם.

47 L. M. Hill, "The Two-Witness Rule in English Treason Trials: Some Comments on the Emergence of Procedural Law", *American Journal of Legal History*, 12, 1968, pp. 95-111.

48 Glenn Shafer, "the Combination of Evidence", *International Journal of Intelligent Systems*, Vol. I, 1986, pp. 155-179.

49 ראו ניתוח על פי תיאוריית המשחקים של משבר ברלין ב־1948 בתוך: Frank C. Zagare, *The Dynamics of Deterrence*, Chicago: University of Chicago Press, 1987, pp. 11-28.

50 Thomas C. Schelling, *the Strategy of Conflict*, Cambridge: Harvard University Press, 1963, p. 69.

51 Greg Rattray, Chris Evans, Jason Healey, "American Security in the Cyber Commons", in: Abraham M. Denmark and James Mulvenon (eds.), *The Future of American Power in a Multipolar World*, Washington D.C.: Center for a New American Security, 2010, pp. 151-172.

52 Daniel L. Shapiro, "Negotiation Theory and Practice: Exploring Ideas to Aid Information Eduction", in: Robert A. Fein, Paul Lehner, Bryan Vossekuil (eds.), *Educing Information*, Washington D.C.: Intelligence Science Board, National Defense Intelligence College Press, 2006, pp. 267-280.

53 M. P. Rowe, "Negotiation Theory and Educing Information: Practical Concepts and Tools", in: Fein, Lehner, Vossekuil (eds.), *Educing Information*, p. 295.

54 וירוס "סטקסנט" עשה שימוש באישורים דיגיטליים של החברות הטיוואניות Realtek ו־JMicron, שעברו מניפולציה. ראו: Falliere, Murchu, Chien, *W32. Stuxnet Dossier*.

55 David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran", *The New York Times*, June 1, 2012.

56 ניתן להתחיל, למשל, במדינות החברות ב"תוכנית לשיתוף פעולה טכני" ("5 eyes" nations"), שיש להן היסטוריה של שיתוף פעולה צמוד בסוגיות קריטיות (למשל, בפעולות סייבר משותפות או בסוגיות לשיתוף מודיעיני), כמו המדינות המשתתפות בברית נגד אל־קאעדה. ראו:
Dana Priest, "Help from France Key in Covert Operations", *The Washington Post*, July 3, 2005.

57 Schelling, *Arms and Influence*, p. 47.

58 לניסוח ראשוני של הביולוגיה האבולוציונית ראו:
Leigh Van Valen, "A New Evolutionary Law", *Evolutionary Theory* 1 (1973), pp. 1-30; Rattray et al., *The Future of American Power in a Multipolar World*, Section "Adaptation and Counter-Adaptation", p. 154; Kevin Mandia, "Cyber Threats and ongoing Efforts to Protect the Nation*"*, Permanent Select Committee on Intelligence, US House of Representatives, October 4, 2011.

59 Edward Rhodes, "Conventional Deterrence", *Comparative Strategy*, 19: 3 (2000), pp. 221-253, in particular pp. 222-223.

60 Robert Axelrod, *the Evolution of Cooperation*, New York City: Basic Books, 1984. ראו עמ' 13 להסבר על "צל העתיד" ועמ' 124 על "הגדלת צל העתיד" לקידום שיתוף פעולה.

61 Edward N. Luttwak, *Strategy – The Logic of War and Peace*, revised and enlarged edition, Cambridge: The Belknap Press of Harvard University Press, 2001, Chapter 11, "Nonstrategies", pp. 168-184.

62 Julian S. Corbett, *Some Principles of Maritime Strategy*, London: Longmans, Green & Co., 1911, p. 90: "Command of the Sea, therefore, means nothing but the control of maritime communications, whether for commercial or military purposes".

63 לדיון על "לוגוס" דיגיטלי ראו: Goldstein "Cyber Weapons and International Stability".

64 Marc Andreessen, "Why Software is Eating the World", *The Wall Street Journal*, August 20, 2011.

65 FLOPS – Floating Point Operations Per Second – יחידת מידה לעוצמתם של מחשבים. מחשב העל המהיר ביותר ב־2010 היה Cray Jaguar, שמהירותו הייתה 1.8 10^15 פלופס: top500.org, November 2009-2010. ביצועים מעבר לאקסא־פלופ אחד או 10^18 פלופס צפויים להיות מושגים עד שנת 2020: Agam Shah, "SGI, Intel Plan to Speed Supercomputers 500 Times by 2018", *Computerworld*, June 20, 2011.

66 יכולות של זטא־פלופ (10^21) עשויות לאפשר יצירת מודלים לחיזוי מדויק של מזג האוויר לתקופה של שבועיים מראש. ראו בעניין זה:
Erik P. DeBenedictis, "Reversible Logic for Supercomputing" *Proceedings of the 2nd Conference on Computing Frontiers*, Sandia National Laboratories, 2005, pp. 391-402.

67 חוקרים דיברו על "חורף של בינה מלאכותית" במהלך שתי תקופות לפחות: בין 1974 ל־1980 ובין 1987 ל־1993. ראו:
Jim Howe, "Artificial Intelligence at Edinburgh University: a Perspective", 1994; Stuart J. Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, 2003, p. 24.

68 באמצע העשור הראשון של שנות האלפיים השתנתה הגישה כלפי הבינה המלאכותית והתחילו לדבר על "אביב" בתחום זה. ראו לדוגמה:
John Markoff, "Behind Artificial Intelligence, a Squadron of Bright Real People", *The New York Times*, October 14, 2005.

69 Zagare, *The Dynamics of Deterrence*, pp. 48-56.

70 Axelrod, *The Evolution of Cooperation*, p. 13 (דיון על "צל העתיד").

71 Goldstein, "Cyber Weapons and International Stability".

72 Zagare, Kilgour, *Perfect Deterrence*, pp. 293-296.