נשק סייבר ויציבות בינלאומית: איומים חדשים על היציבות מחייבים סוגים חדשים של דוקטרינות אבטחה[1]

גיא פיליפ גולדשטיין

מאמר זה בוחן את הסיכונים האסטרטגים של נשק סייבר ואת הנחיצות לפתח דוקטרינות ייחודיות להגנת סייבר, כדי לצמצם ככול האפשר את הסיכון להסלמת משבר עד לכדי יציאתו מכלל שליטה. כיום, לוחמת אינטרנט ממוחשבת, היא אחת מתוך כמה זירות צבאיות שצפויות לצמוח, הן בארצות הברית והן במדינות נאט"ו. המאמר הנוכחי מציע רעיונות ומסגרות עבודה מהספרות ה"קלאסית", העוסקים באסטרטגיה, במטרה לעצב תפישה מוסדרת יותר של הסיכונים הטמונים בנשק הסייבר ליציבות הבינלאומית, ובעקבות זאת, לזהות את סוגיות הליבה בהגנת סייבר, שישמשו נקודת משען לדוקטרינות עתידיות.

מילות מפתח: לוחמת סייבר, הרתעה, דוקטרינת הגנת סייבר, נשק סייבר, ארצות הברית, נאט"ו, אסטרטגיה, הערכת סיכונים

כבר בתחילת 2013, הפך מרחב הסייבר למוקד בעל חשיבות אסטרטגית. מפקדת הסייבר של ארצות־הברית היא מפקדה מאוחדת אחת, הכפופה לפיקוד האסטרטגי האמריקאי מאז 2009. כמו במבצעים אסטרטגיים או מיוחדים אחרים, גם כאן מחייבות החלטות מרכזיות קבלת אישור ישירות מנשיא ארצות־הברית. ההשפעות של נשק סייבר עשויות להיות כה נרחבות, עד ש"יש להתיר את השימוש בו רק בעקבות פקודה ישירה של העומד בראש כוחות הביטחון (המפקד העליון)".[2] לעומת זאת, מבחינת הפנטגון, חבלה ממוחשבת שמקורה במדינה אחרת יכולה להוות עילה למלחמה – כפי שהוצהר בצורה רשמית למחצה במגזין 'וול סטריט' ביוני 2011. האיום של מתקפות סייבר הוצב בראש רשימת סיכוני הביטחון הלאומי,

גיא פיליפ גולדשטיין הוא סופר; מחבר רב המכר **בבל שעת אפס**.

כחלק מהערכת האיומים הכלל־עולמיים של קהילת המודיעין לשנת 2013.[3] כיום, לוחמת רשת ממוחשבת היא אחת מתוך כמה זירות צבאיות שצפויות לגדול, הן בארצות־הברית והן במדינות נאט"ו.[4]

למרות כל זאת, לא פורסמה בנושא כל דוקטרינת שימוש ברורה כגון דוקטרינת ההרתעה הגרעינית. ראשית, דומה שכללים רבים נותרו חשאיים, ואך ורק במסגרת הדרג הגבוה ביותר של הבכירים. כמו כן, התחום עצמו אינו מוגדר בצורה ברורה: הוא יכול להיות תחום של לוחמה[5] או לאו דווקא, למעשה.[6] האם מרחב הסייבר קריטי רק משום שהוא תורם לביטחון הצבאי,[7] או שהוא חיוני בזכות עצמו, בשל ערכם העולה של הנתונים המאוחסנים ומוגנים בו? לבסוף, לפיתוח דוקטרינה נדרשים זמן ותקדימים היסטוריים. למרות שתפיסות של הרתעה גרעינית החלו לצמוח ב־1946 בעקבות עבודות של ברודי,[8] הדוקטרינה של 'השמדה הדדית מובטחת' (Mutually Assured Destruction) לא עמדה למעשה במקום מרכזי לפני סוף שנות החמישים.[9] בברית־המועצות, "גרף הלמידה" של האסטרטגיה הגרעינית היה אף מתקדם פחות.[10] השדה של מחקרי הסייבר עדיין צעיר יחסית, ונשק הסייבר עצמו מתפתח ללא הרף, ברמה ובהיקף.

אולם, מדוע היעדר דוקטרינה מציב בעיה חמורה? ללא מסגרת ניהול ראויה או דוקטרינה של יחסים בינלאומיים – הכנסתה לשימוש של כל טכנולוגיה הרסנית שטרם נבדקה מהווה פוטנציאל להשלכות בלתי־צפויות. הדבר נכון במיוחד בעסקי המלחמה. ללא מסגרת של דוקטרינה, הסתמכות בלעדית על פתרונות טכנולוגיים אינה ערבות לשימור הסטטוס קוו. יציבות במהלך 'המלחמה הקרה' לא הובטחה על ידי טכניקות הגנה כמו מערכות יעילות של טילים אנטי־בליסטיים. לא רק שמדובר בפתרונות טכנולוגיים חמקמקים – הם גם היו בלתי־רצויים לצורך שימור מאזן האימה העומד במרכז דוקטרינת ההשמדה ההדדית המובטחת (MAD). שתי המסקנות הובילו לחתימה על ההסכם להגבלת טילים אנטי־בליסטיים (TreatyABM) ב־1972.[11]

אין בכך כדי לבטל את הנחיצות של התפתחויות טכנולוגיות מסוימות – כמו למשל שיגור טילים בליסטיים מצוללות (SLBM) שמבטיחים יכולת מכה שנייה של השורדים, אולם אלה חייבות להתלוות לדוקטרינה סדורה שתחזק אותן ותמנע סתירות. הדבר נכון במיוחד למרחב הסייבר, שטבעו והסיכונים שבו מצביעים כי הגיע הזמן למאמץ מעין זה. ראשית, הנושא אמנם אינו מפותח דיו עדיין, אולם אין מדובר עוד בשלב הראשוני. אנו נמצאים יותר מ־15 שנה לאחר התרגיל האמריקאי Eligible Receiver בשנת 1997, שעורר בדרג הפדרלי את החשש הממשי הראשון בנוגע ללוחמת סייבר,[12] ומאחורינו כבר למעלה מחמש שנים שעומדות בסימן כמה וכמה תקריות סייבר ביחסים הבינלאומיים, החל מלוחמת הגרילה־סייבר בין רוסיה לאסטוניה ב־2007[13] ועד המתקפות הזרות נגד חברת ארמקו בערב־הסעודית,

שמקורן אולי באיראן.[14] אנו מגיעים לנקודה שבה יש לנו מספיק דוגמאות לניסוח ההנחות הראשונות בסוגיות ובדוקטרינות. שנית, ניתן לגשת לנושא מהזווית הקלאסית של מסגרות פוליטיות ומשפטיות. למרות שחייבת להינתן תשומת הלב לייחודיות התחום, אין צורך בגישת "לוח חלק". דוגמה עדכנית לכך היא Tallinn Manual – מחקר שבחן את ישימות החוק הבינלאומי בלוחמת סייבר, והצליח להחיל תקדימים משפטיים על מצבי לוחמת סייבר.[15] בהמשך לדוגמה זו, המאמר הנוכחי יבקש להחיל מסגרות מספרות האסטרטגיה ה"קלאסית", כדי להציע הערכה מוסדרת יותר של הסיכונים הטמונים בנשק הסייבר ליציבות הבינלאומית, ובעקבות זאת – לזהות את סוגיות הליבה בהגנת סייבר שיחייבו מענה באמצעות דוקטרינות עתידיות.

טיבו של מרחב הסייבר והסיכונים הנוכחיים בו

מהו מרחב הסייבר? השאלה נדונה בהרחבה, לרוב תוך התמקדות במרכיבים הטכנולוגיים (כגון ספקטרום אלקטרומגנטי, טכנולוגיות של מידע ותקשורת).[16] להלן מובאת הצעה למבט משלים שיהיה שימושי למאמר הנוכחי. מרחב הסייבר הוא השם העכשווי לכל מערכות המידע המבוססות על נתונים דיגיטליים. רדיו אלקטרומגנטי אנלוגי אינו חלק ממרחב הסייבר. הוא אינו יודע כיצד "לדבר דיגיטלית". מחשב דנ"א, לעומת זאת, שעובד עם נתונים דיגיטליים, מהווה חלק ממנו. קלטת אלקטרומגנטית שניתן להפעילה במכשיר הקלטה אנלוגי אך היא מקודדת בנתונים דיגיטליים – גם היא חלק ממרחב הסייבר. מידע דיגיטלי הוא השפה שבני־האדם יצרו כדי לדבר עם מכונות. מקורה במהפכה התעשייתית – במכונת האריגה של ז'קרד (Jacquard loom (1801), כאשר המורכבות הגוברת של מכונות חדשות עוררה צורך ביצירת שפה כזאת, וראשיתה בכרטיסי ניקוב. לאחר מכן נדרשו כמעט מאתיים שנה להתפשטות השפה בין המכונות, בייחוד לאור המצאות כמו מכונת החישוב של טיורינג ופרוטוקול האינטרנט. הסייבר מורכב משלושה רכיבים בסיסיים: חומרה (כולל ציוד טלקומוניקציה), תוכנה (כולל פרוטוקולים להעברת נתונים), ו"חוֹשבה" ("brainware") – החלק האנושי. בני־אדם הם חלק מהעברת הנתונים ומהווים נקודות יירוט פגיעות מאוד.[17] בני־אדם הם גם כותבי הקוד: חלק מהנשק המסוכן ביותר במרחב הסייבר כיום הוא המוחות המרושתים של האקרים מוכשרים. מבחינת תפקוד, ניתן לחלק את מרחב הסייבר לשניים: התמיכה הפיזית שמשפיעה באופן חומרי על התקשורת והחישוב, והתחום הסמנטי שמתרגם פעולות מהתמיכה הפיזית לנתונים, לפקודות ולמשמעות, ושולט בתמיכה הפיזית שלו עצמו.

תיאור פשוט זה של מרחב הסייבר מסייע להבין מדוע יש כיום דחיפות להגדיר את התנאים להגנת סייבר, ומהן נקודות התורפה הקריטיות ביותר במרחב הסייבר.

ראשית, החלוקה לנתונים דיגיטליים לעומת אנלוגיים מסייעת להבין מדוע הפכה לוחמת סייבר לנושא אסטרטגי רק לקראת סוף שנות האלפיים. המחשוב מלווה אותנו כבר למעלה מ־65 שנים, מאז תום מלחמת העולם השנייה. עם זאת, בשנת 1986 היוו נתונים דיגיטליים רק 0.6% מכלל הנתונים לאחסון, לתקשורת ולשידור, ו־24% בלבד בשנת 2000, אך שיעורם הגיע ל־93% ב־2007. בנקודה זו, יכולות המידע האנלוגי ה"ישן" הפכו לבלתי־חשובות.[18] כפי שניסח זאת מרק אנדריסן כעבור ארבע שנים: "התוכנה אכלה את העולם".[19] דבר זה יכול להסביר את התפוצה והפיזור של תקריות מתקפת סייבר במהלך הזמן: עד המחצית השנייה של שנות האלפיים העברנו לפורמט דיגיטלי את אחת מהמערכות הקריטיות ביותר שיש לכל מוסד או אורגניזם – את מערכת המידע שלו.

שנית, תיאור זה מדגיש את הממד הסמנטי. ממד זה משקף את מרכז הכובד האמיתי של מערכות מידע מרושתות. היעד של ARPAnet, הרשת שהולידה את האינטרנט, היה "להדגיש עמידות ויכולת הישרדות, לרבות היכולת לעמוד באובדן של חלקים גדולים מרשתות הבסיס".[20] רשתות מיתוג מנות (Packet switching) תוכננו כך שיעמדו בבלאי של חומרה. במרחב הסייבר, הנזק החמור ביותר מתרחש כאשר הנתונים נפגעים ומשמעותם מתעוותת, כפי שניתן היה לראות, למשל, ב"מבצע בוסתן"[21] או בסטקסנט. בשני המקרים, ההשפעה המרבית הושגה בעקבות הפעלת מניפולציה על אנשי שליטה ובקרה, באמצעות פגיעה במערכות פיקוד ובקרה. כמו כן, השחתת בקרים תעשייתיים שקובעים את קצב המנועים בצנטריפוגות p–1 השיגה חבלה ממשית יותר.[22]

מאפיינים של מתקפות סייבר

ביוון העתיקה, פירוש המילה 'לוגוס' היה המילה שנאמרה, המשפט, המשמעות הישירה של התיאור וגם הרעיונות העמוקים שהוא ביטא.[23] הייתה זו הגדרה מבלבלת אך עשירה. היא גם הובילה להאקרים הראשונים: הסופיסטים (המורים הנודדים). הסופיסטים תמרנו את המילים ואת התחביר כדי לעוות את המשמעות. מה שאנו מכנים כיום 'מרחב סייבר' הוא הלוגוס הדיגיטלי החדש שלנו. השפה שלנו מתוכננת לדבר עם מכונות, החל מהתמיכה הפיזית שלה דרך התרגום הסמנטי המיידי לפקודות המכוונות למכונות או לאנשים, ועד "ההזיה המוסכמת"[24] (consensual hallucination) של גיבסון. בלוגוס הדיגיטלי, הסופיסטים המודרניים פועלים כמו שוליית הקוסם של פול דיקא (Paul Dukas): אחד שולח את הקוד, וסביבת המכונות – שהיא מעשה ידי אדם – משתנה. מכונות נבנות כך שיאמינו לפקודות ולטיעונים שגויים. כך הן משנות את העולם הפיזי. איכות המתקפה תלויה בראש ובראשונה בכישרונו של הקוסם.

נשק סייבר פוגעני עושה שימוש בפרצות שנוצרו בעת ייצור המכשור[25] או הקוד או על ידי האדם המפעיל אותו, בין אם באופן טבעי ובין אם בכוונה תחילה, ואז מנצל זאת לפעולה נוספת. כדי להעריך ביתר דיוק את ההשפעות על העולם הפיזי, לוחמי סייבר בונים מודלים של חלקים מהעולם הפיזי, ואז בודקים את המתקפה עליהם[26]. נשק סייבר יכול גם להסתיר את חתימתו ומקורו.[27] מבחינת מידע, מאפיינים אלה מעניקים יתרון אסימטרי לתוקף ברגע שמתגלה ליקוי (או פִּרצה): רק התוקף יודע על הפִּרצה, ורק הוא יודע איזו מדינה תוקפת. אסימטריה זו במידע מעניקה יתרון ברור לתוקף. עם זאת, כיוון שמרחב הסייבר מתעדכן בהתמדה על ידי שדרוגי תוכנה והסביבה הפיזית של הסייבר משתנה בהתאם, יכולת הניצול לרעה מוגבלת וארעית: חיפוש או ייצור של פרצות מחייב מאמץ מתמיד.

השפעות של מתקפות הן מיידיות, ומתרחשות ברגע שהמחשבים מקבלים את המסר – הקוד תוקף ב"שעת האפס". טווח ההשפעות רחב ביותר, בשל השימוש הנרחב שהוסבר לעיל במכונות הדוברות את השפה הדיגיטלית: מריגול (חדירה למחשבים שמאחסנים מידע) וחבלה כלכלית (חדירה ו/או השחתה של מחשבים המאחסנים מידע בעל ערך פיננסי או כתובות IP), ועד חבלה פיזית (מתקפות נגד מחשבים ששולטים ומפקחים על סוגים שונים של תהליכים בתעשייה האזרחית או במערכות נשק טקטי או אסטרטגי). כיוון ש"התוכנה אכלה את העולם" וממשיכה לעשות זאת, אין גבול למה שאפשר לתקוף. להשפעות יש גם מרכיב פסיכולוגי. חובה להחליף ציוד שניזוק במתקפה קינטית. ציוד שנפגע ממתקפת סייבר עשוי להיות עדיין שמיש, אבל הספקות בדבר היכולות שלו יישארו לעד.

חוסר יציבות גאו־פוליטית כתוצאה מנשק סייבר – (I) מגמה התקפית ומהירות

המאפיינים הפוטנציאליים שהוזכרו לעיל במונחים של מגמה התקפית, מהירות ופוטנציאל להשפעות רחבות־היקף יוצרים סביבת טכנולוגיה צבאית שנוטה להפר את הסטטוס קוו. בניתוחו המקורי לתיאוריית התקפה־הגנה טוען רוברט ג'רוויס שתנאי דילמת האבטחה נשענים על שני "משתנים מכריעים": "האם ניתן להבחין בין מדיניות ונשק הגנתיים לבין התקפיים, והאם יש יתרון לאחד מהם – להגנה או להתקפה".[28] שילוב בין שני המשתנים האלה יוצר ארבעה עולמות אפשריים, וג'רוויס מציין שבעולם שבו "לא ניתן להבחין בין עמדה התקפית להגנתית" וכאשר "להתקפה יש יתרון", קשה ביותר למעצמות עולמיות לשמר את הסטטוס קוו. במקרה כזה, האמונות חזקות בדיוק כמו טכנולוגיה. מלחמת העולם הראשונה הייתה תוצאה של עולם כזה, שהוגדר "בעל סכנה כפולה". מעצמות־העל דאז למעשה הוּלכו שולל: הטכנולוגיות של מכונות הירייה ומסילות הרכבת נתנו יתרון

להגנה.[29] אולם עקב הניצחונות המהירים בקרבות של ביסמרק בעשורים שלפני כן, מעצמות־העל האמינו שטכנולוגיות צבאיות עדיין מעניקות יתרון להתקפה.[30]

ההקבלה לסביבה הצבאית שמעוצבת ונשלטת על ידי נשק סייבר היא ברורה. ראשית, קיימת אמונה מוסכמת שנשק סייבר מעניק יתרון למתקיף.[31] יתרון זה עשוי להיות טמון באסימטריה שבין המתקיף למתגונן בכל הנוגע למידע: תחילה, מעצם טבעה של הבעיה, הצד המתגונן מתעלם מקיום הפִרצה כל עוד אינה מוחשית. כמו כן, כאשר קיומה של הפִרצה בא לידי ביטוי זה עלול להיות מאוחר מדי. טיעון זה מצריך חידוד ואולי בחינה נוספת – אולם אינו קשור לענייננו. העובדה שיתרון זה יכול להיות מוגבל וזמני במציאות היא שולית מבחינת ישימות המודל שמציג ג'רוויס. כמו אירופה שלאחר ניצחונותיו של ביסמרק, מה שחשוב הוא האמונה שבאה לידי ביטוי בקונצנזוס הכללי. נקודה שנייה – נשק סייבר אינו ניתן לניטור. בקושי ניתן להבחין בין יכולת הגנה להתקפה. דוקטרינות של שימוש כפול, לרבות שימוש להתקפה והגנה גם יחד הופיעו בסין, אך גם במדינות מערביות מובילות.[32] יכולות הליבה כוללות נכסים שלפחות ממרחק ניתן לפרשם כמיועדים לשימוש התקפי או הגנתי – כמו תשתית IT או כותבי קוד. נכון להיום, בתחום נשק הסייבר, אין מקבילה למה שכונה בשיחות Salt II "ההבדלים הגלויים", כלומר, הסימנים ששימשו לזיהוי מטוסי תקיפה שנושאים טילי שיוט ארוכי־טווח.[33] קשה מאוד להבדיל בין פיתוח יכולת הגנה לפיתוח יכולת התקפה, שכן הגנה מקורה בעיקר בתרגולים של צוותי אבטחת מידע (Red-Team).[34]

הסיכונים של "סכנה כפולה" יכולים להחמיר גם עקב מתקפה מהירה שמשמשת מכת פתיחה. מתקפת פתע כזו שבאה "משום מקום" תהיה כה יעילה, עד שתמנע כל תגובה מהצד המותקף. בניתוח ראשוני של משחקי הרתעה הדדית הראה זאגארה שככל שהמשחק קצר יותר מבחינת מספר המהלכים, כך עולה הסבירות שהוא יפר את הסטטוס קוו.[35] התמריץ להכות ראשון משותף לכוחות שחולקים רמה דומה של פיתוח טכנולוגי. במקרה כזה, התפיסה שמדובר בסיכוני התקפה שווים תוביל למה ששלינג מכנה "חשש הדדי ממתקפת פתע".[36] כפי ששלינג מנסח זאת בספרו Arms and Influence:

> "[...]טכנולוגיה צבאית ששמה דגש על מהירות בזמן משבר שמה דגש על המלחמה עצמה.[...]אם הנשק יכול להיות מופעל מיידית בלחיצת כפתור או במתן "אור ירוק", ויכול להגיע ליעד כמעט ללא התרעה ולהסב הרס מוחלט, תוצאת המשבר תלויה בפשטות בשאלה, מי הראשון שימצא כי המתח בלתי־נסבל[...]"[37]

ניתן לראות ששורות אלה נכתבו כמה שנים לפני הקמתה של ARPAnet. הן מהדהדות בכתובים הראשונים של קציני חיל האוויר האמריקאי על המלחמה

בעידן המידע, כאשר ציינו כי "שימוש בכוח מקדים עשוי להפוך לתנאי מוקדם להצלחה".[38]

הדינמיקה המובילה לעימות מחריפה גם בשל ההשקעה הטכנולוגית המתמשכת במחקר ופיתוח של נשק סייבר. המניע להשקעה נוספת ניזון מהתרחבות מרחב הסייבר ליותר ויותר תחומי חיים אזרחיים וצבאיים, ומהצורך להגן על עולמות חדשים אלה במרחב הסייבר. היות שקשה להבחין בין יכולות מחקר ופיתוח של הגנה לאלה של התקפה, מטבע הדברים נוצר מרוץ חימוש. קצב ההמרה הפנימי של תהליכים לא־מקוונים בסייבר לתהליכים מקוונים אינו תמיד בשליטת הצבא: בהבדל ממהפכות אחרות בתחום הצבא שהונעו מתוך תחרות ממשית, הדחף לדיגיטליזציה של הצבא האמריקאי נמשך בקצב מהיר גם לאחר התפוררות ברית־המועצות.[39] ייתכן שניתן לראות בכך את התגלמות הדינמיקה האוטונומית של נתונים דיגיטליים ושל תוכנה שממשיכה "לאכול" את הצבא. במקרה כזה, גם האבולוציה האיכותנית של הטכנולוגיה עצמה יכולה לשבש את יציבות הסטטוס קוו. כפי שציין קיסינג'ר, מדינות יריבות עלולות לחיות בחשש כי "[...] הסכנה להישרדותן טמונה בפריצת דרך טכנולוגית של היריב".[40] ג'וינט וקורבט ציינו כי קצב השינויים יוצר "אי־ודאות מהותית בנוגע לטכנולוגיות מתקדמות": "[...] טכנולוגיה אינה יכולה לספק את התנאים המספיקים להשגת הרתעה יציבה".[41] ואכן, כדוגמה אזורית מביא הורוויץ את מרוץ חימוש הסייבר במזרח־אסיה כמגביר את אי־היציבות.[42] לבסוף, מעבר לזרועותיו המתארכות של הסייבר, היריבות הפנימית הדינמית והתסיסה המתמדת של תעשיית ה־IT מייצרים שדרוג מתמשך במרחב הסייבר עצמו. אולם שיפורים חיוביים אלה מהווים גם מקור לשינויים חדשים בשדה המשחק הצבאי, כמו למשל בהיבט של פרצות חדשות. די בגורם זה, שאינו תלוי ביריבות צבאית או פוליטית, כדי להאיץ באופן מכני את מרוץ החימוש.

חוסר יציבות גאו־פוליטית כתוצאה מנשק סייבר – (II) ייחוס וסף

בנוסף לתפיסת הסייבר כסביבה במגמה התקפית "נוטה לחיפזון" ותחום המשתנה בהתמדה מבחינה טכנולוגית, מרחב הסייבר מאופיין גם ביכולת לשקול מתקפה גם ללא (1) ייחוס ברור ו־(2) זיהוי ברור של הסף שחצייתו מסוכנת בעקבות המכה הראשונה. גורמים אלה תורמים לערעור נוסף של היציבות.

כפי שכבר צוין לעיל, היעדר חתימה – סוגיית הייחוס – מעניק יתרון לתוקף. אם הותקף, הצד המתגונן אינו יודע במי לנקום. יתרה מכך, הדבר פוגע בהגנה שלו שכן הוא אינו יכול להנחית מכת נגד שתוכל לפגוע ביכולות התוקף, או להרתיע אותו. ללא זיהוי ברור של התוקף, המותקף יתקשה גם להניע קשרים דיפלומטיים

כדי לארגן לחץ נגדי. אם ינקוט פעולת תגמול או הגנה נגד המדינות הלא־נכונות, הוא עלול להגביר את הבידוד שלו עצמו, ואף להביא להסלמה בזירה הבינלאומית. ייחוס אינו סוגיה של מה בכך. במשחקי מלחמה, זוהי אחת השאלות הראשונות ששואל השחקן שעומד בראש מערך ההגנה: "מי עשה את זה"?[43]

כדי לצבור רווח דיפלומטי, הייחוס צריך להגיע לרמה גבוהה של ודאות, ומבחינה טכנית קשה להשיג זאת בזמן מוגבל.[44] תוקפים פוטנציאליים יכולים לנקוט מדיניות של "הכחשה אמינה" (plausible deniability), שתנטרל את הקהילה הבינלאומית ותצמצם את טווח התמרון של המותקף. ניתן להסיק את הייחוס מההקשר הבינלאומי.[45] עם זאת, הדבר אינו שקול ליצירת "אקדח מעשן" באופן שאינו ניתן לסתירה, הדרוש כדי לשלב תמיכה דיפלומטית עם תמיכה צבאית חיצונית, בייחוד לנוכח הכשלים המודיעיניים שהובילו לפלישה לעיראק ב־2003. בנוסף, אפילו ההקשר הבינלאומי עלול להיות עמום. מאז ה־BrainVirus ב־1986, שהדביק דיסקטים דיגיטליים בכל העולם טרום עידן האינטרנט,[46] מרבית ההידבקויות בתוכנות זדוניות היו כלל־עולמיות בטבען. כל המכונות שמדברות בשפה הדיגיטלית רגישות להידבקויות דיגיטליות. למרות שעל סטקסנט נאמר שכוון ספציפית למתקני העשרת הגרעין באיראן, הוא נמצא גם בהודו, בסין, ברוסיה ובארצות־הברית.[47] דבר זה מקל עוד יותר על התוקף לאמץ את עמדת ההכחשה האמינה – גם הוא קורבן.

אי־הכרה בסף ברור מערערת מאוד את היציבות. בעבודתו הקלאסית על מלחמות "Arms and Influence" מציין שלינג את חשיבות הצבת סף בניסוח "סגנון המלחמה"[48] (idiom of war). שלינג מדגיש שעל מנת שהספים יבנו בצורה יעילה את הדיאלוג באווירה האלימה של המלחמה, עליהם להיות "פשוטים, ניתנים לזיהוי ובולטים".[49] לדוגמה, חצייה של נהר או הר, או תנועת כוחות צבא.

השאלה הופכת קריטית, שכן החישוב שמבצע כל שחקן תלוי ב"עקומת האמינות"[50] של כל משתתף – כלומר, בסיכונים שכל מדינה קיבלה על עצמה בעימות, בין אם מרצונה החופשי או מתוך אילוץ שכפה עליה היריב. סיכונים אלה תחומים באותם גבולות שהוזכרו לעיל. הם ממוקמים בתוך מערך היררכי, המארגן בצורה אמינה את שיטת הפעולה המקובלת על הממשלה. ההנחה שיש מידתיות שקשורה למערך ההיררכי היא המפתח לאמינות זו. הנחה זו מאפשרת את השליטה בדיאלוג האלים. אם חלה טעות בהבנת עקומת האמינות של היריב, נוצרת תפיסה של "חוסר איזון בפתרון",[51] שעלולה להכניס את העימות לסחרור.

לדוגמה, מדיניות הנקמה המסיבית לפי מסמך NSC-162/2 הוגדרה על ידי ויליאם קאופמן כחסרת אמינות, משום שיהיה זה 'לא על פי מנהגה של ארצות־הברית' לבצע אותה.[52] מנגד, כפי שזיהו זאגארה וקילגור בעבודתם על 'תיאוריית ההרתעה המושלמת', אמינות ההרתעה הגרעינית טמונה במתן העדפה לנקמה

על פני נסיגה.[53] העדפה זו נשענת על קיומו של איום סביר (במיוחד מכה שנייה של השורדים), אך גם על חישוב מושכל של נקמה: העדפה מושכלת כזו מייצרת אמינות. לדוגמה, אם הפגיעה היא במקום קדוש במדינה, במיוחד במרכזי האוכלוסייה שלה, ואם מדינה זו יכולה להגיב במכת נגד ועדיין לגרום נזק משמעותי לתוקף, אזי קיימת סבירות גבוהה שתעשה כך. הסיכון הגבוה משנה את חישוב התגמול. במצב כזה, המדינה תוכל לנייד משאבים פנימיים ביתר קלות, הודות ללכידות וקונצנזוס לאומי. האפשרות של תגובה חריפה יותר הופכת אמינה. ואכן בתחילת עידן הגרעין, לידל הארט ציין כי "קורבנות של תוקפנות מונעים מדחף בלתי־נשלט להגיב במכת נגד ללא קשר להשלכות [...]", ולכן "התוקף יהסס להפעיל פצצות אטום" בשל הסבירות לנקמה.[54]

כאן טמון קושי נוסף בהקשר של מתקפות סייבר: הן אינן מציעות אפיון פשוט, ניתן לזיהוי ובולט של הסף הנחצה. האם קשיים מסוימים בבנקאות מקוונת יובילו לפניקה פיננסית ולאסון כלכלי? ואם כן, בכמה שעות, ימים או שבועות מדובר? אם בעיר הבירה של המדינה המותקפת יש הפסקת חשמל, כמה אנשים עתידים למות תוך יום אחד? כאשר הייתה הפסקת חשמל בחוף המזרחי של ארצות־הברית במשך יותר מ־52 שעות ב־2003, ההשפעות היו מזעריות למדי, אם כי לא ניתן להתעלם מהן.[55] הפגיעה לאורך זמן אינה מתפתחת בהכרח בקו ישר. הקשיים נובעים גם מהיעדר תקדימים לשימוש בנשק המתפתח בהתמדה. עצם הפלישה ללא הרשאה של חיל אוויר זר למרחב האווירי של מדינה אחרת מהווה הפרה של הריבונות, אולם מה לגבי מתקפות סייבר שפוגעות שוב ושוב בשרתים שמשמשים חברות במדינה, אך ממוקמים מחוץ לגבולותיה? לבסוף, הפגיעות עשויות להיגרם מפעולות לא־ישירות או פסיכולוגיות. לדוגמה, בעצם החדרת ספקות באשר לשימוש הבטוח ביכולות צבאיות או אזרחיות, נשק סייבר יכול לעורר שיתוק גם אם לא חולל זאת ישירות. האם דומה הדבר לשיתוק שהוא תוצאה של פגיעה ישירה?

אפשר לנתח את ההשלכות על יציבות מתוך (1) היעדר ייחוס ו־(2) היעדר סף ברור באמצעות תיאוריית 'ההרתעה המושלמת'.[56] תיאוריה זו מניחה שעל מנת שאיום יהיה מרתיע, הוא חייב להציג מסוגלות: השימוש בו חייב ליצור פגיעה כואבת משמעותית לצד המאוים, כלומר, הצד המאוים יעדיף שלא לספוג אותה. האיום חייב גם להיות אמין: הצד המאיים חייב להיתפס כמי שמעדיף לממש את האיום על פני נסיגה. עם זאת, ללא חתימה, איום ההרתעה אינו כשיר עוד: הצד המאוים אינו יודע במי לנקום. התוקף החסוי אינו מאוים. גם הצד המתגונן אינו אמין אם הוא מאיים לפגוע "בהכול ובכולם" בתגובה למתקפות ממקור לא ידוע. באותה מידה, אם מזוהה ייחוס אולם קשה לאמוד את הפגיעה ולא ניתן להצביע על הסף שנחצה, אזי הנקמה לא תהיה "מידתית", אלא קשה מדיי או קלה מדיי.

ברמת המאקרו יש הסכמה גם בספרות העוסקת באסטרטגיה, כי אסימטריה או פערים במידע הזמין לכל אחד מהצדדים (מי תוקף? מה מותקף?) יובילו לעימות. כניסה לסחרור נחשבת כנובעת משגיאות בהערכה, או כפי שמנסחים זאת זאגארה וקילגור: "[...] אי־ודאות אסטרטגית ותגובה בלתי־צפויה, כאשר שתיהן יכולות להיות בעיקר תוצאה של טעויות שמקורן בכשל מודיעיני, בלבול בירוקרטי, חישוב שגוי או כל ליקוי אחר, בין אם בחשיבה ובין אם באיסוף המידע".[57] הסיכונים של כניסה לסחרור יגברו אם המדינות יגיבו במתקפות שמטרתן ליצור מידע כוזב במערכת של היריב. ניתן לראות גם במלחמה תהליך שנועד לפתור בעיית מידע: מה עוצמת המכה שמדינה יכולה להנחית על היריב?[58] התשובה לשאלה זו תאפשר יצירת סדר היררכי של המדינות. היררכיה זו תשמש מערכת מיקוח מסודרת ומובנת לכול. דבר זה מסביר כיצד הסיכוי למלחמה גובר כאשר שתי המדינות היריבות מחזיקות בעוצמה דומה, בהשוואה למצב פחות שוויוני (שאז תוצאת העימות ברורה).[59] עם זאת, שיטת הפעולה של לוחמת סייבר היא יצירת בלבול בנתונים. אופן פעולה זה מאיים לפגוע במידע אסטרטגי, ולחולל אי־ודאות וסיכונים שיערערו את הסטטוס קוו.

היעדר המחשה אמיתית ובקנה־מידה גדול של מתקפות סייבר הוא אחד הגורמים שהגביל עד כה את סיכון הסחרור. היכולת לפגוע בסוג כזה של נשק אינה ברורה כמו במקרה של נשק קינטי או גרעיני. עם זאת, היכולת של תולעת סטקסנט וההפנמה המתמשכת ש"התוכנה אוכלת את העולם" גם יחד הובילו לאחרונה מעצמות עולמיות להיות חשופות יותר לסיכונים מסוג הנשק החדש. התפיסות אכן משתנות בעקבות שינויים בשטח ושינויים בהכרזות הפומביות. המסגרות הפסיכולוגיות המעורבות במשחק, על פי ג'רוויס ועל פי תיאוריית 'ההרתעה המושלמת', הופכות רלוונטיות לסביבה גאו־פוליטית שנתונה להשפעה מתגברת של נשק סייבר.

סיכום – הצורך בדוקטרינות של "בקרת הסלמה" בהגנת סייבר

אין סיבה להאמין שה"דיפלומטיה של האלימות"[60] – כפי שמנסח שלינג את התעוררות תופעת הלוחמה – עתידה להיעלם במקביל להיטמעות הציוויליזציה שלנו במרחב הסייבר. בזמן בועת האינטרנט של שנות התשעים הראה מייקל פורטר כיצד "הכלכלה החדשה" של האינטרנט עשויה להדגיש סוגים מסוימים של יתרונות עלות על פני אחרים בחיפוש אחר בידול תחרותי[61]; אולם אין זה אומר שהכללים הישנים של האסטרטגיה ייעלמו. להיפך, המנצחים יהיו אלה שיצליחו "לראות באינטרנט השלמה לדרכים המסורתיות של התחרות ולא חלופה להן".[62] באופן דומה, "הכוח להכאיב" מגולם במלואו בסייבר – אבל אינו מחליף את כללי

האסטרטגיה. כפי שמציג זאת ג'ון שלדון, ניתן לבחון את עוצמת הסייבר דרך הממדים הקלאסיים של האסטרטגיה, כפי שהציגו מייקל הוארד וקולין ס. גריי.[63]

טכנולוגיות חדשות אינן מבטלות את סיכוני הסחרור בלוחמה. בקצרה, הדבר תלוי בהשפעות של כל טכנולוגיה על הגורמים הבלתי־משתנים המעוררים לוחמה כוללת: התפיסה שיכולות צבאיות אסטרטגיות נוטות לטובת התוקף, האפשרות שיכולות הצבא המתגונן ישמשו גם הן לתקיפה, מצב כניסה מהירה לפעולה שיקצר את משך ה"משחק" הצבאי, קצב מהיר של שינוי טכנולוגי שיש לו פוטנציאל להפר מחדש את האיזון בין כוחות הצבא (או זו לפחות התפיסה). עוצמתם של גורמים אלה היא שתשפיע על יכולת האיום והאמינות של כל שחקן, וכך תשנה את ההרתעה שבבסיס היחסים בין השחקנים. בסופו של דבר, ניתן לסכם את שאלת מאזן האימה כבעיית מידע: האם זיהיתי במדויק את היכולות האמיתיות של האויב – ושל עצמי? האם האויב יכול להבין את כוונותיי? היכן עוברים הקווים האדומים שלי – והאם אני מבין היכן עוברים הקווים האדומים שלו?

בשל כל השיקולים הללו, ובייחוד עקב היכולת להשחית נתונים ומידע אסטרטגי, נשק סייבר מגביר את הסיכון לכך ששגיאות מידע יסלימו מצב משבר לכדי מלחמה כוללת. הדיון שלעיל על (1) היעדר ייחוס ו־(2) היעדר סף ברור מסייע להסביר מדוע סיכון זה מתממש בצורה כה ברורה בנשק סייבר. יתרה מכך, הפתרון לשתי הסוגיות הופך דוחק אפילו יותר בשל טבעו של המשחק, שמתקצר בעקבות טכנולוגיה שעובדת במהירות האור ונתפסת כמגמה התקפית. כל אלה רק מדגישים עד כמה חיוני הצורך בדוקטרינה שתנהל את משבר המידע. לכן, דוקטרינה ליציבות הסייבר לא תתבסס אך ורק על היכולות לפעולת תגמול – כמו לדוגמה היכולת למכה שנייה מוכחת של השורדים, שנמצאת בלב ההרתעה הגרעינית, אלא, באותה מידה של חשיבות, היא תתבסס על היכולות להשיג בהירות ברמה האסטרטגית. אם לא ניתן לבסס את האמת לגבי הערכת הנזק והייחוס, אזי הצד המתגונן נמצא בסיכון לאחד מהשניים – להודות בתבוסה (אבל בפני מי?) או להיכנס לפעולת תגמול כשהוא "מגשש באפלה", תוך סיכון גבוה לסחרור העימות. לעומת זאת, אם מושגת ידיעת אמת ברורה, לפחות ב"חוֹשבה" של מקבלי ההחלטות האסטרטגיות ואולי אף בכל שאר מערכות התוכנה והחומרה של הצד המתגונן, אזי הצד המתגונן יוכל לפחות לעשות שימוש בכל שאר האופציות המסורתיות שברשותו, מאיומים דיפלומטיים ועד אסטרטגיים, על מנת לאלץ בצורה משכנעת את התוקף לסגת. ההקבלה ליעדי חיפוש האמת בקרב שירותי המודיעין אינה אמורה להפתיע. אם בסייבר, כמו במודיעין, "האמת משחררת",[64] הרי זה בין היתר משום ששניהם פועלים בתחומים אינפורמטיביים – האחד מבוסס על פורמט דיגיטלי והשני מבוסס על "חשאיות".[65]

קווי מתאר כאלה לדוקטרינות להגנת סייבר עשויים להיות דומים לאלה של פעולות הבהרה כגון חקירות משטרה או ריגול נגדי, אם כי בהובלת דרג אסטרטגי – כמו ראש מדינה. חקירות אלה ייתמכו ביכולות טכניות ניכרות ויפעלו לפי מתודולוגיות חדשניות לחיפוש האמת, החל מבדיקה דדוקטיבית לייחוס ועד סימולציית מערכות להערכת קווים אדומים. כמו כן, יהיה בהן מרכיב דיפלומטי משמעותי שימנף כמה מעגלים של שיתופי פעולה הדוקים. לא ניתן להגיע לאמת באמצעות מרכז אחד בלבד. מדובר בתהליך חברתי המבוסס על שיתוף בנתונים התומכים במסקנות ובשקילה זהירה של האילוצים הקיימים על פי ההקשר המודיעיני, או בהתבססות על היכולת לשכפל ניסויים.[66] מבחינה זו, דוקטרינות הגנה צבאיות למרחב הסייבר מקבילות במידה מסוימת לדרך שנקטו לאחרונה הנהלות תאגידים, משיווק[67] עד משאבי אנוש:[68] כזו שמאמצת גישה של פיקוח ומדע לפתרון בעיות. זוהי הדרך הבטוחה ביותר להגיע למקום הטוב ביותר בממלכת המידע: לאמת.

הערות

1 מאמר זה בוחן את הסיכונים האסטרטגים של נשק סייבר ואת הנחיצות לפתח דוקטרינות ייחודיות להגנת סייבר, כדי לקזז את הסיכון של הסלמת משבר עד כדי יציאה מכלל שליטה. פירוט דוקטרינות אלה הוא מעבר להיקף הדיון של המאמר הנוכחי. במאמר שייצא בקרוב אבחן כמה מהפתרונות לבעיות היציבות שיוצגו כאן.

2 David E. Sanger and Thom Shanker , "Broad Powers Seen for Obama in Cyberstrikes", *New York Times*, February 3, 2012.

3 Luis Martinez, Intel Heads Now Fear Cyber Attack More Than Terror, *ABCNews*, March 13, 2013, http://abcnews.go.com/Blotter/intel-heads-now-fear-cyber-attack-terror/story?id=18719593

4 Despite austerity cuts, the UK's cybersecurity budget has been expected to grow by some £650m ($1.07bn) over the 2012-2015 period. In James Blitz,"Country profile: UK defences are boosted to fight e-crime", *Financial Times*, June 2, 2011.

5 Keith B. Alexander, "Warfighting in Cyberspace", *Joint Forces Quarterly*, 46, 3rd quarter (2007): pp. 58-61.

6 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): pp. 325-340.

7 שם.

8 Bernard Brodie, "The development of nuclear strategy", *International Security*, 2, No.4, (1978): pp. 65-83.

9 Lawrence Freedman, *The Evolution of Nuclear Strategy, Third Edition*, (New York: Palgrave Macmillan, 2003), pp.234-236.

10 שם, עמ' 243–244.

11 ראו לדוגמה: Lawrence Freedman (2003), p. 338

12 ראו ריאיון עם ג'ון האמר, לשעבר סגן שר ההגנה בין השנים 1997 ל־1999, בתוך: Michael Kirk, "Cyberwar!", *PBS*, April 24, 2003.

http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hamre.html

13 "Estonia hit by 'Moscow cyber war'", *BBC News*, May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm.

14 Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back", *New York Times*, October 23, 2012.

15 Michael N. Schmitt, Gen. ed.,*Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).

16 Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem", in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington D.C.: National Defense University Press,2009), pp.26-28.

17 שגיאות אנוש בתצורת האבטחה זוהו כ"אחראיות ל־80% מהפגיעויות של חיל האוויר" James A. Lewis ed., *Securing Cyberspace for the 44th Presidency,* Center for Strategic and International Studies, 2008, p. 55. צמיחתה של ההנדסה החברתית ומתקפות 'פישינג' הדגישו את חשיבות "הגורם האנושי" באבטחת סייבר. קווין מנדיה מציין: "בעוד הדורות הקודמים של המתקפות כיוונו לטכנולוגיה כמו רשתות ושרתים וניצלו פגיעויות בתוכנה, כיום התוקפים התפתחו והם מכוונים לחולשות ולליקויים אנושיים" בתוך: Kevin Mandia, "Cyber threats and ongoing efforts to protect the Nation", *Permanent Select committee on Intelligence, US House of Representatives*, October 4, 2011.

18 Martin Hilbert, Priscila Lopez, "The World's Technological Capacity to Store, communicate and compute information", *Science,* 332, no. 6025 (2011):60-65.

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

20 Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, *A Brief History of the Internet* (The Internet Society, 2012). ,http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

21 David A. Fulghum, "Why Syria's Air Defenses Failed to Detect Israelis", *Aviation Week & Space Technology*, October 3,2007.

David A. Fulghum, "Israel used electronic attack in air strike against Syrian : וכן mystery target", *Aviation Week & Space Technology*, October 8, 2007.

22 Nicolas Falliere, Liam O Murchu, Eric Chien, *W32. Stuxnet Dossier*, (Symantec, 2010).

23 Barbara Cassin, CNRS, "Logos et Polis: La force du Discours", in Catherine Golliau ed., *La Sagesse Grecque* (Paris : Le Point Référence, 2011), p.41-43

24 William Gibson, *Neuromancer* (New York: Ace Science Fiction, 1984)

25 See for example the issue of kill switch in chips in Sally Adlee, "the hunt for the kill switch", *IEEE Spectrum*, May 1st, 2008.

26 For example, according to David Sanger (New York Times), when Israel and the US developed a "bug" to derail nuclear enrichment operations at Natanz plant in Iran, research teams "[…]began building replicas of Iran's P-1 centrifuges[…]" since "the bug needed to be tested". See David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran", *New York Times*, June 1, 2012. In particular, the Dimona complex in Israel may serve as a testing ground for cyber-attacks of centrifuges- see

William J. Broad, John Markoff & David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *New York Times*, January 15, 2011.

27 The issue of cyber-attacks attribution is a major difficulty explored in fiction (see for example, Guy-philippe Goldstein, *Babel Minute Zero* (Paris: Denoel,2007) and illustrated in real life episodes such as the cyber-attacks against Estonia in 2007 - see Mikko Hypponen,"9thof May", *F-Secure Weblog*, February 15, 2010, http://www.f-secure.com/weblog/archives/archive-052007.html

28 .Robert Jervis, "The Security Dilemma", *World Politics,* 1978, pp. 187.

29 לדיון מפורט ראו: Charles L. Glaser and Chaim Kaufmann, "What is the Offense-Defense Balance and Can We Measure it?", *International Security*, Vol. 22, No. 4 (Spring, 1998), pp. 44-82.

30 Jervis (1978), p. 190.

31 ב־2009 הציג גרגורי ג'יי. רטריי את הנושא של "דומיננטיות המתקפה" במרחב הסייבר: ראו Gregory J. Rattray, "an environmental approach to understanding cyberpower" in F. Kramer, S. Starr, L. Wentz, "*Cyberpower and National Security*", National Defense University, Potomac Books, 2009. שלוש שנים לאחר מכן, דיויד טי. פרנקרוג מהמשרד להערכת נושאי רשת/משרד ההגנה, ציין כי "ההנחה הנוכחית היא כי בסייבר לתוקף יש את היתרון המוחלט" David T. Fahrenkrug, "Countering the Offensive Advantage in Cyberspace: an Integrated Defensive Strategy", 2012 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn.

32 תוכניות פיתוח צבאי חדשות שהושקו ב־2012 הן עבור DARPA והן עבור חיל האוויר האמריקאי מצביעות על עניין ברור בנשק התקפי, בתוך: Tom Gjelten, "First Strike: US Cyber Warriors Seize the Offensive", *World Affairs*, January-February 2013. בנוסף, במרס 2013, "[...]גנרל קית' אלכסנדר, שעומד בראש הסוכנות האמריקנית לביטחון לאומי ומפקדת הסייבר, העיד בפני המחוקק שהצבא הקים לפחות 13 יחידות שיהיו להן יכולות התקפיות בסייבר". "Obama Calls China Cyber Attacks 'State Sponsored'", News Wires, March 13, 2013). בצרפת, הפרויקט "Livre Blanc" לשנת 2013 ציין את הצורך ב־"Lutte Informatique Offensive") LIO או "לוחמת סייבר התקפית" (בתוך Vincent Lamigeon, "Livre Blanc de la Defense: Les 5 nouvelles priorités imposes à l'armée francaise", Challenges, April 29, 2013).

33 ראו: Thomas K. Longstreth and Richard A. Scribner, "*Verifications of Limits on Air Launched Cruise Missiles*", in Frank von Hippel and Roald Z. Sagdeev, eds., *Reversing the Arms Race: How to Achieve and Verify Deep Reductions in the Nuclear Arsenals* (New York: Gordon and Breach, 1990), pp. 185

34 לסקירה אמריקאית קצרה ביותר, ראו: Zachary Fryer-Biggs, "Building Better Cyber Red Teams", *Defense News*, June 14, 2012.

35 Frank C. Zagare, "The *Dynamics of deterrence*", University of Chicago Press, 1987 – see discussion on rules relaxation and lengthening the game, pp. 48-56.

36 Thomas C. Schelling, "The Strategy of Conflict", Harvard University Press, 1960, Chap. IX, "The Reciprocal fear of surprise attack".

37 Thomas C. Schelling, "*Arms and Influence*", Yale University Press, 1966, pp. 225.

38 ראו: David S. Fadok, Major, USAF, "John Boyd and John Warden: Air Power's Quest for Strategic Paralysis", School of Advanced Air Power Studies, 1995, pp. 49. שנה קודם לכן כבר ציין ג'ון וורדן כי "לכידה וניצול של ספֵרת הנתונים עתידה להיות המאמץ החשוב ביותר ברוב המלחמות העתידיות". כיבוש 'ספֵרת הנתונים' (datasphere) מוגדר כעדיפות להצלחה צבאית, ראו: Col. John A. Warden III, USAF,

"Air Theory for the Twenty-first Century", Chap. 4, in Challenge and Response: Anticipating U.S. Military Security Concerns, ed. Karl P. Magyar, Maxwell AFB, Ala., Air University Press, August 1994.

39 ראו: Keith L. Shimko, "The *Iraq Wars and America's Military Revolution*", Cambridge University Press, p. 129.

40 Henry Kissinger, 'Arms control, inspection and surprise attack', *Foreign Affairs*, xxxviii:3 (April 1961), pp. 370.

41 Carey B. Joynt, Percy E. Corbett, "Theory and Reality in World Politics", Macmillan Press, London, 1978, pp. 92-93.

42 Michael Horowitz, "Information Age Weaponry and the Future Shape of Security in East Asia", *Global Asia*, Vol. 6, Summer 2011.

43 בנושא בכירי ממשל אמריקאיים שמתלבטים בפומבי בסוגיית הייחוס, ראו: John Markoff, David E. Sanger, Thom Shanker, "In Digital Combat, U.S. Finds no easy deterrent", *New York Times*, January 26, 2010; David E. Sanger, Elisabeth Bumiller, "Pentagon to consider cyberattacks acts of war", *New York Times*, May 31, 2011.

44 דוגמה עדכנית – לאחר שדרום־קוריאה התמודדה עם קריסה בו־זמנית של רשתות מחשבים בכמה מהמשדרים והבנקים מרכזיים ב־20 במרס 2013, היא טענה תחילה שמתקפות הסייבר הגיעו מסין Warwick Ashford, "South Korea says cyber attack came from IP address in China", *Computer Weekly*, March 21, 2013. למחרת הודתה דרום־קוריאה בטעות Warwick Ashford, "South Korea admits mistake in linking cyber attacks to China", *Computer Weekly*, March 22, 2013. שלושה שבועות לאחר מכן, האשימה דרום־קוריאה את צפון־קוריאה Warwick Ashford, "South Korea accuses North Korea of launching cyber attacks", *Computer Weekly*, April 11, 2013.

45 לתזה שממזערת את "בעיית הייחוס" באמצעות ניתוח ההקשר הבינלאומי, ראו: Richard L. Kugler, *Deterrence of Cyber Attacks*, Chapter 13, in F. Kramer, S. Starr, L. Wentz, *Cyberpower and National Security*, National Defense University, Potomac Books, 2009.

46 Rupert Goodwins, "Ten Computer viruses that changed the world", *ZDNet*, August 3, 2011.

47 Nicolas Falliere, Liam O Murchu, Eric Chien, W32. Stuxnet Dossier, Symantec, November 2010, pp. 6; Chinese infections in "Stuxnet 'cyber superweapon' moves to China", AFP, September 30, 2010.

48 Thomas C. Schelling, "Arms and Influence", Yale University Press, 1966, pp. 135: "שלבים סופיים בהתפתחות מלחמה או שינוי בהשתתפות. אלה קווי גבול או מקומות עצירה מוסכמים. יש להם אופי חוקי והם תלויים בתקדימים או בהשוואה למקרים דומים. יש להם תכונות שמאפשרות לזהות אותם, והם שרירותיים בחלקם. [...]אנו לא מייצרים אותם או ממציאים אותם, רק מכירים בהם. [...] נראה שכל סוג של עימות מרוסן זקוק לריסון ייחודי ששני הצדדים יכירו בו – נקודות עצירה בולטות, מוסכמות ותקדימים לציון מה נמצא בגבולות ומה מחוץ להם, דרכים להבחין מתי מדובר ביוזמה חדשה ומתי בפעילות שגרתית".

49 Thomas C. Schelling, "*Arms and Influence*", Yale University Press, 1966, pp. 137.

50 ראו: Carey B. Joynt, Percey E. Corbett, *Theory and reality in world politics*, University of Pittsburgh Press (Pittsburgh), 1978, pp. 94-95.

51 ראו: Frank C. Zagare, D.Marc Kilgour, *Perfect Deterrence*, Cambridge studies in international relations, 2000, pp. 301.

52 ראו: Freedman, 2003, p. 96 - citing William Kaufman, Military Policy and National Security, Princeton University Press, 1956, pp. 21, 24-25.

53 Zagare, Marc Kilgour, 2000, chapter 3.

54 ראו: Freedman, 2003 p. 40 citing B. M. Liddell Hart, *The Revolution in Warfare*, London: Faber and Faber, 1946 pp. 85-6.

55 במהלך הפסקת החשמל הגדולה בעיר ניו־יורק חלה עלייה גדולה במקרי התקפי הלב ובעיות נשימה, וכן נרשמו קריאות נוספות לשירותי רפואת החירום (Gary Kalkut, MD, MPH, Effects of the August 2003 blackout on the New York City healthcare delivery system: a lesson for disaster preparedness, Critical Care Medicine, January 2005, Volume 33, Issue 1, pp. S96-S101). לפי דיווחים מהעיתונות שצוטטו בוויקיפדיה, נמנו 11 קורבנות לא־ישירים.
http://en.wikipedia.org/wiki/Northeast_Blackout_of_2003;
עם זאת, מחקר נוסף מציין כי "דווח על מספר מינימלי של מקרי תחלואה ומוות שניתן לייחס לאירוע (בתוך: Kile J, Skowronski S, Miller MD, Reissman SG, Balaban V, Klomp RW,Reissman DB, Mainzer HM, Dannenberg AL: "Impact of 2003 Power Outages on Public Health and Emergency Response", *Pre-hospital and Disaster Medicine* 2005, 20(2), pp. 93-97. ההערכות של סך העלויות בארצות־הברית נעו בין 4 ל־10 מיליארד דולר, או כמעט 0.1% מהתמ"ג האמריקאי, ראו: U.S.-Canada Power System Outage Task Force, August 14th Blackout: Causes and Recommendations, 2004, p.1

56 Frank C. Zagare, D.Marc Kilgour, *Perfect Deterrence*, Cambridge studies in international relations, 2000.

57 Frank C. Zagare, D.Marc Kilgour, *Perfect Deterrence*, Cambridge studies in international relations, 2000, pp. 302.

58 במילים אחרות, אם מדינות היו יודעות את התוצאה של מלחמה אפשרית, וכל אחת מהן הייתה מחזיקה במידע מושלם על היכולות וההחלטות של השנייה, סביר שהן היו נמנעות ממלחמה. ראו: Fearon, James D. 1995. Rationalist Explanations for War. *International Organization* 49 (Summer), pp. 379-414. and Dan Reiter, "Exploring the bargaining model of war", *Perspectives on politics,* Vol. 1, No. 1, March 2003.

59 Stephen L. Quackenbush, "General Deterrence and International Conflict: Testing Perfect Deterrence Theory", *International Interactions*, Vol. 36, pp. 60-85, 2010.

60 Schelling, 1966, Chap 1.

61 Michael Porter, "Strategy and the Internet", *Harvard Business Review*, March 2001.

62 שם.

63 John B. Sheldon, "The Dimensions of Strategy for Conceptualizing Cyberpower: Laying the Foundations for Sensible Cyber Security Policy and Doctrine", Presented to the panel on 'Comparative Cyber Security Strategies: Theory and Practice' International Studies Association Conference, San Diego, 2012.

64 מתוך Gospel according to St.John, נחקק במקור על חזית בניין ה־CIA – ראו: https://www.cia.gov/news-information/featured-story-archive/ohb-50th-anniversary.html

65 Dr. Michael Warner, "Wanted: a definition of intelligence", *Studies in Intelligence*, Volume 46, No. 3, 2002, pp. 20-21.

66 שיתוף נתונים הוא דרישת בסיס בכל הגשת מאמר לכתב־עת עם ביקורת עמיתים (ראו לדוגמה את ההמלצות עבור המגזין Nature בקישור /http://www.nature.com/authors

policies/availability.html); אין ספק שבנושאי מודיעין, שיתוף חייב לאזן את הרווח עם הסיכונים מהחשיפה – או כפי שראש המודיעין הלאומי ג׳יימס ר. קלאפר מכנה זאת, הצורך למצוא את "הנקודה הרכה" בין שיתוף להגנה על מידע. ראו: Remarks and Q & A by Director of National Intelligence, Mr. James Clapper, 2010 Geospatial Intelligence Symposium, New Orleans, Louisiana, November 2, 2010, quoted in Richard A. Bets Jr., *Intelligence Information: Need-to-Know vs. Need-to-Share*, Congressional Research Services, June 6, 2011.

67 ראו את ההשפעה של A/B Testing בהנהלת חברות הסטארט־אפ של עמק הסיליקון ועד גוגל, בתוך:
Brian Christian, "The A/B Test: Inside the Technology That's Changing the Rules of Business", *Wired*, April 25, 2012.

68 ראו: Steve Lohr, "Big Data, Trying to Build Better Workers",*New-York Times*, April 20, 2013.