השימושים האסטרטגיים בעמימות במרחב הקיברנטי

מרטין ס׳ ליביקי

לעמימות אסטרטגית שמור מקום של כבוד במוסכמות המדינאות. חוסר הנכונות המכוונת של מדינות להצהיר על מעשיהן (או על מה שבכוונתן לעשות), בצד העדר הוכחה שהן עשו זאת משחררת מדינות אחרות. הן יכולות לטעון כי משהו נעשה, אך אם צורכיהן מכתיבים זאת, באפשרותן להעמיד פנים כי הדבר לא נעשה. דרגת הספק עשויה להשתנות: מספק מוחלט (איש אינו יודע מה קרה או מה עתיד לקרות) לספק קטן מאוד (לא ״עובדים״ על אף אחד). עם זאת, בכל אחד מהמקרים, מבצעי המעשה סיפקו עלה תאנה, שקוף ככל שיהיה, שמדינות אחרות יכולות לאמץ.

דוגמאות לעמימות אסטרטגית במרחב הפיזי

דוגמה אחת שכבר שנים שמור לה מקום של כבוד, היא סירובה של ישראל להודות (או להכחיש) שהיא מחזיקה בנשק גרעיני. לא יימצא פרשן ראוי לשמו המאמין באמת ובתמים שישראל אינה מחזיקה בנשק גרעיני. אך מאחר שישראל מעולם לא הצהירה שברשותה נשק גרעיני, מדינות אחרות חופשיות להעמיד פנים שישראל לא ׳חצתה את הגבול׳ בתחום הגרעיני. מצב זה נוח למדינות שיהיו נתונות ללחץ של בני עמם להגיב בתוכניות גרעין משלהן במקרה שהמעמד הגרעיני של ישראל יֵצא לאור. מצב זה גם מסייע למדינות שלא היו יכולות לייצא פריטים מסוימים לישראל לו מעמדה הגרעיני היה גלוי יותר.[1] עם זאת, אין אף מדינה המתנהגת כאילו אין לישראל יכולת תגובה גרעינית.

עמימות דומה נוגעת לשימוש המשוער שעושה ארצות־הברית בכטב״מ (כלי טיס בלתי מאוישים) מסוג ״פרדטור״ ובטילי שיוט כדי לפגוע באנשי אל־קאעדה במדינות כמו תימן או פקיסטן. המדיניות הרשמית היא להכחיש את קיומן של טיסות כגון אלה. מנהיג תימן טען, שאלה היו מבצעים של תימן, מה שנשמע לא

ד״ר מרטין ליביקי הוא מדען חבר בצוות הניהול הבכיר במכון ראנד, קליפורניה, ארצות הברית.

סביר, ורק פרשנים בודדים נפלו בפח והאמינו לטענות אלה. ואולם לפחות עד לאחרונה לא הודו ראשי המדינות האמורות בתקיפות שהתרחשו בשטחן, וכך לא נאלצו להתמודד עם הטענה בדבר פגיעה בריבונותן.

דוגמה אחרת היא מדיניות ארצות־הברית כלפי עצמאותה של טייוואן. ארצות־הברית הצהירה שהיא מתנגדת להכרזת עצמאותה של טייוואן וכן לכל ניסיון ליישב את עניין מעמדה של טיוואן בכוח. ארצות־הברית אינה מכירה בטייוואן כמדינה, ולפיכך אין לה הסכם סיוע הדדי איתה. לכן, נשאלת השאלה: האם במקרה שטיוואן תכריז על עצמאות וסין תחליט לכבוש את האי, ארצות הברית תתערב לטובתה של טייוואן? ברור שהאינטרס המובהק של ארצות־הברית הוא שסין תחשוב שזה אכן המצב כדי שלא תפתח במלחמה, וכמעט ודאי שהאינטרס של ארצות־הברית הוא, שגם טייוואן תחשוב שזהו המצב כדי שהיא עצמה לא תעודד את סין לפתוח במלחמה. הבה נניח שהסיכויים של התערבות ארצות־הברית משולים, פשוטו כמשמעו, להטלת מטבע, ונתפסים כך משני צדי המצָרים. בהתאם לכך, טייוואן עשויה להגיע למסקנה, שהערך הצפוי מהכרזת עצמאות הוא שלילי (הוא היה עשוי להיות חיובי אילו ידעה בוודאות שארצות־הברית תחוש לעזרתה) מאחר שארצות־הברית עשויה לא להתערב. בדומה לכך סין משיקולים שלה, עשויה להגיע למסקנה, שהערך הצפוי מפלישה וחציית המצָרים עלול להיות שלילי מכיוון שארצות־הברית עלולה לפעול. כל אפשרות עמומה פחות מזו עלולה לעודד צד זה או אחר לנקוט צעד טיפשי.

המרחב הקיברנטי מתאים לעמימות

מלחמה קיברנטית היא חשאית במהותה. כאשר פורצי מחשבים חודרים למערכת מחשב כדי לשבש את פעולתה, התוצאות הישירות הן על־פי־רוב בלתי נראות לעולם החיצוני. בהתאם לדרגת השיבוש במערכות האלה, גם התוצאות העקיפות עשויות להיות בלתי נראות לעין. תוצאות של מתקפת סייבר על רשת חשמל, הגורמת לכיבוי האורות, ניתנת לצפייה אפילו מהחלל; אבל בהעדר המשך חקירה וגילוי, לא יהיה ברור אם ההאפלה היא פועל יוצא של התקפה מכוונת, או של טעות אנוש, תוכנה לקויה, או (לעתים קרובות) של הטבע עצמו. גם אם יתברר שמערכת השתבשה בגלל התקפה, זהות התוקף עשויה להישאר אפופה במסתורין. לבסוף, אם עצם התקפת הסייבר וזהות מחולליה היו ברורים, מטרתה עשויה להיות מעורפלת ולא ברורה – אחרי הכול, מלחמה קיברנטית לבדה אינה יכולה להרוג איש, או אפילו להרוס יותר מדי (עיין ערך תולעת הסטקסנט – Stuxnet) ועוד פחות מכך לכבוש שטח או לשנות משטר (מלחמה קיברנטית אכן יכולה לאפשר שימושים אחרים בכוח, ושימושים אחרים אלה הם המוחשיים יותר). כמעט כל הפריצות הקיברנטיות נועדו לגנוב מידע או לעשות שימוש במחשב המטרה (כמו

ברובוט), ומעבר לכך להשאיר את המערכת כמות שהיא. אפשר לעצב התקפות כניסיונות להטעות בני אדם (למשל תמונות מכ"ם מסולפות) או את הציוד שלהם (ראו על תולעת הסטקסנט). במקרים האחרונים, המובן מאליו מטבע הדברים פועל כבומרנג; משעה שברור כי הצלחת להערים על מערכת, מנהלי המערכת אינם צפויים לאפשר לה לפעול כפי שפעלה בעבר.

האם תולעת הסטקסנט היא דוגמה יוצאת דופן?

אפשר היה לשער שמתקפת סייבר אשר שיבשה דבר מה בפועל עברה את השלב שבו הכול יכולים להצניע את קיומה. תולעת הסטקסנט התגלתה בחודש יוני 2010, ובספטמבר זוהתה מטרתה – מתקן גרעיני באיראן. החשדות המוקדמים ביותר סימנו את הכור בבושהר כיעד שלה,[2] אך איראן הכחישה שהכור ספג חבלה כלשהי. בתוך כמה שבועות זוהה מפעל הצנטריפוגות בנתנז כמטרת ההתקפה. הכחשות ראשוניות של איראן הופרכו בשלהי נובמבר 2010, ביום שבו חיסלו מתנקשים שני מדעני גרעין איראנים, וכאשר הודה אחמדינג'אד שהייתה תולעת שגרמה בעיות רבות, אך אלה תוקנו.[3] מהו הנזק הממשי שהסבה תולעת הסטקסנט לפיתוח הגרעין האירני? סטטיסטיקה של סבא"א (הסוכנות הבינלאומית לאנרגיה אטומית) מלמדת, כי ייתכן שהתולעת האמורה גרמה להתבלות מוקדמת של עשרה אחוזים מהצנטריפוגות של איראן, ולפיכך הקנתה ליוצרי התולעת כמה חודשי דחייה לכל היותר בלוח הזמנים המשוער שלפיו יהיה בידי איראן די חומר גרעיני לבניית הפצצה הראשונה שלה.[4] בדיווחים אחרים מצוטטים אישים בכירים, המתנבאים (נכון לינואר 2011) שהמועד המוקדם ביותר שבו איראן תוכל להרכיב התקן כזה הוא 2015, כלומר הושג עיכוב של כמה שנים.

רב הנסתר על הגלוי בכל הקשור לתולעת הסטקסנט (למעט מה שידוע שהיא הצליחה להשיג).[5] ראשית, לא ברור איך הצליחה התולעת לחדור למפעל ב־נתנז; דומה כי חשדות ולפיהם יוצרי התולעת קיבלו סיוע ביודעין או שלא ביודעין מקבלנים רוסים חיבלו ביחסי העבודה של האיראנים עם קבלנים אלה.[6] ומה שחשוב מכך – מי כתב את התולעת ומי שחרר אותה? האם היה זה אדם מסוים (התחכום שלה מרמז על אפשרות אחרת)? האם היו אלה ישראלים – כפי שאפשר לשער מכמה רמזים בקוד המקור – אך מי יידע אם רמזים אלה לא הושתלו כדי להטעות? האם היו אלה אמריקנים? האם מדובר בשיתוף פעולה – אמריקני־ישראלי?[7] האם היו אלה הסינים?[8] לנוכח העמימות הרבה, אין פלא שאיראן טרם הגיבה על האירוע הזה. גם סוריה לא הגיבה על ההתקפה על מה שנחשד כמתקן הגרעין שלה, ועיראק לא עשתה דבר חוץ מלהתלונן לאחר שהופצץ הכור שלה באוסיראק – ובשני המקרים הללו לא הייתה שום עמימות בנוגע למְבצעים. קשריה האיתנים של איראן עם חמאס ועם חזבאללה מרמזים כי ייתכן שעמדו לרשותה

כמה דרכים – שלא עמדו לרשותן של סוריה (בשנת 2007) או של עיראק (בשנת 1981) – להביע את חוסר הנחת שלה. יתרה מכך, איראן טרם עשתה "עניין גדול" מהתקרית, ואם לאחר חודשים של שתיקה והכחשות היא תראה בכך אקט של מלחמה, יהיה בכך משום תפנית של 180 מעלות.

יתרונות השימוש בתולעת הסטקסנט במקום בכוח אווירי לצמצום יכולתה הגרעינית של איראן, ברורים למדי (בהנחה שהתולעת אכן עשתה את מה שיוצריה ציפו): השפעה דומה, זריעת חוסר אמון בקרב קורבנותיה ואי־ודאות מי מבין הספקים או הציוד עדיין סובלים משיבושי התולעת, וכל זאת במידה פחותה בהרבה של גינוי (ואולי אף בהערצה כמוסה) ובפחות סיכונים אסטרטגיים מאלה הכורכים בהפעלת כוח אווירי.

שימושי העמימות

ההשערה המוצעת היא, שהתקפת סייבר המשמשת במקום שיטות קינטיות, יוצרת עמימות רבה יותר במונחים של תוצאות, מקורות ומניעים. לפיכך אם מתקפות סייבר פועלות בהצלחה – וסימן השאלה בעניין הזה הוא גדול – הן משנות את פרופיל הסיכון של פעולות מסוימות, כך ובדרך כלל בדרכים ההופכות אותן לחלופות מתאימות יותר. להלן כמה שימושים היפותטיים של מתקפות סייבר.

א. קורבן לתוקפנות בהיקף קטן עשוי להשתמש במתקפות סייבר כדי לבטא את אי־שביעות רצונו, אך הסיכון להסלמה קטן יותר לעומת זה הכרוך בתגובה פיזית. לדוגמה, בשלהי 2010 הפציצו כוחות צפון קוריאה אי בדרום קוריאה והרגו שני אזרחים ושני אנשי צבא. תגובה בדמות מתקפת סייבר, שנועדה לשבש מתקן תעשייה חשוב (אם מתעלמים מן העובדה שצפון קוריאה אינה ממוחשבת היטב ובעלת אפס חיבורי רשת לשאר העולם) הייתה עשויה להעביר את תחושת אי־שביעות הרצון של דרום קוריאה. לו רצתה צפון קוריאה להגיב היה עליה: (1) להודות שאחד ממתקניה נפרץ; (2) לנקוט צעדים שיוכיחו כי דרום קוריאה היא האחראית הבלעדית לכך (זו עשויה להיות ארצות־הברית או אפילו יפן, ואפילו סין). לחלופין, אם צפון קוריאה לא תגיב באופן פומבי, יש לה סיכוי טוב להגביל את מספר היודעים מדוע כמה ממתקניה חדלו מלפעול. תיאור זה מציג מאפיין חשוב נוסף של מלחמה קיברנטית, המעניק לה יתרון על פני לוחמה פיזית: אף־על־פי שהיותך מותקף עשוי להוות מקור לגאווה (תוכל לגלם את דוד לעומת האויב גוליית), העובדה שפרצו למערכות שלך פירושה שנכנסת למרחב הקיברנטי בלי לתת את הדעת על הגנה של מערכותיך. קורבנוּת איננה דבר הראוי להתגאות בו. לפיכך מומלץ למדינות היכולות להסתיר את העובדה שהותקפו לעשות זאת, וכך לשמור על כבודן – אך נתיב זה גם עושה את התגובה לאפשרית פחות. פתוחה לפניהן הדרך להגיב באופן דומה, וכך מאבק של עין תחת עין שהחל בעולמות

הפיזיים, עולה (או יורד) לעולם הקיברנטי. אך נתיב זה עשוי להיות בטוח יותר בכל ההיבטים לעומת הנחתת מכות פיזיות.

ב. מדינה עשירה בלוחמי סייבר עשויה להשתמש באיום בלוחמת סייבר להרתעה מפני הפיכתה למטרה אפשרית של אויביה. לדוגמה, באפשרותה של ישראל לאיים על איראן במתקפות סייבר אם תותקף על־ידי חזבאללה, ארגון בעל קשרים מוכחים עם איראן.[9] במצב עניינים שכזה, קיימת אפשרות שישראל לא תהיה מעוניינת לפרסם ברבים את האיום הזה. איום גלוי יאפשר לחזבאללה לכפות את רצונו על איראן בטענה שהוא מעוניין לתת ביטוי לסוג הפגיעה שתניע את ישראל לתקוף את איראן במרחב המדומה. אך יש מסלולים פרטיים להעברת האיום. יש היגיון באיום שכזה. הבעיה הרווחת בכל הנוגע להרתעת סייבר היא, שהייחוס של ההתקפה הפותחת מהווה בעיה, אך במקרה של התקפה פיזית – נניח, בדמות טילים של חזבאללה המשוגרים לעבר ישראל – יהיה קל מאוד לקבוע זאת. לחילופין, אף על פי שמדינה כמו איראן אינה עשויה בהכרח לחשוש מהתקפה ישראלית ישירה גם בתגובה להתקפה של חזבאללה, (התקפות שכאלה לא התממשו בשנת 2006, למשל), היא עשויה לחשוש ממתקפת־סייבר בהתחשב בעליונות הברורה של פורצי מחשבים ישראלים על פני עמיתיהם האיראנים. עליונות שכזו ממתנת (אם כי לא מבטלת) את החשש כי לאחר שהצהירה על הכוונה לבצע מתקפת־סייבר, לא יהיו לישראל מטרות נגישות באיראן. גם אם ההצלחה של מתקפה בודדה אינה ודאית, הסיכויים כי חלק מהן יצליחו ויגרמו נזק – טובים למדי. הפניית אצבע מאשימה של איראן כלפי ארצות־הברית לאחר מכן עלולה ליצור בעיה עבור ארצות־הברית, אך לעשות חיים קלים יותר עבור ישראל. הסלמה לאלימות איננה באמת אופציה עבור איראן בהתחשב בעליונותה של ישראל בתחום הלוחמה הקונבנציונלית (לפחות אם הקרב יהיה בסמוך לישראל). וליתר דיוק, כפי שצוין, איראן תיאלץ להודות כי המערכות שלה חובלו ולשכנע כי היא יודעת מי עומד מאחורי הפעולה. לבסוף, בעוד שישראל מרושתת יותר מאיראן, לאור יכולות הסייבר שלה, אולי לא יהיה בכך די כדי להטות את הכף לטובתה של איראן היה וזו תשיב מלחמה.

ג. מתקפות סייבר עשויות לשמש מדינה אחת כדי להשפיע על תוצאות סכסוך במדינה אחרת בלי שתצטרך להתחייב לכך בגלוי או אפילו במשתמע. לדוגמה, מלחמת האזרחים בלוב – אילו היה צבא לוב מחובר לאינטרנט באופן כזה שמתקפות סייבר היו יכולות להשפיע על ביצועיו,[10] אזי באמצעות נטרול כוחות הממשל המרכזי, היו פורצי מחשבים מן המערב יכולים להטות במידה ניכרת את כיוון המלחמה. אילו המורדים היו מנצחים, היו ממשלות המערב נשכרות מכך. אפשר שלא היה באפשרותם של כוחות המורדים לדעת שהם קיבלו סיוע, וייתכן שהדבר היה רק לטובה (בייחוד אם מדובר במורדים בעלי נטייה ג'האדיסטית מבין

המורדים בלוב, המקדמים בברכה את התערבות הכוחות האמריקניים). אפשרות אחרת היא לפזר רמזים (למשל, אם יכולת מסוימת תשותק מחר, אתם תדעו את הסיבה לכך). לחלופין, אילו ידה של הממשלה הייתה על העליונה, היא הייתה עשויה לחשוד שכוחות המערב חיבלו במערכות המידע שלה, אך הייתה מתקשה להוכיח זאת. היא הייתה עשויה להתלונן, אך היה צפוי מלוב להאשים את המערב במגרעותיה, ואז לתלונותיה, בהעדר הוכחות, לא היה ניתן לייחס חשיבות כלשהי. ליתר דיוק, היא לא הייתה רוצה לטעון כך אם רצונה היה להעמיד פנים לאחר מכן שאין לה כל סיבה לראות שוב במערב אויב. לו מלחמת האזרחים הייתה נמשכת, יכול היה המערב להעמיד פנים שהוא לא נתן סיוע לפני כן, וממילא גם לא התחייב להגדיל את הסיוע שלו (גם אם נשלחו רמזים למורדים, הם היו מתקשים מאוד להוכיח לאחרים שפורצי מחשבים מן המערב הציעו להם סיוע, שכן בשונה מהממשלה, אין לצפות שתהיה להם גישה למחשבים שחובלו). הבעיה הגדולה ביותר הטמונה בהצעת סיוע שכזה היא האפשרות של חשיפה, אבל אם היעד למתקפות שרוי בסכסוך עם שאר העולם, אין לצפות שהוא יזכה לסיוע ממשי באיתור התוקפים. סיוע שכזה הוא כה מושך (לפחות מנקודת המבט של נותן הסיוע), שהוא עשוי להפוך למאפיין שגרתי – משני הצדדים – בכל סכסוך שבו התוצאה אינה ודאית, ולרשתות יש חשיבות רבה במה שנוגע ליכולות לחימה. יודגש שוב, כי הודאה שהמערכות שלך נפרצו כרוכה תמיד במידה זו או אחרת של מבוכה.

ד. התקפות סייבר אינן צריכות להיות מכוונות בהכרח רק כלפי אויבים, אף־על־פי שהסיכונים שביצירת אויבים חדשים במקרה של חשיפת מקור המתקפות הם ברורים. דמיינו לעצמכם מצב שבו שתי מדינות ניטרליות מתקדמות באיטיות לעבר מלחמה. נניח שמדינה שלישית מסוגלת לגרום שיבושים במערכות המעקב, השליטה והבקרה של שני הצדדים, שיטילו ספק בדבר הצלחתן של שתי המדינות להתגבר על הסכסוך ביניהן. אם מערכות יוצאו מכלל שליטה, צפוי שכל אחת מהמדינות הללו תאשים תחילה את האחרת במקום לתלות את האשמה בצד שלישי. סביר ביותר שההנחה הראשונית – שהנזק נעשה על ידי הצד השני – תשפיע על התגובות ועל הפעילויות שלהן. יתר על כן, סיכוי גבוה הוא שהאשמה כזאת לא תוטח בפומבי עקב המבוכה הכרוכה בכך. עם זאת, תחבולות שכאלה עלולות להוביל מדינות למלחמה אם אחד הצדדים ישכנע את עצמו, למשל, שמתקפות הסייבר שמשגר כלפיו הצד האחר הן בגדר צעד מקדים להזזת כוחות מידית, או שהן מעידות שכוחות האויב אינם פרוסים במערך מסוים בלא סיבה.

ה. עמימות עשויה להועיל במדיניות הצהרתית, כזו המפרטת כיצד המדינה תגיב על מתקפת סייבר כנגדה. לעמימות יש חסרונות ויתרונות כאחד. החיסרון הוא, שאחרים עשויים לחשוב שהם יכולים להתחמק מאחריות לביצוע התקפות

שהם היו נמנעים מביצוען לו היה ברור להם שאלה יגררו פעולות תגמול. היתרון הוא, שסביר להניח שמדינת המטרה לא תרצה לתקוף בחזרה, בייחוד אם היא חוששת ליחס לעצמה את ההתקפה. מדינה הנמנעת מתקיפת־נגד מכיוון שאינה בטוחה, לא תאבד ממעמדה בעיניה שלה – ייחוס המעשה לצד מסוים הוא באמת משימה קשה. עם זאת, אם התוקף (ואחרים) יגיעו למסקנה שהמדינה האמורה ידעה מי התוקף אך העמידה פנים שאינה יודעת, מחשש להתלקחות מלחמה בהיקף מלא, אזי כל איום בנקמה מצדה יישמע לא אמין. אם מדינה ממהרת להבטיח פעולות תגמול בתגובה על מתקפות סייבר ואינה יכולה לעמוד בהבטחותיה, גם יכולתה לממש את איומיה האחרים, תוטל בספק.

מסקנות

העמימויות הטקטיות הרבות של לוחמת הסייבר מחזקות אסטרטגיה המבוססת על עמימויות אסטרטגיות. ייתכנו מקרים רבים שמדינה תוקפנית אינה מעוניינת לפרט מה היא עשתה. אפילו מדינת המטרה, במקרים מסוימים, עשויה להגיע למסקנה שלהעמיד פנים שלא הותקפה (אפילו אם עליה להעלים עין מהראיות) עדיף בעבורה מניסיון להבהיר עניינים.

ואולם יש גם חיסרון בעמימות אסטרטגית. מדינות עשויות ליטול על עצמן, שלא בדין, את הזכות לגרום סוגים שונים של נזקים במרחב הקיברנטי, בהניחן כי לעולם לא יידרשו לשאת באחריות על מעשיהן.. לעתים אין בכך הצדקה, והמדינה מרמה רק את עצמה; ואפילו אם יש הצדקה באי־לקיחת אחריות, היא מספקת לפורצי המחשבים דרגה של חופש שההיסטוריה מלמדת שהיא מסוכנת בפני עצמה.

הערות

1 בניגוד לכך היה צורך בחקיקה בשנת 2006, שתאפשר לארצות־הברית לשתף טכנולוגיה אזרחית עם הודו, שבדומה לישראל אינה חתומה על האמנה לאי־הפצת נשק גרעיני, אבל בשונה מישראל, היא מעצמה גרעינית מוצהרת. ראו: Peter Baker, "Signs India Nuclear Law: Critics Say deal to Share Civilian Technology could Spark Arms Race," Washington Post, December 19, 2006. www.washingtonpost.com/wp-dyn/content/article/2006/12/18/AR2006121800233.HTML

2 Robert McMillan, IDG News, "Was Stuxnet Built to Attack Iran's Nuclear Program?" taken from *PCWorld*, September 21, 2010.

3 William Yong, Alan Cowell, "Bomb Kills Iranian Nuclear Scientists," *New York Times*, November 30, 2010.

4 Joby Warrick, "Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack," *Washington Post*, February 16, 2011. See also the report by the Institute for Science and International Security, http://media.washingtonpost.comqwp-srv/world/documents/stuxnet_update_15Feb2011.pdf

5 הדבר הברור ביותר על תולעת הסטקסנט הוא אופן פעולתה מכיוון שהתולעת נתפסה "בחיים" כביכול, בטרם יכלה להשמיד את עצמה (פעולה שהיה עליה לעשות במקרה שלא יעלה בידה למצוא התקן לוגי מסוים ניתן לתכנות, שעמד בפרמטרים מסוימים קבועים מראש, הקשורים לסוג מסוים של צנטריפוגה).

6 www.economist.com/blogs/babbage/2010/09/stuxnet_worm

7 William Broad, John Markoff, David Sanger, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011.

8 Jeffrey Carr, "Stuxnet's Finnish-chinese Connection", December 14, 2010, www.blogs.forbes.com/firewall/2010/12/14/stuxnets-finnish-chinese-connection/

9 משקיפים רבים חולקים על האפיון של חזבאללה כבובה של איראן. עם זאת, יש הבדל בין חזבאללה הפועל אך ורק בהתאם להוראות מאיראן, לבין מצב שבו לאיראן יש השפעה מספקת על חזבאללה כדי להניאו מלנקוט פעולות לא חכמות.

10 במאמר רב השפעה, שסקר את האפשרויות של התערבות המערב בלוב נזכר הנושא של לוחמה אלקטרונית בדמות שיתוק התקשורת, אך לא צוין דבר בנוגע ללוחמת סייבר: Thom Shanker, "U.S Weighs Options, on Air and Sea," New York Times, March 6, 2011, http://www.nytimes.com/2011/03/07/world/middleeast/07military.html