תגובה מידתית למתקפות סייבר

ז׳רנו לימנל

מחקרים שנעשו בשנים האחרונות מראים כי קיים שוני ניכר בין תגובות של ממשלות שונות למתקפות סייבר. למרות לחצים פוליטיים משמעותיים ״לעשות משהו״ נגד מתקפות כאלו, ניסיון העבר מצביע על כך שרוב התגובות התבססו על מדיניות אד הוק. מצב זה מלמד כי מרחב הסייבר הוא זירת עימות חדשה יחסית, במיוחד עבור קובעי המדיניות, ולכן יש להפנות אליה תשומת לב מיוחדת; כי התגובות למתקפות סייבר הן סוגיה שעדיין לא נחקרה בצורה משביעת רצון; וכי יש צורך במחקר נוסף כדי להבין כיצד על מדינות לאום להגיב בצורה הטובה ביותר לפעולות עוינות בסייבר ובאילו כלים עליהן להשתמש לצורך זה.

מאמר זה מצביע, באמצעות ניתוח מקיף, על כך שיש להתייחס למתקפות סייבר כסוגיה פוליטית. הוא מספק מסגרת כללית שעליה יכולים להתבסס קובעי המדיניות, המשלבת בין השפעת האירוע ובין המדיניות האפשרית כלפיו, ומפרט חמישה משתנים שעליהם לשקול כאשר הם באים להעריך מהי התגובה ההולמת למתקפת סייבר. המאמר מתווה את דרכי הפעולה השונות של ״פוליטיקת הסייבר״ אותן ניתן ליישם כתגובה למתקפות קיברנטיות, כאשר מסגרת התגובה אמורה להיות חלק בלתי נפרד מצעדי ההרתעה של המדינה בתחום הסייבר.

מילות מפתח: אבטחת סייבר, מתקפות סייבר, לוחמת סייבר, אסטרטגיית סייבר, פוליטיקה, פוליטיקת סייבר, תגובה, ביטחון, לוחמה היברידית

מבוא

באוקטובר 2016 יצאו המשרד לביטחון המולדת ומשרד המודיעין הלאומי של ארצות הברית בהכרזה מרעישה, לפיה ממשלת רוסיה עומדת מאחורי מתקפה על

פרופ׳ ז׳רנו לימנל מלמד ביטחון סייבר באוניברסיטת אלטו שבפינלנד.

הדואר האלקטרוני של יחידים ומוסדות בארצות הברית, כולל ארגונים פוליטיים,[1] וקבעו כי "הגניבות והחשיפות שנעשו נועדו להפריע לתהליך הבחירות בארצות הברית".[2] האשמה זו היא יוצאת דופן בשני היבטים. ראשית, במעשה עצמו: הפריצה הייתה סחריר (ספין) פוליטי משמעותי שנוסף לפריצות קודמות, וניתן לראות בה ניסיון ברור להשפיע על הבחירות לנשיאות באמצעות ניצול מרחב הסייבר. הפריצה גם הייתה תזכורת לאופן שבו מתקפות סייבר יכולות לערער את תפיסת הריבונות, לזרוע בלבול בקרב האוכלוסייה האזרחית ולטשטש את הגבולות בין מלחמה לשלום; ההיבט השני קשור לשאלת הייחוס. למרות שייחוס מוחלט של מתקפת סייבר הוא דבר קשה להשגה, במקרה זה קהילת המודיעין האמריקאית הודיעה כי אין לה ספק שהפריצות אושרו ברמות הגבוהות ביותר של הממשל הרוסי.[3] האשמה פומבית ופוליטית ישירה זו מעידה על רמה גבוהה של ודאות לגבי הייחוס. גורמים רוסיים רשמיים הגיבו על כך בביטול ופטרו את ההאשמות כ"שטויות" שנועדו להצית היסטריה אנטי־רוסית.[4]

שני ההיבטים שלעיל מעוררים את השאלה החשובה והמעניינת יותר: מה תהיה התגובה של ארצות הברית לפריצות אלו? כפי שאמר הנשיא הקודם ברק אובמה, מרחב הסייבר הוא "ים לא מוכר", שבו "אין, למשל, פרוטוקולים קובעים בנושאים צבאיים או בסוגיות הנוגעות למערכות נשק, נושאים וסוגיות שבהם נצבר ניסיון בשאלה מה מקובל ומה לא מקובל".[5] המועמדת לנשיאות, הילרי קלינטון, הבהירה מצדה כי "ארצות הברית תתייחס למתקפות סייבר בדיוק כמו לכול מתקפה אחרת".[6]

1 ביולי 2016 פרסם אתר "וויקיליקס" הודעות דוא"ל מביכות שנלקחו מחשבונות המפלגה הדמוקרטית של ארצות הברית. פצחנים השיגו גישה מלאה לרשת ששימשה את צוות מטה הבחירות של המפלגה, לרבות דוא"ל, מזכרים ומחקרים שהתייחסו למועמדים הדמוקרטיים לקונגרס.

2 *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*, October 7, 2016, https://www.dhs.gov/node/23199.

3 *Assessing Russian Activities and Intentions in Recent US Elections*, Intelligence Community Assessment, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

4 Dmitry Solovyov, "Moscow Says U.S. Cyber Attack Claims Fan 'Anti-Russian Hysteria'", *Reuters*, October 8, 2016, http://www.reuters.com/article/us-usa-russia-cyber-ministry-idUSKCN1280DO.

5 *Remarks by President Obama and President Xi Jinping of the People's Republic of China after Bilateral Meeting*, The White House, June 8, 2013, https://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-/.

6 Andrew Blake, "Hillary Clinton: U.S. Will Treat Cyberattacks 'Just Like any Other Attack'", *Washington Times*, October 7, 2016, http://www.washingtontimes.com/

רבים בארצות הברית ובעולם המערבי קראו לממשל האמריקאי לפעול ולהבהיר לרוסיה כי מתקפת סייבר נגד התהליך הדמוקרטי תיענה בתגובה הולמת. ואכן, הנשיא אובמה אישר כי ארצות הברית שוקלת "תגובה מידתית" והוסיף כי עומד לרשותה מגוון של אפשרויות זמינות.[7] ארצות הברית גם הצהירה כי התגובה "תהיה בזמן שנבחר, ובנסיבות שבהן תושג ההשפעה הגדולה ביותר".[8] יחד עם זאת, הנשיא לא הבהיר מהי המשמעות של "תגובה מידתית" מבחינת הפעולה הקונקרטית. יותר מאוחר מסר הנשיא אובמה כי ארצות הברית תטיל סנקציות על תשעה גופים ואישים רוסיים ותגרש 35 דיפלומטים של רוסיה כתגובה על הפריצה וניסיון ההתערבות בבחירות. אובמה גם אמר כי ארצות הברית "תמשיך לנקוט מגוון פעולות" במועד ובמקום שתבחר, שחלקן לא יפורסמו בפומבי.[9] אין ספק כי מדובר במצב חדש עבור הממסד הביטחוני האמריקאי וקובעי המדיניות בארצות הברית.

ההתערבות בבחירות לנשיאות ארצות הברית ושקילת תגובה למתקפת הסייבר הן רק דוגמה אחת לנושא שהמאמר הנוכחי עוסק בו, והיא מעוררת מספר שאלות ובהן: מדוע חשוב לנסח מסגרת לתגובה פוליטית על מתקפות סייבר בעידן הנוכחי ומה צריך להילקח בחשבון כאשר מחליטים על תגובה מידתית למתקפות סייבר? ניסיון ההתערבות בבחירות בארצות הברית הוא גם תזכורת לצורך הדחוף בפיתוח נורמות בין־לאומיות שיצמצמו את האפשרות למתקפות ולפעולות עוינות בסייבר, בעולם ההולך ונעשה יותר ויותר דיגיטלי.

רקע תיאורטי

ביטחון מרחב הסייבר הוא חלק בלתי נפרד מהביטחון, המלחמה והפוליטיקה של ימינו. לכן, חשוב להבין כי אין לבודד מתקפות ופעילויות אחרות במרחב הסייבר מההקשר הפוליטי, האסטרטגי והגיאו־פוליטי הרחב יותר. לדוגמה, מרכיב הסייבר

news/2016/sep/1/clinton-us-will-treat-cyberattacks-just-any-other-/.

7 Julie Davis and Gardiner Harris, "Obama Considers 'Proportional' Response to Russian Hacking in U.S. Election", *New York Times*, October 11, 2016, http://www.nytimes.com/2016/10/12/us/politics/obama-russia-hack-election.html.

8 David E. Sanger, "Biden Hints U.S. Response to Russia for Cyberattacks", *New York Times*, October 15, 2016, http://www.nytimes.com/2016/10/16/us/politics/biden-hints-at-us-response-to-cyberattacks-blamed-on-russia.html.

9 *Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment*, The White House, December 29, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.

היה חלק בלתי נפרד במלחמה המתמשכת באוקראינה, ונתפס כהמשכה של הפוליטיקה באמצעים אחרים.[10]

כל פעולה מורכבת לרוב מחמש רמות: רמת המדיניות והמטרות; רמת האסטרטגיה; רמת המבצעים (כולל מערכות צבאיות); רמת הטקטיקות; רמת הכלים והאמצעים.[11] כל הרמות הללו הן חשובות, אך אנשי מקצוע בתחום הביטחון, העוסקים בשאלת ביטחון הסייבר, מתמקדים לעתים קרובות רק בטקטיקות ובכלים, וגם זאת במיוחד מבחינה טכנולוגית.

מאמר זה עוסק בתחום הסייבר בעיקר מנקודת המבט הפוליטית, וזאת בשל החשיבות הגוברת שיש לדבר בעולם המקושר של היום ובפוליטיקה הבין־לאומית. לשם דוגמה, נאט״ו הכיר במרחב הסייבר כמרחב מבצעי שבו על הארגון להגן על עצמו ביעילות, כפי שהוא עושה באוויר, ביבשה ובים.[12] נאט״ו גם פעל כדי שניתן יהיה להסתייע בסעיף 5 באמנת הארגון בתגובה להתקפות סייבר – מהלך שהוא החלטה פוליטית.

ניתוח של מתקפות הסייבר שהתרחשו בשנים האחרונות מראה שהתגובות הרשמיות להן שונות זו מזו במידה רבה.[13] יש לחץ פוליטי ניכר ״לעשות משהו״ נוכח מתקפות סייבר, אך הניסיון מלמד כי רוב התגובות מתבססות על מדיניות אד הוק. מכאן נובע שתחום הסייבר הוא זירת עימות חדשה יחסית, במיוחד עבור קובעי המדיניות, ולכן הוא זקוק לתשומת לב מיוחדת; שהתגובות על מתקפות סייבר הן עדיין במידה רבה תופעה שלא נבחנה מספיק; וכי יש צורך במחקר נוסף כדי להבין מהי התגובה הטובה ביותר שמדינות לאום צריכות לאמץ לנוכח התקפות סייבר, ומהם הכלים שכדאי להשתמש בהם לצורך זה.

ככול שפעולות סייבר התקפיות הופכות לנפוצות יותר, כך גובר האתגר שניצב מול קובעי המדיניות לפתח תגובות מידתיות להתקפות שהן בעלות אופי של שיבוש או הרס. עם זאת, לפני שמגיבים יש להתחשב במספר משתנים שינותחו בהמשך. בסוף המאמר מופיע תרשים המציג מסגרת כללית הקושרת בין ההשפעות של מתקפת הסייבר ובין אפשרויות התגובה המדיניות, הסיכונים, הזמן, הייחוס והמידתיות,

---

10 גישה זו, ברוח דבריו של קלאוזביץ, הינה שנויה במחלוקת, אך מתארת כיצד פוליטיקה ומלחמה כרוכות זו בזו. ראו למשל: Mary Kaldor, "Inconclusive Wars: Is Clausewitz Still Relevant in these Global Times?", *Global Policy* 1, no. 3 (2010): 271-281.

11 ראו למשל: Richard Bejtlich, "Strategic Defence in Cyberspace: Beyond Tools and Tactics", in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCDCOE, 2015), pp. 159-170.

12 *Warsaw Summit Communiqué*, NATO, July 9, 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

13 ראו למשל: Sico Van der Meer, "Signaling as a Foreign Policy Instrument to Deter Cyber Aggression by State Actors", *Clingeldael*, December 2015, https://www.clingendael.nl/sites/default/files/PB_Signalling_as_a_foreign_policy_instrument_SvdM.pdf.

ומשרטטת בהתאם לכך את המנופים השונים העומדים לרשות "פוליטיקת הסייבר", אותם ניתן ליישם בתגובה לאירועי סייבר מסלימים. מסגרת זו, המהווה ניתוח של "התוצאה הסופית" של פעולות התגובה, יכולה לשמש כבסיס להחלטה אצל קובעי המדיניות.

חשיבות הפוליטיקה בעולם הסייבר

בדיקת הגבולות

מתקפות של פצחנים (בין אם "ממשלתיים" ובין אם לאו) על המערכות הדיגיטליות שבהן תלויות מדינות לקבלת שירותים חיוניים, לשמירת השגשוג הכלכלי ולביטחונן, הפכו בעשור האחרון למתוחכמות יותר ויותר. הפריצות למערכות אלו יצרו איום על תשתיות קריטיות, על קניין רוחני, על הפרטיות של המשתמשים, על מידע חשוב בתחום הביטחון הלאומי ועל נתוני כוח אדם. ההתקדמות הטכנולוגית והתלות הגוברת במרחב הסייבר הפכו את ביטחון הסייבר, כמו גם את הצורך בכללים ובגישות משותפים בסוגיה זו, לנושא מרכזי וחשוב. במקביל, המושגים של התקפה, הגנה, הרתעה, שיתוף פעולה בין־לאומי וריגול קיבלו משמעות חדשה.

ההסתמכות המוגברת על התשתית הדיגיטלית ופגיעותה להתקפות סייבר הובילו ממשלות וגורמים לא מדינתיים לנצל את מרחב הסייבר כדי לתת ביטוי להבדלים הגיאו־פוליטיים ביניהם ולקדם את מטרותיהם הפוליטיות. משמעות הדבר היא גם התחזקות חשיבותה של "הלוחמה הלא קינטית".

זה זמן רב קיים צורך בדיונים ברמה הלאומית והבין־לאומית על התקפות סייבר והתגובה להן, אלא שדיונים כאלה לא התקיימו למרות ההכרה הרחבה לה זוכה החשיבות האסטרטגית של המרחב הדיגיטלי. נכון להיום, "כללי המשחק" הפוליטיים בסייבר עדיין מעטים, אף שהם הולכים ורבים מדי יום. זאת, כתוצאה ממעבר העולם לשימוש אסטרטגי גובר בנשק הסייבר ככלי להביא לשינוי התנהגותו של היריב.

מדינות ושחקנים לא מדינתיים כאחד בוחנים כיום את גבולות "שדה הקרב בסייבר", כאשר מספר פעולות הסייבר הנראות והבלתי נראות הולך וגובר, רמת התחכום שלהן עולה, ודרכים חדשות לנצל את מרחב הסייבר נסללות ומיושמות. בדצמבר 2015 היינו עדים להתקפה המאומתת הראשונה שנועדה להשבית רשת חשמל, אשר השפיעה על כ־225,000 אזרחים באוקראינה.[14] יכולות הסייבר הולכות ומשתכללות, וכך גם הרצון והנכונות להשתמש בהן, ודומה שאין לנו מושג כיצד להתמודד עם המציאות החדשה.

14 "Analysis of the Cyber Attack on the Ukrainian Power Grid", *E-ISAC*, March 18, 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

עליית פוליטיקת הסייבר

נושאים הקשורים לסייבר ולשימושיו חדרו בשנים האחרונות לרמה הגבוהה ביותר של הפוליטיקה. זאת, לעומת העבר, כאשר מרחב הסייבר נחשב בעיקר לסוגיה הקשורה לפוליטיקה ברמה נמוכה, שבמרכזה נושאי רקע ותהליכים. ביטחון הסייבר הפך כיום למוקד של התנגשות אינטרסים, הן מקומיים והן בין־לאומיים, ולזירה שבה מוקרנת עוצמתן של מדינות.[15]

חשוב להבין כי מרחב הסייבר הוא מרחב פוליטי, במיוחד לאחר שתובנה זו נזנחה ונשכחה לעתים קרובות. כאשר בוחנים את מרחב הסייבר מנקודת המבט של מדינת הלאום, מגלים שהשאלות המרכזיות של מרחב זה כיום הן פוליטיות מאוד. לפיכך, יש להתייחס לתחום הסייבר כאל זירה פוליטית בעיקרה, כפי שקורה ביחס לתחומים אחרים. כאשר קיימת מעורבות פוליטית, מתעוררות תמיד גם שאלות הקשורות לכוח. לדוגמה, בהקשר של מלחמה, כלי הסייבר דומה לעוצמתם של כוחות היבשה, הים או האוויר ומשמש כמוהם אמצעי להשגת מטרה פוליטית או לצבירת כוח. זוהי הסיבה להתגברות השימוש האסטרטגי במרחב הסייבר להשגת מטרות פוליטיות ויתרונות גיאו־אסטרטגיים.

התפתחותו של מרחב הסייבר והתלות העמוקה שלנו בו יוצרות זירה חדשה להתנהלות הפוליטית. יותר מכך, אפשר שאנו עדים להיווצרות צורה חדשה של פוליטיקה. מדובר בתהליך שזכה לכינוי "סייבריזציה",[16] המתייחס לחדירתם של ממדים שונים של סייבר לכול תחומי הפוליטיקה. זו גם הסיבה לשימוש הנרחב הנעשה כיום במושג "פוליטיקת סייבר".[17]

פוליטיקת סייבר מתייחסת להתלכדות של שני סוגי תהליכים: התהליכים הנוגעים לפוליטיקה של קביעת "מי מקבל מה, מתי ואיך"; התהליכים העושים שימוש במרחב הסייבר, כלומר, זירה של אינטראקציות דיגיטליות. הפוליטיקה בזירה הפיזית ובזירת הסייבר גם יחד כרוכה בעימותים, במשא ומתן ובמיקוח על מנגנונים, ממוסדים או אחרים, מתוך מטרה לפתור באופן מוסמך מחלוקות סביב נושאי ליבה. לכן, ניתן לומר שכאשר מדינות שוקלות תגובות מידתיות למתקפות סייבר, הדבר הופך את פוליטיקת הסייבר למוחשית.

---

15 Jelle Van Haaster, "Assessing Cyber Power", in *8th International Conference on Cyber Conflict: Cyber Power*, eds. N. Pissanidis, H. Rõigas and M. Veenendaal (Tallinn: NATO CCD COE, 2016), pp. 7-22.

16 Jan-Frederik Kremer and Benedikt Müller, eds., *Cyberspace and International Relations, Theory, Prospects and Challenges* (London: Springer, 2014) pp. xi-xvii.

17 Nazli Choucri, "Cyberpolitics in International Relations", in *Oxford Companion to Comparative Politics*, ed. Joel Krieger (New York: Oxford University Press, 2012), pp. 267-271.

פוליטיקת סייבר מיושמת בעיקר על ידי אנשי אקדמיה המעוניינים לנתח את השימוש שנעשה במרחב הסייבר לצורך פעילות פוליטית, ובכלל זה את היקפו ועומקו של שימוש זה. למרות שפוליטיקת הסייבר קיימת הן ברמה הלאומית והן ברמה הבין־לאומית, ונושאי הסייבר מצויים בלב מדיניות החוץ והביטחון של מדינות, פוליטיקת הסייבר ועולם הסייבר יצרו תנאים חדשים שאין להם תקדים. התכנים האמיתיים של פוליטיקת הסייבר ייחשפו בשנים הקרובות, וסביר להניח שאז נוכל לחזור להשתמש במושג "פוליטיקה" בלבד. זאת, מתוך הנחה שענייני הסייבר יהיו חלק בלתי נפרד מהפוליטיקה, שכן תחום הסייבר אינו שונה, בסופו של דבר, מהמסגרות המקובלות שלה.

נורמות סייבר גלובליות נמצאות עדיין בחיתוליהן

ב־2015 ניסתה קבוצה של מומחים באו"ם לפתח כללים בתחום המידע והטלקומוניקציה בהקשר של ביטחון בין־לאומי.[18] הדוח שהם כתבו הרחיב באופן משמעותי את הדיון בסוגיה גם לנורמות, לכללים ולאמצעים לבניית אמון במרחב הסייבר. קבוצת המומחים המליצה כי מדינות ישתפו פעולה ביניהן כדי למנוע שימוש מזיק בסייבר, וקבעה כי עליהן למנוע שימוש ביודעין בטריטוריה שלהן לביצוע פעולות בין־לאומיות פוגעניות באמצעות טכנולוגיות מידע ותקשורת (ICT). אחת ההמלצות החשובות של הקבוצה גרסה שהמדינה אינה צריכה להוביל פעילות בתחום טכנולוגיות המידע והתקשורת שכוונתה לפגוע או לשבש בדרך אחרת את השימוש והתפעול של תשתיות קריטיות, או לתמוך ביודעין בפעילות כזו. דוח מומחי האו"ם הדגיש כי "הפיכת מרחב הסייבר ליציב ובטוח יכולה להתבצע רק באמצעות שיתוף פעולה בין־לאומי", וחייב את המדינות לנקוט אמצעים מתאימים כדי להגן על התשתיות הקריטיות שלהן. עם זאת, הדוח לא כלל הנחיות לתגובה, במיוחד על התקפות סייבר שנעשות בחסות מדינות. כמו כן נכתב בדוח כי העובדה שמקורה של מתקפת סייבר הוא בשטחה של מדינה מסוימת, או שמתקפה כזאת שוגרה מתשתית של טכנולוגיות מידע ותקשורת הנמצאת בתחומה, אינה מספיקה כדי לייחס אותה לאותה מדינה.[19]

למדינות שמורה זכות טבעית להגנה עצמית לפי סעיף 51 של מגילת האו"ם במצבים של איום ממשי עליהן. לפיכך, התנהגות המדינה במרחב הסייבר צריכה גם היא לעלות בקנה אחד עם הנאמר במגילת האו"ם. עם זאת, האתגר של קביעת הייחוס ושל הבנת היקף הנזק ממתקפה ברשת עלול לסבך את המצב. הזכות להגנה

18 "Developments in the Field of Information and Telecommunications in the Context of International Security", United Nations General Assembly, July 19, 2016, http://www.un.org/ga/search/view_doc.asp?symbol=A/71/172.

19 שם.

עצמית, ובכלל זה לשימוש בכוח, תחול אם מתקפת הסייבר תגיע לרמה של "התקפה חמושה", אך הדיון המשפטי על מה מהווה "התקפה חמושה" במרחב הסייבר נמצא רק בראשיתו. בכול מקרה, ניתן לשער כי פעולה עוינת בסייבר, אותה ניתן לייחס למדינה, יכולה להיחשב כהפרה של סעיף 2 (4) של מגילת האו"ם, וזאת בהתאם לאופייה ולתוצאותיה.[20] הדבר גם מעורר את השאלה הכללית כיצד יש להעריך את השפעתה של מתקפת סייבר, במיוחד כאשר לא נגרם בעקבותיה נזק פיזי.

מתקפת סייבר לא צריכה לגרום בהכרח לנזק פיזי כדי להיחשב לחמורה. הרס פיזי זוכה להדגשה רבה, אולי בגלל המסורת הארוכה של עיסוק בביטחון פיזי, וגם משום שהשלכות פיזיות ברורות יותר לעין. לכן, דרך החשיבה הישנה היא שמתקפת סייבר "חמורה" צריכה לכלול הרס פיזי, כולל מוות ופגיעה בתשתיות קריטיות. עם זאת, ככול שאנו נעשים תלויים יותר ויותר בנתונים ובנכסים לא קינטיים, נשאלת השאלה האם יש להתייחס למניפולציה על רשומות בריאותיות או פיננסיות, למשל, באותה רמה של חומרה כמו להשלכות פיזיות.[21] יתרה מכך, יש לשאול האם קיים הבדל בין מניפולציה על נתונים בנקאיים ובין מניפולציה על נתונים בריאותיים, כשהראשונה עלולה לגרום לשיבושים כלכליים חמורים, אך האחרונה עלולה לגרום במקרים קיצוניים למוות. התשובה לכך לא ברורה. כמו כן, לא ברור מה המשמעות בפועל של מתקפת סייבר "רחבת היקף". חשוב להבין שהתשובה לשאלה האם התקפת סייבר היא מעשה מלחמה או לא, היא במהותה החלטה פוליטית.

חמישה משתנים

בבואם לקבוע מהי התגובה הראויה למתקפת סייבר, על קובעי המדיניות לשקול את חמשת המשתנים הבאים, המהווים שאלות שיש להשיב עליהן לפני החלטה על תגובה.

מי עשה את זה?

ייחוס מתקפת סייבר לנותן החסות – השחקן המדינתי או הלא מדינתי שמאחורי ההתקפה – נותר אתגר משמעותי, שכן הוא מחייב אמצעים יעילים ויכולת לזהות את העומדים מאחורי ההתקפה. בעיית הייחוס מורכבת ביותר ולא תמיד ניתנת

20 סעיף 2 (4) של מגילת האו"ם קובע: "במסגרת היחסים הבין־לאומיים שלהן, יימנעו כל המדינות החברות מאיום או משימוש בכוח נגד השלמות הטריטוריאלית או העצמאות המדינית של מדינה כלשהי, או מכול התנהגות אחרת שאינה עולה בקנה אחד עם מטרת האומות המאוחדות".

21 Jarno Limnéll and Charly Salonius-Pasternak, "Challenge for NATO – Cyber Article 5", Briefing Paper, Center for Asymmetric Threat Studies, Swedish Defense University, June 2016.

לפתרון. מרחב הסייבר מאפשר מידה רבה של אנונימיות, וניתן לנתב התקפות דרך שרתים בכול רחבי העולם כדי להסוות את מקורן. ייחוס שגוי של המתקפה עלול להוביל לתגובה שתהיה מכוונת אל יעד לא נכון. כאשר בוחנים את סוגיית התגובה המידתית, על קובעי המדיניות לדעת מה רמת הביטחון שבידם לגבי ייחוס המתקפה.[22] לדוגמה, אם רמת הביטחון בייחוס היא נמוכה, מקבלי ההחלטות יהיו מוגבלים בבחירת התגובה שלהם, גם אם חומרת הפגיעה היא גבוהה. על מדינות לחשב את העלויות הכרוכות בייחוס שגוי של מתקפה ולשקול את העלויות הפוטנציאליות של הסלמה. לפיכך, מידת ודאות הייחוס משפיעה על הפעולה שתינקט.

היכולת לייחס מתקפה למקור מסוים חשובה לצורך שמירה על האמינות ולהבטחת הלגיטימיות מבית ומחוץ. האתגר נובע מכך שניתן לאסוף ראיות מספיקות לייחוס באמצעות מקורות מידע מודיעיניים חשאיים או דרך מדינות ידידותיות, אך לרוב המדינה אינה מעוניינת לחשוף את מקורות המודיעין הללו בפומבי. עם זאת, אם מדינה רוצה לבנות לגיטימציה בין־לאומית לפעולת התגמול שהיא נוקטת, חיוני שתפרסם הוכחה כלשהי לקביעת הייחוס.

לייחוס יש היבטים רבים, כולל טכניים, משפטיים ופוליטיים. זהו נושא רב־ממדי הדורש ניתוח של מקורות מידע רבים, כולל ממצאים פורנזיים, דוחות מודיעין אנושי, מודיעין אותות, היסטוריה וגיאו־פוליטיקה. כפי שטוענים ריד וביוקנן, הייחוס הוא תרגיל של צמצום אי־הוודאות בשלוש רמות: הרמה הטקטית, שבה הייחוס הוא אמנות לא פחות ממדע; הרמה המבצעית, שבה הייחוס הוא תהליך מורכב ולא בעיה של שחור־לבן; הרמה האסטרטגית, שבה הייחוס הוא פונקציה של מה מונח על כפות המאזניים מבחינה פוליטית.[23] ייחוס מוצלח דורש מגוון של כישורים בכול הרמות, ניהול זהיר, עיתוי, מנהיגות, בדיקת יכולת העמידה בלחץ, תקשורת שקולה והכרה במגבלות ובאתגרים. אמנם, העניין הרב של מומחי הביטחון ברמות השונות של הייחוס הביא להגברת היכולת לייחס מתקפות, אך ההחלטה הסופית לגבי הייחוס לצורך נקיטת צעדי תגובה היא תמיד פוליטית.

מה ההשפעה?

על קובעי המדיניות להבין מה הייתה השפעת מתקפת הסייבר, שכן זו תקבע את סוג התגובה ורמתה. כמה מהשאלות שיש לשאול בהקשר זה הן: כמה מזיקה הייתה הפגיעה בביטחון הלאומי ובחברה? איזה סוג של שירותים נפגעו או הושפעו

22 Tobias Feakin, "Developing a Proportionate Response to a Cyber Incident", *Council on Foreign Relations*, August 2015, http://www.cfr.org/cybersecurity/developing-proportionate-response-cyber-incident/p36927.

23 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies* 38, no. 1-2 (2014): 4-37.

מהתקיפה? האם ההתקפה גרמה לאובדן משמעותי של אמון במוניטין של המדינה? הניתוח יכול לקחת שבועות, אם לא חודשים או שנים, עד שמומחי מחשבים יקבעו במדויק את היקף הנזק שנגרם לרשתות המחשב של הארגון שהותקף. כך, למשל, נדרשו לשלטונות ערב הסעודית כשבועיים כדי להבין את היקף הנזק שנגרם מהנוזקה Shamoon, אשר מחקה נתונים של 30,000 מחשבים בחברת "אראמקו" הסעודית. לעתים קורה שחברות או ארגונים ממשלתיים מבינים שנפרצו רק חודשים או שנים לאחר מעשה.

ברור שקל יותר להעריך השפעה פיזית של מתקפה. כאשר ההשפעות של מתקפת סייבר לא תמיד ברורות, קשה למקבלי ההחלטות לקבוע אם הפעולה העוינת היא ברמה של התקפה ואם נדרשת תגובה. יש דוגמאות רבות למתקפות סייבר שכשלו בהשגת המטרה, והפכו למטרד או לסוג של פעולת ריגול רגילה למדי.[24]

חישוב מידתיות התגובה למתקפת סייבר הוא אתגר הנובע מרמת החשאיות של המתקפה ומהמהירות בה בוצעה. ככלל, קשה לקבוע את סדר הגודל של מתקפת סייבר ואת השלכותיה, מה גם והמידע הדרוש כדי להבין השלכות אלו יכול גם הוא להיות קשה להשגה. לדוגמה, מוסדות פיננסיים וחברות פרטיות עשויים לסרב לספק מידע על הנזק שנגרם להם בשל שיקולים של סודיות עסקית.[25]

אילו כלים יכולים לשמש בתגובה?

כאשר בוחנים תגובה מידתית למתקפות סייבר, ההחלטה היא תמיד נגזרת של האפשרויות העומדות לרשות המדינה. נהוג לומר שלכול מדינה יש לפחות ארבעה כלים לתגובה: דיפלומטיה (כלומר, כלי מדיניות חוץ, כגון תקשורת דיפלומטית, אזהרות וסנקציות), כלי מידע, צבא וכלכלה.[26] על קובעי המדיניות לשקול את מלוא טווח התגובות העומד לרשותם, החל מנזיפה דיפלומטית שקטה ועד מתקפה צבאית.

אין סיבה להניח שתגובה מידתית לפעולה עוינת בסייבר צריכה להיות מוגבלת רק למרחב הסייבר. אדרבא, אין להגביל את התגובה למרחב הסייבר בלבד ואין דבר המונע מהמדינה מלהשתמש באמצעים אחרים, אם כי כל אחד מאמצעים אלה נושא את הסיכונים הפוליטיים שלו. מערכת הביטחון האמריקאית אף הציעה שארצות הברית לא תשלול תגובה גרעינית במקרה של מתקפת סייבר קיצונית במיוחד.[27]

24 James Stavridis, "How to Win the Cyberwar against Russia", *Foreign Policy*, December 12, 2016, http://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/.

25 Marco Roscini, *Cyber Operations and the Use of Force in International Law* (New York: Oxford University Press, 2014).

26 Timothy Thomas, "Creating Cyber Strategists: Escaping the 'DIME' Mnemonic", *Defence Studies* 14, no. 4 (2014): 370-393.

27 *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, Department of Defense, Defense Science Board, January 2013, http://www.dtic.

בדרך כלל מקובל שתגובות קינטיות מותרות רק כאשר להתקפה יש כוונות קטלניות ואם היא גרמה לסבל אנושי או לאובדן חיים, או הייתה הפרה מפורשת של זכויות אדם.[28] עם זאת, כשעוסקים בחברות שהדיגיטציה בהן הולכת וגוברת, מדובר בגישה צרה מדי, כפי שנטען בראשיתו של מאמר זה. בכול מקרה, נכון להיום, קשה להצדיק תגובה צבאית למתקפת סייבר, אם זו לא גרמה נזק פיזי במובן המקובל.[29]

הסוגיה המרכזית בהקשר זה היא הצורך לשקול אילו אמצעי נגד (פיזיים, בסייבר או אחרים) יכולים לשמש כחלק מ"ארסנל התגובה" של מדינת הלאום ואילו מהם צריכים לשמש בכול אחד מהמקרים. זוהי שאלה של מינוף העוצמה הלאומית העומדת לרשות המדינה ונכונותה להשתמש בה. תגובה להתקפות סייבר עשויה להתבצע בצורה גלויה או בחשאי. אם נבחרו שיטות סייבר, קשה יהיה לפתח תגובה חשאית במהירות, אלא אם הממשלה כבר בנתה מראש יכולות נגד יעד מסוים. במקרה כזה, סביר להניח שיכולות אלו יסתמכו על ריגול סייבר קודם ועל לימוד נקודות התורפה של המטרה. מנגד, תגובה פחות חשאית תורמת להרתעה גם נגד מדינות אחרות.

לתגובות סייבר גלויות יש גם חסרונות: מדינות עשויות לאבד את היכולת לשגר תגובות סייבר דומות נגד מטרות אחרות בעתיד, והן גם חושפות את עצמן לתגובה נגדית. אם התגובה גלויה לציבור, היא צריכה להיות מלווה גם בנרטיב של צדק ולא של נקמה. מדינות יכולות גם לבחור להפקיד את פעולת התגובה בידי קבוצות פצחנים חיצוניות הפועלות כשלוחה שלהן (proxy). עם זאת, שימוש בדרך זו עשוי להגבילן בשליטה על התגובה ואולי אף לגרור אותן לפעולות מסלימות.

מהן הנחיות המדיניות?

על קובעי המדיניות לשקול את אסטרטגיות הביטחון הלאומי ואבטחת הסייבר הקיימות, המתוות את הקווים המנחים של המדיניות הכללית של המדינה בכול הנוגע לנכונותה הפוליטית לפעול ולמנף את כוחה. אם המדינה חברה בבריתות ובארגונים בין־לאומיים, יהיה עליה לשקול גם את הנחיות המדיניות של ישויות אלו בבואה לגבש את התגובה המידתית, אחרת ניתן יהיה להאשים אותה שאינה מקיימת את המדיניות המוסכמת המשותפת. כאמור, מרחב הסייבר אינו חסין בפני הנורמות המשפטיות המחייבות את אומות העולם להגיב באופן מידתי על התקפה.

---

mil/get-tr-doc/pdf?AD=ADA569975.

28 ראו למשל: Thomas Wester, "Just Cyberwar", Cyber Security Policy and Research Institute, The George Washington University, November 24, 2014.

29 Patrick Lin, Neil Rowe and Fritz Allhoff, "Is it Possible to Wage a Just Cyberwar?", *Atlantic*, June 5, 2012, http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-justcyberwar/258106/.

מתקפת סייבר יכולה לגרום לכך שקובעי המדיניות יחליטו על תגובת יתר. מספר מומחי סייבר העריכו כי הסכנה לתגובת יתר היא ממשית מאוד ולכן על מקבלי ההחלטות לשקול בזהירות כל הסלמה אפשרית לפני שהם מגיבים. ליביצקי טוען בהקשר זה כי על מקבלי ההחלטות להבין מה מונח על כפות המאזניים, כלומר, מה הם מקווים להרוויח מתגובה בשיטה כזו או אחרת.[30]

למומחי ביטחון סייבר עשוי גם להיות תמריץ להאדיר את איום מתקפות הסייבר, שבתורו יגביר את הסיכון לתגובת יתר. גם אם הלחץ הפוליטי בעקבות מתקפת סייבר הוא רב, דרושה זהירות פוליטית, ולפחות יש לעודד רמה מסוימת של איפוק. איפוק עצמי הוא מושג הרלוונטי למניעת הסלמה במצב, במיוחד אם נשקלת תגובה קינטית. ככלל, כדי להרתיע מפני הסלמה, על היריב להאמין שתוצאת ההסלמה תהיה הרבה יותר גרועה מזו של האיפוק. איפוק יכול לעתים להיות אמצעי חזק יותר לביטוי עוצמה לאומית.

עד כמה דחופה התגובה?

הזמן הוא נושא רלוונטי בפוליטיקה. הלחץ הפוליטי להגיב מתגבר במיוחד כאשר תוצאת מתקפת הסייבר נחשפת בפומבי וזהות התוקף מוכרזת רשמית. תגובה שאינה מהירה מספיק יכולה להביא לפגיעה במוניטין ובאמינות הפוליטית. יריבים פוליטיים עשויים גם הם להפעיל לחץ "לעשות משהו". רמת ודאות נמוכה של הייחוס עשויה לשמש כתירוץ לא לעשות דבר.

מסגרת לתגובה

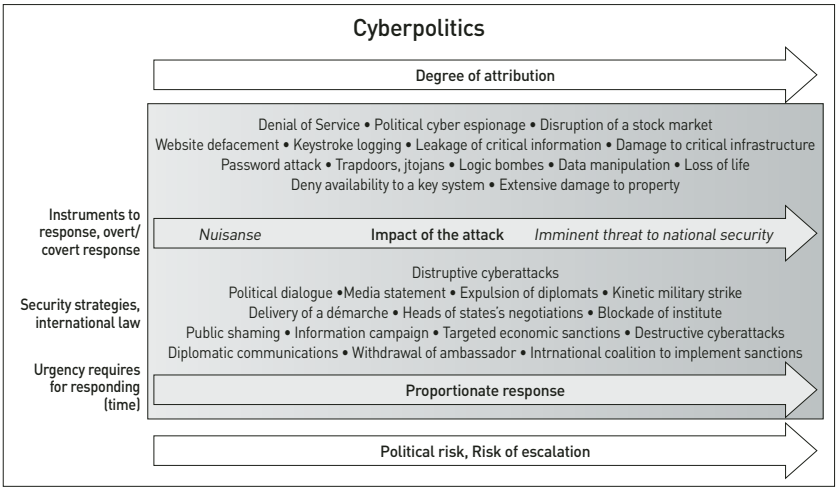
פעולות עוינות בסייבר מציבות ממשלות בפני תהליך מורכב של קבלת החלטות, החל מהבנת רמת הייחוס וחומרת הפגיעה ועד הערכת התגובה המידתית הראויה והסיכונים הכרוכים בנקיטת דרכי פעולה מסוימות. מקבלי ההחלטות גם חייבים להעריך את היכולות של הכלים הקינטיים והלא קינטיים שבידיהם, וזאת במצב של לחץ זמן ושל לחץ פוליטי גובר. פסיביות מול מתקפת סייבר עלולה לעודד יריבים להיות יותר אגרסיביים.

קובעי המדיניות צריכים להיות פרואקטיביים בקביעת אפשרויות התגובה המתאימות. פיתוח מסגרת תגובה למתקפות סייבר יאפשר לקובעי המדיניות לשקול פתרונות במהירות ולאמץ אופציות שכבר נותחו מבחינת יתרונות והשלכות אפשריות. זיהוי מראש של התגובה הראויה יכול לחסוך למדינה טעויות העלולות לסכן שלא במתכוון אינטרסים פוליטיים, כלכליים, מודיעיניים וצבאיים. למרות

30 Martin C. Libicki, "Cyberwar Fears Pose Dangers of Unnecessary Escalation", *RAND Review*, Summer 2013, http://www.rand.org/pubs/periodicals/rand-review/issues/2013/summer/cyberwar-fears-pose-dangers-of-unnecessary-escalation.html.

שכול תגובה היא ספציפית למקרה (תלוית מצב), המסגרת תאפשר לקובעי המדיניות לשקול במהירות את האפשרויות העומדות לרשותם.

תרשים 1 מציג דוגמה כללית למסגרת שעל קובעי המדיניות לבנות כדי לקבוע את התגובות הפוטנציאליות לפעולה עוינת בסייבר עוד לפני שזו התרחשה. המסגרת נותנת למקבלי ההחלטות בסיס לביצוע הערכות לגבי המהלך שיש לנקוט בעת משבר. בעזרת שילוב של מידת הייחוס, השפעת האירוע, האפשרויות המדיניות, הסיכונים, אסטרטגיות הביטחון, הדין הבין־לאומי, הדחיפות והמידתיות, מתוארים המנופים השונים של פוליטיקת הסייבר שיש ליישמם כתגובה לרמות ההסלמה וחומרת ההתקפה. מטרתה של המסגרת (שמוצגת כאן בהפשטה מכוונת) היא להמחיש את ההיבטים השונים שעל קובעי המדיניות לנתח בזהירות כאשר מדינה שוקלת מגוון אפשרויות ותגובות למתקפת סייבר, כולל החלטה לא לעשות דבר. על פי המסגרת, ככול שמתקפת הסייבר חמורה יותר, כך התגובה צריכה להיות חזקה יותר. המסגרת מדגימה את השפעתה וחומרתה של מתקפת סייבר, כאשר הפלת אתר נמצאת בקצה אחד של הסולם ואובדן חיים – בקצה השני. ממד זה מנותח כנגד רמת התגובה, שנעה מהצהרות לתקשורת ועד תגובה צבאית. אפשרויות התגובה יכולות להיות חשאיות לחלוטין ו/או גלויות לחלוטין, ולעשות שימוש בכלים שונים. קשת התגובות מציגה הן את הסיכונים הפוליטיים והמשפטיים הטבועים בכול החלטה והן את העלייה בסיכון במקביל לעלייה ברמת התגובה.



תרשים 1: מסגרת תגובה פוליטית

על פי Feakin, קובעי המדיניות צריכים להבין היטב את העלויות הכרוכות בכול תגובה.[31] לכול תגובה תהיה השפעה על היחסים הדיפלומטיים, המוניטין, העוצמה והפעולות הצבאיות והמודיעיניות של המדינה. ההשלכות צריכות להיות ברורות לפני בחירת התגובה. הערכת האופציות מחייבת תשומות מצד גורמים ממשלתיים רלוונטיים, וכן מצד חברות פרטיות שפעילותן ועסקיהן עשויים להיות מושפעים מהתגובה.

אין לפרש את המסגרת כ"קווים אדומים" פוליטיים לתגובות מסוימות. שני ממדים צריכים להילקח בחשבון בעת קביעת "קווים אדומים" לגבי פעולות עוינות בסייבר: מצד אחד, "קו אדום" מזמין יריבים לפעול מתחת לו, מתוך מחשבה שהם ייהנו מחסינות או מסיכון פוליטי נמוך בביצוע פעולות מסוג זה. "קווים אדומים" גם יכולים לדחוף מדינה לפינה, כך שתיאלץ להגיב כאשר הקו נחצה כדי לשמור על אמינותה. לפיכך, יש להניח שמדינות יעדיפו לא להיות ספציפיות מדי בעת שהן משתפות את הציבור בתגובותיהן האפשריות לחצייה "קווים אדומים"; מצד שני, קביעת "קווים אדומים" היא מסר חזק של הרתעה ליריביה של מדינה, שמבהיר כי המדינה תגיב אם הגבול שנקבע ייחצה. מידה מסוימת של עמימות עשויה להיות הפתרון הטוב ביותר מבחינה פוליטית: המדינה מודיעה כי תהיה תגובה, אך אינה חושפת את פרטי התגובה מראש.

מסקנות

עולם הסייבר מעצב יותר ויותר את סביבת הביטחון העולמית ואת הדינמיקה של הכוח בין מדינות ושחקנים אחרים. במקביל, יכולות הסייבר הולכות ומשתכללות. העולם נכנס לעידן לא יציב ולא ודאי, ועושה זאת ללא מפת דרכים ברורה של עקרונות פוליטיים. מדינות המבקשות להגיב על פעולות עוינות בסייבר מנסות לנווט בגבולות המקובל והמידתי. כאשר מדינות מנסות לקבוע מהי הדרך המידתית להגיב לסוגים שונים של מתקפות ברשת, גובר הצורך שלהן בהבנה פוליטית ובמחויבות פוליטית. כשמדובר בביטחון סייבר, פעמים רבות מדי מושם דגש על הפרטים הטכניים, מבלי להבין את ההקשר הפוליטי. בסופו של דבר, ההחלטה אם התקפה ברשת היא מעשה מלחמה או משהו אחר היא קביעה פוליטית, בייחוד במקרים הנמצאים בתוך "השטח האפור" שבין התקפה שתוצאתה היא שיבוש בלבד ובין התקפה המנסה לשים קץ לעצם קיומה של מדינה.

נדרשות מומחיות פוליטית ובקיאות בנושאי סייבר כדי לפעול כיום בתוך "סביבת ביטחון היברידית ובלתי צפויה". אין ספק שהחשיבות של פוליטיקת הסייבר תגדל בשנים הקרובות. יותר מכך, קובעי המדיניות ייאלצו להמשיג מחדש

31 Feakin, "Developing a Proportionate Response to a Cyber Incident".

את המונחים "לוחמת סייבר" או "עימות סייבר" ולראות בהם צורה של "לוחמה היברידית" המתנהלת גם בימי שלום.

הפרוטוקולים המשמשים כיום למתן מענה לפעולות עוינות בסייבר אינם ברורים, ויש לפרש מצב זה כהיעדר עוצמה מספקת להתמודד עם מרחב זה. מאמר זה ביקש להציג מסגרת לתגובה פוליטית על מתקפות סייבר, שתשמש כנקודת מוצא לממשלות ולמקבלי החלטות לגיבוש דרכי פעולה ותגובות ספציפיות לכול מדינה. הלחץ הצפוי על ממשלות להגיב על התקפות סייבר מחייב את קובעי המדיניות לפתח מסגרת תגובה הולמת קודם להתרחשותן של פעולות עוינות או הרסניות במרחב הסייבר. המסגרת שהמאמר הציע מציגה את המשתנים העיקריים שיש לקחת בחשבון בעת גיבוש תגובה להתקפת סייבר. היא גם מעודדת ממשלות לפתח את מוכנותן ויכולותיהן כדי לגבש תשובות לשאלות המוצגות במסגרת המוצעת, וזאת לפני שיחליטו כיצד להגיב.

הכנת מסגרת לתגובה פוליטית אין פירושה שייעשה בה שימוש בדיוק באותה דרך. סיבה אחת לכך היא התפתחותן הרצופה של שיטות חדשות לניצול מרחב הסייבר. בפוליטיקה וגם בפוליטיקת הסייבר נשמרת תמיד גמישות, וזאת בהתאם לזהותם של מקבלי ההחלטות ולעמימות המצב. מאחר שלכול מדינה יש מאפיינים תרבותיים, פוליטיים וצבאיים משלה, כל מדינה צריכה לפתח מסגרת מדיניות מותאמת לה. מה שנכון למסגרת לאומית אחת, אינו נכון בהכרח למסגרת לאומית אחרת.