ארבעה עקרונות ועוד אחד: מודל חדש להגנת סייבר

מת׳יו כהן, צ׳אק פרייליך, גבי סיבוני

כמו בכול האיומים המתעוררים, גם מרחב הסייבר מציב סכנות חדשות שלא קל לתת להן מענה. מאמר זה טוען כי איומי הסייבר אינם שונים במהותם מאיומים אסימטריים אחרים, ומציג מודל קונצפטואלי לפיתוח תגובה, תוך הסתמכות על העקרונות הקלאסיים של האסטרטגיה הצבאית: התרעה, הרתעה, התגוננות והכרעה, ולצד אלה את עקרון החוסן. המאמר מציע מודל למדיניות המתייחסת לכול אחד מהעקרונות הללו, באופן שישפר את הביטחון של מערכות סייבר לאומיות. המסגרת המוצעת תאפשר פיתוח אסטרטגיות ותוכניות מפורטות שיענו על הדרישות הספציפיות הנובעות מאיומי הסייבר, בין אם הם באים מצד מדינות ובין אם מצד שחקנים לא מדינתיים או מצד גורמים יחידים.

מילות מפתח: סייבר, התרעה, הרתעה, התגוננות, הכרעה, חוסן

מבוא

מרחב הסייבר הוא מקום מסוכן עבור מדינות. ב־2016 הודיעה קבוצה שכינתה עצמה "סוחרי הצללים" ("Shadow Brokers") כי גנבה בהצלחה קוד מסווג של תוכנות נוזקה שהיו בשימושה של הסוכנות לביטחון הלאומי של ארצות הברית (NSA) – גוף המסווג כסודי ביותר. חלק מהקוד, שנועד לפעולות ריגול, זמין כעת להורדה באינטרנט, ואת חלקיו האחרים הציעו ה"סוחרים" למכור לכול מי שיהיה מוכן לשלם להם את המחיר הגבוה שדרשו.[1]

1 Paul Szoldra, "New Snowden Documents Prove the Hacked NSA Files are Real", *Business Insider*, August 19, 2016, http://www.businessinsider.com/snowden-confirm-hacked-nsa-files-2016-8.

מת׳יו כהן הוא דוקטורנט ומרצה במחלקה למדעי המדינה באוניברסיטת Northeastern בארצות הברית. ד"ר צ׳ק פרייליך הוא עמית בכיר במרכז בלפר באוניברסיטת הרווארד, לשעבר סגן ראש המל"ל. ד"ר גבי סיבוני הוא חוקר בכיר וראש תוכנית צבא ואסטרטגיה ותוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.

ב־2015 הודיעה ארצות הברית כי פצחנים (האקרים) חדרו למערכות מחשב רגישות בבית הלבן, וציינה שהאירוע נחשב לאחת ממתקפות הסייבר המתוחכמות ביותר ששוגרו אי פעם נגד מערכות הממשל בארצות הברית. החשודה המתבקשת באירוע זה הייתה רוסיה.[2] באותה שנה שיגרה קוריאה הצפונית מתקפת סייבר נגד מתקן הגרעין של קוריאה הדרומית, אירוע שעורר חששות לגבי מידת הבטיחות של תחנות הכוח הגרעיניות של האחרונה.[3] ב־2014 תקפו פצחנים את השרתים של חברת "סוני", פרסמו הודעות דוא"ל פרטיות ושלחו איומים חריפים נגד החברה ונגד כל בית קולנוע שיעז להקרין סרט סטירי על קוריאה הצפונית. ארצות הברית האשימה את פיונגיאנג במתקפה, וציינה כי תגיב עליה "באופן מידתי". זמן קצר לאחר מכן חווה שירות האינטרנט של קוריאה הצפונית שיבושים שנמשכו מספר ימים.[4] אלו הן דוגמאות מעטות בלבד למתקפות סייבר מהשנים האחרונות.

מאמר זה מבקש לטעון כי למרות שאיומי הסייבר הם בעלי מאפיינים שחלקם מאתגרים במיוחד, ניתן לגבש להם תגובה יעילה. לשם כך דרוש מודל קונצפטואלי שיהווה מסגרת לדיון על חומרתם של איומי הסייבר השונים, הטכנולוגיות שיש לפתח והמדיניות הממשלתית הנדרשת בעניין זה. המאמר מציע מודל קונצפטואלי כזה באמצעות הסתמכות על ארבעת העקרונות הקלאסיים של האסטרטגיה הצבאית – הרתעה, התרעה, התגוננות והכרעה – ולצדם המושג הידוע פחות – חוסן. בנוסף לכך מנתח המאמר כיצד ממשלות, צבאות וגופים פרטיים יכולים לפעול יחדיו בתוך המסגרת המוצעת כדי להתמודד עם איומים במרחב הסייבר.

ארבעת העקרונות הקלאסיים שהוזכרו לעיל מוכרים ומיושמים על ידי ממשלות ברחבי העולם, אולם מוגדרים לעתים בצורה שונה על ידי שורה של חוקרים ומדינות. לדוגמה, "האסטרטגיה הלאומית למאבק בטרור" של ארצות הברית משנת 2003 מיישמת מודל של ארבעה עקרונות שהיא מכנה בשם "הבסה, מניעה, צמצום והתגוננות" (Defeat, Deny, Diminish, Defend).[5] לעומת זאת, ישראל מבססת את תפיסת הביטחון הלאומי שלה מזה עשרות שנים על מודל שלושת

---

2 Evan Perez and Shimon Prokupecz, "How the U.S. Thinks Russians Hacked the White House", *CNN*, April 8, 2015, http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html.

3 K. J. Kwon, "Smoking Gun: South Korea Uncovers Northern Rival's Hacking Codes", *CNN*, April 22, 2015, http://www.cnn.com/2015/04/22/asia/koreas-cyber-hacking/index.html.

4 Haroon Siddique, "North Korea Responds with Fury to US Sanctions over Sony Pictures Hack", *The Guardian,* January 5, 2015, http://www.theguardian.com/world/2015/jan/04/north-korea-fury-us-sanctions-sony.

5 "National Strategy for Combating Terrorism", US Department of State, February 2003, https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf.

העקרונות – התרעה, הרתעה והכרעה[6] – ומאוחר יותר הוסיפה עיקרון רביעי התופס גם עבור איומי הסייבר – התגוננות.[7]

שום מחקר לא החיל עד היום אסטרטגיה מקיפה של ארבעת העקרונות דלעיל על איומי הסייבר, אם כי היו מחקרים שעסקו בכול אחד מעקרונות אלה בנפרד. כל מחקר כזה העלה תובנות חשובות על מרחב הסייבר, אך ארבעת העקרונות, בשילוב מושג החוסן, כוללים מרכיבים בעלי קשר הדדי שעלולים להיעלם כאשר סוקרים אותם בנפרד. לפיכך, רק מסגרת אנליטית הוליסטית הבוחנת עקרונות אלה ביחד תוכל להגיע להבנה מלאה יותר של איום הסייבר, וזאת לא רק למטרות אקדמיות, אלא גם לצורך קביעת מדיניות.

הגדרת עולם הסייבר

מונחים רבים הנוגעים למרחב הסייבר חסרים הגדרות ברורות ומוסכמות. לצורך הטיעונים של מאמר זה, מתקפת סייבר תוגדר כשימוש פוגעני במרחב הסייבר, אשר משבש מחשבים, רשתות או טכנולוגיות אחרות, או מנצל אותם למטרות פוליטיות או פליליות מזיקות, הרסניות או משבשות.[8] בדומה לצורות אחרות של לוחמה, גם מתקפות סייבר בעלות מניע פוליטי נועדו לספק יתרון אסטרטגי, דיפלומטי, כלכלי או צבאי על פני היריב, או לאלץ אותו לנקוט פעולה נגד רצונו.[9] מתקפות סייבר יכולות להיות משוגרות על ידי מדינות, ארגונים שאינם מדינה או אנשים.

הגנת סייבר כוללת את המאמצים שנועדו להבטיח את שמירת השליטה על ספקי שירותי האינטרנט (ISP) ועל התעבורה הנכנסת והיוצאת, וכן את היכולת לעצור מתקפות בעת התרחשותן.[10] ריגול סייבר מתייחס לשימוש שעושות מדינה או סוכנויות לאומיות כמו ה־NSA (לעתים קרובות באמצעות תוכנות זדוניות או

---

6 Matthew S. Cohen, Chuck Freilich and Gabi Siboni, "Israel and Cyberspace: Unique Threat and Response", *International Studies Perspectives* 17 (2016): 307-321; Chuck D. Freilich, "Why Can't Israel Win Wars Anymore?", *Survival* 57, no. 2 (2015): 79-92.

7 "The IDF Strategy", IDF Chief of the General Staff, Israel Defense Forces, July 2016, https://www.idfblog.com/s/Desktop/IDF%20Strategy.pdf.

8 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Rand Corporation: Project Air Force, 2009); Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Harper Collins, 2012); Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015).

9 Jeffrey Carr ed., *Inside Cyber Warfare* (Cambridge: O'Reilly, 2012); Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber-Attack", *California Law Review* 100, no. 4 (2011): 817-886; Valeriano and Maness, *Cyber War versus Cyber Realities*.

10 Chris C. Demchak, *Wars of Disruption and Resilience* (Athens: University of Georgia Press, 2011); Valeriano and Maness, *Cyber War versus Cyber Realities*.

פריצות, כגון spear-phishing) במטרה לגנוב או לאסוף מידע, או כדי לדעת מהי יכולת התוקפים לחדור לרשתות.[11]

ארבעה עקרונות ועוד אחד

בחלק זה אנו מבקשים לטעון כי ניתן לטפל ביעילות באיומי סייבר על סמך העקרונות הבסיסיים של האסטרטגיה הצבאית ובאמצעות כמה התאמות שלהם. מדובר בהרתעה, התרעה, הכרעה והתגוננות, ובנוסף לכך במושג החוסן החדש יותר.

הרתעה

כדי להרתיע יריב, יש לזהות ולהכיר את "כתובת המען" שלו שנגדה ניתן לפעול. אחד האתגרים הקשים במיוחד בתחום הסייבר הוא הייחוס. ההרתעה במרחב הסייבר מסובכת גם בשל העובדה שלא תמיד ניתן לדעת מתי נגרם נזק, וייתכן מצב שבו המטרה אפילו לא תדע שהיא הותקפה.[12]

רמת הוודאות של הייחוס היא שתקבע את סוג התגובה שעל המדינה ליישם. רמה נמוכה יחסית של ודאות מספיקה כדי להפעיל דיפלומטיה "מאחורי הקלעים". במגעים דיפלומטיים כאלה, מדינה יכולה להאשים מדינה אחרת על שניסתה להתערב ולהשפיע על התנהגותה, גם אם אין לה הוכחה מוחלטת לכך. להאשמה פומבית נדרשת כבר רמה בינונית של ודאות, ולביצוע פעולה משפטית או צבאית תידרש רמת הוודאות הגבוהה ביותר.

במקרים של מתקפות סייבר הניתנות לייחוס, סוג השחקן (מדינה, ארגון טרור, ארגון לא מדינתי או גורם יחיד) ממלא תפקיד חשוב בקביעת אופייה של מדיניות ההרתעה. הרתעת גורמים מדינתיים מפני ביצוע מתקפות סייבר אינה שונה מהותית מהרתעתם מפני עימותים מסוגים אחרים. במקרה זה, המדינה המותקפת יכולה להגיב בכול קשת היכולות העומדות לרשותה – סייבר, דיפלומטיה, צבא או כלכלה.

הרתעת ארגוני טרור מלבצע מתקפות סייבר דומה למניעת פיגועים פיזיים, וכוללת הפעלת מגוון רחב של פעולות תגמול אפשריות בסייבר ומחוץ לסייבר. מרבית ארגוני הטרור פועלים לכאורה בשם ערכים מסוימים, אם כי החשיבות שהם מייחסים לערכים אלה והמוכנות שלהם לסבול בגינם עשויות להיות שונות מאלו של מדינות. יכולת התגמול על מתקפות סייבר של ארגוני טרור הינה מוגבלת בשל אותם שיקולים החלים על ההחלטה לנקוט נגדם תגמול פיזי, לרבות שיקולי מרחק ופגיעות. הרתעת טרוריסטים היא אתגר מורכב בדיוק כמו בעולם הפיזי, ולכן גם קשה להרתיע ארגוני טרור מלתקוף במרחב הסייבר.

---

11 P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York: Oxford University Press, 2014); Valeriano and Maness, *Cyber War versus Cyber Realities*.

12 Libicki, *Cyberdeterrence and Cyberwar*.

המספר הרב של ארגונים לא מדינתיים ושל תוקפים בודדים (פצחנים ואקטיביסטים) פוטנציאליים המפוזרים ברחבי העולם מהווה אתגר ליכולות הניטור והייחוס הנדרשות לצורך ההרתעה. עם זאת, יכולות הסייבר המתוחכמות של המדינה עשויות להקשות על ארגון או אדם להסתיר את זהותו. "החדשות הטובות" בנוגע ליחידים ולארגונים לא מדינתיים הן שלרוב יש להם פחות משאבים כדי לשגר מתקפות סייבר משתקות נגד מדינות מפותחות. זאת ועוד, אחד המניעים העיקריים שלהם הוא לעתים קרובות עצם הפרסום, עובדה שמסייעת לייחס את הדברים לאותם יחידים וארגונים לא מדינתיים. גם פיתוח כלים טובים יותר לזיהוי פלילי – מאמץ שכבר נמצא בעיצומו – יעזור לקבוע מי שיגר את המתקפה.

התרעה

זיהוי מראש או התרעה מוקדמת של התקפות מתקרבות הם קריטיים במרחב הסייבר, כמו בעולם הפיזי. מניעת המתקפה היא אפשרית רק אם יש התרעה מוקדמת מספיקה. בדרך כלל גם קל יותר להתגונן מפני התקפה שלגביה יש התרעה. למדינות מעטות בלבד, לא כל שכן לגורמים לא מדינתיים, יש את היכולות הנדרשות כדי לנהל בהצלחה מתקפת סייבר גדולה נגד מדינה בעלת יכולות הגנה משוכללות. האתגר האמיתי של גילוי מתקפת סייבר טמון לא במספרם העצום של התוקפים הפוטנציאליים ברחבי העולם, אלא במספרם המוגבל למדי של המתוחכמים שבהם. במצב זה, ההתמודדות עם המתקפה הופכת לאפשרית יותר.

המרכיב שמסבך את התמונה הוא התחזקות הקשרים ההדדיים בין הרשתות הממשלתיות, הצבאיות והפרטיות. רשתות של המגזר הפרטי יכולות כיום לשמש כשער כניסה לרשתות ממשלתיות וצבאיות מסוימות, ופירוש הדבר הוא שהמגזר הפרטי מהווה נקודת תורפה לפגיעויות. על רקע זה, מדינות מתמודדות עם הצורך לספק התרעה מוקדמת לא רק למערכות ממשלתיות ולתשתיות קריטיות, אלא גם לחברות ולארגונים מרכזיים. חלק מהמדינות כבר החלו להשקיע מאמצים מוגברים באיסוף מודיעין והגדילו את שיתוף המידע עם המגזר הפרטי, אך שיתוף מידע בין ממשלות לחברות פרטיות נותר עדיין, ככלל, אתגר משמעותי. הגברת מאמצים לשיתוף פעולה כזה עשויה לחייב, ככול הנראה, שינויים משפטיים, ארגוניים ופוליטיים בממשלות ובארגונים גם יחד.[13]

הטכנולוגיה היא מרכיב קריטי במערכות לאומיות שנועדו להתריע בפני איומי סייבר. מאמצי ההתרעה נגד מתקפות סייבר יקבלו חיזוק משמעותי על ידי הגברת

13 Aviram Zrahia, "A Multidisciplinary Analysis of Cyber Information Sharing", *Military and Strategic Affairs* 6, no. 3 (2014): 59-77.

איסוף המודיעין המסורתי על תוקפים פוטנציאליים, וזאת לצד המידע שנאסף עליהם באינטרנט.[14]

מספר גורמים פועלים לטובת הצד המתגונן. מתקיפים מבַצעים לעתים קרובות "משימות סיור בסייבר" כדי להעריך את נקודות התורפה במערכות הצד המתגונן.[15] ככול שמתקפת סייבר מתוכננת או מתמשכת היא גדולה יותר, כך קל יותר ליירט את התקשורת בין התוקפים וליישם פעולת הגנה. זאת ועוד, המספר הקטן של כבלי התקשורת הנושאים את תעבורת האינטרנט הופך את בעיית ההתרעה לפשוטה יותר עבור מדינות רבות.

התגוננות

התגוננות עוסקת במניעה ובצמצום של מתקפות על רשתות תשתית צבאיות, ממשלתיות וקריטיות, וכן על רשתות פרטיות, עסקיות ושל יחידים. שחקנים שונים מסוגלים לבצע סוגי מתקפות בעלות אופי שונה ודרגות חומרה מגוונות, ולכן מקור המתקפה קובע מהם האמצעים הטובים ביותר להתגונן מפניה. בדרך כלל קשה יותר להתגונן מפני התקפות מצד מדינות, בעוד שהיכולות הטכנולוגיות של ארגונים ואנשים שאינם מדינה הן פחות מתקדמות, וניתן לטפל בהן באמצעות פתרונות טכנולוגיים פשוטים יחסית.

הטכנולוגיה ממלאת תפקיד מרכזי במאמץ ההגנתי ומדינות שונות כבר החלו בבניית תוכניות שיסייעו בהגנה על רשתות ומערכות סייבר. פיתוח של טכנולוגיות המסוגלות להתמודד עם סוגים שונים של איומים הוא כמובן מטרה רצויה, אך אילוצי המשאבים מחייבים מדינות לתת עדיפות לאיומים הדחופים ביותר, שבהם הן יוכלו למקד את משאביהן. זהו תחום נוסף שבו ממשלות והמגזר הפרטי יכולים לפעול יחדיו. שיתוף פעולה כזה יגדיל את יכולתם של שני הצדדים לזהות את האיומים הגדולים וליצור כלים חדשים להגנה מפניהם. גם אם חברות אבטחת סייבר פרטיות יבחרו שלא לשתף פעולה עם ממשלות, אותן ממשלות יוכלו להפיק תועלת מעצם ההתבוננות מקרוב באיומים בהם עוסקות אותן חברות, כבסיס להערכת האיומים שהן יבצעו. ממשלות גם יכולות לשתף פעולה עם גורמים פרטיים כדי להבטיח שמערכות אבטחה ברשתות המתחברות למערכות ממשלתיות ישמרו על עדכניותן.[16]

---

14 Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy* (Tel Aviv: Institute for National Security Studies, 2016).

15 Ned Moran, "A Cyber Early Warning Model", in *Inside Cyber Warfare*, ed. Jeffrey Carr.

16 William J. Lynn, "Defending a New Domain", *Foreign Affairs*, October 2010, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain; Milton L. Mueller, Andreas Schmidt and Brenden Kuerbis, "Internet Security and

הגנת סייבר לא יכולה להיעשות רק באינטרנט. נדרש מאמץ רב־שכבתי של איסוף מידע מודיעיני, שיבוש מתקפות ואבטחת רשתות, נקיטת צעדים משפטיים, גיבוש נורמות התנהגות חדשות ועידוד שיתוף פעולה אפקטיבי עם ממשלות זרות. נכון להיום, אין נורמות או חוקים בין־לאומיים ברורים לגבי התנהגות במרחב הסייבר,[17] אף שאמנות, חוקים ונורמות יכולים להתגלות כיעילים להגבלת פעולות זדוניות של מדינות במרחב זה. כדי להשיג יעילות בהתגוננות מפני התקפות סייבר, על מדינות להסכים ביניהן מהם סוגי הפעילות הרלוונטיים, מה אחריות המדינה במסגרת ההסכמה ומה יהיה העונש על הפרתה. בנוסף, מדינות יצטרכו להקים גופים בין־לאומיים שיפקחו על הציות לאותן הסכמות.[18]

חשיבות רבה יש לשיתוף פעולה בין־לאומי. גידול במספר המדינות שישתפו פעולה ביניהן בנושא ביטחון הסייבר יביא תועלת למדינות רבות. שיתוף מודיעיני, הסכמים דו־צדדיים ורב־צדדיים ושיתוף פעולה משופר עם רשויות אכיפת החוק במדינות אחרות, יכולים לתרום רבות לתכנון אסטרטגיות הגנה.[19] יהיה צורך בשיפור שיתוף הפעולה בין מדינות גם כדי להבטיח את אכיפת החוקים והנורמות החדשים.[20]

הבסה

עקרון ההבסה בעולם הסייבר אין פירושו מניעה מוחלטת של כל התקפת סייבר. למעשה, הבסה מוחלטת היא נדירה למדי הן בעולם הפיזי והן בעולם הסייבר. לכן, יש לראות את הבסת היריב בסייבר כמפחיתה את ההיקף והחומרה של המתקפות

Networked Governance in International Relations", *International Studies Review* 15, no. 1 (2013): 86-104; Ido Naor, "ATMZombie: Banking Trojan in Israeli Waters", *SecureList*, February 29, 2016, https://securelist.com/blog/research/73866/atmzombie-banking-trojan-in-israeli-waters/; Teri Radichel, "Case Study: Critical Controls that could Have Prevented Target Breach", *SANS Institute*, 2014, https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.

17 Abraham D. Sofaer, David Clark and Whitfield Diffie, "Cyber Security and International Agreements", *Proceedings of a Workshop on Deterring Cyber-Attacks: Informing Strategies and Developing Options for U.S. Policy* (Washington DC: National Academies Press, 2010), http://www.nap.edu/catalog/12997.html; Valeriano and Maness, *Cyber War versus Cyber Realities*.

18 Sofaer, Clark and Diffie, "Cyber Security and International Agreements".

19 "International Public Private Partnership in Cyber Governance (Panel)", *CYFY, 2013 Report*, The India Conference on Cyber Security and Cyber Governance, Observer Research Foundation, http://www.bic-trust.eu/files/2014/04/CYFY-2013-Report-WEB-version-15Apr14.pdf.

20 Sofaer, Clark and Diffie, "Cyber Security and International Agreements".

לרמה המאפשרת לחברה לשמור על אורח חייה ולחזור במהירות לשגרה לאחר המתקפה (ראו בהמשך פירוט בסוגיה זו בפסקה על נושא החוסן).

כדי להשיג הבסה בעולם הסייבר, על המדינה להיות מסוגלת להוכיח ליריביה שביכולתה למנוע מתקפות סייבר גדולות; שהתקפות הסייבר שהיא לא הצליחה למנוע אינן משיגות את מטרתן, בין משום שהן לא גרמו נזק משמעותי ובין משום שהמדינה יודעת לחזור במהירות לשגרה; וכן שמתקפות סייבר ייתקלו בפעולת תגמול כזו או אחרת. כללית ניתן לקבוע כי השגת הבסה מחייבת מדינות להיות מסוגלות ליישם בהצלחה את כל אחד מארבעת העקרונות שנמנו עד כה, בתוספת עקרון החוסן.

מדינות צריכות לייחס למתקפות סייבר את אותה החשיבות שהן מייחסות למתקפות פיזיות, ובמידת הצורך להשתמש בשיטות ובאסטרטגיות דומות, כמו תגובה שאינה מגבילה עצמה לכלי סייבר אלא פונה גם ליכולות צבאיות.[21] שיגור התקפות צבאיות נגד מדינות הוא מהלך ישיר וברור, אך כשמדובר בשחקן לא מדינתי, המהלך הרבה יותר מסובך ומחייב את יוזם ההתקפה הצבאית להשיג את אישורה של המדינה המארחת, שאם לא כן הוא מסתכן בהסלמה צבאית. בנוסף לכך, יש לקחת בחשבון כי התגובה הציבורית לתקיפה צבאית שתבוא כצעד תגובה למתקפת סייבר של גורם לא מדינתי, עשויה להיות שלילית.

אופיו הלא ממוקד של איום הסייבר גורם לכך שמדינות אינן יכולות לצפות למנוע את כל מתקפות הסייבר מכול גורם יחיד או ארגון לא מדינתי בכול רחבי העולם. מדינה יכולה להביס את היריב במרחב הסייבר על ידי מזעור הסיכוי להתקפה גדולה שיש בה כדי להסב שיבושים או נזקים נרחבים. אם היריב לא הצליח להוציא לפועל מתקפה גדולה, הוא למעשה הובס. במרבית המתקפות מצד יחידים וגורמים לא מדינתיים, התגובה ההולמת יותר היא ההגנה, שיש בה שימוש נכון יותר במשאבים, במיוחד כאשר הגורמים התוקפים לא מחזיקים ביכולות לגרימת נזקים חמורים.[22] הגברת שיתוף הפעולה הבין־לאומי יכולה לשפר את יכולתן של מדינות להכריע שחקנים כאלה באמצעות הטלת עונשים משפטיים ופליליים על התקפות חוצות גבולות.[23] בסופו של דבר, על מדינות להציב מטרות מציאותיות יותר בבואן להביס מדינות, ארגוני טרור וארגונים לא מדינתיים המשתמשים בנשק הסייבר.

---

21 Robert Hackett, "Let's Get Physical? United States Weighs Options When it Comes to Cyber Attacks", *Fortune*, May 12, 2015, http://fortune.com/2015/05/12/rogers-cyber-attacks-us-response/.

22 Herbert S. Lin, "Offensive Cyber Operations and the Use of Force", *Journal of National Security Law and Policy* 4, no. 63 (2010): 63-86.

23 Valeriano and Maness, *Cyber War versus Cyber Realities*.

חוסן

כאשר מתקפה מצליחה, מתעוררת השאלה כיצד יש לנהל את המערכת הפגועה ולהתאושש מהר ככול האפשר, כלומר כיצד יש לבנות מראש מערכות בעלות "חוסן". מערכות שונות יחייבו רמות שונות של חוסן. רשתות מסוימות צריכות לחזור במהירות לרמה מינימלית בלבד של תפקוד, בעוד שאחרות חייבות לחזור לרמת התפקוד המקורית שלהן בהקדם האפשרי.

תהליך הבנייה של מערכות בעלות חוסן במרחב הסייבר מתחיל בניסוח תרחישים בעלי סבירות גבוהה ועלות נמוכה, לצד תרחישים בעלי סבירות נמוכה אך עלות גבוהה. לאחר שלב גיבוש התרחישים, ניתן לבנות תוכניות וכלים להתמודדות עם האיום. דבר זה חייב להתבצע לפני שלב הכישלון בהתגוננות, ולכלול אמצעים טכנולוגיים, פיתוח משאבי אנוש, אימונים ותרגילים, וכן אמצעי יישום.[24] החוסן בהקשר של תחום הסייבר חייב לכלול גם תוכניות לשיקום מפגיעות פיזיות בעקבות מתקפות סייבר.

משאבים הינם מצרך מוגבל מטבעו, ופירוש הדבר שיש חשיבות קריטית לתעדוף המערכות הדורשות חוסן. לדוגמה, מערכות צבאיות ורשת החשמל חשובות למדינה הרבה יותר מאשר רשתות אחרות. ניתן לפתח מדדים כדי לקבוע אילו מערכות הן הקריטיות ביותר והיכן יש להשקיע משאבים טכנולוגיים.[25] ההשפעה של רשת או תשתית פגועות על המורל הציבורי ועל אמונת האזרחים ביכולת ממשלתם לספק מוצרים ציבוריים בסיסיים, היא שיקול מרכזי שיש להתחשב בו.

בניית החוסן גם דורשת עבודה צמודה עם המגזר הפרטי, מה גם וחברות פרטיות אחראיות פעמים רבות על תחזוקת מתקנים ורציפות פעילותם ועל טיפול באיומים. ממשלות צריכות לעבוד במשותף עם המגזר הפרטי, ובמקביל לפקח עליו, וזאת כדי להבטיח קיומן של תוכניות נאותות להתמודדות עם שירותים שנפגעו.[26]

המציאות מלמדת שיש להתכונן לכשלים בלתי צפויים בהגנת הסייבר, וכי התוצאות של כשלים כאלה עלולות להיות קיצוניות. מערכת בעלת חוסן יכולה ליצור את ההבדל בין התאוששות מהירה יחסית ובין תוצאות חמורות. איסוף מודיעין על תוכניות האויב או על יכולותיו הכלליות הינו חיוני לצורך תכנון

24 Singer and Friedman, *Cybersecurity and Cyberwar*; Valeriano and Maness, *Cyber War versus Cyber Realities*.

25 שם.

26 Dana Pasquali, "3 Steps Towards Building Cyber Resilience into Critical Infrastructure", *Dark Reading*, August 2, 2016, http://www.darkreading.com/vulnerabilities---threats/3-steps-towards-building-cyber-resilience-into-critical-infrastructure/a/d-id/1326464; Jan Trobisch, *Challenges in Protection of US Critical Infrastructure in the Cyber Realm* (Fort Leavenworth, KS: School of Advanced Military Studies, United States Army Command and General Staff College, 2014), https://www.hsdl.org/?abstract&did=791151.

ההתאוששות.[27] מערכות בעלות חוסן מצמצמות את השפעת ההתקפה, ובכך מקטינות את התמורה שמקבל התוקף.[28] עובדה זה כשלעצמה מקטינה את הסבירות לעצם התרחשות ההתקפה מלכתחילה.

עם זאת, גם לחוסן יש מגבלות. בסופו של דבר, מתקפה יכולה להפיל גם את המערכת וגם את אמצעי התגובה המיועדים להתמודד עם הפגיעה. מדינות חייבות להיות מוכנות לאפשרות כזו ולפתח תוכניות נוספות שיאפשרו המשך פעילות גם ללא המערכת, אפילו לתקופה ממושכת. מצב כזה צפוי לגרום לכפילות מסוימת ולהביא לפיתוח תוכניות שאינן תלויות בטכנולוגיה.

השלכות על המדיניות

בחלק זה נבקש לדון בהמלצות מדיניות ספציפיות שנגזרות ממודל ארבעת העקרונות ועקרון החוסן. כדי להשיג הרתעה, על מדינות להבהיר ליריביהן מהן פעולות התגמול הצפויות ואיזה מחיר הם עשויים לשלם. הצגת עמדותיו וכוונותיו של המרתיע יכולה להיעשות באמצעות הצהרות פומביות ו/או בערוצים סודיים.[29] הקושי הוא בקביעת הייחוס, שכן לא תמיד ברור מי צריך להיות היעד להצגת עמדות וכוונות אלו, אולם ניתן להתגבר על כך ככול שיכולות הייחוס הולכות ומשתפרות. יכולות ייחוס משופרות ישכנעו את היעד להרתעה כי הוא עתיד לשלם מחיר, ובנוסף לכך יסייעו למדינות למקד את עצמן ביתר יעילות באויבים הרלוונטיים.

אופי הממשל במדינה שממנה מגיעה מתקפת הסייבר, ובמיוחד נכונותו של אותו ממשל לשתף פעולה עם התוקפים, הם שני גורמים חשובים ביכולת של הגורם המותקף להגיב. במקרה כזה פעולת תגמול בסייבר אינה אפשרית, אלא אם כן המדינה המותקפת מוכנה לפגוע בריבונות המדינה שאירחה את תוקפי הסייבר. לחילופין, מדינה עשויה להצליח ליצור הרתעה באמצעות פעולה מול גופי המודיעין ורשויות החוק של הממשלה המארחת את תוקפי הסייבר. במקרים מסוימים, עצם הסיכוי לנקיטת צעדים משפטיים חמורים עשוי ליצור הרתעה מספקת. דרך זאת הינה מוגבלת למדי בשימוש כיום, דבר המאפשר לארגונים וליחידים לבצע התקפות סייבר.

כאשר מקורן של התקפות הסייבר הוא במדינות שאינן משתפות פעולה בהתמודדות עם איום הסייבר או אינן יעילות בכך, היכולת להרתיע אותן באמצעים משפטיים תהיה כמובן מוגבלת יותר. שאלת ההרתעה תהיה במקרה כזה דומה

27 Demchak, *Wars of Disruption and Resilience*.

28 "The DoD Cyber Strategy", US Department of Defense, 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

29 שם.

יותר לפעולת תגמול על התקפה פיזית, ותתמקד ביכולות הסייבר של התוקף או ביכולות אחרות שראוי לתקוף, ובמידת ישימותה של דרך פעולה כזו.

כמו בעולם הפיזי, כך גם בעולם הסייבר הבעיה האמיתית בהרתעת גורמים לא מדינתיים היא מידת הנזק שהם גורמים, שהוא בדרך כלל מוגבל. זאת, בעוד שיכולת הספיגה של אותם גורמים עולה לא פעם על עוצמת התגמול שהמדינה המותקפת מוכנה להפעיל. הדבר נכון במיוחד לגבי הדמוקרטיות המערביות. כמובן שדמוקרטיות מסוגלות להביס איומים מצד גורמים לא מדינתיים, אולם המאמץ הנדרש מהן כדי לעשות זאת, ובכלל זה הפגיעה והמחיר בחיי אדם, נתפס בדרך כלל כגבוה מדי בהשוואה למידת האיום שאותם גורמים מציבים על האינטרסים של המדינה. דבר דומה נכון גם לגבי מתקפות סייבר. יחד עם זאת, אם גורם לא מדינתי יוציא לפועל מתקפת סייבר קיצונית, או שיתגלה מידע אמין על מתקפה קרֵבה כזאת, אין ספק שהמדינה שתהיה נתונה למתקפה או לסכנה למתקפה כזאת תפגין מוכנות רבה יותר להפעיל אמצעי הרתעה חמורים.

כדי להשיג הרתעה, על מדינות להיות מסוגלות לקבוע ייחוס למתקפה. לשם כך, מדינות צריכות לעשות שימוש בכלים טכנולוגיים ומודיעיניים ולשפר אותם באופן מתמיד, כולל איסוף מידע על היכולות הטכנולוגיות של יריבים פוטנציאליים ועל יעדיהם.[30] זהו תחום שראוי שגופים פרטיים וממשלתיים ישקלו לשתף פעולה בו, וזאת נוכח העובדה שחברות פרטיות העוסקות בביטחון סייבר יכולות לזהות תוכנות זדוניות ולהציע תובנות לגבי מקורותיהן.[31]

קושי נוסף בהתמודדות עם התקפות סייבר הוא שניתן לנתב אותן באמצעות ספקי שירותי אינטרנט במדינות "צד שלישי". ממשלות יכולות לפעול יחד עם ספקי שירותי אינטרנט או הממשלות המארחות אותם, או להפעיל עליהם לחץ כדי שיעצרו את מתקפות הסייבר טרם התרחשותן.[32] אם לא מושג שיתוף פעולה כזה, ניתן לשקול תגובה שתכלול פרסום וביוש (שיימינג) פומבי של אותם מדינה, ארגון או אדם העומדים מאחורי המתקפה. יתרון נוסף של מהלך כזה הוא האזהרה שהוא מספק לשירותי הביטחון בעולם לגבי התוקף, אשר מקטינה את יכולתו לבצע מתקפות נוספות.

המאמצים לשיפור ההתרעה על מתקפות סייבר צריכים להתבסס הן על אמצעים מותאמים במיוחד לאיסוף מודיעין סייבר והן על הגדלת נתח משאבי המודיעין האלקטרוני והאנושי הקיימים שכבר מושקעים בתחום זה. טכנולוגיית הסייבר

30 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies* 38, no. 1-2 (2015): 4-37.

31 Grant McCool, "Computer Spying Malware Uncovered with 'Stealth' Features: Symantec", *Reuters*, November 23, 2014, http://www.reuters.com/article/us-symantec-malware-regin-idUSKCN0J70SH20141123.

32 Clarke and Knake, *Cyber War*.

אמנם יוצרת בעיות התרעה חדשות, אך גם מספקת אפשרויות חדשות בתחום ההתרעה.[33] כך, למשל, אסטרטגיית הסייבר הלאומית של אוסטרליה מדגישה נקודה זו, כשהיא קוראת להתרעה משופרת באמצעות ניטור רציף באינטרנט בזמן אמת.[34]

למרות שניתן לשגר בו־זמנית מספר עצום של מתקפות סייבר ממקורות שונים, טכנולוגיות סייבר יכולות לזהות מספר גדול לא פחות של מתקפות ולפעול נגדן. אחת האפשרויות (המתאימה בעיקר נגד תוקפים לא מדינתיים ונגד תוקפים יחידים) היא להתחזות לאקטיביסטים וחברים ברשתות הסייבר, וזאת כדי לאסוף מודיעין ומידע על יכולות ואמצעים.[35]

אחד הקשיים בגילוי מתקפות סייבר מצד מדינות או גורמים לא מדינתיים הוא שיגורן ממדינות ידידותיות, דבר המגביל את היכולת לעקוב אחריהן מבלי לפגוע בקשרים דיפלומטיים. הטכנולוגיה יכולה לסייע בכך, שכן היא מאפשרת גילוי מרחוק מבלי לפגוע בריבונותה של המדינה. מנגד, דווקא במצבים כאלה גובר הצורך בשיתוף פעולה בין־לאומי ובשיתוף מידע.

מדינות המעוניינות לחזק את יכולותיהן במונחים של התגוננות יכולות להתמקד בשיפור השימוש שהן עושות בטכנולוגיה. הגנה על עולם הסייבר מחייבת שיפור הטכנולוגיות הקיימות ויצירתן של טכנולוגיות חדשות. מנגנון ההגנה גם חייב להתאים למצב השורר ברגע נתון: בשלבים הראשונים של המתקפה, לפני שנגרם נזק ממשי או לפני שנפרצה מערכת כלשהי, ייתכן שיהיה די במאמצים לשבש או להטות את כיוון המתקפה. אם המערכת נפרצה או שנגרם נזק, על מנגנון ההגנה לנסות ולבלום את המתקפה, ובמקביל למנוע מהתוקף לדעת שהפריצה התגלתה ונבלמה בהצלחה.[36]

הגנה על רשתות הן במגזר הממשלתי והן במגזר הפרטי תדרוש חקיקה ותקנות חדשות. ייתכן שגם יהיה צורך בהקמת סוכנויות ממשלתיות חדשות שיעסקו בניסוח הדרישות הספציפיות ויבטיחו את יישומם של מנגנוני ההגנה. פיקוד הסייבר האמריקאי ורשות הסייבר הלאומית בישראל הם דוגמאות לגופים מרכזיים האחראים לפקח על גיבושן ויישומן של אסטרטגיות התגוננות בסייבר, במקביל למאמצי שיתוף פעולה עם המגזר הפרטי.

---

33 "The National Strategy to Secure Cyberspace", Department of Homeland Security, February 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

34 "Australian Government Cyber Security Strategy", Commonwealth of Australia, 2009, http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

35 "Impersonation", Microsoft, http://technet.microsoft.com/en-us/library/cc961980.aspx.

36 Siboni and Assaf, *Guidelines for a National Cyber Strategy*.

ממשלות, חברות פרטיות ואנשי אקדמיה צריכים לשתף פעולה ביניהם כדי לפתח אסטרטגיות וכלים טכניים חדשים להגנה וכדי לשפר את הכלים הקיימים. ממשלות יכולות להציע תמריצים כספיים על פי הצורך לגופים פרטיים שיסייעו בבניית הגנות איתנות.[37] צעדים פשוטים עשויים להתגלות כיעילים למדי, כמו למשל חיוב עובדים של סוכנויות ממשלתיות וגופים פרטיים המחוברים לרשתות ממשלתיות להשתמש בסיסמאות חזקות המוחלפות באופן קבוע, כמו גם חיובם לעבור הכשרה כיצד לזהות ולמנוע איומי סייבר.[38]

המתגוננים חייבים גם לשקול את שרשרת האספקה המשמשת לתכנון וייצור הציוד שבו הם מסתייעים. נכון להיום, חומרה, קושחה ותוכנה נוצרים ונבנים בכול העולם, עובדה המקשה לוודא שהמוצר אכן מאובטח. החברות והמדינות שבהן ציוד כזה מתוכנן ומיוצר עלולות לשלב בו קודים מוסתרים שיאפשרו פריצה למכשירים בבוא העת. על ממשלות לשקול פעילות משותפת עם חברות ומדינות זרות במטרה לפתח מערכת הסמכה שתבטיח שקיפות בתהליכי התכנון והייצור.[39] יחד עם זאת, תוכנית כזו יוצרת סיכון מסוים, משום שהיא עלולה להקשות על שמירת קניין רוחני, להעלות את מחיר הציוד בשל עלויות נוספות ואולי אף לדכא את קצב החדשנות.[40]

גיבוש חוקים גלובליים, נורמות והסכמים בין־לאומיים יסייע לחיזוק הגנת הסייבר. נראה כי התמקדות בהגנה על תשתיות קריטיות ואזרחיות (לדוגמה, איסור התקפות על בתי חולים או חדירות למערכותיהם) היא בעלת הסיכוי הרב ביותר לגייס הסכמה.[41] מדינות צריכות לנסות למלא תפקיד פעיל בניסוח חוקים ונורמות אלה, שכן ככול שמדינה תהיה מעורבת יותר, כך תגדל יכולתה להגן על האינטרסים שלה בעת עיצוב המערכת העתידית.[42] הניסיון לגבש חוקים ונורמות הוא משימה לא יקרה, שעשויה לשפר את ביטחון הסייבר של מדינות בכול העולם. אם תצלח, יהיו בידינו אמצעים לחזק לא רק את ההתגוננות, אלא גם את ההתרעה, ההרתעה ויכולת ההבסה.[43]

---

37. Radichel, "Case Study: Critical Controls that could Have Prevented Target Breach".
38. שם.
39. David Inserra and Steven Bucci, "Cyber Supply Chain Security: A Crucial Step toward U.S. Security, Prosperity and Freedom in Cyberspace", *Heritage Foundation*, March 6, 2014, http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace.
40. Sofaer, Clark and Diffie, "Cyber Security and International Agreements".
41. Clarke and Knake, *Cyber War*; Sofaer, Clark and Diffie, "Cyber Security and International Agreements"; Valeriano and Maness, *Cyber War versus Cyber Realities*.
42. Siboni and Assaf, *Guidelines for a National Cyber Strategy*.
43. "International Public Private Partnership in Cyber Governance (Panel).

למרות כל הנאמר לעיל, כוחם של הנורמות והחוקים הבין־לאומיים במרחב הסייבר הוא מוגבל. אופיו המבוזר של מרחב הסייבר יוצר קושי לדעת עד כמה יעילים יהיו החוק והנורמות הבין־לאומיים.[44] יתר על כן, מדינות עלולות לסרב לנסח הסכמים שישפיעו לרעה על השימוש בסייבר, במיוחד כאשר הוא מועיל לאינטרסים הלאומיים שלהן, וזאת גם לאור העובדה שמדובר בתחום חדש שלא עבר תהליכי הרשאה מספיקים.[45] לבסוף, העובדה שקשה לדעת מתי מתקפה תתרחש, ובדיעבד למי לייחס אותה, מביאה מדינות להאמין שהן יכולות לפעול ללא חשש מפעולת תגמול.

מדינות יכולות לנקוט כמה צעדים כדי להגביר את יכולתן להביס תוקפים בסייבר. הן יכולות לנסות לבודד מדינות תוקפניות ולהפנות נגדן כלים כגון סנקציות כלכליות או דיפלומטיות, מתוך כוונה לשכנע אותן שהמשך הפעולה ההתקפית יגבה מהן מחיר יקר מדי. הסיכוי להביס אויב במרחב הסייבר יגבר, אם מדינות יתמקדו בדרכים להרוס את יכולות הסייבר של אותו אויב. זאת, בשל התכנון המקיף והציוד היקר הדרושים כדי לאפשר לו שיגור מתקפות מתוחכמות.[46]

בנוסף לצעדים משפטיים, מדינות יכולות לנקוט מהלכים שיצמצמו את האיום מצד תוקפים יחידים. בידוד של פצחנים יחידים מהקהילה שעליה הם נמנים ומסתמכים, בין אם באמצעות שיבוש הקשרים האינטרנטיים שלהם ובין אם בדרך של הפצת מידע שיסב להם נזק בתוך הקהילה שלהם, יכול לפגוע ביכולתם לתכנן או לשגר מתקפה.[47] בנוסף, מדינות יכולות לנסות לגייס פצחנים לשמש כמודיעים, או לחדור לרשתות של פצחנים על ידי שתילת סוכנים בהן. אסטרטגיות כאלו עשויות להועיל גם נגד חלק גדול מהגורמים הלא מדינתיים, שגם אצלם יש הסתמכות על קהילות דומות לצורך תמיכה. אמנם, אסטרטגיה זו יוצרת סיכון נוכח החוק הבין־לאומי (והמקומי), אך היעדר חקיקה בין־לאומית ברורה בשאלות הנוגעות ספציפית למרחב הסייבר מקטין סיכון זה.

כדי לשפר את החוסן בתחום הסייבר, מדינות צריכות לשאוף לגיוון ציוד הסייבר. חומרה ותוכנה לא אמורות להגיע ממקור אחד או מחברה אחת. ציוד מגוון יאפשר למדינות לבודד מהר יותר את הבעיה, לעבור לציוד של חברה אחרת ולחדש את הפעילות, אם כי מערך כזה עלול להגדיל סיכונים בשרשרת האספקה.

---

44 Valeriano and Maness, *Cyber War versus Cyber Realities*.

45 Sofaer, Clark and Diffie, "Cyber Security and International Agreements"

46 Jonathan Silber, "Cyber Vandalism – Not Warfare", *Ynet*, January 26, 2012, http://www.ynetnews.com/articles/0,7340,L-4181069,00.html.

47 Scott D. Applegate, "The Principle of Maneuver in Cyber Operations", in *Fourth International Conference on Cyber Conflict*, ed. C. Czosseck, R. Ottis and K. Ziolkowski (Tallinn: NATO CCD COE, 2012), https://ccdcoe.org/publications/2012proceedings/3_3_Applegate_ThePrincipleOfManeuverInCyberOperations.pdf.

בעת תכנון רשתות, ניתן לכלול בהן תכונות שנועדו לשפר את החוסן ולתמוך בתהליך ההתאוששות. כדי לעזור בבניית חוסן של הרשתות הקריטיות ביותר, על מדינות לעצב ארכיטקטורת סייבר שתציע ערוצי גישה שונים למערכות הבקרה.[48] יש לכלול מראש מעקפים פיזיים כדי להבטיח דרכים נוספות להשתלטות מחדש על מערכות קריטיות. לדוגמה, ניתן לתכנן מערכת רכבות עם יכולת לעצור רכבת שנחטפה, באמצעות בקרות פיזיות שאינן תלויות במערכות הסייבר.

מסקנות

מתקפות סייבר אינן שונות במהותן מאיומים אחרים, וניתן להתמודד אתן באמצעות יישום ארבעת העקרונות הקלאסיים של האסטרטגיה הצבאית, בשילוב רעיון החוסן. ייתכן שעקרונות אלה לא יספקו מענה מלא, כשם שהם אינם נותנים מענה מלא לאיומים אסימטריים וקונבנציונליים אחרים, ובהחלט אפשר שיידרשו התאמות על פי האתגרים הספציפיים שמציבים איומי הסייבר. עם זאת, בתחומים שבהם הוכחה יעילותם של עקרונות אלה, אנו משוכנעים שנראה פיתוח של יכולות חדשות במהלך הזמן, כפי שקורה תמיד כאשר מתעוררים איומים חדשים.

מחקר ופיתוח הם נקודת המפתח במאמץ לגבש את היכולות החדשות על בסיס ארבעת העקרונות הקלאסיים והעיקרון הנוסף – החוסן. מדינות מתקדמות כבר הצליחו במידה רבה להבטיח שמנגנוני ההגנה שלהן יהיו טובים יותר מהיכולות ההתקפיות שבידי הגורמים הלא מדינתיים. עם זאת, אין ביטחון שכך יהיה גם בעתיד, במיוחד אם מדינות ייטו לא להתייחס ברצינות לאיומים.

מאמר זה הוא מאמץ מקיף ראשון ליישם את המודל של "ארבעה עקרונות ועוד אחד" על איומי הסייבר, במטרה להפוך אותו למסגרת מושגית שתוכל להנחות אסטרטגיות של מדינות בתחום הסייבר. הסתמכות על המודל הבסיסי תאפשר פיתוח של תוכניות מפורטות יותר, שיתנו מענה לדרישות הספציפיות שמעוררים האיומים השונים. המאמר גורס כי שיפור המודיעין, הקניית חוסן לארכיטקטורת הסייבר והידוק שיתוף הפעולה בין הממשלה ובין המגזר הפרטי, וכן בזירה הבין־לאומית, הם האמצעים המרכזיים ליישום עקרונות אלה. נדרש מחקר שיסייע בקביעת דרכים נוספות שיאפשרו להתאים או להרחיב את המודל גם לעולם הסייבר.

48 "The DoD Cyber Strategy".