הארכיטקטורה הפגיעה של מערכות אוויריות בלתי מאוישות: מיפוי והתמודדות עם איומים במתקפות סייבר

גבריאל בוליאן גוביי ולירן ענתבי

כלי טיס בלתי מאוישים (כטב"מים), המכונים לעיתים קרובות בשם מל"טים (מטוסים ללא טייס), הפכו לכלי חיוני ודומיננטי בשימושם של כוחות צבא מתקדמים, בייחוד כאלה המעורבים בלוחמה אסימטרית. במקרים אלה הם משמשים בעיקר למשימות איסוף מודיעין, מעקב והכרת שטח האויב וכן לצורך מבצעים שונים המחייבים תקיפות מדויקות. ככול שגוברת ההסתמכות על מערכות בלתי מאוישות לשימושים צבאיים, כך גם עולה פגיעות הכוחות למתקפות סייבר, שהן תוצאה של התלות ההולכת וגוברת במערכות מבוססות מחשב.

מאמר זה ממפה את הסוגים השונים של מתקפות סייבר נגד מערכות אוויריות בלתי מאוישות, מעריך את הסיכויים להתרחשותן, ומציע מספר הצעות למדיניות מומלצת לאלה המשתמשים במערכות אלו.

מילות מפתח: מתקפות סייבר, אבטחת סייבר, טכנולוגיה צבאית, כלי טיס בלתי מאוישים (כטב"מים).

מבוא

התפקיד אותו ממלאים כלי טיס בלתי מאוישים (כטב"מים) בלוחמה בת זמננו התרחב מאז כניסתם לראשונה לשימוש מבצעי משמעותי בתחילת שנות השבעים

גבריאל בוליאן גוביי הוא סטודנט לתואר ראשון במשפט אזרחי בפקולטה למשפטים, אוניברסיטת מק'גיל. הוא בעל תואר שני בביטחון ודיפלומטיה מאוניברסיטת תל אביב ותואר שני במדע המדינה מאוניברסיטת אוטווה. ד"ר לירן ענתבי היא עמיתת מחקר במכון למחקרי ביטחון לאומי, מרצה באקדמיה וחברה ב־IPRAW (הפאנל הבין־לאומי לרגולציה של נשק אוטונומי). המחברים מבקשים להודות למר ניב דוד על הערותיו המועילות לטיוטה המוקדמת של מאמר זה.

של המאה העשרים.[1] כלים אלה, שהמשתמש העיקרי בהם הוא צבא ארצות הברית, מכוונים על ידי דניאל ביימן כ"נשק המועדף" על וושינגטון.[2] אופיים הבלתי מאויש, המאפשר הפעלת כוח ללא צורך במשלוח חיילים מעבר לקווי האויב וסיכון חייהם, הגביר את כוח המשיכה שלהם בעיניהם של שחקנים אחרים.[3] ואולם, המאפיין המאפשר את הפעלתם ממרחק מהווה חרב פיפיות פוטנציאלית, שכן הוא מותיר את הטכנולוגיה פגיעה לאיומי סייבר. חרף העובדה כי כטב"מים מתאפיינים ברמת מחשוב גבוהה ביותר ונהנים מן היתרון שבהיעדר נוכחותם של מפעילים אנושיים בתא הטייס, מאפיין זה הוא גם שמאפשר להאקרים לנצל את מערכות הכטב"מים.

מאמר זה מבקש להסב את תשומת הלב לפגיעויות אלו של כטב"מים. קיימת סבירות גבוהה כי אלה העושים שימוש בכטב"מים ויהיו מודעים לפגיעויות המערכת יהיו ערוכים טוב יותר למנוע מתקפות סייבר פוטנציאליות ולהתגונן מפניהן. המאמר נפתח בבחינה של המרכיבים השונים הכרוכים בהפעלה נרחבת של כטב"מים. ניתוח המערכת יאפשר לנו להבין את פגיעותם של כטב"מים למתקפות סייבר פוטנציאליות. האקרים שואפים לזכות בגישה למערכת עצמה, אך עושים זאת באמצעות שימוש במרכיב אחד שלה לפחות כנקודת כניסה לתוכה. בהמשך מפרט המאמר מתקפות סייבר נגד מערכות כטב"ם שהתרחשו בעבר, ודן בכאלו שהן סבירות מבחינה טכנולוגית. מתקפות סייבר מסוימות עשויות להתבצע על ידי האקרים בודדים, אך מתקפות מתוחכמות דורשות יכולות מתקדמות יותר וניתנות לביצוע אך ורק על ידי שחקנים המחזיקים במשאבים רבים יותר, כגון ארגוני טרור, תאגידים מסחריים או אפילו מדינות. יחד עם זאת, כפי שיפורט במאמר, אפילו מתקפות הסייבר הפשוטות ביותר עלולות להוות סיכון לגורמים המפעילים כטב"מים. המאמר מסתיים בהמלצות למדיניות המיועדת לסייע בהתמודדות עם האיומים הנובעים ממתקפות סייבר כאלו.

שאלות המחקר ומבנה המאמר

הספרות בנושא כלי טיס בלתי מאוישים, אשר קיבלה תנופה בחמש השנים האחרונות, חוקרת מספר שאלות חשובות הקשורות ספציפית לשימוש בכטב"מים לצורך חיסולים ממוקדים.[4] חלק ניכר מספרות זו ניסה לקבוע האם תקיפות כטב"מים

1 Ty McCormick, "Lethal Autonomy", *Foreign Policy*, January 24, 2014, pp.18-19.

2 Daniel L. Byman, "Why Drones Work: The Case for Washington's Weapon of Choice", *Brookings Institution,* June 17, 2013, https://www.brookings.edu/articles/why-drones-work-the-case-for-washingtons-weapon-of-choice./

3 Sarah Kreps, *Drones: What Everyone Needs to Know* (Oxford: Oxford University Press, 2016), p. 60.

4 למעשה, כטב"מים (המכונים לעיתים קרובות בשם מל"טים) נשלטים על ידי מפעיל אנושי מרחוק. מכאן שההגדרה הנכונה יותר שלהם תהיה "כלי טיס הנשלטים (או מאוישים)

המיועדות לחסל ארגוני טרור הינן אפקטיביות מבחינה אסטרטגית.[5] מחקר נוסף בחן האם דרכי השימוש בכטב"מים עומדות בסטנדרטים של החוק והאתיקה הבין־לאומיים, וזאת בניסיון להבין את ההשלכות של השימושים השונים בטכנולוגיה זאת.[6]

אף על פי כן, מעולם לא הוצגה על ידי מומחים סקירה מקיפה של המגבלות הטבועות בארכיטקטורה הטכנית של כטב"מים, למעט ההתייחסות השטחית לעובדה שכטב"מים רגישים למתקפות סייבר.[7] מטרתו העיקרית של מאמר זה היא, לפיכך, למלא חלל זה, ובכך לתרום לפתיחת דו־שיח בין הספרות האקדמית העוסקת בכטב"מים ובין המחקרים העדכניים בתחום לימודי הביטחון הצומח במהירות, קרי תחום אבטחת הסייבר.

המאמר מתחלק לשלושה חלקים. החלק הראשון מסביר את אופן פעולתם של כטב"מים ושל המערכת הגדולה יותר שהם מהווים חלק אינטגרלי ממנה. דיון זה הינו שלב נדרש בטיפול בשאלת המחקר העיקרית של מאמר זה, המוצגת בחלק השני, והיא: מהן הפגיעויות הנובעות מאופן פעולתם של כטב"מים? לאחר זיהוי פגיעויות אלו, החלק השלישי של המאמר מתמודד עם שאלה חשובה נוספת: כיצד ניתן להתמודד עם האיומים הנובעים מאותן פגיעויות? מטרתו הרחבה של המאמר, במסגרת זיהוי פגיעויות הסייבר, היא להבין כיצד הארכיטקטורה של טכנולוגיית הכטב"מים הופכת אותם לפגיעים למתקפות סייבר שונות. כל זאת,

---

מרחוק", כפי שהגדיר לאחרונה חיל האוויר הישראלי. עם זאת, בהתחשב בעובדה כי מונח זה אינו נפוץ בספרות, נעשה במאמר זה שימוש במונח המוכר יותר – כטב"ם.

5 Stephanie Carvin, "The Trouble with Targeted Killing", *Security Studies* 21 (2012); Matt Frankel, "The ABCs of HVT: Key Lessons from High Value Targeting Campaigns Against Insurgents and Terrorists", *Studies in Conflict and Terrorism* 34 (2011); Jenna Jordan, "Attacking the Leader, Missing the Mark: Why Terrorist Groups Survive Decapitation Strikes", *International Security* 38, no. 4 (2014); Avery Plaw, "Terminating Terror: The Legality, Ethics and Effectiveness of Targeting Terrorists", *Theoria: A Journal of Social and Political Theory* 114 (2007); Bryan C. Price, "Targeting Top Terrorists: How Leadership Decapitation Contributes to Counterterrorism", *International Security* 36, no. 4 (2012).

6 Grégoire Chamayou, *Théorie du drone* (Paris: La Fabrique éditions, 2013); John Kaag and Sarah Kreps, *Drone Warfare* (Cambridge: Polity, 2014).

7 Kaag and Kreps, *Drone Warfare*, pp. 44-45; Kreps, *Drones*, p. 39; Peter W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin, 2009), p. 253; Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), pp. 314-315; Robert O. Work and Shawn Brimley, *20YY: Preparing for War in the Robotic Age* (Washington, DC: Center for a New American Security, 2014), p. 23, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_20YY_WorkBrimley.pdf.

במטרה להציע המלצות למדיניות, אשר יסייעו לצמצם את הסיכונים הכרוכים בשימוש בכטב"מים.

מאמר זה מתייחס לכטב"מים המסווגים על ידי צבא ארצות הברית כ"קבוצה 4" ו"קבוצה 5".[8] שתי קבוצות אלו כוללות כטב"מים שמשקלם הוא מעל 1,320 פאונד (כ־600 ק"ג) ומסוגלים לטוס בגובה של עד 18,000 רגל (כטב"מים בקבוצה 4) ומעל 18,000 רגל (כטב"מים בקבוצה 5). כטב"מים דוגמת Predator, Reaper ו־Global Hawk, הנמצאים כיום בשימוש צבא ארצות הברית, משתייכים לשתי קטגוריות אלו, ועל כן מאמר זה מתמקד בהם. כטב"מים קטנים יותר, שלצורך הפעלתם נדרש "קשר עין" ועל כן הינם בעלי ארכיטקטורה השונה מזו של קבוצות 4 ו־5, לא יידונו במאמר זה. אין פירוש הדבר שכטב"מים מקבוצות 1 עד 3 אינם פגיעים לפריצות. בניגוד לכטב"מים מקבוצות 4 ו־5, המשמשים ליעדים אסטרטגיים, כטב"מים מקבוצות 1 עד 3 משמשים לרוב במשימות טקטיות, כמו למשל ה־Raven. מכאן שסביר להניח כי הקדשת משאבים להגנה על כטב"מים מקבוצות 1 עד 3 מפני מגוון רחב של מתקפות סייבר תהיה בלתי אפקטיבית במונחי עלות, מכיוון שפעולה זו עלולה לפגוע באפקטיביות של אותם כלים, הנובעת מעובדת היותם קלי משקל, ניידים, זולים יחסית ולא מתוחכמים במיוחד. במילים אחרות, הבחירה ב־Raven היא בחירה מודעת להשתמש בכטב"ם המיועד להעניק יתרונות טקטיים מסוימים, מתוך ידיעה שאלה עלולים להצטמצם עקב הוספת מנגנון אבטחה מורכב.

יתרה מזאת, מאמר זה מתמקד באופן בלעדי בכטב"מים מקבוצות 4 ו־5 מכיוון שבניגוד לדגמים מקבוצות 1 עד 3, הם מתאפיינים ברמת מחשוב גבוהה וכוללים תתי־מערכות רבות, ההופכות אותם לפגיעים במיוחד למתקפות סייבר. כטב"מים המסווגים כקבוצות 4 ו־5 טומנים בחובם גם סיכונים רבים יותר בהתחשב בעובדה כי ניתן לציידם בטילים ולהשתמש בהם לביצוע סיכולים ממוקדים, וזאת בניגוד לכטב"מים מקבוצות 1 עד 3. כמו כן, פלטפורמות נשק מתוחכמות יותר דורשות תשומת לב מיוחדת, מכיוון שהפגיעויות שלהן כרוכות בסיכון כספי וביטחוני גבוה יותר בהשוואה לסיכון הכרוך במערכות מתקדמות פחות, דוגמת כטב"מים מקבוצות 1 עד 3. הוספת מנגנון אבטחה לכטב"מים מקבוצות 4 ו־5 תבוא באופן בלתי נמנע על חשבון הפחתת האפקטיביות שלהם (כגון במקרה של לוויינים, בו הצפנת קישור הנתונים של לוויין במטרה לאבטח את השידור של מידע רגיש מאלצת בהכרח את המפעיל להקדיש זמן רב יותר לפענוח המידע). עם זאת, עלויות אלו פחותות יחסית ליתרונות אותם הן מעניקות לאבטחה הכוללת של המערכת.

הופעתם של הכטב"מים הביאה עמה יתרונות חשובים במסגרת האינטראקטיביות הטכנולוגית של המלחמה. יתרון ברור אחד הוא הוצאתם הפיזית של חיילים משדה

8 "'Eyes of the Army': U.S. Army Roadmap for Unmanned Aircraft Systems 2010-2035", *United States Army*, 2010, p. 12.

הקרב. כמו כן, מורכבותם הטכנולוגית של הכטב"מים נסמכת על רשתות מחשבים, המכונות לעיתים קרובות בשם "מערכות אווירית בלתי מאוישות",[9] שייצורן הוא משימה טכנית מסובכת.[10] כטב"מים הם מערכות טכנולוגיות מתוחכמות יחסית, אשר בנייתן והפעלתן דורשות משאבים וידע ניכרים. יתרה מכך, הפלטפורמה המוטסת שלהם, הטסה בגובה רב יחסית, הופכת את תקיפתם באמצעים קינטיים למסובכת יותר, ומכאן שנדרשות יכולות מתקדמות יותר כדי להפילם. מסיבות אלו סביר להניח כי שחקנים המעוניינים לתקוף כטב"מים יחפשו חלופות בעולם הסייבר. מתקפות סייבר מהוות תחליף הגיוני למתקפות קינטיות, מכיוון שהארכיטקטורה של כטב"מים, כלומר הסתמכותם על מערכות ממוחשבות, הופכת אותם לפגיעים מטבעם להאקרים המבקשים לנצל את מגבלותיה של הטכנולוגיה. לכן, חשוב שגורמים העושים שימוש בכטב"מים יבינו כיצד ניתן לנצל את הטכנולוגיה שלהם, כדי שיוכלו להתמודד עם האיומים הנובעים ממנה. אינטראקציות אלו בין מפעילי כטב"מים ובין האקרים ראויות לתשומת לב מיוחדת הן במסגרות הביטחוניות והן בחוגים האקדמיים. זוהי המשימה הניצבת בפני מאמר זה.

שלושה מרכיבים מרכזיים של מערכות כטב"ם: כיצד כטב"מים פועלים?

כטב"מים הינם חלק ממערכת סבוכה המורכבת ממספר רכיבים משולבים הקשורים ביניהם, הנדרשים כולם כדי שהכטב"ם יוכל לבצע את משימות איסוף המודיעין, המעקב והכרת שטח האויב, או אפילו איתור מטרות ופגיעה בהן. אף על פי שמערכת זו מכילה מספר חלקים, מתמקד המאמר באופן בלעדי בשלושת המרכיבים העיקריים הבאים: (1) הבסיס הצבאי או מרכז הפיקוד והשליטה ממנו שולט המפעיל על הכטב"ם; (2) הלוויין המקשר בין הכטב"ם ובין מרכז הפיקוד והשליטה; (3) הכטב"ם – משמע כלי הטיס עצמו.[11] מרכיבים אלה מתבססים על מפת הדרכים של חיל האוויר של ארצות הברית, הרואה ב־Predators וב־Reapers יותר מאשר כלי טיס בלבד, ובעצם "מערכות" שלמות.

---

9 Kaag and Kreps, *Drone Warfare*, pp. 49-50.

10 Kreps, *Drones*, p. 63.

11 להמחשה ויזואלית של שלושת חלקי המערכת ראו איור 1; להמחשות גרפיות שימושיות אחרות של מערכת זו ראו: "MQ-9 Reaper", *United States Air Force Eye in the Sky*, directed by Gavin Hood (Toronto: Entertainment One, 2015); Derek Gregory, "From a View to a Kill: Drones and Late Modern War", *Theory, Culture and Society* 28, no. 7-8 (2011): 197; Ian G. R. Shaw, "The Rise of the Predator Empire: Tracing the History of U.S. Drones", *Understanding Empire*, 2014, https://understandingempire.wordpress.com/2-0-a-brief-history-of-u-s-drones/.

בסיס קרקעי נוסף, המכונה תחנת שיגור והתאוששות, חיוני אף הוא כדי שהכטב"ם יוכל להמריא לפני ביצוע המשימות ולנחות אחריהן. תחנות אלו, העשויות להיות גם נושאות מטוסים המשמשות לתדלוק ולאחסון כטב"מים כאשר אינם בשימוש, מהוות חלק מן המערכת. עם זאת, הן אינן נדונות כאן, משום שהסבירות שהן יהיו מטרה למתקפות סייבר נמוכה בהשוואה לסבירותן של מתקפות קינטיות עליהן. יתרה מזאת, כל אחד מן החלקים של מערכת כטב"ם מכיל טכנולוגיות דומות העלולות להיות חשופות למתקפות סייבר. לדוגמה, מרכז הפיקוד והשליטה מצויד במספר טכנולוגיות תקשורת המאפשרות תקשורת עם הכטב"ם, אשר כל אחת מהן עלולה לשמש מטרה נפרדת להאקרים. כפי שיידון בקצרה במאמר, גם טילים או מטען ייעודי הנמצאים על כטב"מים עלולים להוות מטרה למתקפות סייבר. אף על פי כן, אין ביכולתו של מאמר זה לדון בכול הדרכים הרבות מספור בהן ניתן לפרוץ למגוון החלקים העצום של המערכת. על כן, די אם נתעכב על שלושת המרכיבים שנזכרו לעיל במערכות הכטב"מים כדי לאפשר לקורא לזהות את נקודות החדירה העיקריות לתוך כטב"ם במקרה של מתקפת סייבר.

מרכיב 1: מרכז הפיקוד והשליטה

המרכיב הראשון של המערכת – מרכז הפיקוד והשליטה – הוא האתר הקרקעי ממנו הטייסים והמפעילים שולטים ומפקחים על המערכת מרחוק. אף על פי שמרכז פיקוד ושליטה הממוקם בארצות הברית למשל עשוי להפחית את החשיפה של הצוות לפגיעה פיזית, סביר להניח כי הוא ישמש מטרה למתקפות סייבר. מרכזי הפיקוד והשליטה מצוידים במגוון מחשבים וטכנולוגיות והינם חיוניים לצורך תפעול הכטב"מים, אך הם גם פגיעים לחדירות סייבר חיצוניות ופנימיות.

מרכיב 2: הלוויין

בניגוד לכטב"מים קטנים יותר, התלויים באות רדיו לצורך תמרונם ונשארים בדרך כלל בקו הראייה של המפעיל, הכטב"מים המסווגים על ידי צבא ארצות הברית כקבוצות 4 ו־5 תלויים בלווייניים, שהם המרכיב השני של המערכת. לווייניים אלה פועלים כמתווכים בין הכטב"מים עצמם לבין המפעילים. הם מאפשרים שידור מכלי הטיס של תמונות ונתונים הנקלטים באמצעות המצלמות והחיישנים המותקנים על הכטב"מים אל מרכז הפיקוד והשליטה, ובאופן דומה בכיוון הפוך – שידור של פקודות מן הבסיס בחזרה לכטב"מים. הלוויין ממלא חלק מכריע במערכת, משום שהוא מספק לכטב"ם ולמפעיל את המיקום המדויק שלו ומאפשר לכטב"ם לאתר את מטרתו. כמו כן, כפי שמציין איאן שואו, השימוש בלווייניים לצורך קישור בין כטב"מים לבין מפעיליהם הוא שמאפשר להגדיל באופן משמעותי את המרחק בין

שני חלקים אלה של המערכת.[12] שואו מסביר כי לפני השימוש בלווויינים, כטב"מים היו מצוידים בקישור נתונים בעל טווח קצר לצורך פיקוד ושליטה, שלא אִפשר להפעיל כטב"ם במזרח התיכון מבסיס הנמצא בארצות הברית, כפי שניתן לעשות כיום עם Predators, Reapers ו־Global Hawk.

הלוויין ממלא, אפוא, שתי פונקציות מפתח עבור הכטב"ם: הוא מהווה חלק בלתי נפרד ממערכת ה־GPS שלו, והוא משמש כערוץ התקשורת העיקרי לצורך כל תעבורת הנתונים בין כלי הטיס ובין המפעילים האנושיים. מכיוון שהלוויין משמש להעברת מידע חיוני, חיבור הנתונים העובר דרכו מהווה מטרה אסטרטגית עבור כל האקר המעוניין להפריע ולשבש את פעילותם של כטב"מים (אפשרויות אלו יידונו בפירוט רב יותר בהמשך).

מרכיב 3: כלי הטיס (כטב"ם)

המרכיב השלישי של המערכת הוא הכטב"ם – כלי הטיס עצמו. כפי שצוין קודם לכן, אחד התמריצים העיקריים לשימוש בכטב"מים הוא ההגנה על טייסים מפני פגיעה פיזית בעת פעולה בזירות לחימה שונות. מסיבה זו ניתן להפעיל כטב"מים באזורים הנמצאים אלפי קילומטרים מן המקום בו נמצאים המפעילים. ברם, העובדה שהמפעילים אינם נמצאים בתא הטייס מאלצת אותם לסמוך על הנתונים המתקבלים מן הכטב"ם. לכן, כטב"מים מצוידים גם במצלמות צמצם וגם במצלמות אינפרה אדום, המאפשרות למפעילים לכוון אותם ולעקוב אחר תוואי השטח שמתחתם גם בתנאי מזג אוויר קשים.[13] במילים אחרות, מצלמות הכטב"ם משמשות כעיניו של המפעיל, מלקטות מידע ומעבירות אותו באמצעות תמונות המופיעות על מסכי המחשב של המפעילים, המסתמכים על ההזנה האופטית הרציפה בשידור חי המופיעה בפניהם לצורך תמרון הכטב"ם. הרזולוציה הגבוהה של המצלמות המותקנות על הכטב"מים והעובדה שהתמונות מוזרמות באופן חי יוצרות מצב של פגיעות פוטנציאלית וניצול לרעה. לדוגמה, מערכות Gorgon Stare ו־ARGUS כוללות בהתאמה 12 ו־29 מצלמות ברזולוציה גבוהה, הניתנות להתקנה על כטב"מים לצורך שדרוג המצלמות הפחות מתוחכמות שלהם.[14] מכיוון שהכמות העצומה של התמונות המצולמות על ידי Gorgon Stare ו־ARGUS עלולה להציף את המפעיל האחראי על המעקב אחריהן, ייתכן שאותו מפעיל לא יוכל לדעת האם הכטב"ם הפך למטרה להאקר. מצב זה מדגיש עוד יותר את פגיעותה של המערכת.

---

12 Shaw, "The Rise of the Predator Empire".

13 שם.

14 Noah Shachtman, "Air Force to Unleash 'Gorgon Stare' on Squirting Insurgents", *Wired*, February 19, 2009, https://www.wired.com/2009/02/gorgon-/stare.

מיפוי מתקפות הסייבר הסבירות ביותר על מערכות כטב"ם

מכיוון שכטב"מים הם מכונות מורכבות מבחינה טכנולוגית, ייתכן שהדרך הקלה ביותר העומדת בפני יריב המעוניין לתקוף כטב"מים אינה להתחרות עימם, אלא דווקא לנצל את החולשה של הארכיטקטורה שלהם. יתרה מכך, ארצות הברית משתמשת בעשורים האחרונים בכטב"מים בראש ובראשונה נגד שחקנים לא מדינתיים דוגמת טרוריסטים, ובעיקר במצבים של "עליונות אווירית". בהתחשב ביתרון תחרותי זה, השחקנים השואפים לתקוף כטב"מים יגלו כי תקיפה באמצעים קינטיים הינה קשה יותר מאשר אם היו בידיהם כלי נשק מתוחכמים יותר. מכאן שחלופה סבירה עבור שחקנים לא מדינתיים היא לנצל את הארכיטקטורה של הכטב"מים, דבר אותו ניתן לעשות גם באמצעות משאבים מוגבלים ביותר (בטבלה 1 מפורטים הסוגים השונים של מתקפות סייבר העלולות להיות מכוונות נגד מערכות אוויריות בלתי מאוישות).

השתלטות מלאה על כטב"ם (כפי שהיו עושים שודדי ים לו היו מצליחים לעלות על ספינה) מחייבת מתקפת סייבר הדורשת מידה רבה של תחכום. לעומת זאת, קבלת מידה מסוימת של "גישה" לכטב"מים היא משימה לא מורכבת באופן יחסי, בהתחשב בעובדה שהיא מבוססת על הרכיבים הממוחשבים של המערכת. הרכיב הפגיע ביותר של המערכת האווירית הבלתי מאוישת הוא קשר הלוויין בין המטוסים ובין מרכז הפיקוד והשליטה עימו הם עומדים בקשר. למעשה, האקרים מסוגלים להתחבר למערכות קישור הנתונים והתקשורת של המטוסים ולנצלן כדי לגנוב מידע מודיעיני רב ערך. לדוגמה, צבא ארצות הברית תיעד מספר מקרים שבהם האקרים הצליחו להשיג גישה לסרטי הווידאו של כטב"מים מסוג Predator.[15]

15 Siobhan Gorman, Yoshi J. Dreazen and August Cole, "Insurgents Hack U.S. Drones: $26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected", *Wall Street Journal*, December 17, 2009, http://www.wsj.com/articles/SB126102247889095011.

טבלה 1: מתקפות סייבר המכוונות נגד מערכות כטב"ם והיכולות הנדרשות לצורך ביצוען[16]

סוג מתקפת הסייבר	רכיב מותקף; סוג הכטב"ם	שחקנים בעלי יכולת מינימלית נדרשת[16]	דוגמאות היסטוריות	דרכי התגוננות אפשריות
גישה לסרטי הווידאו	קישור נתוני לוויין; מל"ט סיור ותקיפה	בודדים	האקרים נגד Predators. ארצות הברית ובריטניה נגד ישראל	הצפנת קישור נתונים
גישה לסרטי הווידאו ומתקפות DoS (מניעת שירות)	קישור נתוני לוויין; מל"ט סיור ותקיפה	בודדים או ארגוני טרור	לא פורסמו עד כה	הצפנת קישור נתונים
גישה לסרטי הווידאו והחלפת סרטון בסרטון חלופי	קישור נתוני לוויין; מל"ט סיור ותקיפה	תאגידים	לא פורסמו עד כה	הצפנת קישור נתונים
שיבוש GPS (spoofing)	קישור נתוני לוויין; מל"ט סיור ותקיפה	מדינות	לכאורה, איראן נגד RQ-170 Sentinel	קריפטוגרפיה, זיהוי עיוות אות, ו/או חישת כיוון הגעה (direction-of-arrival)
פריצה למחשבים השולטים על חיבור הווידיאו	מרכז הפיקוד והשליטה	מדינות	וירוס מסוג Key logger בבסיס חיל האוויר Creech	"פער אווירי" (Airgap) סביב מרכז הפיקוד והשליטה; שימוש מוגבל בכוננים נשלפים; שימוש מוגבל בטכנולוגיות חיצוניות (לדוגמה, טלפונים חכמים או מחשבים ניידים פרטיים בקרבת או בתוך מרכז הפיקוד והשליטה)

16 קטגוריה זו כוללת ארבעה סוגי שחקנים. בסדר עולה, המבוסס על המשאבים הזמינים העומדים לרשותם לצורך ביצוע מתקפות סייבר. שחקנים אלה הם: אנשים בודדים; ארגוני טרור; תאגידים; מדינות. על הקורא לשים לב כי קטגוריה זו מהווה סף מינימום משוער. כלומר, מתקפת סייבר הניתנת לביצוע על ידי אדם בודד תוכל להתבצע גם על ידי ארגוני טרור, תאגידים ומדינות, שכן לרשות האחרונים עומדים משאבים רבים יותר בהשוואה לאנשים בודדים. יחד עם זאת, מתקפת סייבר הניתנת לביצוע על ידי מדינה ככול הנראה לא תוכל להתבצע על ידי בודדים, ארגוני טרור ותאגידים, אשר המשאבים העומדים לרשותם מעטים יותר.

פיטר סינגר ואלן פרידמן מסבירים כי ההאקרים לא נזקקו במקרים אלה ליותר מאשר למחשב נייד ול־"Skygrabber" – תוכנה שפותחה ברוסיה, שמחירה 29.95 דולר, אותה ניתן להשיג בקלות באינטרנט.[17] Skygrabber אפשרה להאקרים ליירט ולנצל תשדורות לוויין בלתי מוצפנות בין כטב"מים ובין מרכזי פיקוד ושליטה ולהשיג שעות של צילומי וידאו אותם הם שיתפו עם עמיתיהם.[18] העובדה שעלות הפריצה לקישורי נתונים של כטב"מים היא כה נמוכה, בעוד שעלות אבטחתם מגיעה למיליונים, מביאה את סינגר ופרידמן לשאול: "[האם] עולם אבטחת הסייבר מקנה עדיפות לחלש או לחזק?"[19]

מתקפת סייבר מסוג זה היא אחת מן ההתקפות הפשוטות אך המדאיגות ביותר את המשתמשים הצבאיים. היכולת לראות מה האויב עושה עשויה לספק להאקר מודיעין קריטי. לדוגמה, הגישה לסרטי וידאו של כטב"ם מאפשרת להאקר ללמוד על יכולות איסוף המודיעין של המשתמש, כולל אופיין וזהותן של מטרות, שיטות ורוטינות של איסוף מודיעין, מעקב והכרת שטח האויב. אמנם, היכולת לראות מה האויב (או הידיד) עושה אינה מאפשרת לקבוע אלו תהליכי חשיבה מתקיימים ומהי האסטרטגיה מאחורי מה שנראה לעין; עם זאת, היא מסייעת ללא ספק לצפות את הצעד האפשרי הבא של המשתמש ומאפשרת להאקר להימצא צעד אחד לפניו, ובכך היא עשויה להעניק לו יתרון מכריע בשדה הקרב.

דוגמה נוספת ומתוחכמת יותר לגישה חשאית למצלמות של כטב"ם תוארה על ידי האתר *The Intercept*. לדברי קורה קורייר והנריק מולטקה, מספר כטב"מים ישראליים, חלקם מדגמי "הרמס" ו"מחץ", נפרצו על ידי סוכנויות המודיעין של ארצות הברית ובריטניה.[20] לפי טענת השניים, הסוכנות לביטחון לאומי של ארצות הברית (NSA) וגוף התקשורת של בריטניה (GCHQ) הקימו בסיס בקפריסין לצורך יירוט האותות של כטב"מים ישראליים ואספו בהצלחה צילומי וידאו, בהם השתמשו כדי לעקוב אחר פעילותה של ישראל ברצועת עזה ובגדה המערבית. קורייר ומולטקה מוסיפים כי תוכנית סודית משותפת זו, אשר כונתה בשם "האנרכיסט", אפשרה לאמריקאים ולבריטים לעקוב אחר נתיבי הטיסה של כטב"מים ישראליים, דבר המצביע על כך שארצות הברית ובריטניה מסוגלות, קרוב לוודאי, גם לזהות את מיקומן של תחנת השיגור וההתאוששות של מרכז הפיקוד והשליטה הישראלי.

17 Singer and Friedman, *Cybersecurity and Cyberwar*, pp. 260-261.

18 Gorman et al., "Insurgents Hack U.S. Drones".

19 Singer and Friedman, *Cybersecurity and Cyberwar*, p. 260.

20 Cora Currier and Henrik Moltke, "Spies in the Sky: Israeli Drone Feeds Hacked by British and American Intelligence", *The Intercept*, January 29, 2016, https://theintercept.com/2016/01/28/israeli-drone-feeds-hacked-by-british-and-american-intelligence./

העובדה שארגונים או מדינות מסוגלים להתחבר למצלמה של כטב"ם ולראות את הדברים שהכטב"ם עצמו רואה אכן מהווה נקודת תורפה, כפי שהוסבר לעיל. עם זאת, השלכות התופעה עלולות להיות חמורות הרבה יותר אם ההאקר יצליח להתחבר לא רק למצלמה, אלא גם ללוח הבקרה של הכטב"ם. לדוגמה, די בהתקפת מניעת שירות (DoS) כדי לגרום למפעיל לאבד קשר עין עם המטרה למשך פרק זמן כזה שיאפשר למטרה להימלט. התקפת מניעת שירות כזו עלולה, בהתאם למועד התרחשותה (לדוגמה, ממש לפני ההמראה או הנחיתה של הכטב"ם), להביא גם להתרסקותו של הכטב"ם, מכיוון שמפעיל "עיוור" לא יהיה מסוגל להתחמק ממכשולים בקרבת הכלי. לארגונים לא מדינתיים עשוי להיות תמריץ חזק לבצע התקפה כזאת בשעה שהם מנסים לחמוק מכטב"ם המרחף מעליהם. ככול שמתקפת ה־DoS ארוכה יותר, יהיה לאותם גורמים זמן רב יותר לעזוב את האזור שמעליו אורב הכטב"ם.

מתקפת סייבר המכוונת לפגוע בקישור נתונים עלולה להשחית את סרטי הווידאו ולהסיט את המפעילים מנתיב הטיסה. תרחיש כזה תואר בסרטים רבים, בהם אדם בודד או ארגון פורצים למערכת מחשב ולמצלמות מעקב המחוברות למערכת כלשהי ומקרינים צילומים שונים (לעיתים מדובר בצילומים חוזרים ונשנים של אותו אתר עצמו) בהם לא מתרחש שום דבר חריג, כך שהאנשים העוקבים אחר המצלמות לא יידעו כי הם מולכים שולל. ניתן למתוח קו מחבר בין כטב"מים ובין תסריט קולנועי טיפוסי כזה, מכיוון שמצלמות של כטב"מים הן האמצעי העיקרי המאפשר למפעיל לראות מה מתרחש. לכן, אם האקר יצליח לפרוץ למצלמה של כטב"ם (כפי שממחישה הדוגמה של Skygrabber) ולשלוח סרטון וידאו שיראה כאילו הכטב"ם מרחף מעל למדבר, ייתכן שהמפעיל לא יוכל להבין כי למעשה הוא אינו רואה את מה שהכטב"ם רואה בפועל. הכוונה שגויה עלולה, בסופו של דבר, לסכן את הצלחת המשימות ואף מעבר לכך.

קישורי נתונים לוויניים הופכים את הארכיטקטורה של מערכת הכטב"ם לפגיעה מסיבה חשובה נוספת, וזאת משום שקישורים הם הערוץ המשמש להעברת נתוני GPS מן הכטב"ם למרכז הפיקוד והשליטה. במתקפות מסוג spoofing, הדומות לתסריט הקולנועי שהוזכר לעיל, יכול ההאקר לפרוץ לתשדורת ה־GPS, להנחות את הכטב"ם בנתיב שגוי ולגרום למפעיל להאמין כי הכטב"ם נמצא במקום שונה מזה שבו הוא נמצא בפועל. דוגמה בולטת למתקפת סייבר מסוג זה התרחשה ב־2011, כאשר איראן ביצעה לכאורה spoofing של מערכת ה־GPS של כטב"ם חמקן מדגם RQ–170 Sentinel. איראן טענה אז כי פרצה למערכת ה־GPS של אחד

מן הכטב"מים האמריקאיים, גרמה לו לכבות את הטייס האוטומטי שלו ושלחה לו קואורדינטות GPS שונות, אשר הובילו אותו בסופו של דבר לנחות באיראן.[21]

מומחים רבים העלו ספקות באשר ליכולתה של איראן לבצע פריצה מסוג זה.[22] יחד עם זאת, ריצ'רד לנגלי, מומחה ל־GPS, טוען כי "מבחינה תיאורטית קיימת אפשרות להשתלט על מל"ט באמצעות שיבוש קוד ה־P(Y), ובכך לגרום למַקלט ה־GPS להשתמש בקוד ה־C/A הבלתי מוצפן כדי לאתר בקלות רבה יותר את ההכוונה המגיעה מלווייני ניווט".[23] קוד ה־C/A הוא האות המשמש את כל מערכות ה־GPS לצורך שידור מידע ללווייינים. קודים אלה אינם מוצפנים, ולכן קלים יותר לפענוח. הקוד "המדויק" (קוד P) הוא גרסה עוצמתית ומדויקת יותר של קוד C/A וממלא את אותו התפקיד. ה־Y נוסף לאחר ה־P כדי לציין כי הקוד המדויק מוצפן, משום שאות מוצפן מאובטח יותר מקוד בלתי מאובטח.

אין ודאות כי ההאקר יצליח לפענח את נתוני ה־GPS המשודרים באמצעות קוד P(Y), וזאת בשל ההצפנה. אף על פי כן, יש באפשרותו לשנות את האות שלו ולאלצו לעבור לקוד C/A, שכאמור אינו מוצפן. לאחר המעבר לקוד C/A ניתן יהיה ליירט את נתוני ה־GPS הבלתי מוצפנים, כפי שקרה במתקפה שהתבססה על Skygrabber. מכאן, שגם אם איראן לא הצליחה לפרוץ ל־RQ-170 Sentinel בשנת 2011, האפשרות ששחקנים אחרים יוכלו לעשות זאת שרירה וקיימת, בתנאי שברשותם ידע טכנולוגי מספיק לשם כך. בהתחשב ברמת התחכום הנדרשת, סביר להניח כי היכולת לבצע מתקפות spoofing שמורה לקומץ שחקנים מדינתיים בלבד.[24]

"קריפטוגרפיה", "גילוי עיוות אות" ו"חישת כיוון הגעה" הם שלושת מנגנוני ההגנה המסוגלים להתמודד עם מתקפות spoofing נגד מערכות GPS.[25] פסיאקי והאמפריז מסתמכים על נתונים, אליהם הגיעו באמצעות גילוי מתקפות spoofing נגד מערכת ה־GPS של כלי שיט גדול, כדי לציין כי ייתכן שלא יהיה די במנגנוני הגנה מורכבים כאלה לצורך הגנה מפני מתקפות מסוג זה, אם השימוש בכול אחד ממנגנונים אלה ייעשה בנפרד. לעומת זאת, הפעלתם במשותף מגבירה את הסבירות להתגוננות מוצלחת.[26] אף על פי כן, ייתכן כי חלק מן המנגנונים אינם

21 Adam Rawnsley, "Iran's Alleged Drone Hack: Tough, but Possible", *Wired*, December 16, 2011, https://www.wired.com/2011/12/iran-drone-hack-gps/.

22 David Axe, "Nah, Iran Probably Didn't Hack CIA's Stealth Drone", *Wired*, April 24, 2012, https://www.wired.com/2012/04/iran-drone-hack/; Rawnsley, "Iran's Alleged Drone Hack".

23 Rawnsley, "Iran's Alleged Drone Hack".

24 Mark L. Psiaki and Todd E. Humphreys, "Protecting GPS from Spoofers is Critical to the Future of Navigation", *IEEE Spectrum*, July 29, 2016, http://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation.

25 שם.

26 שם.

מתאימים ל־RQ–170 Sentinel או לכטב"מים חמקנים אחרים. זאת, משום שהוספת מערכות הגנה לכטב"ם עלולה לפגוע ב"חמקנות" שלו, אלא אם המערכת מצוידת באותה טכנולוגיית חמקן של כלי הטיס עצמו. אם מערכת ההגנה אינה חמקנית, היא עלולה להתגלות על ידי מערכות המכ"ם של האויב, ובכך להוציא את העוקץ ממטרתו העיקרית של הכלי.

בהתחשב בעובדה שה־RQ-170 Sentinel הוא אחד מן הכטב"מים הסודיים והמתקדמים ביותר מבחינה טכנולוגית המצויים בידי ארצות הברית, האפשרויות התיאורטיות שהובאו לעיל מדגישות עוד יותר את פגיעותה של ארכיטקטורת הכטב"מים האמריקאיים.[27] כפי שצוין, בניגוד ל־Sentinel, הכטב"מים מסוג Predator ו־Reaper עדיין אינם עושים שימוש בקישורי נתונים מוצפנים, ולכן מערכות ה־GPS שלהם רגישות עוד יותר למתקפות spoofing.

מעֵבר לערך האסטרטגי הטמון ביכולת ההאקרים לראות באמצעות מתקפות spoofing את מה שהאויב רואה, יש להם תמריץ לבצע מתקפות כאלו כאשר כטב"ם מרחף מעל אזור שהינו בעל חשיבות עבורם־הם. התמריץ הופך לחזק אף יותר במקרה של כטב"ם תקיפה, במיוחד אם ההאקר סבור כי הימנעותו מפעולה תאפשר לכטב"ם לפגוע במקום המחבוא של חמושים, עליהם מנסה ההאקר להגן. במקרה זה ייתכן כי לא יהיה די במתקפת DoS בלבד, משום שבניגוד ללוחמים חמושים המסוגלים לנסות להימלט מפני כטב"ם הרודף אחריהם, תשתית פיזית, כגון מקום מחבוא או מחנה אימונים, אינה ניתנת להעתקה בקלות ובמהירות, אם בכלל.

לא רק הנתונים המקשרים בין כטב"מים לבין מרכזי הפיקוד והשליטה הם רכיבים פגיעים בארכיטקטורה של מערכות הכטב"ם, אלא גם מרכזי הפיקוד והשליטה עצמם. אלה רגישים למתקפות סייבר מעצם העובדה שהם פועלים באמצעות מערכות מחשב בלבד. רשתות אלו מוגנות באמצעות "כיסי אוויר" (air gaps), אך הדבר לא מנע את הדבקתן בנוזקות, כפי שהוכח מחדירה של וירוס מסוג key logger למערכות המחשב הצבאיות בבסיס חיל האוויר Creech ב־2011.[28] רשת פרטית נחשבת למוגנת באמצעות "כיס אוויר" כאשר היא מנותקת מן הרשתות הציבוריות הסובבות אותה. הדבר נעשה כדי להבטיח שהרשת תהיה מאובטחת ושלא ניתן יהיה להגיע אליה באמצעות אחת מן הרשתות הציבוריות הפועלות בקרבה אליה. במילים אחרות, "כיס האוויר" מבודד את הרשת הפרטית (כלומר, הרשת בה נעשה שימוש במרכז הפיקוד והשליטה), כך שההאקר יוכל לפרוץ לרשת

27 אף על פי שבאתר האינטרנט של חיל האוויר של ארצות הברית מופיע ב־2009 דף נתונים של ה־RQ-170 Sentinel, לא פורסמו במסגרתו נתונים טכניים כלשהם על יכולותיו של כלי הטיס ומאפייניו העיקריים, וזאת בניגוד ל־MQ-1B Predator ול־MQ-9 Reaper.

28 Noah Shachtman, "Exclusive: Computer Virus Hits U.S. Drone Fleet", *Wired*, October 11, 2011, https://www.wired.com/2011/10/virus-hits-drone-fleet/.

רק באמצעות גישה פיזית למחשבים המחוברים אליה, דבר שמצמצם את הסיכוי לפגיעה בה. מכיוון שלא פורסם כל מידע פומבי על הווירוס הספציפי שתקף את בסיס חיל האוויר Creech, קשה לקבוע במדויק כיצד הוא פגע ברשת המחשבים שם, אולם הסברה היא כי הווירוס הגיע לרשת באמצעות כוננים נשלפים שהוכנסו על ידי מפעילי הכטב"מים עצמם, ומאז לא נעשה בהם שימוש בצבא ארצות הברית.[29]

אירוע זה ממחיש את פגיעותו של הגורם האנושי.[30] פירוש הדבר הוא כי אף שהמפעילים אינם נוכחים באופן פיזי בשדה הקרב, נותר בעינו הסיכון לניצולם על ידי האקרים לצורך השגת גישה בלתי מורשית למערכת. לסיכון זה עלול להיות מגוון רחב של השלכות מבצעיות: הדבקה פשוטה של הרשת באמצעות וירוס עלולה להביא להפצת מידע מסווג שנאסף על ידי כטב"מים לגורמים עוינים; מתקפת נוזקה מתוחכמת יותר מסוגלת לשלוח פקודות לא מוסמכות לכטב"ם, ובה בעת לשדר לצגים של המפעילים כי הכול פועל כשורה, באופן דומה לפעולתה של "תולעת סטקסנט" שפגעה במתקני העשרת האורניום של איראן ב־2009.[31] אף שמתקפות אלו אינן מורכבות במיוחד מבחינה קיברנטית, הן עדיין מתוחכמות למדי, משום שהן דורשות גישה פיזית למרכז הפיקוד והשליטה, דבר העשוי להתברר כמהלך מסורבל ומורכב בהתחשב ברמת האבטחה הפיזית הגבוהה סביב אתרים אלה.

אף כי מתקפות המכוונות נגד מרכזי פיקוד ושליטה הינן קשות ביותר לביצוע, כפי שהוסבר לעיל, יש להאקרים תמריצים משמעותיים לממש אותן, וזאת בהתחשב בערך האסטרטגי הטמון במתקפות מוצלחות כאלו. לדוגמה, השתלת נוזקה בעלת רמת תחכום גבוהה מאפשרת להאקר ליצור אפקט קינטי על כטב"ם תקיפה באמצעות מתן פקודה לשגר את הטילים שלו על מטרות לא נכונות. יתרה מכך, הנוזקה עלולה לגרום לטילים של הכטב"ם, הכוללים מחשבים קטנים החשופים אף הם למתקפות סייבר, לצאת מכלל פעולה או אף להתפוצץ בעודם על הכטב"ם, ובכך להרוס את כלי הטיס. העובדה שארגוני טרור חסרים לעיתים קרובות את היכולת לבצע התקפות אוויר־קרקע יוצרת להם תמריץ נוסף לבצע מתקפות סייבר, שכן אלו עשויות לאפשר להם להשיג מידה מסוימת של שליטה על המטען הייעודי של

29 שם.

30 מתקפות המתבססות על הגורם האנושי עשויות להיראות על פניהן כמתוחכמות פחות, שכן הן אינן כרוכות בידע טכנולוגי מתקדם. למרות זאת, אין להמעיט בנזק הפוטנציאלי שהן עלולות להסב. כך, תולעת הכופר WannaCry, אשר זכתה למידה רבה של הד בתקשורת כאשר הגיעה ב־12 במאי 2017 ל"עשרות אלפי" מחשבים בלא פחות מ־74 מדינות", ניצלה למעשה פגיעות במערכת ההפעלה "חלונות" של "מייקרוסופט", עבורה כבר היה קיים עדכון אבטחה מאז 14 במארס 2017, אלא שהאנשים שהמחשבים שלהם נדבקו פשוט לא טרחו להתקינו.

31 Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon", *Wired*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet./

הכטב"מים ולהשתמש בו כאילו היה שלהם. האפשרויות של מתקפות סייבר כאלו הן אינסופיות ולא ניתן לעסוק בהן כאן באופן מקיף. עם זאת, עצם ההיתכנות להתרחשותן אמורה להספיק כדי להתריע בפני הקורא (והכוחות העושים שימוש בכטב"מים) מפני איומים פוטנציאליים אלה.

בלי קשר לסוג המתקפה אותה ההאקרים מנסים להוציא לפועל, יש להם תמריץ ליצור נוזקות שיישארו סמויות במשך זמן רב, וזאת כדי שניתן יהיה לנצל את המערכת במשך פרק זמן ארוך ככל הניתן. גורם במשרד ההגנה של ארצות הברית ניסח זאת באופן הבא: "עבור יריב מתוחכם, יש יתרון בכך שהרשת שלכם תמשיך לפעול. הוא יכול לגלות מה אתם יודעים, הוא יכול לגרום לבלבול, לעכב את זמני התגובה שלכם ולעצב את פעולותיכם".[32] ומכיוון שכטב"מים זכו למעמד כה חשוב בצבא ארצות הברית, הפריצה לתוכם הופכת לבעלת ערך רב, ייתכן אף יותר מאשר הפלתם. במילים אחרות, ככול שכלי הנשק רב־עוצמה ואפקטיבי יותר, כך הוא יהפוך ליעד נחשק יותר עבור שחקנים שמטרתם היא לזכות ביתרונות מבצעיים.

סיכום והמלצות

כטב"מים נמצאים כיום בלב המאבק בטרור שמנהלות כמה מן המדינות המובילות בעולם, ביניהן ארצות הברית, ישראל ובריטניה. לפי שרה קרפס, המתייחסת להערכה של מכון ראנד משנת 2014, סין, הודו, איראן, רוסיה, טייוואן, טורקיה ואיחוד האמירויות הערביות מפתחות כיום כטב"מים משלהן.[33] לדבריה, "העולם הופך למוצף במל"טים, והסימנים מצביעים על כך שהם לא יישארו בהיקפם הנוכחי, אלא מספרם ילך ויגדל".[34] על כן, הנושא הופך לחשוב ולרלוונטי ביותר עבור כל המדינות המפעילות אותם במשימות צבאיות.

הפיכתן של מערכות כטב"ם לחלק בלתי נפרד מן הצבאות הסדירים הביאה לכך שאיום הסייבר הנשקף למערכות אלו הפך לתכוף יותר וממומש על ידי מגוון של יריבים. ואולם, כפי שהוסבר לעיל, לא כל היריבים מסוגלים להוציא לפועל את כל סוגי מתקפות הסייבר נגד כטב"מים. חלק חשוב בהתמודדות עם האיומים מתחיל ביצירת מודעות לקיומם – שהיא מטרתו של מאמר זה. אלא שאין די במודעות בלבד לקיומן של נקודות תורפה, וחובה לנקוט פעולות נוספות כדי לצמצם את הנזק הפוטנציאלי העלול להיגרם למשתמשים בכטב"מים כתוצאה ממתקפות סייבר.

---

32 צוטט ב: Nathan Hodge and Noah Shachtman, "Insurgents Intercept Drone Video in King-Size Security Breach (Updated, with Video)", *Wired*, December 17, 2009, https://www.wired.com/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach./

33 Kreps, *Drones*, p. 60.

34 **שם**, עמ' 160.

רצוי להתייחס לשלוש ההמלצות שלהלן כאל צעדים קריטיים שיש לנקוט כדי לטפל בפגיעויות של כטב"מים למתקפות סייבר ולחזק את מערכות ההגנה שלהם:

- השלב הראשון הוא **הערכת הפגיעות** של המערכות על ידי המדינות המשתמשות. על הערכה זו להתבסס הן על הארכיטקטורה של המערכת, הכוללת את מרכז הפיקוד והשליטה, הלוויין וכלי הטיס, והן על מודיעין בנוגע ליכולותיהם של היריבים או של גורמים אחרים שיש להם עניין לפרוץ למערכת.
- על הגורמים המשתמשים בכטב"ם ליצור פתרונות טכנולוגיים לגיבוי, אשר יתריעו או **יציינו כי בוצעה גישה למערכת** על ידי שחקן בלתי מורשה, ועל כן היא נמצאת בסכנה. בהיעדרה של מערכת התרעה כזו, לא יהיה ביכולתו של המפעיל לגלות כי מתקפת סייבר התרחשה או נמצאת בעיצומה, והסבירות כי יוכל להתגונן מפניה תפחת.
- יש להשקיע מאמצים רבים יותר ב**הצפנת קישורי נתונים המשמשים לשידור מידע** מחלק אחד של המערכת למשנהו. על המפעיל לתכנן גם שיטות התגוננות אחרות, בייחוד עבור מערכות חמושות, אף אם אלו פרוסות בזירות בהן ההערכה לקיומו של איום נמוכה יותר, שכן גם מתקפות הסייבר הפחות מתוחכמות עלולות לגרום נזק למערכת.

אין ספק כי המלצות אלו מוסיפות לעלותה של המערכת, הן מבחינה כספית והן במונחים של האפקטיביות היחסית שלה. לדוגמה, הצפנה של קישורי נתונים אמנם הופכת אותם למאובטחים יותר, אך מאריכה באופן בלתי נמנע את תהליך הפענוח. בכל מקרה, סביר להניח שהנזק הפוטנציאלי העלול להיגרם עקב מתקפת סייבר מוצלחת על מערכת כטב"ם גובר על העלויות. מודעות היא המפתח, והערכה מציאותית של פגיעויות המערכת, אשר אינה ממעיטה מן הנזק הפוטנציאלי של מתקפת סייבר בודדת המבוצעת על ידי אדם יחיד, ארגון טרור או אפילו מדינה, היא הצעד ההכרחי הראשון לקראת יצירתם של אמצעי הגנה יעילים עבור הכטב"מים.