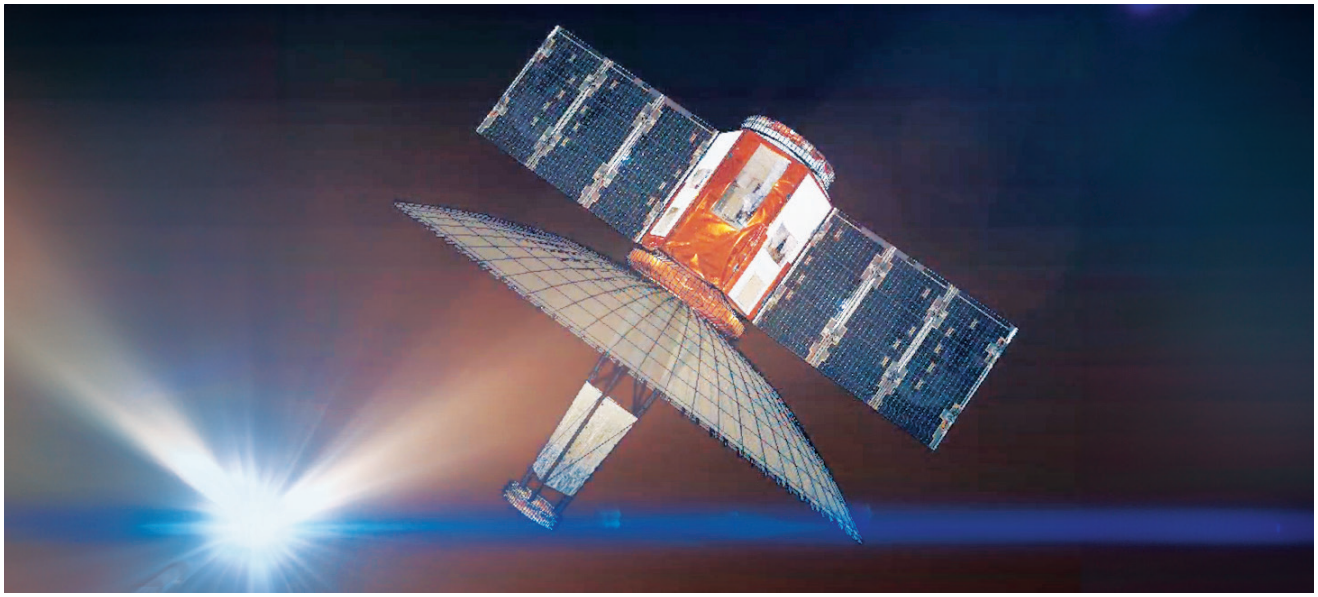
החלל כזירת לוחמה: בינה מלאכותית ואבטחת סייבר בחלל והשלכותיהן על הביטחון הלאומי

כחלק מצמיחת ענף החלל, חלה מגמת פיתוח מחשבי קצה המותאמים להתקנה בקרב מערכות המוצבות בחלל, ובכללן לווויינים. מגמה זו טומנת בחובה יתרונות רבים, ובהם היכולת להטמיע מודלים של בינה מלאכותית בקרבם, שצפויה להוביל לשינויים מהותיים באופן שבו מידע הנאסף בחלל מעובד ונשלח לכוחות בשדה הקרב. לצד זאת, השימוש בבינה מלאכותית צפוי לשנות את מצב אבטחת הסייבר שלהם ושל שירותיהם, באופן המחייב חשיבה מעמיקה על החולשות והאיומים החדשים שהטכנולוגיה צפויה להציב



אופק 13 (הדמיה). מחשוב הקצה מסייע בהנגשת שירותי לוויין ליחידות המוצבות באזורים מרוחקים, לכוחות במשימה מעבר לקווי אויב, לגורמי חילוץ והצלה ועוד. מקור: ויקיפדיה/משרד הביטחון

בעשורים האחרונים מתחוללות תמורות והתפתחויות חשובות בענף החלל, המובילות למהפכות טכנולוגיות הרלוונטיות גם לתחומי הצבא והביטחון. מגמה אחת היא הטמעת מחשוב הקצה במערכות המוצבות בחלל, המובילה לשיפורים רבים בכוח המחשוב של לווויינים וצפויה להרחיב את יכולות המחשוב והעיבוד שלהם ולשנות, באופן הדרגתי, את מידת התרומה והשירותים המתקבלים מהחלל. כחלק מכך, אפשר להצביע על ניצניה של מגמת משנה, שבמסגרתה מדינות וגורמי תעשייה מנסים להטמיע טכנולוגיות בינה מלאכותית בלווויינים עצמם, בניגוד להטמעתן במרכזי נתונים ובענן, כמקובל כיום.

הטמעת הבינה המלאכותית בלווויינים טומנת בחובה יתרונות רבים הנוגעים למהירות קבלת נתוני הלוויין והפצתם, חיסכון בכוח האדם והאצה ואוטומציה של משימות חיוניות נוספות. לצד זאת, בינה מלאכותית צפויה להוביל לשינויים במצב אבטחת הסייבר של הלווויינים, במפת האיומים ובטכניקות התקיפה, אך גם בשיטות ההגנה. מגמה זו מתקיימת על רקע תחרות עולמית אסטרטגית הנערכת בחלל, בין המעצמות, ומטרתה להשיג דומיננטיות וחופש פעולה בחלל אך גם לשלול חופש פעולה זה ממדינות יריבות.

נושאי הטמעת הבינה המלאכותית על גבי לווויינים והשלכותיה על אופן קבלת התוצרים מנכסי חלל, וכן על הגנת הסייבר של נכסים אלה, רלוונטיים לישראל בכלל ולצה"ל בפרט. רלוונטיות זו נובעת מהשימוש הגובר בלווויינים ובתוצריהם לצרכים צבאיים כגון תקשורת עם יחידות מרוחקות, ניווט, צילום וקבלת מודיעין חזותי המועבר לגופי המודיעין וליחידות הלוחמות בשטח. כמו כן, התמודדותו של צה"ל עם יריבים בשטחי מדינות זרות, ובהן יריבים במעגל השלישי, נסמכת על שירותי לווויינים, והפגיעה בהם עלולה להוביל להשבתת השירות או למניפולציות בתוצריהם, באופן שעלול לשבש משימות ולהוביל לאבדות בנפש ובציוד. שנית, התחרות האסטרטגית המתחוללת בין המעצמות בחלל עלולה להשפיע

עמרי וקסלר, חוקר במרכז לחקר סייבר בין־תחומי ע"ש בלווטניק וחוקר בכיר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון באוניברסיטת תל־אביב

גם על תוכנית החלל של ישראל ועל נכסי חלל המשמשים את צה"ל. זאת עקב שיתוף הפעולה ההולך ומתהדק בין רוסיה, הנחשבת מדינה מובילה בתחומי החלל והסייבר, ובין איראן, העושה מאמצים לפתח יכולות עצמאיות בשני ממדי לחימה אלה.

בהיעדר מידע אמפירי, ובהתחשב בכך שמדובר במגמות מתהוות, מאמר זה תאורטי בעיקרו, ומטרתו להפנות את הזרקור אל סוגיה שהדיון בה צובר תאוצה בקרב גופים צבאיים ותעשייתיים ובקרב מקבלי החלטות ברחבי העולם.

מחשוב קצה בחלל ויתרונותיו

מחשוב קצה (Edge Computing) הוא ארכיטקטורת IT מבוזרת, שבה פעולות חישוב ועיבוד מתבצעות על גבי המכשיר או הפלטפורמה האוספים את המידע או בקרבתם. מטרתה של ארכיטקטורה זו להחליף את הפרדיגמה השלטת כיום, שבה מידע שנאסף מחיישנים וממכשירי האינטרנט של הדברים (IoT) נשלח למרכזי נתונים ריכוזיים לצורך עיבוד, ניתוח ואחסון.

בעשורים האחרונים מתחולל מסחור מואץ של טכנולוגיות חלל שבא לידי ביטוי בפתיחתו של שוק שירותי החלל המסחריים ליותר מפעילים ויצרנים, במגוון רחב יותר של שירותי לווייניים ובמתן גישה הולכת וגוברת לחלל. מגמה זו מובילה לעלייה ניכרת בכמויות המידע הנאספות בו, ולכך ששיטות שליחת המידע ועיבודו על פני הקרקע כבר אינן מספיקות.[1] עם זאת, יותר חברות מתחילות לפתח מחשבים ומעבדים עוצמתיים המותאמים לשימוש בחלל, וכן חומרים פולימריים שונים שיוכלו להגן על מחשבים אלה מפני קרינה.[2] מגמה זו מתאפשרת הודות למזעור מערכות מחשוב וחומרה, המאפשר להתקינם על גביי לווייניים ולהוזיל את עלויות פיתוחם ושיגורם לחלל.

יתרונות מחשוב הקצה בלוויין מתייחסים לאופן ניהול המידע הנאסף וייעול העיבוד. לווייני צילום מייצרים נתונים במשקל של למעלה ממאה טרה־בייטים ביום,[3] בעוד לווייני תקשורת צפויים לייצר כ־90% מכלל הנתונים המופקים בחלל בעשור הנוכחי.[4] במצב הקיים, שליחת המידע אל תחנת הבקרה לצורך עיבוד וניתוח, מעמיסה ומקשה על רוחב הפס של שידור הנתונים בין הלוויין לקרקע. לעומת זאת, מחשוב קצה חוסך את שידור כל המידע הנאסף אל הקרקע, ובכך חוסך ברוחב פס ומקל את העומס משום שהחישוב והעיבוד מתקיימים במקום שבו המידע נוצר או נאסף. בהקשר הצבאי, מחשוב הקצה מסייע בהנגשת שירותי לוויין ליחידות המוצבות באזורים מרוחקים, לכוחות במשימה מעבר לקווי אויב, לגורמי חילוץ והצלה, ועוד.

הטמעת בינה מלאכותית במערכות חלל

יתרון מרכזי של מחשוב הקצה בחלל מתייחס להטמעת טכנולוגיות בינה מלאכותית בקרב מערכות המוצבות בחלל. בעת כתיבת שורות אלה משמשות מערכות הבינה המלאכותית, הממוקמות במרכזי נתונים על הקרקע, לניהול מערכי לווייניים, תיעדוף משימותיהם, ניהול דרישות וזמן המתנה, ניתוח המידע המגיע מהלוויין ועוד.[5] עם זאת, הצבת מערכות בינה מלאכותית בחלל צפויה לייצר הזדמנויות חדשות עבור מקטע החלל, ובמרכזן ייעול משימות וביצוע אוטומציה מלאה של פעולות ומשימות המתקיימות על גבי הלוויין.[6]

יתרונות השימוש בבינה מלאכותית בחלל כוללים ייעול ניכר של משימות חלל, תוך כדי הגבלה של כמות המידע הנשלחת לקרקע, ושליחת מידע מעובד הרלוונטי לצוותי הקרקע או ללקוחות השירות הלווייני בלבד. כמו כן, מודלים של בינה מלאכותית יוכלו לסייע בביצוע אוטומציה של משימות רבות כגון מיקום לווייני במסלולם, חישוב וניטור מצבם, מיקומם ופעילותם, ובתיקונם במידת הצורך.[7] בינה מלאכותית אף עשויה לשמש חלק ממערכות אוטונומיות שיסייעו ללווייני לחמוק או להסיט פסולת חלל, שהתנגשות עימה עלולה לפגוע בלוויין ובמשימתו.[8] דוגמה לכך היא תוכניתה של סוכנות החלל הבריטית לשגר ב־2025 לווייני אוטונומיים המבוססים על בינה מלאכותית, שיוכלו להסיט ולהסיר פסולת חלל.[9]

בתחום הביטחון והמודיעין, טכנולוגיות בינה מלאכותית על גבי לווייני תצפית וחישה מרחוק יוכלו לבחור אזורים או עצמים לצילום, לזהות עצמים כגון ספינות, כוחות אויב ועוד, לעבד קטעי וידיאו גדולים במיוחד בלי לשלוח אותם אל הקרקע, ולשלוח למקבלי ההחלטות, לגופי המודיעין וליחידות

בינה מלאכותית. המודלים יוכלו לסייע בביצוע אוטומציה של משימות רבות כגון מיקום לווייני במסלולם, חישוב וניטור מצבם, מיקומם ופעילותם, ובתיקונם במידת הצורך. הדמייה באמצעות Adobe Firefly

הלוחמות תובנות מודיעיניות מוגמרות. באופן זה, מפקד חי"ר או מפקד טנק יוכלו לקבל מידע מודיעיני שוטף ובזמן אמת על מיקום כוחות האויב והתקדמותו, על הפעלתן של מערכות לוחמה אלקטרונית ועוד. בהסתכלות על זירות הלחימה בעזה ובלבנון, מהפכות טכנולוגיות אלה ישפרו את היכולת לזהות בזמן אמת שיירות להעברת נשק לחזבאללה או הצבת מארבים על ידי פעילי טרור, לחזות את המשך תנועתם ועוד.

הטמעת בינה מלאכותית בקרב הלוויינים עשויה לשמש גם לצרכים כגון התרעה מוקדמת מפני טילים. כיום, חיישני חום המותקנים על גבי לווינים מסייעים באיתור טילים בליסטיים היוצאים מהאטמוספרה. משימה זו מחייבת זמן המתנה נמוך ככל האפשר שיאפשר היערכות והתרעה מוקדמת. הדרישה לזמן המתנה מינימלי מתחדדת לנוכח הפיתוח והשימוש בטילים היפרסוניים, שמהירותם גבוהה פי חמישה ממהירות הקול. מהירותם של טילים אלה הופכת את מלאכת הזיהוי והמעקב אחר תמרון הטילים לקשה ומאתגרת יותר. לפיכך, הטמעת מודלים של בינה מלאכותית שתוכל לזהות את יציאת הטילים מהאטמוספרה, לחשב את מסלולם ולהעביר מידע מעובד ומזוקק לקרקע, עשויה לשפר ולסייע בהתמודדות עם אתגרים אלה.

עם זאת, החלל הופך לאיטו למרחב שבו מתקיימת תחרות אסטרטגית בין המעצמות, והשימוש בבינה מלאכותית בחלל טומן בחובו אתגרים ברמה הבין־לאומית וסיכונים ביטחוניים, בהם גם איומי סייבר.

טיל היפרסוני בפריסה לצורך ניסויים, בקייפ קנוורל. הטמעת בינה מלאכותית בקרב הלוויינים עשויה לשמש גם לצרכים כגון התרעה מוקדמת מפני טילים. מקור: ויקיפדיה

מגמת חימוש החלל ומשמעות איום הסייבר

במקביל להתפתחותו כמרחב החיוני לכלכלה העולמית ולביטחונן הלאומי של מדינות, התחזקה תפיסתו של החלל כמרחב לחימה פוטנציאלי, שבו מתקיים מרוץ חימוש. תפיסה זו הובילה למגמת החימוש בחלל, שבאה לידי ביטוי בפיתוח ובניסויים במערכות נשק נגד לווינים, לווינים בעלי יכולת פגיעה בלוויינים אחרים ועוד.[10] דוגמאות לכך הן ניסוי שערכה רוסיה במאי 2024 לבחינת ההצבה של נשק גרעיני בחלל, וניסוי נוסף שערכה ב־2021 בטיל נגד לווינים.[11] על פי דוח הערכת האיומים השנתי לשנת 2024 של משרד ראש המודיעין הלאומי האמריקני, רוסיה וסין ממשיכות לפתח נשק אנטי־לווייני כגון מערכות לוחמה אלקטרונית, מערכות אנרגיה ממוקדת וטילים נגד לווינים.[12] גם איראן פועלת להרחיב את תוכניות החלל הצבאית והאזרחית שלה באמצעות מחקר ופיתוח ושיגור של לווייני מעקב ותצפית. תוכנית החלל של איראן מקודמת בשיתוף פעולה עם רוסיה, ובעוד איראן לא נתפסת כמעצמה בחלל, החשש הוא ששיתוף הפעולה המתהדק עם רוסיה וסין יקדם את יכולותיה הטכנולוגיות בשנים הקרובות.[13]

אחד האיומים המרכזיים על לווינים ועל ענף החלל בכללותו, שבו דנה קהילת המחקר, הוא איום הסייבר. איום זה בא לידי ביטוי בכמה תקריות של פריצה ושיבוש של שירותים ותשתיות חלל, הבולטת שבהן היא תקיפת חברת התקשורת הלווינית Viasat, טרם פלישת רוסיה לאוקראינה בפברואר 2022. מטרת המתקפה, שיוחסה לרוסיה, הייתה לשבש את יכולת התקשורת הלווינית של צבא אוקראינה, אולם היא הובילה לשיבושים ולהפרעות גם בגרמניה, בצרפת, בפולין ובמדינות נוספות.[14]

התחרות האסטרטגית המתחוללת בין המעצמות בחלל עלולה להשפיע גם על תוכנית החלל של ישראל ועל נכסי חלל המשמשים את צה"ל. זאת עקב שיתוף הפעולה ההולך ומתהדק בין רוסיה, הנחשבת מדינה מובילה בתחומי החלל והסייבר, ובין איראן, העושה מאמצים לפתח יכולות עצמאיות בשני ממדי לחימה אלה

יש כמה יתרונות ליכולות סייבר התקפיות, שעלולים להפוך אותן לאיום מרכזי על לווינים ומערכות חלל. ראשית, כלי פריצה ונוזקות נתפסים כזולים וזמינים יותר ביחס ליכולות קינטיות שונות.[15] בעוד מערכות אנרגיה ממוקדת וטילים אנטי־לווייניים נחשבים לאמצעים יקרים לפיתוח ולרכש, כלי תקיפת סייבר ניתנים להפצה מהירה, אין צורך בציוד יקר לצורך פיתוחם ויש מגוון רחב יותר של גורמי איום המסוגלים לפתחם. לצד זאת, מתוקף היותן מקטעי קוד, נוזקות ניתנות לתפוצה רחבה הרבה יותר. מקרי עבר הדגימו כיצד יכולות סייבר התקפיות שפותחו על ידי עברייני סייבר נמצאו בשימוש גופי מודיעין זרים. דוגמה לכך היא קבוצת ההאקרים הרוסית Sandworm, המקושרת למודיעין הצבאי של רוסיה (GRU) שנצפתה משתמשת בנוזקות שפותחו על ידי עבריינים ונמכרות ברשת האפלה על מנת לפרוץ למערכות תשתיות חיוניות באוקראינה.[16]

שנית, יכולות סייבר מאפשרות לגורמים זדוניים מרחב הכחשה, וקיים קושי לייחס את המתקפה לתוקף. כמו כן, תוקפים

משתמשים לעיתים בתשתיות של צד שלישי ואף של חברות או ארגונים לגיטימיים לביצוע תקיפות, ופועלים לטשטש את עקבותיהם, דבר המקשה אף יותר על הייחוס. שלישית, יכולות סייבר התקפיות מעניקות לתוקף יתרון של גמישות הבא לידי ביטוי ביכולת לגרום לנזק זמני בלבד או מוגבל בהיקפו. לצד זאת, היכולת לשבש את פעילותם של לוויינים באמצעות תקיפות סייבר עשויה למזער את הסיכון ליצירת פסולת חלל. פסולת זו עשויה, בין השאר, מִשְׁבְּרי לוויינים הנעים במסלול ההקפה ועלולים לגרום לנזק של ממש ללוויינים ולנכסי חלל, בהם נכסי חלל השייכים לתוקף.[17] על כן, יכולות סייבר צפויות להמשיך לשמש יכולות חשובות המאפשרות לבצע מניפולציות, לגנוב מידע, לשבש ולהשבית תשתיות חלל, ובכלל זאת, לוויינים. כטכנולוגיה חדשה, המוטמעת באופן הולך וגובר בקרב ענף החלל ואף בלוויינים עצמם, לבינה המלאכותית צפויות להיות השלכות על אבטחת הסייבר של ענף החלל.

השלכות הטמעת הבינה המלאכותית בחלל על תחום אבטחת הסייבר

למגמות ולשינויים המתחוללים בתחום המחשוב בענף החלל בכלל ובלוויינים בפרט, ובראשם הטמעת בינה מלאכותית בלוויינים, צפויות להיות השלכות בנות משמעות רבה על הארכיטקטורה של מערכות ונכסי חלל, ולפיכך גם על אבטחת הסייבר של מערכות חלל, דבר שעלול להשליך ישירות על הזמינות, האמינות והאיכות של המידע המגיע למקבלי ההחלטות בכל הרמות וליחידות הלוחמות בשטח. השלכות אלה אפשר לחלק על פי היתרונות שהטכנולוגיה צפויה לתרום למידת אבטחת הסייבר של מערכות חלל, ועל פי החולשות ופערי האבטחה הצפויים לצוץ או להתגבר בעקבות הטמעת הבינה המלאכותית בחלל.

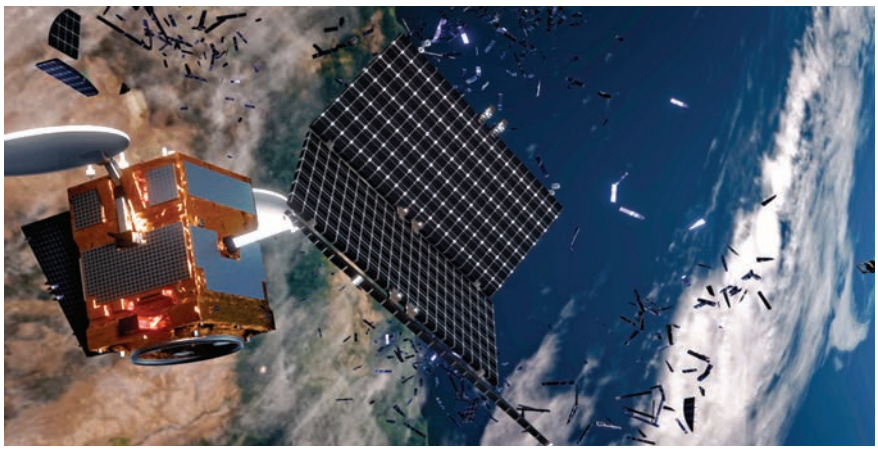
השימוש בבינה מלאכותית לצורכי הגנה

מקרי שימוש לצורכי הגנה. מערכות בינה מלאכותית עשויות לשמש לצורכי אבטחת סייבר, ובשנים האחרונות יש עלייה בשילובן במערכות ובמוצרי אבטחה. ספציפית, בינה מלאכותית עשויה לשמש לצורך שיפור מידת העמידות (Robustness) של מערכות באמצעות ניטור התנהגות המערכת, זיהוי אנומליות, סריקה, דירוג ותיקון חולשות במערכות הלוויין,[18] וכן בשיפור חסינות (Resilience) כגון באמצעות סיוע בתגובה לתקריות ובהחזרתן לפעילות שגרתית.[19] כיום מתגבר השימוש בבינה מלאכותית המוטמעת במערכות אבטחת סייבר קרקעיות, אולם הטמעתה בלוויינים עשויה להפחית את זמן ההמתנה הנובע מהצורך שבשליחת המידע הרלוונטי לקרקע.

לבסוף, בינה מלאכותית עשויה להגיב לתקריות סייבר ואף לפעול פרו־אקטיבית נגד איומים. דוגמה לכך היא יצירה אוטומטית של מלכודות פיתוי (honeypots) הנראות כמו סביבות שהתוקפים מעוניינים לפרוץ אליהן, ומשמשות לצורך לימוד הכלים והטקטיקות של התוקף ולצורך התרעה על נוכחות גורם זדוני במערכת, או פיצול הרשת למקטעים.[20] לנוכח המעבר לשימוש במערכי לוויינים, המשמשים כרשת הממוקמת בחלל, פיצול הרשת באופן דינמי ואוטונומי עשוי להיות פתרון יעיל בתרחישים שבהם תוקף הצליח לקבל גישה, להתקין נוזקה או להשתלט על לוויין או על קבוצת לוויינים מתוך המערך.

הקטנת הגישה ללוויין מהקרקע. נכסי חלל ניתנים לחלוקה למקטעים טכנולוגיים ואופרטיביים האחראיים לפונקציות שונות, ולפיכך גם חשופים לאיומים שונים: מקטע הקרקע, הכולל את המערכות הקרקעיות המנטרות ושולטות בלוויין ומפיצות את תוצריו; מקטע החלל, המורכב מהלוויין עצמו, רכיביו השונים והמטע"ד (המטען הייעודי) האחראי לביצוע משימותיו; מקטע העברת הנתונים שבין הלוויין ובין הקרקע, שכולל את ערוץ התקשורת ושידור הנתונים, ולבסוף, מקטע המשתמש - המאפשר למשתמשי הקצה של שירותי הלוויין לקיים אינטראקציה עם אותות הלוויין, ישירות או באמצעות מערכות ויישומים אחרים של מקטע הקרקע.[21]

בבחינת ארבעת המקטעים, המקטע הקרקעי משמש באופן יחסי כווקטור הפריצה הפשוט ביותר למערכות חלל. תחנות הקרקע מבוססות על ציוד ותשתיות IT נפוצים המוכרים גם לגורמים זדוניים.[22] על סמך היכרות זו, תוקפים עלולים לפרוץ לתשתיות קרקעיות כדי לקבל גישה ללוויין עצמו. נוסף על כך, תקיפת סייבר נגד תחנת קרקע השולטת על מערך לוויינים עלולה לשמש כנקודת כשל בודדת, ופריצה אליה עלולה להוביל לשיבושים ולהשבתת מערכי לוויינים הכוללים עשרות או מאות לוויינים.[23] הטמעת בינה מלאכותית בקרב הלוויינים עצמם עשויה להפוך את הלוויין לעצמאי יותר ולצמצם את תלותו בקרקע. בעוד ערוץ תקשורת ויכולת לשלוט על הלוויין מהקרקע צפויים להישאר, צמצום התלות והשליטה על הלוויין מהקרקע צפוי להגביל את יכולתם של תוקפים פוטנציאליים להשתמש בפריצה לרשת מקטע הקרקע, כפעולת הכנה לקראת קבלת גישה ללוויין עצמו. מנגד, תוקפים פוטנציאליים עלולים להתמקד בדרכים אחרות כדי לקבל גישה אל הלוויין, כגון ניצול חולשות בשרשרת האספקה.[24] יכולתם של



פסולת חלל – אילוסטרציה של לוויין מתפרק בחלל. סוכנות החלל הבריטית מתכננת לשגר לוויינים אוטונומיים מבוססי בינה מלאכותית, שיוכלו להסיט ולהסיר פסולת חלל.
מקור: ויקיפדיה

לוויין איראני. בעוד איראן לא נתפסת כמעצמה בחלל, החשש הוא ששיתוף הפעולה המתהדק עם רוסיה וסין יקדם את יכולותיה הטכנולוגיות בשנים הקרובות. מקור: Mehr News agency/Creative Commons

אלגוריתמים ללמוד ולהשתפר, ובייחוד בשיטות כגון למידה באמצעות חיזוקים (Reinforced learning), המאפשרת למודל הבינה המלאכותית ללמוד מניסוי וטעייה, עשויה להיות חיונית עבור לוויינים, בהינתן הגישה הפיזית המוגבלת אליהם.

חולשות וסיכונים הנובעים מהטמעת בינה מלאכותית

חולשות שמקורן בהטמעת מחשוב קצה ובינה מלאכותית בלוויינים. תפיסת ההגנה של מערכות חלל מהדורות הקודמים התבססה על רעיון ה"אבטחה באמצעות אי־בהירות" (Security through obscurity), כלומר שמורכבותן של מערכות אלה תקשה על גורמים זדוניים לרכוש היכרות עימן ולפרוץ אליהן.[25] עם זאת, מחשוב קצה על גבי הלוויין, הטומן בחובו שימוש ברכיבי מחשוב, תוכנות ומערכות הפעלה נפוצות, צפוי לחשוף את הלוויינים לאיומי סייבר נפוצים יותר, המוכרים ממערכות IT קרקעיות, כגון איומי כופרה, גנבת מידע, תקיפות מניעת שירות (DoS) ועוד. דוגמה לכך היא ניסוי שנערך באפריל 2023 במסגרת תוכנית ה־OPS-SAT של סוכנות החלל האירופית, ושבמהלכו חוקרים מחברת Thales פרצו לננו־לוויין של הסוכנות, השתלטו על מצלמת הלוויין, על מערכות הניווט, על מערכת בקרת הגובה ועוד.[26]

איומי סייבר הרלוונטיים למערכות בינה מלאכותית. הטמעת בינה מלאכותית בקרב הלוויינים צפויה לחשוף את פעילותם לאיומי סייבר הרלוונטיים למערכות בינה מלאכותית. לדוגמה: גישה בלתי מאושרת למידע המשמש לאימון האלגוריתמים, עלולה לאפשר לתוקף "להרעיל" את המידע מבעוד מועד, כלומר להחדיר למאגר הנתונים מידע מזויף, שעלול לשבש את פעילות האלגוריתם בשלב מאוחר יותר. גישה ללוויין עצמו עשויה לאפשר ביצוע מניפולציות מזעריות, בלתי נראות לעין האנושית, במידע המתקבל לניתוח (הקֶלֶט), ובכך לשבש את עיבוד וסיווג המידע ולהוביל להצגת פֶּלֶט שגוי.[27] תוקף פוטנציאלי המעוניין לבצע מניפולציות במידע אינו זקוק להיכרות מעמיקה עם המודל ואינו צריך לשנות את המידע לחלוטין כדי לשבש את פעילותו. מצב זה מגביר את האיום ומקל את ביצוע המתקפה.[28]

יתרה מכך, שיבוש או עריכת מניפולציות במידע המתקבל במערכות הלוויין יכולים להתבצע באמצעות גישה פיזית ללוויין. איום קיים בחלל הוא ניצול הלוויינים לשימוש כפול (dual use) לצורך מבצעי תמרון וקרבה (RPO). לוויינים אלה מתמרנים בקרבת לוויינים אחרים ועשויים לשמש לצורך תיקון תקלות ותחזוקה, אולם גם לריגול, לגרימת נזק ולפגיעה בלוויין ובמרכיביו השונים.[29] באופן זה, לוויינים עוינים עלולים לפגוע במצלמות ובחיישני הלוויין, להסתיר אובייקטים לצילום, "לעוור" חיישנים ולשדר מידע שגוי ללוויין. שיבוש פעילות איסוף המידע של הלוויין יכול להתבצע גם מהקרקע, באמצעות מערכות להקרנת אלומות לייזר המסוגלות לסנוור חיישנים המותקנים על גבי הלוויין, או לשבש שידור נתונים המתבצע באמצעות תקשורת אופטית.[30] איומים אלה רלוונטיים ללוויינים גם כיום, אולם בהינתן בקרה מוגבלת מצד מפעילים אנושיים, ובהינתן שעיבוד המידע מתקיים על גבי הלוויין, מסקנות ותובנות שגויות עשויות להישלח אל הקרקע. כמו כן, קרבה פיזית של לוויינים יריבים ללוויין עשויה לאפשר למפעיליהם לבחון את תגובתו לסביבה ולהאזין לתוצריו המשודרים לקרקע כדי ללמוד על הפֶּלֶט של המודל. למידת הפֶּלֶט עלולה לאפשר לתוקפים לבצע הנדסה לאחור של המודל וללמוד כיצד הוא בנוי, באופן שיאפשר להם לנסח דרכים שונות לתקוף או לבצע בו מניפולציות.[31]

היעדר הַסְבָּרָתִיוּת של מערכות בינה מלאכותית

חולשות אבטחה נוספות נובעות מהיעדר הסברתיות (Explainability) של מודלים של בינה מלאכותית. הסברתיות מתייחסת למידת היכולת לשקף את ההיגיון או להבין כיצד מקבל האלגוריתם את החלטותיו. שקיפות והסברתיות של תהליך קבלת ההחלטות של האלגוריתמים נתפסות כעקרונות חיוניים המשפרים את מידת האמון של המשתמש האנושי במערכות אוטונומיות, ומכך גם את שיתוף הפעולה ואת היעילות של צוותי אדם-מכונה מעורבים. נוסף על כך, היעדר שקיפות וחוסר יכולת להסביר את תהליך קבלת ההחלטות של האלגוריתמים עלולים לפתוח חלון הזדמנויות לתוקפים פוטנציאליים לערוך מניפולציות במידע או בתהליך בלי שאלה יתגלו על ידי המפעיל האנושי.[32] היעדר השקיפות

כלפי המפעיל האנושי מוביל גם למידה מסוימת של אי־ודאות, ולפגיעה ביכולת חיזוי ההתנהגות של המודל ובהתמודדותו עם מצבים חדשים.[33] הסיכון למידה פחותה של אמון או לחוסר ודאות בנושא פעילותה של מערכת אוטונומית בחלל עשוי להחריף לנוכח מורכבותה של סביבת החלל, ההולכת והופכת למאוכלסת אף יותר לנוכח שיגור מתמשך של מערכי לוויינים, ניסויים בנשק חלל שמקיימות מדינות ועוד. סיבה נוספת לאי־ודאות בנושא פעילותן של מערכות אוטונומיות בחלל היא היעדר גישה פיזית למערכת. בניגוד להרבה מערכות קרקעיות, אי אפשר לגשת ללוויין ולכבותו ידנית בתרחיש שבו הוא מתנהל בניגוד למצופה.

כיצד צפויה הגנת הסייבר של לווייניים להשתנות

חשיבותו הגוברת של מרחב החלל בחשיבתן האסטרטגית של מדינות ומגמת חימוש החלל, לצד הופעתן של טכנולוגיות חדשות, מחייבת חשיבה מחודשת על הגנת הסייבר של מערכות חלל. חשיבה זו מחייבת ניסוח אסטרטגיה ותוכניות פעולה להגנה על מערכות חלל וכן התאמה של עקרונות ומסגרות הגנה על מודלים של בינה מלאכותית ומיקודן, לצורך מתן מענה לתנאים השונים השוררים בחלל. על מסגרות אלה לתת מענה לסיכונים שמקורם בעיצוב ארכיטקטורת מערכות הלוויין ובפיתוחן ובתפעול השוטף של מערכות החלל.

דוגמה שימושית היא ארכיטקטורה המבוססת על עקרונות "אפס אמון", השמים דגש על אכיפת בקרת גישה למערכות מידע, זיהוי משתמשים ואי־מתן אמון במכשירים המחוברים לרשת הארגונית, גם אם אומתו בעבר.[34] בעוד בעבר, מגבלות כוח מחשוב וזיכרון הציבו אתגר ליישום עקרונות אפס האמון בקרב לווייניים, מגמות במחשוב קצה בחלל צפויות לאפשר את הטמעת הארכיטקטורה בלווייניים חדשים. ארכיטקטורה זו עשויה להיות יעילה עבור מודלים של מערכי לווייניים, המבצעים אימות הדדי ומשמשים חלק מהרשת.

השינויים והמגמות בענף החלל, הן בהיבט הטכנולוגי הן בהיבט האסטרטגי והצבאי, מחייבים תהליכים מתמשכים של ניהול סיכונים, המביאים בחשבון סיכונים בתחומי הפיתוח והשימוש בבינה מלאכותית, אולם גם סיכונים בחלל, כגון היעדר גישה פיזית ללוויין מרגע ששוגר, וכן סיכונים אסטרטגיים הנובעים ממרוץ החימוש המדינתי בחלל. כחלק מניהול סיכונים זה, יש לקבוע את מידת האוטונומיה של מערכות הבינה המלאכותית המותקנות על גבי הלוויין, לה השלכות על סוג הסיכונים וחומרתם, ואת סוג הבקרה האנושית ומידת האינטראקציה של המערכות עם מפעיליהן האנושיים. הגדרות אלה יסייעו לפתח יכולות מענה ותגובה לתקריות סייבר, בהן תקלות או תקיפות הקשורות למודל הבינה המלאכותית המוטמע בקרבן. לצד זאת, מחשוב הקצה צפוי לאפשר שילוב חכם וגמיש יותר של אמצעי הגנת סייבר על הלוויין בהשוואה למשאבי המחשוב המוגבלים, שהיו זמינים בעבר. לדוגמה: הצפנה של תעבורת רשת מהלוויין אל הקרקע הובילה בעבר להאטה במהירות שידור הנתונים, אולם העלייה בכוח המחשוב של הלוויין עשויה לאפשר הטמעה של מנגנוני הצפנה על הלוויין עצמו.[35] לבסוף, על תפיסת ההגנה של מערכות חלל להביא בחשבון את חוסר הוודאות המתלווה לשימוש במערכות בינה מלאכותית, ולהכיר בכך שאי־הוודאות עלולה לגבור בחלל. על שינוי תפיסתי זה לבוא לידי ביטוי בפיתוח מנגנוני שקיפות שיאפשרו למערכת לספק הסבר לקבלת ההחלטות האוטונומית, וכן בעיצוב הארכיטקטורה של הלוויין, כך שתכלול שכבות הגנה חלופיות שיוכלו לתת מענה למצבים שבהם מערכת הבינה המלאכותית מתנהגת באופן לא צפוי. לשם כך, יש לאמץ מנגנוני בדיקה וניסוי לקביעת מידת הדיוק ואופן ההתנהגות של מודל הבינה המלאכותית, לנוכח תרחישים ומצבים שונים.

סיכום

כחלק מצמיחת ענף החלל, חלה מגמת פיתוח מחשבי קצה המותאמים להתקנה בקרב מערכות המוצבות בחלל, ובכללן לווייניים, והצפויים להגביר באופן ניכר את כוח המחשוב ואת הזיכרון שלהן. מגמה זו טומנת בחובה יתרונות רבים, ובהם היכולת להטמיע מודלים של בינה מלאכותית בקרב הלווייניים. יתרון זה צפוי להוביל לשינויים מהותיים באופן שבו מידע הנאסף בחלל מעובד ונשלח לקרקע. המהלך יאפשר לכוחות בשדה הקרב לקבל מידע חזותי מעובד ותובנות מודיעיניות מוגמרות בזמן אמת, לצד חיזוי דפוסים אוטונומי, באופן שישפר מהותית את יכולת קבלת ההחלטות בשטח. מנקודת המבט של תפעול הלוויינים, הטכנולוגיה תסייע לבצע באופן אוטונומי משימות חיוניות, כגון מיקום ותנועת הלוויין בהקפה, תיקון תקלות, הסטת פסולת חלל, איתור וסיווג איומים ועצמים בחלל ושיפור תוצרי הלוויין.

השימוש בבינה מלאכותית בקרב לווייניים צפוי לשנות את מצב אבטחת הסייבר של הלווייניים ושל שירותיהם, באופן המחייב חשיבה מעמיקה על החולשות והאיומים החדשים שהטכנולוגיה צפויה להציב, על האופן שבו תשנה את שיטות התקיפה של גורמים זדוניים, וכן על היתרונות שאפשר להפיק ממנה לצורך שיפור מידת האבטחה של המערכות. איומים וסיכונים אלה מתרחבים לנוכח מגמת הפיכתו של החלל למרחב לוחמה פוטנציאלי בין המעצמות

לצד זאת, השימוש בבינה מלאכותית בקרב לווייניים צפוי לשנות את מצב אבטחת הסייבר של הלווייניים ושל שירותיהם, באופן המחייב חשיבה מעמיקה על החולשות והאיומים החדשים שהטכנולוגיה צפויה להציב, על האופן שבו תשנה את שיטות התקיפה של גורמים זדוניים, וכן על היתרונות שאפשר להפיק ממנה לצורך שיפור מידת האבטחה של המערכות. איומים וסיכונים אלה מתרחבים לנוכח מגמת הפיכתו של החלל למרחב לוחמה פוטנציאלי בין המעצמות, ניסיונן של מדינות אזוריות, כגון איראן, להפוך למעצמות בחלל, ולנוכח היתרונות הרבים שיכולות סייבר התקפיות צפויות להעניק לתוקפים פוטנציאליים, חלקן תוך ניצול טכנולוגיות הנמצאות בשימוש צבאות.

איומי הסייבר והחולשות המובְנות, הן בטכנולוגיות בינה מלאכותית הן במערכות המוצבות בסביבת החלל, מחייבים שינויים מחשבתיים והתאמות של טכניקות ובקרות אבטחת סייבר המוכרים מעולמות הסייבר ואבטחת המידע לנוכח המגמות המתחוללות בענף החלל, וכן מחקרים עתידיים שמטרתם לבחון את יתרונותיה של טכנולוגיית הבינה המלאכותית ורתימתה לצורכי הגנה על מערכות חיוניות אלה.

ההערות למאמר זה מתפרסמות בסוף הגיליון.

מקומית (סאל"ם). בין הקטבים 1, עמ' 97–156

2 על אודות מבצע "שכנות טובה": דרור, א' (2023). לחבק את האויב, מערכות ומודן

3 לסלוי, א' (פברואר 2014). התכסית האנושית כבסיס להפעלת כוח: ההתמודדות עם הבדווים בנגב במלחמת העצמאות. בין הקטבים 1, עמ' 7–27

4 שם, עמ' 12

5 שם, עמ' 20

6 קליימן, ש' ושובל, ל' (2024, 15 בספטמבר). חטיבה בצפון פיזרה ללא אישור כרוזים בדרום לבנון: "עזבו את הבתים באופן מיידי"; צה"ל: "בודקים ומתחקרים". ישראל היום

7 Al-Kafur, W. (2024, August 17). Shock, grief as Israeli Lebanon strike kills 10 Syrians. France 24

ההפתעה האסטרטגית של 7 באוקטובר כהפתעה בסיסית-אבסורדית (עמ' 48)

1 לניר, צ' (1983). ההפתעה הבסיסית. שער ראשון. הקיבוץ המאוחד

2 Wohlshtater, R. (1962). Pearl Harbor: Decision and Warning. Stanford University Press

3 קם, א' (1990). מתקפת פתע. חלק ג'. מערכות

4 טאלב, נ"נ (2007). הברבור השחור. פרק 10. דביר

5 לניר, צ' (1983). עמ' 87-88

החלל כזירת לוחמה: בינה מלאכותית ואבטחת סייבר בחלל והשלכותיהן על הביטחון הלאומי (עמ' 54)

1 What is Orbital Edge Computing and Why is it Important? (2023, December 17). New Space Economy

2 Werner, D. (2022a, September 12). Startups to test advanced computing technology on lunar missions. Space News

3 Mohney, D. (2020, April 28). Terabytes from space: Satellite imaging is filling data centers. Data Center Frontier

4 Currivan, H. (2022, October 24). Satcom Data Traffic in GEO. NSR

5 Williams, L. (2023, May 23). NRO, Awash in Satellites and Their Data, Hope AI Can Help It Cope. Defense One

6 Labrèche, G., Evans, D., Marszk, D., Mladenov, T., Shiradhonkar, V., Soto, T., & Zelenevskiy, V. (2022, March). OPS-SAT spacecraft autonomy with tensorFlow lite, unsupervised learning, and online machine learning. In 2022 IEEE Aerospace Conference (AERO) pp. 1-17

7 Werner, D. (2022, January 24). Living on the edge: Satellites adopt powerful computers. Space News

8 Marr, B. (2023, April 10). Artificial Intelligence in Space: The Amazing Ways Machine Learning is Helping to Unravel the Mysteries of the Universe. Forbes

9 Press Release: New funding to support sustainable future of space. (2022, January 31). UK Space Agency

10 שפירא, ז' וברעם, ג' (2019). מירוץ החימוש בחלל: מגמות עולמיות ואינטרסים מדינתיים. סייבר, מודיעין וביטחון. 3(2). עמ' 4

11 Hadley, G., & Gordon, C. (2024, May 21). Russia's New Counterspace Weapon Is in the Same Orbit as a US Satellite. Air and Space Forces Magazine

12 Annual Threat Assessment of the U.S. Intelligence Community. (Unclassified report). (2024, February). Office of the Director of National Intelligence. Pp. 11, 17

13 בן ארי, ל' (2024, 15 בנובמבר). טילים, מודיעין וגרעין: מירוץ החימוש של איראן מגיע לחלל. Ynet; Gambrell, J. (2024, January 28). Iran launches 3 satellites into space that are a part of a Western-criticized program as tensions rise. AP News

14 Ikeda, S. (2022, March 17). Ukraine satellite internet service hit by cyber attack, intelligence agencies investigating. CPO Magazine

15 Schulze, M. (2020). Cyber Conflict in International Law: Challenges of Attribution and Thresholds of Cyber Operations. In 2020 12th International Conference on Cyber Conflict (CyCon). NATO Cooperative Cyber Defence Centre of Excellence. Pp. 184, 191

16 Toulas, B. (2022, September 19). Russian Sandworm hackers pose as Ukrainian telcos to drop malware. Bleeping Computer

17 Unal, B (2020, December 22). We're not ready for the coming wave of space cyberattacks. Wired

18 Belani, G. (2021, January 16). The Use of Artificial Intelligence in Cybersecurity: A Review. IEEE Computer Society

19 Irei, A. & Froehlich, A. (2024, January 22). Incident response automation: What it is and how it works. TechTarget

20 Pupillo, L., Fantin, S., Ferreira, A., & Polito, C. (2021, May). Artificial Intelligence and Cybersecurity: Technology, Governance and Policy Challenges. Centre for European Policy Studies (CEPS). P. 20

21 Baram, G., & Wechsler, O. (2020). Cyber Threats to Space Systems: Current Risks and the Role of NATO. Joint Air & Space Power Competence Center

22 Lipkin, Y., Shlomo, A., Paz, A., Menaker, D., Mizrahi, G. & David, N. (2015). Critical Infrastructure and Operational Technology Security. Cybersecurity-Review. p. 35

23 Decker, A. (2023, April 4). Satellite ground stations are vulnerable, US warns. Defense One

24 Garamone, J. (2024, April 2). New Space Strategy Looks to Integrate DOD, Commercial Efforts. U.S. Department of Defense

25 Falco, G. (2018). Job One for Space: Space

Asset Cybersecurity. Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs. p. 10
26 Thales seizes control of ESA demonstration satellite in first cybersecurity exercise of its kind (2023, April 25). Thales
27 No. NIST Artificial Intelligence AI 100-2 E2023. Adversarial machine learning: A taxonomy and terminology of attacks and mitigations
28 Qiu, S., Liu, Q., Zhou, S., & Wu, C. (2019). Review of artificial intelligence adversarial attack and defense technologies. Applied Sciences, 9(5), p. 909
29 U.S. Defense Intelligence Agency (2022). Challenges to Security in Space. [PDF]. p. 29; Secure World Foundation (2023, July). Chinese Co-Orbital Anti-Satellite Capabilities. [PDF] p. 1
30 Secure World Foundation (2019, April). Global Counterspace Capabilities: An Open Source Assessment. pp. 18-20
31 OWASP (2023). ML03:2023 Model Inversion Attack. OWASP Machine Learning Security Top 10
32 Breda, P., Markova, R., Abdin, A., Jha, D., Carlo, A., & Manti, N. P. (2022). Cyber vulnerabilities and risks of AI technologies in space applications. In 73rd International Astronautical Congress (IAC), Paris, France. p. 5
33 Bailey, M. (2023, September 13). Why humans can't trust AI: You don't know how it works, what it's going to do or whether it'll serve your interests. The Conversation; Heikkilä, M. (2024, March 5). Nobody knows how AI works. MIT Technology Review
34 National Institute of Standards and Technology. (2020). Zero trust architecture ((NIST Special Publication No. 800-207
35 Pavur, J. & Martinovic, I. (2020). SOK: Building a 35 for Impactful Satellite Cybersecurity Research. arXiv e-prints

איך לנצח מלחמה בלי מגפה? (עמ' 60)

1 צוות חקירה חיל הרפואה (2022, 13 במאי). סקירה רפואית – מלחמת רוסיה אוקראינה. עדכון מס' 6. בה"ד 10
2 Byerly C.R. (2010). The U.S. Military and the Influenza Pandemic of 1918-1919. NIH
3 Ibid
4 Wever, P. C., & van Bergen, L. (2014). Death From 1918 Pandemic Influenza During the First World War: A Perspective From Personal and Anecdotal Evidence. NIH
5 Shanks, G. D., Burroughs, S., Sohn, J. D., et al. Variable Mortality From the 1918-1919 Influenza Pandemic During Military Training. NIH
6 Shanks, G. D., Waller, M., Mackenzie, A., & Brundage, J. F. (2011). Determinants of Mortality in Naval Units During the 1918-19 Influenza Pandemic. NIH
7 Walters, W. A., Reyes, F., Soto, G. M., et al. (2020). Epidemiology and Associated Microbiota Changes in Deployed Military Personnel at High Risk of Traveler's Diarrhea. NIH
8 Hyams, K. C., Bourgeois, A. L., Merrell, B. R., & et al. (1991). Diarrheal Disease During Operation Desert Shield. NIH
9 Sanders, J. W., Putnam, S. D., Frankart, C., et al. (2005). Impact of Illness and Non-Combat Injury During Operations Iraqi Freedom and Enduring Freedom (Afghanistan). NIH
10 Ibid
11 Riddle, M. S., Savarino, S. J., & Sanders, J. W. (2015). Gastrointestinal Infections in Deployed Forces in the Middle East Theater: An Historical 60 Year Perspective. NIH
12 צוות חקירה חיל הרפואה (2022)
13 שם

טיפולוגיה חדשה של רמות המלחמה (עמ' 66)

1 תמרי, ד' (יוני 1980). הרהורים על הטקטיקה. מערכות 273-274, עמ' 2
2 נוה, ש' (2001). אמנות המערכה – התהוותה של מצוינות צבאית. מערכות, עמ' 150
3 תמרי, ד' (2012). האומה החמושה – עלייתה ושקיעתה של תופעת המילואים. מערכות ומודן
4 פרידמן, ב"א (2022). על הטקטיקה – תיאוריה של ניצחון בקרב. מערכות ומודן
5 קהלני, א' (1976). עז 77. שוקן
6 אורי, א' (דצמבר 2003). טכנו־אסטרטגיה – השפעת תמורות טכנולוגיות על החשיבה האסטרטגית. מערכות, עמ' 4–8, 392
7 פרידמן (2022), עמ' 83–101
8 אשר, ד' (2003). לשבור את הקונספציה. מערכות, עמ' 125
9 בוימפלד, מ' (2017). "קפיצה למים הקרים" – המגעים המדיניים בין ישראל, מצרים וארה"ב בשנים שקדמו למלחמת יום הכיפורים 1970-1973. אפי מלצר בע"מ, מחקר והוצאה לאור

לקריאת הגיליון המקוון:

https://www.maarachot.idf.il/31243#211410712