מכון ירושלים לאסטרטגיה ולביטחון
The Jerusalem Institute
for Strategy and Security

שימוש של ארגוני טרור בבינה מלאכותית ובטכנולוגיות מתקדמות

גבי סיבוני
סיימון ציפיס

מכון ירושלים לאסטרטגיה ולביטחון
The Jerusalem Institute
for Strategy and Security

שימוש של ארגוני טרור בבינה מלאכותית ובטכנולוגיות מתקדמות

גבי סיבוני
סיימון ציפיס

אוקטובר 2025
תשרי התשפ״ו

שימוש של ארגוני טרור בבינה מלאכותית ובטכנולוגיות מתקדמות

1 מבוא

סייבר ובינה מלאכותית מהווים כיום נדבך משמעותי בפעולתם של ארגוני טרור וגרילה. בין הסיבות לכך: הצורך של הארגונים להתאים עצמם לאמצעים טכנולוגיים מתקדמים של כוחות ביטחון ואכיפה מדינתיים שעימם הם מתמודדים; האפשרות להגדיל באמצעות בינה מלאכותית ולוחמת סייבר את שטח הפעילות, לגרום לנזק רב יותר; ולהפחית ולמזער עלויות, משאבים, מגע פיזי עם כוחות ביטחון המסכן את הארגונים.

טכנולוגיות אינטרנט כגון רשתות חברתיות, פלטפורמות שיח וערוצי תוכן, מטבע ספרתי ואמצעי פריצה מאפשרים לארגוני טרור להפיץ תעמולה, לגייס לשורותיהם תומכים ולוחמים, לגייס אמצעי מימון ותרומות ולהישאר עלומים, מה שמקשה על תפיסתם. דיגיטליזציה אפשרה לתשתיות קריטיות להיות מנוהלות טוב יותר, אך גם הפכה אותן לפגיעות יותר על ידי קבוצות עוינות.

אמצעי סייבר ובינה מלאכותית מאפשרים גם לארגוני טרור וגרילה לנהל לחימה באופן יעיל יותר ואף מפחיתה עלויות. אחד היתרונות המובהקים הוא היכולת להקצין באמצעות סייבר תומכים בכמויות גדולות ומסביב לעולם – הישג אדיר לעומת זמנים קודמים. זריעת פחד וערעור שלטון הינו היבט נוסף אשר מושג באמצעי סייבר ואשר מהווה מטרה מרכזית של טרור כאמצעי לחימה.

גיוס כספים ומימון טרור הינו תוצר נוסף, משמעותי לא פחות, אשר מושג באמצעות פלטפורמות אינטרנט מגוונות המאפשרות גיוס כמעט בלתי מוגבל ואי תלות בנותני חסות מדינתיים (כגון מדינות תומכות ו/או מממנות טרור), מה שמאפשר חופש פעולה אידאולוגי, פוליטי וגאוגרפי.

עבודה עם אמצעי סייבר ובינה מלאכותית גם מעלה את רמת ההתמחות והמומחיות של פעילי טרור וגרילה. זה, בתורו, יוצר יתר שוויון בין לוחמי ארגונים אסימטריים לבין כוחות הביטחון של מדינות ושלטונות הנלחמים מולם.

ארגוני טרור וקבוצות מורדים וגרילה אינם היחידים שאימצו בינה מלאכותית ואמצעי סייבר. אנו עדים למיזוג של ארגוני טרור, קבוצות גרילה ופשע מאורגן חוצה גבולות. מה שהחל כמיזוג של סחר בסמים וארגונים מהפכניים באמריקה הלטינית בתקופת המלחמה הקרה, כאשר סחר בסמים סיפק מימון למורדים וארגוני גרילה סיפקו אמצעי לחימה לסוחרי סמים ממשיך כמאבק אחיד אנטי-ממשלתי, ושני העולמות משתפים ביניהם ידע ויכולות ספרתיים. כך, ארגוני סמים באמריקה הלטינית מאמצים יכולות סייבר ובינה מלאכותית בלחימה נגד כוחות ביטחון מקומיים. גם הימין הקיצוני אימץ אמצעים אלה במאמציו לערער שלטון יריב.

2 ניתוח טכנולוגיות מתקדמות בשימוש ארגוני וטרור

2.1 מחקר ופיתוח צבאי בשירות קבוצות טרור וגרילה

במהלך ההיסטוריה, מחקר ופיתוח צבאי (מו"פ) השפיע באופן ניכר גם על גורמים לא-מדינתיים, כולל קבוצות טרור וגרילה, וזאת באמצעות הפצת טכנולוגיה, רכישות בשוק השחור או עיבוד של חידושים בקוד פתוח (מקורות פתוחים) ופיתוחים לא מסווגים. זה קורה לעיתים קרובות באמצעות ציוד שנתפס, הנדסה הפוכה או שלוחות מסחריות (commercial offshoots) של טכנולוגיה צבאית.

מו"פ צבאי מונע בעיקר על ידי גורמים מדינתיים כמו ארה"ב, ברית המועצות ובהמשך רוסיה, סין ואחרים ומתמקד בנשק, בשיטות לחימה, במערכות סייבר ובינה ואף בבינה מלאכותית. המחקר והפיתוח של טכנולוגיות ואמצעי לחימה זולג ויכול להתפשט, בשוגג או במכוון, לגורמים לא מורשים במגוון דרכים.

נשק וציוד צבאי עודף או גנוב ממלחמות וסכסוכים מסביב לעולם מגיעים לשוק השחור ומחמשים קבוצות באזורים כמו המזרח התיכון, אפריקה ואמריקה הלטינית. שיטות גרילה שפותחו בסכסוכים במאה ה-20 (למשל על ידי מאו צה-טונג או צ'ה גווארה) כללו מארבי "פגע וברח" ופעולות פסיכולוגיות, וזאת לצד חלחול תוצרים של מו"פ טכנולוגי צבאי וטכנולוגיות דו-שימושיות (יישומים אזרחיים וצבאיים) כמו רחפנים או גילוי חומרי נפץ. תוכניות מחקר ופיתוח הופכות לנגישות דרך שווקים מסחריים או זליגה של קוד פתוח (עבודת מודיעין דרך OPINT).

בנוסף, קבוצות יכולות לקבל תמיכה ממדינות יריבות, ומקבלות גישה לפיתוחי מחקר ופיתוח צבאיים (למשל, במהלך מלחמות שליחים [proxy] של המלחמה הקרה). כך היה גם עם מדינות תומכות וממנות טרור ופעולות טרור בחסות המדינה (כדוגמת לוב תחת שלטונו של קדאפי, סוריה תחת שלטונו של אסד ועיראק תחת שלטונו של חוסיין). ארגונים קיבלו (בתקופת המלחמה הקרה על ידי שת"פ צבאי הדוק, וסביר להניח שגם היום) פיתוחים צבאיים מתקדמים של רוסיה, צפון קוריאה, קובה וסין.

קבוצות גרילה, שלעיתים קרובות נלחמות למען מטרות פוליטיות ואידאולוגיות, שונות מקבוצות טרור בהיקף ובמטרות – גרילה פועלת בדרך כלל נגד כוחות צבאיים, בעוד שגורמי טרור מתמקדים באזרחים לצורך פרסום וזריעת פחד – אך שניהם מנצלים אסימטריה במחקר ופיתוח. הבחנה זו היא גמישה, כפי שניתן לראות בוויכוחים על התיוג שבו מדינות מסווגות יריבים באופן משתנה מסיבות פוליטיות.[1]

2.2 דוגמאות לזליגה של פיתוחים צבאיים

כלי נשק חם ונשק קל איקוניים כמו ה-AK-47 (מחקר ופיתוח סובייטי משנות ה-40) יוצרו בהמוניהם, הועתקו והופצו ברחבי העולם. קבוצות גרילה בווייטנאם, באפגניסטן ובאמריקה הלטינית (למשל FARC בקולומביה) השתמשו בהם במשך עשרות שנים בשל אמינותם. ארגוני טרור במזרח התיכון אימצו באופן דומה מגוון גרסאות באמצעות רשתות הברחה.

1 G. Petrakis. 1978. "Problem of Definition - Guerrilla, Terrorist, Political, Transnational." *Detective* 6 (4): 11–18. https://www.ojp.gov/ncjrs/virtual-library/abstracts/problem-definition-guerrilla-terrorist-political-transnational. Also in Berger Hobson, Ronit, and Assaf Moghadam. 2023. "Terrorism, Guerrilla, and the Labeling of Militant Groups." *Terrorism and Political Violence* 36 (4): 567–84. https://www.tandfonline.com/doi/full/10.1080/09546553.2023.2183052.

חומרי נפץ ומטענים מאולתרים וחומרי נפץ ברמה צבאית ממחקר ופיתוח בתחום התחמושת (למשל פיתוחים אמריקאיים במלחמת העולם השנייה וסכסוכים אחריה) נוצלו מחדש על ידי מורדים סביב העולם. בעיראק ובאפגניסטן, קבוצות כמו אל-קאעידה והטליבאן אלתרו מטעני נפץ (IEDs) מתחמושת שלא התפוצצה או מדשן מסחרי, תוך התאמתו, כדי לייצר מוקשי נ"א. תופעה זו משקפת טקטיקות גרילה המדגישות אימוץ של כלי נשק בעלות נמוכה לצרכים צבאיים מתקדמים.[2]

סיכונים עתידיים כוללים טרוריסטים שמתאימים תכונות מתקדמות כמו נחילי רחפנים או מיקוד באמצעות בינה מלאכותית.

רחפנים ומערכות בלתי מאוישות אשר נלקחו במקור ממו"פ צבאי אמריקאי (למשל תוכניות DARPA בשנות ה-90 והלאה) זלגו לגורמי טרור. רחפנים מסחריים הפכו לקטלניים על ידי קבוצות כמו דאעש למטרות סיור והפצצה בסוריה ובעיראק. סיכונים עתידיים כוללים טרוריסטים שמתאימים תכונות מתקדמות כמו נחילי רחפנים או מיקוד באמצעות בינה מלאכותית. דיווחים מאזורי סכסוך מציינים קבוצות שרוכשות רחפנים ברמה צבאית באמצעות הברחות.[3]

כלי סייבר ולוחמה אלקטרונית ממו"פ מדינתי, כגון תוכנות פריצה או משבשי אותות, שימשו קבוצות לתעמולה, לשיבוש ולאיסוף מודיעין. לדוגמה, חיזבאללה בלבנון השתמש בלוחמה אלקטרונית בהשפעת טכנולוגיה צבאית איראנית, כולל שיבוש רחפנים ישראליים.[4] חיזבאללה טען והדגים הצלחות בהפלת מל"טי מעקב ישראליים, כגון דגמי הרמס 450, הרמס 900 וסקיילרק, באמצעות שימוש בטילי קרקע-אוויר (SAM). הטכנולוגיה ליירוטים אלה מסתמכת על כלי הגנה אווירית מתוחכמים שנרכשו ועובדו ממקורות זרים כמו איראן וסוריה, הדורשים שילוב משמעותי של מו"פ לשימוש יעיל נגד רחפנים ישראליים מתקדמים. פעילי חיזבאללה גם פירקו רחפנים שנתפסו כדי לבצע הנדסה חוזרת של רכיביהם, ובכך שיפרו את יכולותיהם באמצעות תהליכי מו"פ צבאיים.[5] מתקפות סייבר של קבוצות כמו אנונימוס או האקרים הנתמכים על ידי המדינה מראות כיצד שיטות שנחשפו מתפשטות.[6]

טכנולוגיות מעקב מתקדם ובינה מלאכותית עלולות להגיע לידי ארגוני טרור וגרילה דרך שת"פ צבאי וייצוא. מוצרי מו"פ צבאי ישראלי בתחום מערכות מבוססות בינה מלאכותית, שנוסו בלחימה, יוצאו ברחבי העולם ואומצו לעיתים על ידי גורמים לא-מדינתיים באמצעות הדלפות או הנדסה לאחור (reverse engineering). קבוצות גרילה משתמשות בעיבודים מסחריים של חיישנים ביולוגיים (biosensors) צבאיים או בטכנולוגיות חיזוי (predictive tech) לצורך פריצות.[7]

---

2 Richard J. Hughbank. 2009. "Guerilla W Guerilla Warfare & Law Enfor e & Law Enforcement: Combating the 21st Centur Cement: Combating the 21st Century Terrorist Cell within the U.S. ." *Journal of Strategic Security* 2 (4): 39–52. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1066&context=jss.

3 Thomas G. Pledger. 2021. "The Role of Drones in Future Terrorist Attacks." *The Association of the United States Army* 137 (Land Warfare Paper). https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf.

4 Maya Gebeily, and Laila Bassam. 2024. "How Hezbollah Used Pagers and Couriers to Counter Israel's High Tech Surveillance." *Reuters*, June 9, 2024. https://www.reuters.com/world/middle-east/pagers-drones-how-hezbollah-aims-counter-israels-high-tech-surveillance-2024-07-09.

5 FDD. 24AD. "Hezbollah Shoots Down Israeli Drone With Surface-to-Air Missiles." FDD Foundation for Defense of Democracies. February 26, 24AD. https://www.fdd.org/analysis/2024/02/26/hezbollah-shoots-down-israeli-drone-with-surface-to-air-missiles.

6 Terry Gross. 2021. "U.S. Cyber Weapons Were Leaked — And Are Now Being Used Against Us, Reporter Says." Nrp. February 10, 2021. https://www.npr.org/2021/02/10/966254916/u-s-cyber-weapons-were-leaked-and-are-now-being-used-against-us-reporter-says.

7 @grimeywun in X. 2025. "AI Tools Deployed on Palestinians." X. X. https://x.com/grimeywun/status/1968027043590967613?referrer=grok-com.

גם התחום הלא-קונבנציונלי לא נפקד. האם אפשרית גישה לכלים ביולוגיים וכימיים על ידי ארגונים אסימטריים? מחקר ופיתוח היסטוריים בתחום הנשק הביולוגי (למשל, תוכניות אמריקאיות באמצע המאה ה-20) היוו השראה לשימוש מוגבל על ידי טרוריסטים, כמו מתקפת הסארין של אום שינריקיו ביפן בשנת 1995, תוך שאיבת ידע שאינו סודי. חשש עולה גם מעריכה של גנים או שימוש לרעה בחיישנים מבוססי נגיפים ממעבדות צבאיות.[8]

2.3 סיכום ביניים

קבוצות טרור שילבו טקטיקות גרילה עם טכנולוגיות שמקורן במחקר ופיתוח צבאי כדי להתמודד עם כוחות יריבים עדיפים. זה, בתורו, הוביל למחקר ופיתוח נגדי, כמו מאמצי ארה"ב בהגנה מפני רחפנים או חיזוי התנהגותי (behavioral prediction). עם זאת, התפשטות נשק וטכנולוגיות צבאיות מעלה סוגיות אתיות, שכן טכנולוגיות המיועדות להגנה יכולות להזין מעגלי אלימות.

קיימות תאוריות קונספירציה הטוענות שסוכנויות כמו ה-CIA מפתחות במכוון כלים שמגיעים לידי יריבים מסיבות גאופוליטיות, אם כי אלה חסרות בסיס מלבד תוכניות של הסוכנות שמעליהן הוסר צו איסור פרסום וסיווג, כמו הניסויים ההתנהגותיים של MKUltra.[9] בסך הכול, בעוד שמחקר ופיתוח צבאי מספק יתרונות אסטרטגיים למדינות, התפשטותו הלא-מכוונת מדגישה את האתגרים של בקרת נשק בעולם הגלובלי.

3 לוחמת סייבר על ידי ארגוני טרור

ארגוני טרור וגרילה משלבים באופן גובר לוחמת סייבר בתפיסת הלחימה האסימטרית שלהם תוך מינוף כלים דיגיטליים כדי להגביר את השפעתם, וזאת תוך מזעור סיכונים פיזיים ישירים ועלויות במשאבים וכוח אדם. גישה זו מאפשרת לגורמים לא-מדינתיים לפגוע במדינות, בתשתיות ובאוכלוסיות ברחבי העולם, לעיתים קרובות בהקשרים היברידיים של לוחמה המשלבים פעולות מקוונות עם טקטיקות מסורתיות של פעולות קינטיות במסגרת מאבקי התקוממות וטרור.

3.1 שיטות עיקריות בלוחמת סייבר על ידי ארגוני טרור

קבוצות טרור משתמשות במדיה חברתית, באתרי אינטרנט ובפורומים מקוונים לקמפיינים של תעמולה והפצת מידע שקרי כדי להנחיל אידאולוגיות קיצוניות, להפיץ חדשות כזב ולבצע פעולות פסיכולוגיות שמטרתן להקצין אנשים, לזרוע פחד ולערער את אמון הציבור בגופי ממשל. לדוגמה, ארגונים קיצוניים אלימים מנצלים מערכות כמו רשת X ויוטיוב כדי להגיע לקהלי יעד רחבים במטרה להפיץ מסרים המציגים את פעולותיהם כמוצדקות.[10] שיטה זו יעילה במיוחד עבור תנועות טרור וגרילה בסכסוכים מתמשכים, שבהם נרטיבים מקוונים יכולים לגייס תמיכה ולגרום לדמורליזציה של יריביהם.

8 Chemla Y., Levin I., Fan Y., Johnson A.A., Coley W.C., and Voigt C.A. 2024. "Hyperspectral Reporters for Long-Distance and Wide-Area Detection of Gene Expression in Living Bacteria." *Nature Biotechnology*, August.

9 Robert Brown Asprey. 2025. "Guerrilla Warfare." Britannica, August. https://www.britannica.com/topic/guerrilla-warfare. Also in L'America in X. 2025. "U.S. Government Mind Control & Behavioral Experiments (1920s–1970s)." *X*. X. https://x.com/MFTXAC/status/1967745798692643204?referrer=grok-com.

10 Norwich University. n.d. "Information Warfare and Terrorism: How Extremist Organizations Exploit Modern Platforms." Accessed September 8, 2025. https://online.norwich.edu/online/about/resource-library/info-warfare-terrorism.

כלי סייבר מאפשרים פנייה ישירה לקהילה תומכת ולמגויסים פוטנציאליים באמצעות חדרי צ׳אט, יישומים מוצפנים ותוכן מקוון ממוקד. קבוצות טרור מפרסמות חומרי גיוס, כולל מדריכי פעולה והדרכה ומפיצות קריאות לפעולה, כדי למשוך ולהדריך תומכים. לעיתים קרובות הקבוצות מתמקדות במגזרים דמוגרפיים פגיעים כמו צעירים,[11] מובטלים, חסרי בית ופושעים. ארגוני גרילה משתמשים באופן דומה בשיטות אלו כדי לבנות רשתות פעילים ולתאם את פעולתם.

יכולות סייבר מאפשרות איסוף מודיעין וכריית נתונים ממקורות פתוחים. מידע בקוד פתוח מהאינטרנט, כגון מאגרי מידע ציבוריים, אתרי חדשות ומדיה חברתית, נאסף כדי לזהות מטרות, פגיעויות ומודיעין מבצעי. איסוף זה כולל סיור בתשתיות קריטיות כמו תחנות כוח או מערכות תחבורה ללא סיור פיזי בהן, לדוגמה שימוש בשירותי מפות גוגל הכוללים תמונות עדכניות של כמעט כל מקום בעולם.[12]

מערכות מקוונות מאפשרות העברת תרומות, גיוס כספים ורכישת משאבים באמצעות אתרי אינטרנט, מטבעות מבוזרים (קריפטו) או רשתות ארגוני צדקה, ואלה מאפשרים לארגוני טרור וגרילה לקיים את פעילותם. ארגונים מסוימים מספקים פרטי בנק או משתמשים בחדרי צ׳אט כדי לגייס כספים מתומכים ברחבי העולם. כמו כן, תרומות באמצעות אינטרנט מאפשרות לתורמים להישאר עלומים.[13]

תקשורת מוצפנת ומבנים רשתיים מקוונים מבוזרים (לצורכי גיוס תומכים, גיוס כספים, תעמולה וכו׳) מסייעים בשמירה על קשרים רופפים בין תאי טרור פעילים ומאפשרים תכנון ושיתוף פעולה בזמן אמת מעבר לגבולות מדינתיים. תיאום זה קריטי ללוחמת גרילה, שבה יחידות מפוזרות צריכות לסנכרן התקפות או לשתף שיטות לחימה.[14]

קבוצות טרור וארגוני גרילה מבצעים התקפות סייבר ישירות ופעולות שיבוש כמו פריצה למערכות ממשלתיות, שיגור התקפות מבוזרות של מניעת שירות (DDoS), או מיקוד בתשתיות קריטיות כמו בתי חולים, רשתות חשמל ורשתות פיננסיות (בכלל אלה קרנות פנסיה) כדי לגרום נזק כלכלי ולהטיל פחד ואימה. גופי טרור בחסות מדינה או שליחים (proxy), כמו אלו המקושרים לאיראן, החריפו שיטות כאלה ליצירת מתיחות גאופוליטית.[15] כוחות גרילה הפעילים באזורי מלחמה, כמו בסוריה או אוקראינה, משלבים בפעילותם לוחמה אלקטרונית כדי לשבש את תקשורת האויב המדיני ולתמוך בפעילותם הקרקעית.[16]

אתרי אינטרנט ופורומים של רשת אפלה (dark net) מאפשרים לשתף ידע מבצעי באופן חסוי, מארחים מדריכים המלמדים על טקטיקות, החל מבניית מטעני חבלה מאולתרים ועד לביצוע פעולות סייבר, המאפשרים העברת ידע בין שלוחות של הארגון ותאיו. אפשרות זו הופכת את המומחיות לפתוחה וחופשית עבור גורמי טרור וגרילה.[17]

---

11 Gabriel Weimann. 2024. "How Modern Terrorism Uses the Internet." http://usip.org/sites/default/files/sr116.pdf.

12 Andre Slonopas. 2024. "What Is Cyber Warfare? Various Strategies for Preventing It." American Public University. April 16, 2024. https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-cyber-warfare. Also in Gabriel Weimann. 2024. "How Modern Terrorism Uses the Internet." http://usip.org/sites/default/files/sr116.pdf.

13 Gabriel Weimann. 2024. "How Modern Terrorism Uses the Internet." http://usip.org/sites/default/files/sr116.pdf.

14 Cleveresq in X. 2024. "Hybrid Warfare Is a Good Description of What Russia Is Doing, Has Done, and Continues to Do." *X*. X. https://x.com/cleveresq/status/1788173986079113600?referrer=grok-com. Also in Gabriel Weimann. 2024. "How Modern Terrorism Uses the Internet." http://usip.org/sites/default/files/sr116.pdf.

15 Andre Slonopas. 2024. "What Is Cyber Warfare? Various Strategies for Preventing It." American Public University. April 16, 2024. https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-cyber-warfare.

16 InfoSiftWeekly in X. 2024. "Cyber Attacks - HIGH Threat Level." *X*. X. https://x.com/InfoSiftWeekly/status/1865724584437108759?referrer=grok-com.

17 Gabriel Weimann. 2024. "How Modern Terrorism Uses the Internet." http://usip.org/sites/default/files/sr116.pdf.

שיטות אלו הן לעיתים קרובות חלק מתפיסת לוחמה משולבת רחבה יותר, שבה אלמנטים בסייבר משלימים פעולות פיזיות.[18] קבוצות כמו דאעש, אל-קאעידה, חמאס ופלגי מורדים שונים בסכסוכים (למשל בסוריה או נגד אינטרסים מערביים) מדגימות התפתחות זו, תוך הסתגלות לסביבה הדיגיטלית במטרה להשיג הישגים רחבים יותר.[19] עם זאת, צעדי נגד מצד הממשלות, כולל ניטור משופר ושיתוף פעולה בינלאומי, ממשיכים לאתגר מאמצים אלה.[20]

כלי בינה מלאכותית מאפשרים יצירה מהירה של תעמולה ומידע שקרי [...] הקבוצות משתמשות בבינה מלאכותית לגיוס ממוקד והקצנה.

4 שימוש בבינה מלאכותית על ידי ארגוני טרור

קבוצות טרור וגרילה משלבות בינה מלאכותית (AI) באסטרטגיה שלהן ללוחמה פסיכולוגית, הכוללת מניפולציה של תפיסות, רגשות והתנהגויות כדי לערער יריבים, לגייס תומכים או להפיץ פחד. שימוש זה מתמקד לעיתים קרובות בהגברת מאמצי תעמולה, הפצת מידע שקרי וגיוס בקנה מידה גדול, אם כי ראוי לציין שחלק ניכר מהפעילות המתועדת נותר ניסיוני או אקראי ולא מתוחכם יתר על המידה. להלן נפרט דרכים מרכזיות שבהן הדבר נצפה או נותח, תוך הסתמכות על דיווחים על קבוצות כמו דאעש, חיזבאללה ורשתות קיצוניות שונות אחרות.

4.1 שימוש בבינה מלאכותית ללוחמה פסיכולוגית

כלי בינה מלאכותית, בייחוד אלה המבוססים על מודלים של שפת תכנות גדולה (LLMs) או מחוללי תמונות/וידאו, מאפשרים יצירה מהירה של תעמולה ומידע שקרי, זאת גם באמצעות תוכן מותאם אישית שנועד לעורר תגובות רגשיות חזקות כמו פחד, כעס או סולידריות.[21]

הקבוצות משתמשות בבינה מלאכותית כדי לייצר כזב עמוק (deepfakes), סרטונים ומאמרים ריאליסטיים המתארים זוועות מפוברקות, מהללים לוחמים או עושים דמוניזציה של האויב. לדוגמה, תמונות שנוצרו על ידי בינה מלאכותית של פשעי מלחמה לכאורה יכולות להיות מופצות ברשתות החברתיות כדי לעורר זעם או להעלות את המורל בקרב אוהדים. כלי זה מגביר את התעמולה ביעילות ניכרת.

במקום עריכה ידנית, בינה מלאכותית הופכת את התהליך לאוטומטי, ומאפשרת תוכן רב-לשוני המכוון לקבוצות דמוגרפיות ספציפיות, כגון נוער פגיע באזורי סכסוך, מדינות עולם שלישי, אזורי סיכון וכדומה. המטרה היא לכרסם באמון במקורות רשמיים, ליצור בלבול ולקטב את דעת הקהל.[22]

---

18 Kyle.Moon in X. 2025. "I Have a Feeling This Is the Beginning of Hybrid Warfare by USA on Mexico. Analogous to Russo-Georgian Conflict 2008-2009." X. X. https://x.com/GanseKyle/status/1892951048807141778?referrer=grok-com. Also in Cleveresq in X. 2024. "Hybrid Warfare Is a Good Description of What Russia Is Doing, Has Done, and Continues to Do." *X*. X. https://x.com/cleveresq/status/1788173986079113600?referrer=grok-com.

19 Gabriel Weimann. 2024. "How Modern Terrorism Uses the Internet." http://usip.org/sites/default/files/sr116.pdf.

20 OSCE. n.d. "Countering the Use of the Internet for Terrorist Purposes." Organization for Security and Cooperation in Europe. Accessed September 8, 2025. https://www.osce.org/secretariat/107810.

21 LLMs (מודל שפה גדול) הוא סט משנה של למידת מכונה המכונה "למידה עמוקה" המשתמשת באלגוריתמים הפועלים על סטים גדולים של נתונים כדי לזהות דפוסים מורכבים. ברמת היסוד, הם לומדים להגיב לבקשות המשתמש עם תוכן רלוונטי בהקשר שנכתב בשפה האנושית – סוג המילים והתחביר שאנשים משתמשים בהם במהלך שיחה רגילה. המילים אחרות, LLMs היא קטגוריית משנה מתקדמת של בינה מלאכותית שמתמקדת בהבנה, חיזוי ויצירת טקסט דמוי אדם. LLMs הוא רכיב קריטי ביכולת בינה מלאכותית, מה שהופך אותם לכלים רבי עוצמה למגוון משימות עיבוד שפה טבעית כגון חיפוש, תרגום וסיכום טקסט, מענה לשאלות, יצירת תוכן חדש כולל טקסט, תמונות, מוזיקה וקוד תוכנה. ראו: מהו מודל שפה גדול?, SAP, 2 ביולי 2024.

22 Jim Stewartson, Antifascist in X. 2024. "The Failure to Recognize the Power of Psychological Warfare on Civilians May End up Being *the* Fatal Error." X. X. https://x.com/jimstewartson/status/1846392462266478840?referrer=grok-com.

הקבוצות משתמשות בבינה מלאכותית לגיוס ממוקד והקצנה. אלגוריתמים של בינה מלאכותית עוזרים לזהות וליצור קשר עם מגויסים פוטנציאליים על ידי ניתוח התנהגות מקוונת, אינטראקציות במדיה חברתית ונתונים ציבוריים. הצ'אטבוטים,[23] או מערכות העברת הודעות המונעות על ידי בינה מלאכותית, מדמים שיחות אנושיות כדי לבנות קרבה, לענות על שאלות לגבי אידאולוגיה ולכוון אנשים לעבר דעות קיצוניות. כלים אלה יכולים לפעול 24/7, להתאים תגובות על סמך סנטימנט המשתמש כדי להעמיק את מעורבותו וכך לגייס מספר תומכים ולוחמים גדול מאוד, לעומת תקופות קודמות.[24]

ניתוח הלך רוח (סנטימנטים) המופעל על ידי בינה מלאכותית סורק פורומים, תגובות ופוסטים כדי לאתר אנשים המראים סימני אכזבה או כעס, ולאחר מכן מספק תעמולה מותאמת אישית. ניתוח זה משקף טקטיקות שיווק מסחריות אך משמש כנשק לשכנוע אידאולוגי, מה שמוביל לעיתים קרובות להקצנה מקוונת שגולשת לפעולה בעולם האמיתי (כגון ביצוע פיגועי בודדים).[25]

בפעולות פסיכולוגיות, בינה מלאכותית משפרת את המאמצים להחדיר פחד וטרור ללא אלימות פיזית ישירה, תוך התמקדות בשיבוש דיגיטלי. בוטים אוטומטיים מציפים פלטפורמות חברתיות בקמפיינים מתואמים של מידע שגוי ותעמולתי, כגון דיווחים כוזבים על מתקפות קרבות או טענות מוגזמות על כוח, כדי ליצור פאניקה ולאלץ הסטת משאבים על ידי כוחות הביטחון של השלטונות.[26]

קבוצות מסוימות מתנסות בבינה מלאכותית לצורך ניבוי (predictive modeling) של תגובות ציבוריות, תוך סימולציה של האופן שבו מסרים מסוימים עשויים להתפשט באופן ויראלי כדי למקסם את ההשפעה הפסיכולוגית. התנסות זו כוללת שימוש בבינה מלאכותית לזיוף מסמכים או קטעי שמע הזורעים חוסר אמון בקרב שורות האויב, כולל אוכלוסיות אזרחיות.[27]

4.1.1 אתגרים ומגבלות

בעוד שבינה מלאכותית מציעה יתרונות במהירות ובקנה מידה ניכר, אימוצה על ידי קבוצות אלו מוגבל על ידי הצורך בגישה לטכנולוגיה מתקדמת זו, מומחיות ותשתיות. רבות מהן מסתמכות על כלים זמינים לציבור ולא על מערכות מותאמות אישית. מנגד, אמצעי נגד כמו ניהול תוכן וזיהוי בינה מלאכותית מפותחים על ידי הרשויות כדי להתמודד עם שיטות של שימוש בבינה מלאכותית על ידי קבוצות טרור ו/או פשע מאורגן. דיווחים מצביעים על כך שגורמים מדינתיים ומאמצי לוחמה בטרור מתמקדים יותר ויותר בניטור ושיבוש השימוש בכלים אלה כדי לשמר את הטכנולוגיות בסוג מסוים של שליטה ופיקוח ולמנוע זליגה.[28]

---

23 צ'אטבוט הוא תוכנת מחשב המדמה ומעבדת שיחה אנושית (בכתב או בדיבור), ומאפשרת לבני אדם לקיים אינטראקציה עם מכשירים דיגיטליים כאילו הם מתקשרים עם אדם אמיתי. צ'אטבוטים יכולים להיות פשוטים, כמו תוכניות בסיסיות שעונות על שאילתה פשוטה עם תגובה בשורה אחת, או מתוחכמים, כמו עוזרים דיגיטליים שלומדים ומתפתחים כדי לספק רמות הולכות וגדלות של התאמה אישית בזמן שהם אוספים ומעבדים מידע. ראו: https://www.oracle.com/il/chatbots/what-is-a-chatbot.

24 Lidia Bernd. n.d. "AI-Enabled Deception: The New Arena of Counterterrorism." *Georgetown University*, no. Georgetown Security Studies Review. Accessed September 19, 2025. https://gssr.georgetown.edu/the-forum/topics/technology/ai-enabled-deception-the-new-arena-of-counterterrorism.

25 Maverick News Agency in X. 2025. "The Most Concerning Version Is an 'Untethered' AI Is Doing It through Social Platforms." *X*. X. https://x.com/mavnewsagency/status/1966917963346571693?referrer=grok-com.

26 Austin Coombs. 2024. "Persuade, Change, and Influence with AI: Leveraging Artificial Intelligence in the Information Environment." *Modern War Institute*, October. https://mwi.westpoint.edu/persuade-change-and-influence-with-ai-leveraging-artificial-intelligence-in-the-information-environment.

27 The Chronology in X. 2025. "From CIA, ISI Learnt Many Techniques of Psychological Warfare Which CIA Was Using to Train Mujahedeen." *X*. X. https://x.com/TheChronology__/status/1938559139879563542?referrer=grok-com.

28 Clarisa Nelu. 2024. "Exploitation of Generative AI by Terrorist Groups." International Centre for Counter-Terrorism (ICCT). June 10, 2024. https://icct.nl/publication/exploitation-generative-ai-terrorist-groups. Also in UNICRI and UNCCT. 2021. "Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes." https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

בסך הכול, בינה מלאכותית משמשת כמכפיל כוח ללוחמה פסיכולוגית בכך שהיא מאפשרת פעולות יעילות, ממוקדות ומטעות יותר, אך היא נותרה חלק מארגז כלים רחב יותר הכולל שיטות מסורתיות כמו הפצת עלונים, תעמולה במסגדים (עבור אסלאם רדיקאלי) או שידורים באינטרנט.

תומכי דאעש השתמשו בכלים דוגמת ChatGPT כדי ליצור מהדורות חדשות, והפכו תעמולה כתובה לקטעי אודיו או לשידורים מזויפים על פיגועים באזורים כמו אפריקה והמזרח התיכון.

4.2 טרור ובינה מלאכותית במזרח התיכון

ארגוני טרור וגרילה במזרח התיכון, כולל קבוצות כמו המדינה האסלאמית (דאעש), שלוחות אל-קאעידה, כמו גם חיזבאללה וחמאס, החלו להתנסות בטכנולוגיות בינה מלאכותית (AI). אימוץ זה מונע במידה רבה על ידי הגישה לכלי בינה מלאכותית גנריים כמו ChatGPT המאפשרים לקבוצות אלו לשפר את פעילותן מבלי להזדקק למומחיות טכנית מתקדמת.

בעוד שהשימוש בבינה מלאכותית נותר בשלבים מוקדמים ועדיין אינו שימושי עבור התקפות פיזיות, הוא מקדם ומעצים בעיקר שיטות קיימות כגון הפצת תעמולה וגיוס. דיווחים של מומחים ללוחמה בטרור, מכוני מחקר וכלי תקשורת מצביעים על כך שקבוצות אלו מתאימות בינה מלאכותית כדי להתגבר על מגבלות, ליצור תוכן מולטימדיה דיגיטלי ולחקור יישומים כמו פעולות והתפתחויות סייבר עתידיים. עם זאת, חלק ניכר מהמידע הזמין מגיע ממקורות מערביים ובינלאומיים, אלה אשר עשויים להיות מוטים באשר לאיומים מצד קבוצות אסלאמיות. לעומת זאת מעט מידע קיים באשר לשימוש של גורמים מדינתיים, בייחוד כוחות ביטחון וארגוני מודיעין ממלכתיים, בבינה מלאכותית.[29]

4.2.1 מקרים מדווחים

היישום המתועד ביותר של בינה מלאכותית על ידי ארגונים אלה הוא ב"תעמולה ויצירת תוכן". בינה מלאכותית גנרטיבית מאפשרת הפקה מהירה של טקסט, תמונות, סרטונים ואודיו המחקים מדיה מקצועית, ומסייעים לקבוצות להתחמק מזיהוי אוטומטי בפלטפורמות חברתיות. לדוגמה, תומכי דאעש השתמשו בכלים דוגמת ChatGPT כדי ליצור מהדורות חדשות, והפכו תעמולה כתובה לקטעי אודיו או לשידורים מזויפים על פיגועים באזורים כמו אפריקה והמזרח התיכון.[30]

קבוצות המקושרות לאל-קאעידה פרסמו מדריכים לשימוש בצ'אטבוטים של בינה מלאכותית והכריזו על סדנאות מקוונות להכשרת עוקבים בטכנולוגיות אלה.[31] שימוש זה מאפשר יצירת "תוכן רגשי" שמעודד תומכים, כגון סרטונים שנוצרו על ידי בינה מלאכותית של נשיאי ארה"ב שרים שירי מלחמה של דאעש או תמונות מניפולטיביות המשותפות במרחבים ורשתות קיצוניים.[32]

29 The Soufan Center. 2024. "Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment Efforts." October 3, 2024. https://thesoufancenter.org/intelbrief-2024-october-3.

30 Makuch, ben. 2025. "They're Fighting Dirty. We're Fighting Back." *The Guardian*, 2025. https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence. Also in Cathrin Schaer. 2024. "How Extremist Groups like 'Islamic State' Are Using AI." *DW*, October 7, 2024. https://www.dw.com/en/how-extremist-groups-like-islamic-state-are-using-ai/a-69609398.

31 Cathrin Schaer. 2024. "How Extremist Groups like 'Islamic State' Are Using AI." *DW*, October 7, 2024. https://www.dw.com/en/how-extremist-groups-like-islamic-state-are-using-ai/a-69609398.

32 Gabriel Weimann, Alexander T. Pack, and Et.Al. 2024. "Generating Terror: The Risks of Generative AI Exploitation." *Combating Terrorism Center* 17 (1). https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation.

בינה מלאכותית מנוצלת גם לגיוס והקצנה. על ידי יצירת נרטיבים משכנעים ובעלי השפעה גבוהה, כלים אלה עוזרים להתאים מסרים לקהילות ספציפיות, כולל קמפיינים לגיוס כספים עם ביטויים משכנעים כמו הצגת דאעש כלוחם ב"ממשלות מושחתות ומדכאות".[33] בשנת 2023 הפיץ דאעש מדריך לשימוש מאובטח בבינה מלאכותית גנרטיבית, והדגיש את תפקידה במניעת צנזורה ובהפצת מסרים קיצוניים.[34]

קבוצות טרור יכולות להשתמש בבינה מלאכותית לגיוס באמצעות צ'אטבוטים או לתזמור מתקפות מורכבות, כפי שניתן לראות בתרחישים היפותטיים שבהם בינה מלאכותית משתלבת עם טכנולוגיית רחפנים ל"רובוטים קטלניים" (killer robots).

ראיות מסוימות מצביעות על "שיפורים תפעוליים", כגון שימוש בבינה מלאכותית לפיתוח אתרים, יצירת אפליקציות או תכנון בסיסי. גורמי טרור התנסו במודלים מורחבים של שפות תִכנוּת מתוחכמות (כגון LLMs) כדי ליצור הוראות לפעילויות כמו קמפיינים של דיסאינפורמציה או גיוס כספים, לעיתים קרובות באמצעות הנחיות עקיפות כדי לעקוף את אמצעי ההגנה של בינה מלאכותית.[35] קבוצות אזוריות, כולל אלו המזוהות עם ארגונים קיצוניים אלימים, שיתפו למעלה מ-5,000 פריטי תוכן שנוצרו על ידי בינה מלאכותית במרחבים מקוונים, בעיקר לא לצורך התקפות ישירות אלא כדי להגביר תעמולה.[36]

ארגוני גרילה, כמו אלה שבסוריה או בתימן (למשל החות'ים), הראו אימוץ מועט של שימוש בבינה מלאכותית, אך מגמות אזוריות רחבות יותר מצביעות על ניסויים דומים בלוחמה אסימטרית, כמו שילוב של בינה מלאכותית עם רחפנים לצורך מיקוד – אם כי זה נותר ספקולטיבי ואינו מבוסס באופן נרחב על מקורות פתוחים.[37]

4.2.2 סיכונים פוטנציאליים והשלכות עתידיות

בינה מלאכותית עלולה לאפשר איומים מתוחכמים יותר, כולל מתקפות סייבר, כלי נשק אוטונומיים או תכנון משופר לצורכי הונאה, גיוס, תעמולה ומימון. לדוגמה, הם עשויים לסייע בפיתוח תוכנות כופר, מתקפות DDoS או אפילו עיצובים של נשק כימי/ביולוגי, אם כי השימושים הנוכחיים מוגבלים להרחבה ולמחקר ופיתוח, על ידי ארגוני טרור עם גישה מוגבלת ליכולות חדשות.[38]

33 Gabriel Weimann, Alexander T. Pack, and Et.Al. 2024. "Generating Terror: The Risks of Generative AI Exploitation." *Combating Terrorism Center* 17 (1). https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation. Also in Lidia Bernd. 2024. "AI-Enabled Deception: The New Arena of Counterterrorism." *Georgetown Security Studies Review*, no. Cyber&Artificial Intelligence, Terrorism&Transnational Threats (May). https://georgetownsecuritystudiesreview.org/2024/05/03/ai-enabled-deception-the-new-arena-of-counterterrorism.

34 INTELBRIEF. 2024. "Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment Efforts." October 3, 2024. https://thesoufancenter.org/intelbrief-2024-october-3.

35 Gabriel Weimann, Alexander T. Pack, and Et.Al. 2024. "Generating Terror: The Risks of Generative AI Exploitation." *Combating Terrorism Center* 17 (1). https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation.

36 Tech Against Terrorism. n.d. "Terrorist Use of Generative AI ." Tech Against Terrorism. Accessed September 1, 2025. https://techagainstterrorism.org/gen-ai.

37 Jacob Ware. 2019. "Terrorist Groups, Artificial Intelligence, and Killer Drones." War On The Rocks. September 24, 2019. https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones. Also in Vision of Humanity. 2023. Preventing Terrorists from Using Emerging Technologies." *Vision of Humanity*, September. https://www.visionofhumanity.org/preventing-terrorists-from-using-emerging-technologies.

38 Clarisa Nelu. 2024. "Exploitation of Generative AI by Terrorist Groups." International Centre for Counter-Terrorism (ICCT). June 10, 2024. https://icct.nl/publication/exploitation-generative-ai-terrorist-groups. Also in UNICRI and UNCCT. 2021. "Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes." https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

קבוצות טרור יכולות להשתמש בבינה מלאכותית לגיוס באמצעות צ'אטבוטים או לתזמור מתקפות מורכבות, כפי שניתן לראות בתרחישים היפותטיים שבהם בינה מלאכותית משתלבת עם טכנולוגיית רחפנים ל"רובוטים קטלניים" (killer robots).[39] דוחות האו"ם מדגישים את "השימוש הזדוני" בבינה מלאכותית למטרות טרור, תוך הדגשת הסיכונים במזרח התיכון, שם לקבוצות כמו דאעש יש היסטוריה של אימוץ טכנולוגיות מתפתחות ומתקדמות.[40]

עם זאת, חלק מהניתוחים ממעיטים בחשיבות הסכנות המיידיות, ומציינים כי בינה מלאכותית משלימה ואינה מחוללת מהפכה באיומים, כאשר מתקפות ב"עולם האמיתי", לצורך תעמולה וגיוס, עדיין מסתמכות על גורמים גאופוליטיים, דוגמת הסכסוך בעזה.[41] כלי תקשורת של בעלי עניין כמו המכון לדיאלוג אסטרטגי (ISD) ומרכז המאבק בטרור (CTC) מדגישים כי הפגיעויות נובעות יותר מירידה בחוסן כנגד קיצוניות מקוונת, מאשר מהבינה המלאכותית עצמה.[42]

4.2.3 אמצעי נגד והקשר רחב יותר

מאמצים בינלאומיים, כולל התמקדות ברית נאט"ו בטכנולוגיה ללוחמה בטרור ויוזמות של האו"ם, שואפים לרסן סיכונים אלה באמצעות שיתוף מודיעין, הכשרה ותגובות מדיניות.[43] פלטפורמות טכנולוגיה מתבקשות לשפר את ניהול התוכן שלהן באמצעות בינה מלאכותית (אבטחת סייבר מבוססת בינה מלאכותית), כגון זיהוי סמנטי (semantic detection), כדי להתמודד עם שיטות התחמקות.[44] דיווחים ממקורות מגוונים, כולל מכוני מחקר אמריקאים וכלי תקשורת אירופאים, מספקים ריכוז של חוות דעת ונקודות מבט, אם כי לעיתים קרובות הם נותנים עדיפות לאיומים מצד גורמים לא-מדינתיים על פני שימושים מדינתיים בבינה מלאכותית.[45]

לסיכום, בעוד שבינה מלאכותית מעצימה וממריצה קבוצות טרור וגרילה במזרח התיכון להרחיב פעולות דיגיטליות, השפעתה כיום אבולוציונית ולא מהפכנית, ומתמקדת בלוחמת מידע. ניטור מתמשך מצד גופים גלובליים חיוני להתמודדות עם סיכונים הולכים וגדלים.

---

39 Jacob Ware. 2019. "Terrorist Groups, Artificial Intelligence, and Killer Drones." War On The Rocks. September 24, 2019. https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones. Also in Anthony C. Pfaf. 2025. "The Weaponization of Artificial Intelligence the Next Stage of Terrorism and Warfare." Ankara. https://www.tmmm.tsk.tr/publication/researches/21-TheWeaponizationofAI-TheNextStageofTerrorismandWarfare.pdf.

40 UNICRI and UNCCT. 2021. "Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes." https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

41 Cathrin Schaer. 2024. "How Extremist Groups like 'Islamic State' Are Using AI." *DW*, October 7, 2024. https://www.dw.com/en/how-extremist-groups-like-islamic-state-are-using-ai/a-69609398. Also in David Wells. 2024. "The Next Paradigm-Shattering Threat? Right-Sizing the Potential Impacts of Generative AI on Terrorism." Middle East Institute. March 18, 2024. https://mei.edu/publications/next-paradigm-shattering-threat-right-sizing-potential-impacts-generative-ai-terrorism.

42 Makuch, ben. 2025. "How Terrorist Groups Are Leveraging AI to Recruit and Finance Their Operations." The Guardian, June 8, 2025. https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence. Also in Gabriel Weimann, Alexander T. Pack, and Et.Al. 2024. "Generating Terror: The Risks of Generative AI Exploitation." *Combating Terrorism Center* 17 (1). https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation.

43 NATO. 2025. "Countering Terrorism." Nato.Int. August 6, 2025. https://www.nato.int/cps/en/natohq/topics_77646.htm.

44 Tech Against Terrorism. n.d. "Terrorist Use of Generative AI." Tech Against Terrorism. Accessed September 1, 2025. https://techagainstterrorism.org/gen-ai.

45 Susan Sim, Eric Hartunian, and Paul J. Milas. 2024. "Emerging Technologies and Terrorism: An American Perspective." *Strategic Studies Institute* USAWC Press (April). https://press.armywarcollege.edu/monographs/967. Also in Asha Hemrajani. 2024. "The Use of AI in Terrorism." *RSIS*, no. 124 (August). https://rsis.edu.sg/wp-content/uploads/2024/08/CO24124.pdf.

4.3 קרטלי סמים באמריקה הלטינית ובינה מלאכותית

קרטלים משתמשים בניתוחים מבוססי בינה מלאכותית כדי לזהות דפוסים בנתונים פיננסיים, מה שמאפשר להם להלבין כספים באמצעות מטבעות מבוזרים

קרטלי סמים מקסיקניים, ובייחוד קרטל הדור החדש של חליסקו (CJNG) וקרטל סינלואה, מאמצים יותר ויותר בינה מלאכותית (AI) כדי לשפר את פעילותם הפלילית. להלן סקירה המבוססת על מידע זמין:

4.3.1 הונאה פיננסית ופשעי סייבר

קרטלים כמו CJNG משתמשים בבינה מלאכותית לקמפיינים מתוחכמים של הונאה, כולל מודלים של שפת תכנות גדולה (LLMs), כדי לבצע הונאה פיננסית מתקדמת יותר. שימוש זה כולל יצירת מיילים משכנעים של דיוג (Phishing), התחזות עמוקה ותוכניות הונאה אוטומטיות המחקות תקשורת לגיטימית כדי להונות קורבנות (דוגמת פלטפורמות מסחר בבורסה לא-אמיתיות המחקות מסחר אמיתי). בינה מלאכותית עוזרת לקרטלים ליצור הודעות מותאמות אישית כדי להערים על אנשים לשתף מידע, למסור מידע אישי כולל סיסמאות, או אישורים רגישים.[46]

בינה מלאכותית משמשת גם כדי לטשטש את מקורותיהם של כספים לא-חוקיים ומסייעת בהלבנת הון בממדים גדולים. קרטלים משתמשים בניתוחים מבוססי בינה מלאכותית כדי לזהות דפוסים בנתונים פיננסיים, מה שמאפשר להם להלבין כספים באמצעות מטבעות מבוזרים, או רשתות מורכבות של חברות קש. שימוש זה מאפשר להם להתחמק מגילוי על ידי הרשויות.[47]

4.3.2 סחר באנשים וגיוס

על פי הדיווחים, קרטל ה-CJNG משתמש בבינה מלאכותית כדי להרחיב את פעולות הסחר בבני אדם, ולפתות אנשים לפעילויות בלתי חוקיות במסווה של הצעות עבודה לגיטימיות. כלי בינה מלאכותית מסייעים באוטומציה של תהליכי גיוס, כולל על ידי כפייה והונאה, תוך מיקוד באוכלוסיות פגיעות באמצעות פלטפורמות מדיה חברתית.[48]

קרטלים מנצלים מדיה חברתית וממנפים זיהוי פנים וניתוח נתונים מבוססי בינה מלאכותית כדי לזהות ולגייס סוחרי סמים ללא ידיעתם באמצעות פלטפורמות כמו פייסבוק. לדוגמה, חקירה פדרלית השתמשה בזיהוי פנים מבוסס בינה מלאכותית כדי לזהות מגייס לאחר שלא היה פעיל במשך שנה, והדגימה כיצד קרטלים מנצלים פלטפורמות אלו לגיוס.[49]

4.3.3 לוחמה ומעקב באמצעות רחפנים

46 AI incident database. n.d. "Incident 725: Cartels Reportedly Using AI to Expand Operations into Financial Fraud and Human Trafficking." Accessed August 31, 2025. https://incidentdatabase.ai/cite/725.

47 AP news. 2022. "Mexican Cartels Turn to Bitcoin, Internet, e-Commerce." March 10, 2022. https://apnews.com/article/business-caribbean-mexico-crime-drug-cartels-1bb5ebf84fbf71baf6a845648bad4990. Also in Robert Muggah, and Misha Glenny. 2025. "The Coming Golden Age of Crime." FP. February 17, 2025. https://foreignpolicy.com/2025/02/17/drug-cartels-organized-crime-mafia-cybercrime-money-laundering-corruption-smuggling.

48 AI incident database. n.d. "Incident 725: Cartels Reportedly Using AI to Expand Operations into Financial Fraud and Human Trafficking." Accessed August 31, 2025. https://incidentdatabase.ai/cite/725.

49 Clearview AI. n.d. "Uncovering Members of an International Drug Smuggling Network." Clearview AI. Accessed August 31, 2025. https://www.clearview.ai/success-stories/uncovering-members-of-an-international-drug-smuggling-network.

קרטל ה-CJNG היה החלוץ בשימוש ברחפנים חמושים מבוססי בינה מלאכותית הן למעקב והן לתקיפות. רחפנים אלה, המצוידים בחיישנים ובמצלמות, משמשים לניטור קרטלים יריבים, למעקב אחר משלוחי סמים ואף להעברת חומרי נפץ וכלי נשק בסכסוכים כמו במיצ'ואקאן.[50] בסכסוך זה ציידו הכנופיות רחפנים בחומרי נפץ מסוג C4 ובכדורי מתכת, מה שהפך אותם ל"מטעני חבלה מעופפים".[51]

קרטלי סמים אחדים במקסיקו מחזיקים במעבדות פנטניל – סם סינטטי המיוצר במדינות מסוימות כחלופה וכאמצעי ריפוי בתוכניות גמילה. רשויות ארה"ב, תחת ממשל טראמפ, פרסו רחפנים מבוססי בינה מלאכותית של ה-CIA כדי לרגל אחר מעבדות פנטניל של הקרטלים במקסיקו, לזהות פליטות כימיות ולנטר פעילות מעבדות בזמן אמת. מעבר להיבט הסיכולי, יש לקחת בחשבון את האפשרות שקרטלים עשויים להשתמש בטכנולוגיית רחפנים דומה המונעת על ידי בינה מלאכותית כדי להגן על פעילותם.[52]

4.3.4 סחר בסמים ולוגיסטיקה בסיוע בינה מלאכותית

אנליטיקה חזויה (predictive analytics) ולמידת מכונה (machine learning) מהווים חידוש משמעותי וכלים ביישום בינה מלאכותית לניתוח מערכי נתונים עצומים, כגון רישומי משלוח, כדי לייעל נתיבי הברחה ולהתחמק מאכיפת החוק. לדוגמה, קרטלים משתמשים בבינה מלאכותית כדי לזהות דפוסים חשודים בסחר העולמי, כגון משלוחי כימיקלים מסין למקסיקו, כדי לייעל את ייצור הסמים הסינטטיים פנטניל ומתאמפטמין.[53]

כמו כן, בינה מלאכותית תומכת ומסייעת בפיתוח שיטות הברחה חדשות ומתוחכמות, כגון אופטימיזציה של חפירת רשתות מנהרות או תיאום משלוחי סמים על ידי רחפנים מעבר לגבול ארה"ב-מקסיקו.[54]

4.3.5 אתגרים ואמצעי נגד

סוכנויות אמריקאיות כמו ה-DEA ומשרד האוצר מתמודדים עם השימוש בבינה מלאכותית על ידי קרטלים באמצעות כלים משלהן המונעים גם על ידי הבינה המלאכותית, כגון אנליטיקה גאו-מרחבית (geospatial analytics), כדי למפות רשתות סחר ולחזות תנועות קרטלים.[55] כדי להילחם ברחפנים של קרטלי סמים הרשויות בוחנות ומפתחות טכנולוגיות נגד רחפנים, אמצעי נגד המבוססים על בינה מלאכותית כמו משבשי תדר רדיו ומערכות גילוי רחפנים.[56]

---

50 Wikipedia, The Free Encyclopedia. n.d. "Operation Michoacán." Accessed August 31, 2025. https://en.wikipedia.org/wiki/Operation_Michoac%C3%A1n.

51 HOZINT. 2021. "Mexico | The Use of Weaponized Consumer Drones by Drug Cartels." Hozint.Com. October 26, 2021. https://www.hozint.com/2021/10/mexico-the-use-of-weaponized-consumer-drones-by-drug-cartels. Also in Gabriel Mondragón Toledo. 2023. "NarcoDrones Have Become a Growing Scare Tactic in Mexico's Drug Wars." INKSTICK. November 7, 2023. https://inkstickmedia.com/narcodrones-have-become-a-growing-scare-tactic-in-mexicos-drug-wars.

52 Jon Michael Raasch. 2025. "Trump Secretly Sends CIA Drones into Mexico to Spy on Drug Cartel Labs." *Daily Mail*, February 18, 2025. https://www.dailymail.co.uk/news/article-14409511/amp/trump-cia-drones-mexico-spy-drug-cartels.html.

53 3GIMBALS. 2025. "Data-Driven Intelligence for Combating Drug Cartels." 3gimbals.Com. January 30, 2025. https://3gimbals.com/insights/data-driven-intelligence-drug-trafficking.

54 Albert Stepanyan. n.d. "Southern Border: Cartels, Wagner, and Drone Warfare." SCYLLA. Accessed August 31, 2025. https://www.scylla.ai/southern-border-cartels-wagner-and-drone-warfare.

55 3GIMBALS. 2025. "Data-Driven Intelligence for Combating Drug Cartels." 3gimbals.Com. January 30, 2025. https://3gimbals.com/insights/data-driven-intelligence-drug-trafficking.

56 Gabriel Mondragón Toledo. 2023. "NarcoDrones Have Become a Growing Scare Tactic in Mexico's Drug Wars." INKSTICK. November 7, 2023. https://inkstickmedia.com/narcodrones-have-become-a-growing-scare-tactic-in-mexicos-drug-wars.

קיום פערים חקיקתיים מהווה מכשול משמעותי עבור רשויות החוק וכוחות הביטחון המקומיים. מקסיקו מפגרת במידה רבה בחקיקה ספציפית לבינה מלאכותית, מה שמותיר פגיעויות בוויסות השימוש של קרטלים בטכנולוגיות אלו. הברית הלאומית לבינה מלאכותית (ANIA) של מקסיקו שואפת לטפל בכך, אך ההתקדמות בתחום זה איטית מאוד.[57]

בעוד שבינה מלאכותית אינה יוצרת באופן מהותי קטגוריות חדשות של איומים, היא מעצימה קטגוריות קיימות על ידי שיפור היעילות, יכולת ההרחבה וטקטיקות התחמקות.

4.3.6 השלכות עתידיות ומגמות עולמיות

האינטרפול מציין כי קרטל ה-CJNG וקרטלים אחרים הם חלק ממגמה עולמית שבה קבוצות פשע מאורגן ברחבי אירופה, אסיה ואפריקה מאמצות בינה מלאכותית למטרות הונאה, סחר בבני אדם ופשעים אחרים.[58] אחרים מציינים כי קיים גם היבט חברתי-כלכלי. בעוד שקרטלים משתמשים בבינה מלאכותית כדי להרחיב את מרחב הפעולה שלהם, יש הטוענים כי פעילותם מביאה יתרונות כלכליים מקומיים, כגון מקומות עבודה ותשתיות, אם כי אלה מגיעים במחיר של אלימות ושחיתות.[59] ניתן להניח שתהליכים אלה אינם פוסחים על ארגוני טרור בכלל, ובמזרח התיכון בפרט.

4.3.7 סיכום ביניים

גם אם הרשויות האמריקאיות והמקסיקניות מפריזות במידה מסוימת בתיאור חומרת השימוש של הקרטלים בבינה מלאכותית כדי להצדיק תגובות צבאיות ופעולות חוצות מרחבים, כגון הגדרת קרטלים כארגוני טרור, הרי שמדובר בתחום מאתגר העלול להוות דוגמה גם לגורמי טרור. חוקרים, כמו אוסוולדו זוואלה (Oswaldo Zavala), טוענים כי כוחם של קרטלים מוצג מוגזם ולעיתים קרובות מסתמך על מסרים של המדינה, דבר המצביע על כך שהשימוש בבינה מלאכותית עשוי להיות פחות אוטונומי ויותר קשור לרשתות מושחתות.[60] סיכום זה משקף את התפקיד המורכב והמתפתח של בינה מלאכותית בפעולות קרטלים, תוך איזון עם ספקנות לגבי היקף יכולותיהם והמניעים העומדים מאחורי נרטיבים רשמיים.

5 מימון טרור

קבוצות טרור וארגוני גרילה משלבים בינה מלאכותית בפעילותם, כולל מאמצי מימון וגיוס כספים. בעוד שבינה מלאכותית אינה יוצרת באופן מהותי קטגוריות חדשות של איומים, היא מעצימה קטגוריות קיימות על ידי שיפור היעילות, יכולת ההרחבה וטקטיקות התחמקות. להלן סקירה כללית של שיטות שדווחו, שנלקחו מניתוחים של מומחים ללוחמה בטרור, ארגונים בינלאומיים ודיווחי תקשורת. שימושים אלה חופפים לעיתים קרובות לתעמולה, גיוס ופעילויות מבוססות סייבר, אך המוקד כאן הוא על היבטים פיננסיים.

57 Latisha Harry. 2024. "Digital Surveillance and the Specter of AI in Mexico." Advox Global Voices. February 20, 2024. https://advox.globalvoices.org/2024/02/20/digital-surveillance-and-the-specter-of-ai-in-mexico.

58 AI incident database. n.d. "Incident 725: Cartels Reportedly Using AI to Expand Operations into Financial Fraud and Human Trafficking." Accessed August 31, 2025. https://incidentdatabase.ai/cite/725.

59 Tommy E. Murphy, and Martín A. Rossi. 2020. "Following the Poppy Trail: Origins and Consequences of Mexican Drug Cartels." *Journal of Development Economics* 143 (102433). https://www.sciencedirect.com/science/article/abs/pii/S0304387819303098.

60 Kate Linthicum. 2024. "Are Mexican Drug Cartels as Powerful as People Think?" *Los Angeles Times*, August 28, 2024. https://www.latimes.com/world-nation/story/2024-08-28/are-mexican-drug-cartels-as-powerful-as-people-think.

5.1 תעמולה וגיוס תורמים

קבוצות כמו המדינה האסלאמית (דאעש) משתמשות בכלים יצירתיים של בינה מלאכותית כדי לייצר תוכן מולטימדיה מותאם אישית, כגון תמונות, אודיו וסרטונים, אשר מגבירים את הנראות ומושכים תומכים ותורמים. הדבר מסייע בעקיפין לגיוס כספים על ידי שיפור ההסברה במדיה החברתית ובערוצים מוצפנים, עידוד תרומות באמצעות פניות רגשיות מוגברות או קריאות לפעולה.[61] קיצונים ימניים משתמשים באופן דומה בבינה מלאכותית לגרפיקה ולדיסאינפורמציה כדי להרחיב את הרשתות של התומכים שלהם, ובכך להגדיל את התרמותיהם מרצון.

5.2 זיופים עמוקים (deep fakes) והתחזות על ידי תוכנות הונאה

זיופים עמוקים המופעלים על ידי בינה מלאכותית, ובייחוד גרסאות אודיו, מאפשרים הונאות התחזות שבהן גורמים מחקים קולות כדי להונות אנשים ולגרום להם להעביר כספים או לחשוף מידע פיננסי. מצב זה סומן על ידי מומחים להונאות סייבר כסיכון לגיוס כספים לפעולות טרור, בהתבסס על מקרים מתועדים של שיבוט קולי המשמש בפעולות הונאה רחבות יותר, שניתן להתאימן להונאות כספים בלתי חוקיות.[62] טכניקות כאלה מורידות את המחסומים בפני קבוצות פחות מתוחכמות ומאפשרות לבצע הונאות בקני מידה גדולים.

5.3 בינה מלאכותית בפשעי סייבר ומתקפות כופר

גורמי טרור ממנפים בינה מלאכותית כדי לתזמן מתקפות סייבר, כולל פריסת תוכנות כופר, המייצרות כספים באמצעות סחיטה. בינה מלאכותית מסייעת באוטומציה של איסוף מידע, ניתוח נתונים ויצירת פרופילים של קורבנות, ומאפשרת אפילו לפעילים בעלי כישורים נמוכים למקד ארגונים ו/או אנשים פרטיים לצורך הונאה וחילוץ כספים.

התהליכים משתרעים על פני פעולות הונאה שבהן בינה מלאכותית מעבדת נתונים גנובים או יוצרת זהויות בדויות כדי להקל על סחיטה ותנועת הכספים (העברות כספים דרך בנקים, יישומים או מטבעות מבוזרים).[63] דוחות מדגישים זאת כחלק ממגמה רחבה יותר שבה בינה מלאכותית משתלבת בזרמים פליליים של ארגוני טרור ופשע מאורגן חוצה גבולות למטרות רווח דרך הונאה דיגיטלית.

5.4 מטבעות מבוזרים ובינה מלאכותית

הכלים של בינה מלאכותית מנתחים נתוני שוק ומאפשרים אוטומציה של מסחר במטבעות מבוזרים, ומספקים אמצעים לספקולציות ויצירת כספים באופן אנונימי. גישה זו מתבססת על השימוש המסורתי של טרוריסטים במטבעות מבוזרים למימון טרור, כאשר בינה מלאכותית עשויה לסייע בגנבת ארנקים דיגיטליים, ערפול עסקאות או אופטימיזציה של עסקאות להלבנת הון או גיוס כספים ללא מעורבות ישירה של תורמים,[64] וללא חשיפת זהות בעלי הון.

---

61 Makuch, ben. 2025. "How Terrorist Groups Are Leveraging AI to Recruit and Finance Their Operations." *The Guardian*, June 8, 2025. https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence. Also in UNICRI and UNCCT. 2021. "Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes." https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

62 UNICRI and UNCCT. 2021. "Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes." https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

63 Threat Intelligence Report: August 2025. 2025. "Detecting and Countering Misuse of AI: August 2025." ANTHROP\C. August 27, 2025. https://www.anthropic.com/news/detecting-countering-misuse-aug-2025. Also in Gabriel Weimann, Alexander T. Pack, and Et.Al. 2024. "Generating Terror: The Risks of Generative AI Exploitation." *Combating Terrorism Center* 17 (1). https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation.

64 UNICRI and UNCCT. 2021. "Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes." https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

5.5 שילוב עם מימון המונים (crowdfunding)

אף על פי שלא תמיד מדובר בפלטפורמות ספציפיות לבינה מלאכותית, טרוריסטים מנצלים לרעה פלטפורמות מימון המונים על ידי קידום קמפיינים באמצעות מדיה חברתית ונכסים וירטואליים. בינה מלאכותית מגבירה זאת באמצעות יצירת תוכן אוטומטי לקמפיינים או צ׳אטבוטים לאינטראקציה עם תורמים, מה שמקשה על זיהוי שימוש לרעה במסגרת פעולות לגיטימיות בכמויות גדולות. הסיכונים כוללים תשלומים מקוטעים והעברות כספים אנונימיות חוצות גבולות.[65]

סוכנויות לוחמה בטרור מציינות כי יישומי בינה מלאכותית אלה חופפים לאתגרים כמו שחיקת פיקוח וגישה מהירה לטכנולוגיה, מה שעלול להאיץ ולהגביר את האיומים. עם זאת, אימוץ שיטתי משתנה בהתאם לקבוצה, כאשר ארגונים בעלי ידע טכנולוגי רחב יותר, כמו דאעש, מובילים בניסויים ובמירוץ הדיגיטלי. המאמצים להתמודד עם התופעה כוללים מערכות זיהוי משופרות ושיתוף פעולה בינלאומי בנושא שליטה וניהול בינה מלאכותית.[66]

לסיכום, ארגוני טרור, קבוצות גרילה ומורדים משתמשים בבינה מלאכותית למימון פעילויותיהם על ידי אמצעי מרמה, הונאה ותרמיות דיגיטליים על בסיס בינה מלאכותית, כגון גנבת זהויות, כספים, כרטיסי אשראי וכדומה. לא מן הנמנע כי ההונאה הגלובלית העכשווית של פלטפורמות חיקוי מסחר בבורסות בינלאומיות תגבר. הונאות אלה כבר גבו מחיר מקורבנות רבים בעולם, ולא ידוע מי בדיוק עומד מאחוריהן ומה מקורן. אין לשלול כי הן קשורות לפשע מאורגן עולמי, קרטלי סמים, קבוצות מורדים וארגוני טרור חובקי עולם.[67]

6 סיכום

ארגוני טרור וגרילה מצליחים במקרים רבים לשים את ידם על פיתוחי מו״פ צבאי. עם סיום המלחמה הקרה הפך שוק אמצעי הלחימה, ובעיקר זה הטכנולוגי, לשוק פרוץ ברובו. כמויות אדירות, ברובן ממחסנים של מדינות ברית ורשה ואזורים פוסט-סובייטיים, הציפו את השוק השחור. סוחרי אמל״ח סחרו עם כל הבא ליד, כולל ארגוני פשע, מורדים, ארגוני טרור, גרילה וקרטלי סמים. בנוסף לכך, שורה של נפילות של משטרים סביב העולם, ובעיקר במזרח התיכון בעקבות פירוק ברית המועצות והאביב הערבי, גרמו להפצת אמצעי לחימה ונפילתם לידיים של קבוצות טרור וארגוני גרילה ברחבי האזור.

כך הוצפו גם חמאס והג׳יהאד האסלאמי באמצעי לחימה שמקורם באיראן, צפון קוריאה ומדינות נוספות, מה שאפשר להם להעצים את הפעולה הצבאית ולהפוך לארגוני גרילה חמושים עד צוואר. יחד עם אמצעי הלחימה, ארגוני טרור השיגו תוצרי מו״פ צבאי של מעצמות כמו רוסיה, סין, הודו וצפון קוריאה, מכיוון שמשטרים שנפלו קיימו בזמן המלחמה הקרה שיתוף פעולה צבאי ארוך שנים עם מדינות אלה. כך הגיעו למעשה תוצרי המו״פ הצבאי לידי ארגוני טרור וגרילה.

---

65 FATF. 2023. "Crowdfunding for Terrorism Financing." *FATF*. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf. Also in Makuch, ben. 2025. "How Terrorist Groups Are Leveraging AI to Recruit and Finance Their Operations." The Guardian, June 8, 2025. https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence.

66 FATF. 2023. "Crowdfunding for Terrorism Financing." *FATF*. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf. Also in Makuch, ben. 2025. "How Terrorist Groups Are Leveraging AI to Recruit and Finance Their Operations." The Guardian, June 8, 2025. https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence.

67 Task Force to Investigate Terrorism Financing. 2016. "Trading with the Enemy: Trade-Based Money Laundering Is the Growth Industry in Terror Finance." https://www.govinfo.gov/content/pkg/CHRG-114hhrg23565/html/CHRG-114hhrg23565.htm. Also in Harry Freeborough. 2024. "Online Investment Scams: Inside a Fake Trading Platform." March 13, 2024. https://www.netcraft.com/blog/inside-a-fake-trading-platform.

מדובר בעיקר על כלי נשק רקטי, כולל נ"ט מתקדמים, כלי נשק אוטומטיים, חומרי נפץ ומטענים מתקדמים נגד חי"ר ושריון, רחפנים ומזל"טים. יש לבחון באיזו מידה מתקדמת המגמה להשגת נשק "מלוכלך" לא קונבנציונלי, כגון נשק ביולוגי וכימי. חלק מאמצעי הלחימה שמקורם במו"פ המדינתי הושג כאשר הוא מוכן לשימוש, וחלק אחר הושג באמצעות ביצוע הנדסה לאחור בידי מומחים או מהנדסים העובדים בשירות ארגוני טרור.[68] כך רואים מגמה גוברת של גיוס והעסקת מומחים ומהנדסי מו"פ צבאי ממדינות הגוש הסוציאליסטי לשורות ארגוני טרור ופשע לאחר פירוק הגוש הסובייטי. כך לדוגמה פיתוח רובוטים קרביים על ידי מדינות רבות עלול גם בעתיד להוביל להשגת מו"פ זה על ידי ארגונים אסימטריים.

באשר לממד הקיברנטי, הרי שמו"פ צבאי המבוסס על סייבר הופיע רק בשנות ה-2000 המוקדמות, ובשל כך זלג בינתיים פחות לידיים של ארגוני טרור, אולם האחרונים השיגו, וממשיכים לשפר יכולות סייבר בעצמם, הן כתוצאה מהעסקה של מומחים בשכר גבוה[69] ו/או דחף אידאולוגי, וכן כתוצאה מהשוק הפרוץ של שימוש בבינה מלאכותית, פיתוח עצמי של יישומים ותוכנות זדוניות, מתקפות סייבר והעסקת קבוצות האקרים.

יכולות סייבר ובינה מלאכותית משמשות ארגוני טרור לזריעת פחד, בלבול בקרב האוכלוסייה המקומית, ערעור על שלטונות מדינתיים על ידי שיבוש תשתיות קריטיות, קווי תקשורת, מדיה ותעמולה והפצת מידע כוזב, גיוס תומכים ולוחמים וגיוס תרומות למימון פעילותם, כולל שימוש נרחב במטבעות מבוזרים, והשגת מודיעין אסטרטגי וטקטי בקוד פתוח, כולל למטרת ביצוע פיגועים.

בינה מלאכותית הופכת לחלק בלתי נפרד מהפעילות של ארגונים אסימטריים. השימוש בה הינו רחב היקף, ומקיף את כלל האלמנטים של לוחמה אסימטרית. הארגונים מייצרים תוכן על ידי AI בעיקר למטרות גיוס, תעמולה, מימון, זריעת פחד, ערעור שלטון ועל ידי כך, בעקיפין, משיגים תוצר משמעותי – לחץ בינ"ל על ממשלות שמולן הם נלחמים. בדרך זו למשל הם מגבירים את הלחץ על ממשלת ישראל באמצעות הגברת הלחץ על מנהיגי העולם.

בנוסף, בינה מלאכותית מאפשרת אוטומציה של תהליכים, מה שמאפשר לקצר במידה ניכרת תהליכים הנדרשים ללוחמה אסימטרית. היא מאפשרת תיאום מוצפן בין תאי טרור, ארגונים וקבוצות מסביב לעולם, ניתוח וניבוי מהונדס, כולל חיזוי תגובות-נגד על ידי כוחות הביטחון של ממשלות, למידת מכונות, יצירת זיופים עמוקים, לוחמה פסיכולוגית, תרמית והונאות פיננסיות. אתגרים מערכתיים אלה מחייבים פיתוח גישה מערכתית ללוחמה בטרור מאורגן ולוחמת-נגד אסימטרית.

68 Cordesman, A H. 2016. "The Road to Hell in Iraq and Syria." *CSIS Center for Strategic and International Studies*, no. October 6, 2016. https://www.csis.org/analysis/road-hell-iraq-and-syria?block1.

69 US. Department of State. 2019. "Country Reports on Terrorism 2019." https://www.state.gov/reports/country-reports-on-terrorism-2019.

תשרי תשפ"ו / אוקטובר 2025

מכון ירושלים לאסטרטגיה ולביטחון
אבא אבן 16 בשדרת הנשיא השישי, ירושלים
www.jiss.org.il
info@jiss.org.il

אל"מ (מיל') פרופ' גבי סיבוני היה ראש תכנית צבא ואסטרטגיה ותכנית ביטחון סייבר במכון למחקרי ביטחון לאומי בין השנים 2006-2020. במסגרת זו הוא ייסד שני כתבי עת אקדמיים בתחומים המחקר האמורים. בין עיסוקיו הוא משמש כיועץ לצה"ל ולגופי ביטחון אחרים כמו גם לתעשייה הביטחונית. סיבוני הוא בעל תואר ראשון ושני בהנדסה מאוניברסיטת תל אביב ותואר שלישי במערכות מידע גיאוגרפיות מאוניברסיטת בן גוריון שבנגב.

סיימון ציפיס בעל תואר דוקטור במדעי מדינה ויחסים בינלאומיים מאוניברסיטת בון בגרמניה ותואר שני במדעי המדינה וביטחון לאומי מאוניברסיטת תל אביב. הוא מומחה לטרור, ביטחון סייבר ופוליטיקה פוסט-סובייטית במזרח אירופה ובאירו-אסיה.

www.jiss.org.il