סייבר, מודיעין וביטחון

כרך 4 | גיליון 1 | מרץ 2020

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

סייבר, מודיעין וביטחון

כרך 4 | גיליון 1 | מרץ 2020

תוכן

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
אוניברסיטת תל אביב
TEL AVIV UNIVERSITY

סייבר, מודיעין וביטחון

כתב העת **סייבר, מודיעין וביטחון** מיועד להעשיר, להפרות ולהעמיק את השיח הציבורי באשר לנושאים רלוונטיים.

המאמרים המופיעים בכתב עת זה, הרואה אור שלוש פעמים בשנה, נכתבים על ידי חוקרי המרכז ואורחיו והדעות המובעות בהם הן של המחברים לבדם.

כתב העת **סייבר, מודיעין וביטחון** רואה אור במסגרת תוכנית המחקר 'ביטחון סייבר', המתנהלת במכון למחקרי ביטחון לאומי.

עיצוב גרפי: מיכל סמו־קובץ ויעל ביבר, המשרד לעיצוב גרפי, אוניברסיטת תל אביב
דפוס: אליניר, פתח־תקווה

כתובת:
המכון למחקרי ביטחון לאומי, רח' חיים לבנון 40, ת"ד 39950, תל־אביב 6997556.
טל' 03-6400400, פקס' 03-7447590, דוא"ל: info@inss.org.il

המאמרים המתפרסמים בכתב העת סייבר, מודיעין וביטחון
מוצגים באתר המכון: www.inss.org.il

ISSN 2519-6685 (מקוון) • ISSN 2519-6677 (מודפס)

המערכה החשאית של מִבצעי השפעה בסייבר וכיצד לזהותם

דוד טיורי

הרשתות החברתיות הן דרך יעילה להשפיע על החברה וההתנהגות האנושית ולעצב דעת קהל. מבצעי השפעה בסייבר פירושם שימוש בכלי סייבר ושיטות סייבר כדי לתמרן את דעת הקהל. מדינות רבות משתמשות כיום במרחב הסייבר, ובמיוחד ברשתות החברתיות, כדי לנהל מבצעי השפעה כחלק מלוחמת מידע כוללת. מרבית הפעולות הללו נעשות באופן מוסווה, ולכן עצם הזיהוי שלהן מהווה אתגר. יתר על כן, לא פשוט להבדיל בין פעולות השפעה לגיטימיות ובין פעולות זדוניות. מאמר זה מתאר מִבצעי השפעה בסייבר, את פוטנציאל הנזק שלהם וכיצד הם מתנהלים. כמו כן, הוא מנתח את האתגרים הניצבים בפני זיהוי מִבצעי השפעה בסייבר ומפרט כמה פרמטרים אינדיקטיביים לזיהוי כזה.

מילות מפתח: השפעה בסייבר, מבצע השפעה, רשת חברתית, הנדסה חברתית, לוחמת סייבר

מבוא

העידן הדיגיטלי שינה את האופן שבו אנו מתקשרים. שיחות ומערכות יחסים בין אנשים מתקיימות כיום ברשת ובאמצעות תקשורת דיגיטלית. רשתות חברתיות, כמו "פייסבוק" ו־"אינסטגרם", ואפליקציות חברתיות כמו "ווטסאפ" ו־"טלגרם", מאפשרות לנו לשמור על קשר עם חברים ומשפחה, לשתף פוסטים, מסרונים, תמונות וסרטונים, לחלוק את החוויות שלנו זה עם זה, להתעדכן בסטטוס החברים שלנו ולקרוא פוסטים שהם כותבים.

רשתות חברתיות שנמצאות בשימוש נרחב על ידי רבים בכל רחבי העולם הן גם דרך יעילה להשפיע על החברה וההתנהגות האנושית ולעצב את דעת הקהל.

דוד טיורי הוא סגן ראש מינהל להנדסה במינהל סייבר לאומי ותעופה, מפעל הסייבר, אלתא מערכות בע"מ, התעשייה האווירית לישראל. המחבר מבקש להודות למר אהרון (רוני) אילת ולמר מארק אלינס, שעברו על מאמר זה ותרמו את הארותיהם.

על ידי שיתוף פוסט, ציוץ דעה, השתתפות בדיון בפורום או שיתוף תמונה בעלת ערך רגשי או פוליטי, אנו יכולים להשפיע על דעות של אחרים ואולי אף לשכנע אותם. דמיינו שהייתם יכולים לקחת חלק במאות ואלפי שיחות דיגיטליות; במצב כזה היה לכם סיכוי להשפיע על קהילות גדולות.

שימוש בכלים ובשיטות של סייבר כדי לתמרן את דעת הקהל נקרא "מבצע השפעה בסייבר" ("Cyber Influence Operation"). יכולות להיות מטרות שונות למבצעים מסוג זה: השפעה פסיכולוגית, פגיעה במורל ובמוּדעות הציבור, ערעור תחושת השליטה והיכולת להגן על שגרת החיים, ועוד. פעולות כאלו עלולות לגרום לנזק (פסיכולוגי), ולכן הן מכונות גם "מתקפות סייבר להפצת דיסאינפורמציה".

מדינות רבות משתמשות כיום במרחב הסייבר, ובמיוחד ברשתות החברתיות, כדי להוציא לפועל מְבצעי השפעה כחלק מלוחמת מידע כוללת. מרבית המבצעים הללו נעשים בצורה חשאית, כך שבמקרים שהמבצע נחשף קשה להוכיח מי עומד מאחוריו. מבצעי השפעה יכולים להיות מיועדים לקהל הרחב ואז לכלול אמירות כלליות, או להיות מופנים לקהל יעד ספציפי ואז לכלול מסרים ממוקדים שישיגו השפעה אפקטיבית יותר ושליטה בתוצאות. דוגמה לתוצאה כזו יכולה להיות הצבעה למועמד או למפלגה ספציפיים בבחירות, כפי שניתן היה לראות בבחירות לנשיאות ארצות הברית בשנת 2016.

זיהוי מבצעי השפעה בסייבר מהווה אתגר. לא קל לזהות השפעה, ובמיוחד קשה להבחין בין פעולת השפעה לגיטימית לזדונית. קידום מוצר או רעיון תמים הוא דבר לגיטימי, אפילו כפעולת השפעה. הסתה, קידום מעשים רדיקליים או אלימים, או התערבות בבחירות דמוקרטיות הם דוגמאות לשימוש זדוני בפעולות השפעה. חשוב שממשלות, באמצעות ארגוני ביטחון וגופי אכיפת החוק שלהן, יצליחו לזהות מבצעי השפעה זדוניים, כדי שניתן יהיה למנוע אותם או לפחות לצמצם את נזקיהם. נכון להיום, אין דרך שיטתית לזהות מבצעי השפעה בסייבר או להבדיל בין פעולות השפעה לגיטימיות לזדוניות.

בפרקים הבאים יתאר המאמר מהם מבצעי השפעה בסייבר ומה היכולת שלהם להסב נזק, כיצד מתנהלים מבצעי השפעה בסייבר ואילו טקטיקות הם מנצלים. המאמר גם ינתח את האתגרים בזיהוי מבצעי השפעה בסייבר ויפרט כמה פרמטרים אינדיקטיביים העוזרים בזיהוי. בחלק האחרון שלו יציג המאמר מקרי בוחן של מְבצעי השפעה בסייבר.

מבצעי השפעה בסייבר

מבצע השפעה בסייבר מוגדר כ־"מאמצים ממוקדים להכיר ולערב קהלים חשובים באמצעות תכניות, נושאים, מסרים ומוצרים המתואמים ביניהם, במטרה ליצור,

לחזק ולשמר תנאים הנוחים לקידום מדיניות, מטרות ואינטרסים מסוימים".[1] במילים אחרות, מבצעי השפעה בסייבר מייצרים מסרים ואינטראקציות במטרה להביא קהלי יעד לשנות את דעתם ו/או התנהגותם. אם המטרה היא שליטה בתגובות של חברי הקבוצה, הדבר נקרא "ניהול תפיסה" ("Perception Management").

תיאוריה דומה ל"ניהול תפיסה", שנחקרה בעיקר ברוסיה, נקראת "שליטה רפלקסיבית" ("Reflexive Control").[2] "שליטה רפלקסיבית" מוגדרת כדרך להעביר לשותף או ליריב מידע שהוכן במיוחד כדי להביא אותו לקבל החלטה שיוזם הפעולה מעוניין בה. "רפלקס" מתייחס לתהליך של חיקוי היגיון היריב, או התנהגות אפשרית שלו, באופן שיגרום לו להחליט אחרת מִשרצה תחילה. ניתן ליישם "שליטה רפלקסיבית" על תהליכי קבלת החלטות של מדינה דרך השפעה על משאבי המידע שלה. הדרך הטובה ביותר להשיג מטרה זו היא לייצר מידע מסוים, או מידע שגוי, כך שישפיע על משאב מידע ספציפי. הצלחה בהשגת "שליטה רפלקסיבית" על היריב תאפשר להשפיע על תכניותיו, על עמדתו לגבי סיטואציה מסוימת, או על האופן שבו יילחם. במילים אחרות, הצד המשפיע יצליח להשליט את רצונו על הצד השני ולגרום לו לקבל החלטה שאינה הולמת מצב נתון.

מונח הקרוב במשמעותו להשפעה בסייבר ולקוח מההקשר הצבאי הוא "תמרון משפיע" ("Influencing Maneuver"). בתהליך זה נעשה שימוש בפעולות סייבר כדי לחדור למעגל ההחלטות של האויב, ואולי אף לאלץ את מעגל ההחלטות לבצע פעולות ישירות או עקיפות. מדובר בצורת תמרון רחבה, שנועדה להשיג ולשמר עליונות ודומיננטיות במידע ולשמור על חופש התמרון במרחב הסייבר.[3] "תמרון משפיע" יכול לשמש לפעולות ישירות או עקיפות. דוגמה להשפעה ישירה של התמרון הן פעולות כמו פגיעה במערכות פיקוד ושליטה או מניפולציה סמויה בנתונים, שיספיקו כדי לערער את הביטחון שיש למפקד במערכות ויאטו את מעגלי ההחלטות. פעולות עקיפות יכללו הזנת התקשורת בנתונים לקויים ושגויים כדי לאלץ תגובה רצויה מסוימת אצל היריב. מאמר זה מתמקד בפעולות עקיפות.

מבצעי השפעה הופכים בהדרגה למקור דאגה מרכזי בכל העולם. הם מופיעים תחת שמות וביטויים שונים – חדשות כוזבות (Fake News), דיסאינפורמציה, קמפיין פוליטי שבו המשתתפים מתחזים לאזרחים רגילים (Political Astroturfing),

1 Eric V. Larson and others, *Understanding Commanders' Information Needs for Influence Operations* (Santa Monica: Rand Corporation, 2009).

2 Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military", *Journal of Slavic Military Studies* 17, no. 2 (2004): 237-256.

3 Scott D. Applegate, "The Principle of Maneuver in Cyber Operations", *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, (Tallinn: NATO CCD COE Publications, 2012), https://www.ccdcoe.org/publications/2012proceedings/3_3_Applegate_ThePrincipleOfManeuverInCyberOperations.pdf

מתקפות מידע וכדומה. מבצעי השפעה יכולים להיות חלק מלוחמה היברידית ולהשתלב במתקפות סייבר מסורתיות (כמו שימוש בתוכנה זדונית), בפעולה צבאית קונבנציונלית או במתקפות קינטיות חשאיות.[4]

למבצע השפעה יכולות להיות מטרות שונות והשפעות/נזקים פוטנציאליים שונים. בעיתות שלום, מטרת מבצעי השפעה יכולה להיות קידום רעיונות רצויים או הכוונת אוכלוסיות לכיוון הרצוי, כמו למשל מפלגה פוליטית המנהלת קמפיין לשכנע את בוחריה להצביע לה. אולם, אם אותה פעולה תתבצע על ידי מדינה זרה, הדבר ייחשב, כמובן, כהתערבות חיצונית בענייניה הפנימיים של מדינה ריבונית. התערבות זרה עלולה לפגוע באמון שיש לאזרחים בממשלתם, שכן הם לא יוכלו להיות בטוחים שאותה ממשלה היתה נבחרת לולא ההתערבות הזרה.

בתקופות של סכסוך או מלחמה, מטרת מבצעי ההשפעה יכולה להיות יצירת שיח נגד הממשלה, הסתת דעת הקהל נגד פעולות הממשלה (למשל, נגד המלחמה), פגיעה במורל הציבורי (למשל, לעורר תחושת חוסר ביטחון בפעולות הממשלה), וכן הלאה. כל זאת, כדי ליצור תחושה שלממשלה אין שליטה או יכולת להגן על שגרת החיים, וכך להביא להחלשת צבאה של המדינה בשדה הקרב.

מבצעי השפעה יכולים להתמקד בציבור הרחב או לפנות לקהל ספציפי בעזרת מאגרי נתונים מקוונים או רשתות חברתיות. מבצעי השפעה המכוונים לקהל הרחב יכללו אמירות כלליות שצפויה להן השפעה מזערית בלבד על יחידים ברמת המיקרו, אך עדיין הן ישיגו את האפקט הרצוי ברמת המאקרו. מבצעי השפעה המכוונים לקהלים ספציפיים ישתמשו באמירות המותאמות במיוחד לקהלים אלה כדי להיות יעילות יותר.

כיצד מתנהלים מבצעי השפעה בסייבר

השלב הראשון בניהול מבצע השפעה אפקטיבי בסייבר הוא הגדרת המטרה והגישה להשגתה. הגישה יכולה להיות בקמפיין חיובי – קידום נושא מסוים, חיזוקו ושיפור דעת הקהל לגביו – או בקמפיין שלילי – תקיפת מתנגדים, החלשת יריבים ויצירת דעת קהל שלילית. השלב השני הוא זיהוי קהל היעד: הציבור הרחב, קבוצות ממוקדות או קבוצה קטנה של משפיענים; קבוצות קיצוניות או כאלו שבקונצנזוס; המגדר, הגיל, הגזע, הדת וכדומה שישרתו את המטרה בצורה הטובה ביותר. השלב השלישי הוא בחירת הרשתות והפורומים החברתיים שבהם תתבצע פעולת ההשפעה וקביעת האינטראקציה בין המדיה שנבחרה ובין גורמים

4 "Army Researchers Join International Team to Understand, Defeat 'Disinformation' Cyberattacks", *ARL Public Affairs*, December 5, 2017, https://www.army.mil/article/197316/army_researchers_join_international_team_to_understand_defeat_disinformation_cyberattacks.

מתווכים אחרים. השלב הרביעי הוא קביעת הכלים להפצת המסרים: פרופילים מזויפים, בוטים או טרולים. לפרופילים מזויפים יש אולי מוניטין טוב יותר יחסית לשאר הכלים, אך הם יזדקקו למעורבות אנושית. בוטים ניתן לתכנת כדי להגיב אוטומטית לתוכן מוגדר, אך קל יותר לזהות אותם כבוטים. טרולים משמשים להעברת תכנים שליליים אגרסיביים, לרוב כאשר המטרה היא לתקוף יריבים. השלב האחרון בניהול מבצעי השפעה הוא הגדרת המסרים המתאימים ופרסום אינטנסיבי שלהם, בהתאם למטרה ולקהל שהוגדרו. תרשים 1 מתאר את השלבים בהוצאה לפועל של מבצע השפעה בסייבר.

תרשים 1. השלבים בהוצאה לפועל של מבצעי השפעה בסייבר

תעמולה היתה מאז ומתמיד דרך נפוצה להשפיע על אנשים. התעמולה המודרנית יעילה מאוד, מכיוון שהיא מסתמכת על מדיה דיגיטלית וחברתית. היא יכולה להגיע בקלות לאנשים רבים או לקבוצות נבחרות, ולהשתמש במספר רב של פוסטים כדי להשיג את מטרתה. מבצעי השפעה בסייבר יכולים להשתמש בטכניקות כמו תעמולה כדי להשפיע בצורה מוצלחת על אנשים.[5] דוגמאות לכך הן:

- **גירוי רגשות עזים**, כמו פחד, תקווה, כעס, תסכול ואהדה, כדי לכוון את הקהל אל המטרה הרצויה. זהו משחק מוחות שבו מפעיל ההשפעה המיומן יודע לנצל את הפחדים והדעות הקדומות של אנשים, להתאים פסיכולוגית את המסרים לרגשות, וכך ליצור תחושה של התרגשות ועוררות, המדכאת חשיבה ביקורתית ומתסיסה רגשות.
- **פישוט מידע ורעיונות** על ידי שימוש במידע שחלקו מדויק ואמיתי וחלקו חצאי אמיתות, דעות, שקרים והטעיות. מבצע השפעה מוצלח יספר סיפורים פשוטים

5 "Recognizing Propaganda", *Mind Over Media*, https://propaganda.mediaeducationlab.com/techniques.

שנשמעים מוכרים ואמינים, לרוב תוך שימוש במטפורות, דימויים וחזרות, כדי לגרום להם להיראות טבעיים או "אמיתיים". פישוט יתר הוא אמצעי יעיל: ביטויים קצרים, קליטים וזכירים מחליפים חשיבה ביקורתית. פישוט יתר של מידע אינו תורם לידע או להבנה, אולם מכיוון שבני אדם נוטים מטבעם לצמצום מורכבויות, טכניקה כזו של פעולת השפעה יכולה להיות אפקטיבית.

- **מתן מענה לצרכים ולערכים של קהל היעד** באמצעות העברת מסרים, נושאים ושפה הפונים ישירות, והרבה פעמים גם באופן בלעדי, לקבוצות ספציפיות ומובחנות בתוך האוכלוסייה. מפעיל השפעת סייבר עשוי לפנות לאנשים דרך תחושת הזהות הגזעית או האתנית שלהם, התחביבים, ידועים האהובים עליהם, האמונות והערכים, או אפילו השאיפות והתקוות האישיות לעתיד. משימה זו הופכת לקלה ויעילה יותר כאשר עושים שימוש בפרופילים שונים ברשתות החברתיות, מכיוון שניתן להתאים כל פרופיל לקהל היעד וכך להשיג תוצאה מיטבית. לפעמים הפניה תהיה לערכים האנושיים הבסיסיים ביותר, כמו הצורך לאהוב ולהיות נאהב, לחוש תחושת שייכות ותחושת מקום. מסרים הפונים ישירות לצרכים, לתקוות ולפחדים של קבוצות ספציפיות הופכים את פעולת ההשפעה לאישית ורלוונטית. כאשר המסר רלוונטי באופן אישי, אנשים שמים לב אליו וסופגים דרכו מידע ורעיונות מרכזיים.
- **תקיפת יריבים** כסוג של לוחמה פוליטית וחברתית שנועדה לזהות ולהשמיץ את המתנגדים. ניתן להטיל ספק בלגיטימיות, באמינות, ברמת הדיוק ואפילו באופי של יריבים וברעיונותיהם. מכיוון שאנשים נמשכים מטבעם לעימותים, פעולת השפעה יכולה לעשות שימוש אסטרטגי במחלוקות כדי לזכות בתשומת לב. תקיפת יריבים גם מעודדת חשיבה מסוג "או–או" או "אנחנו והם", המדכאת חשיבה על מידע ורעיונות מורכבים יותר. מבצעי השפעה יכולים לשמש גם כדי להכפיש אנשים, להרוס את המוניטין שלהם, להחריג קבוצות אוכלוסייה ספציפיות, להסית לשנאה או לעודד אדישות.

האתגרים הניצבים בפני זיהוי מבצע השפעה בסייבר

כדי לזהות מבצעי השפעה בסייבר, עלינו לזהות תחילה השפעה חברתית או השפעה בסייבר. לכן, אחד האתגרים הבסיסיים הוא להגדיר מהי השפעה חברתית וכיצד למדוד אותה ברשת. השפעה חברתית מוגדרת כ־"שכנוע אחרים, במודע או שלא במודע, במחשבות, באמונות ובמעשים שלך".[6] כשבאים להגדיר השפעה חברתית, משתמשים בשלוש קטגוריות: **שחקנים**, **אינטראקציות** ו**רשתות**.

6 D.M. Kahan, "Social Influence, Social Meaning and Deterrence", *Virginia Law Review* 83, no. 2 (1997): 349-395.

מפעילי סייבר יעדיפו במקרים רבים לפנות למשפיענים, כדי להגיע לקהל הגדול ביותר האפשרי. ישנם אינדיקטורים שונים כדי לדעת מהו הפוטנציאל של **שחקן משפיע** (משפיען): בעל מוח יצירתי, קובע טרנדים, בעל נוכחות והשפעה חברתית, פעיל ברשתות החברתיות, כריזמטי, בעל מומחיות, בעל סמכות, בעל מספר עוקבים/חברים גדול ועוד. לשחקן יש השפעה ברשת אם המסרים שלו או שלה משותפים גם מחוץ לאותה רשת; אם המסר משותף על ידי אחרים באותה רשת; אם לשחקן יש מספר גדול של אנשי קשר; אם השחקן גורם לכך שעוד אנשים יקראו את המסר; אם המהירות שבה המסר מופץ ברשת היא גבוהה.

את **האינטראקציה המשפיעה** ניתן למדוד בעזרת אינדיקטורים שונים. חוקרים הולנדים גילו שהשפעת האינטראקציה תלויה במידה רבה במספר השיתופים שקיבל המסר; בסוג התגובות שהמסר מעורר; במספר הפעמים שהמסר צוטט; במספר הקוראים/המאזינים שהמסר הגיע אליהם; האם המסר הביא לכניסת מספר רב של מבקרים ייחודיים.[7]

בין האתרים הנפוצים והמשפיעים ביותר על אינטראקציות במרחב הסייבר ניתן לציין אתרי בלוגים ברשת. להלן קריטריונים לבדיקת השפעה בהקשר של בלוגים ברשת:[8]

- **דירוג המרכזיות ברשת** – מודד את המוניטין של האדם: האם הוא או היא אישיות מרכזית ברשת או בעלת מספר מוגבל בלבד של אנשי קשר?
- **דירוג היפר־קישוריות** – מודד את מספר הקישורים לבלוג כקריטריון השפעה.
- **דירוג התנועה באתר** – מודד את מספר המבקרים באתר האינטרנט.
- **דירוג הפעילות בקהילה** – מתייחס למספר התגובות שהבלוג מעורר.

מחקרים נוספים קישרו אינדיקטורים ל**רשת חברתית (אישית) משפיעה**. אלה כוללים את המרחק החברתי בין שני שחקנים, מידת ההדדיות, כמות הקשרים השונים בין שני שחקנים ברשת (multiplexity), גודל הרשת, צפיפות הרשת, קישוריות, מרכזיות, ערך רגשי, לכידות קבוצתית ואשכולות (האם ניתן לחלק את הרשת לקבוצות קוהרנטיות). אינדיקטורים מוגדרים אלה יכולים לשמש לאיתור שחקנים, אינטראקציות ורשתות של בעלי השפעה, שבתורם יעזרו לנו לזהות טוב יותר השפעה חברתית. תרשים 2 מסכם את האינדיקטורים להשפעה חברתית.

---

7 Wouter Vollenbroek, Sjoerd de Vries, Efthymios Constantinides and Piet Kommers, "Identification of Influence in Social Media Communities", *International Journal of Web Based Communities* 10, no. 3 (2014): 280-297.

8 Dave Karpf, "Measuring Influence in the Political Blogosphere: Who's Winning and How Can We Tell?", *Politics and Technology Review* (2008): 33-41, http://www.the4dgroup.com/BAI/articles/PoliTechArticle.pdf.

שחקן משפיע	אינטראקציה משפיעה	רשת חברתית משפיעה
מוחות יצירתיים (Active Minds)	מספר הפעמים שמסר שותף	המרחק החברתי בין שני שחקנים
קובעי טרנדים		הדדיות
נוכחות והשפעה חברתית	מספר התגובות שמסר עורר	גודל הרשת
פעילות חברתית	מספר הפעמים שמסר צוטט	צפיפות הרשת
כריזמה		קישוריות
מומחיות	מספר הקוראים/מאזינים שמסרים הגיעו אליהם	מרכזיות
סמכות	אם מסר עורר מספר גדול של מבקרים ייחודיים	ערך רגשי
מספר החברים		לכידות קבוצתית

תרשים 2. אינדיקטורים להשפעה חברתית

לאחר שמזהים השפעה חברתית, האתגר הבא הוא להבחין בין פעולות השפעה לגיטימיות ובין כאלו שהן זדוניות. לעיתים הלגיטימיות של פעולת ההשפעה היא בעיני המתבונן. רוב האנשים יסכימו כי הסתה וקידום מעשים קיצוניים או אלימים מהווים פעולות השפעה זדוניות, וכי קידום רעיון תמים הוא בדרך כלל בגדר חופש דיבור לגיטימי. אבל מה לגבי אמירות או רעיונות פוליטיים שיוצאים נגד הנהגת המדינה? הדבר תלוי בערכי המדינה ובמשטר שלה. הבה נניח שמדובר במשטר דמוקרטי, שבו אדם יכול לבקר כל דבר וכל איש, לרבות את מנהיג המדינה. גם אז, אם הדבר נעשה על ידי צבא בוטים שתוכנתו להפיץ באופן אוטומטי אמירות נגד מפלגת השלטון, לגיטימיות ההצהרות אינה ודאית, במיוחד לאור העובדה שהשימוש בבוטים אסור על ידי מרבית המדינות. אם צבא בוטים כזה היה מנוהל על ידי שחקן זר, זה היה נחשב, ככל הנראה, התערבות זרה בדמוקרטיה של מדינה ריבונית.

כדי להשיג השפעה אפקטיבית, נעשה לא פעם שימוש בידיעות כוזבות. כך, למשל, ערב הסעודית ואיחוד האמירויות פעלו כדי להסית את דעת הקהל האמריקאית ומדינות ערביות אחרות נגד קטר, וזאת באמצעות קמפיינים באינטרנט וברשתות חברתיות שהאשימו את קטר בתמיכה בטרור ובערעור היציבות באזור. קטר דחתה האשמה זו, שבסופו של דבר התבררה כלא נכונה. עם זאת, תוצאת הקמפיינים

של ערב הסעודית ואיחוד האמירויות היתה שמדינות ערביות ניתקו את היחסים הדיפלומטיים שלהן עם קטר במהלך יוני 2017.[9]

ניתן להסכים כי השימוש בחדשות כוזבות אינו לגיטימי ומעיד על השפעה זדונית, אך האתגר האמיתי הוא עצם הזיהוי שלהן. לרוב, חדשות כוזבות מתפרסמות לצד ידיעות אותנטיות, וכך הן מקשות על זיהוין ככאלו. גם זיהוי תמונות מזויפות מהווה אתגר, לאור שפע הכלים המתקדמים הזמינים כיום לעריכת תמונות. המצב מסתבך עוד יותר כאשר פוסט מסוים עשוי לכלול גם עובדות נכונות, גם ידיעות כוזבות וגם דעות, שבאופן טבעי הן סובייקטיביות ומותאמות לערכים ולאמונות שבהם מחזיק הכותב. פוסט כזה יזכה ברשתות החברתיות לתגובות שישקפו את דעותיהם ונקודות המבט של המגיבים, וכך יגבר עוד יותר הקושי לזהות את האלמנטים השקריים.

אתגר נוסף בזיהוי מְבצעי השפעה בסייבר הוא הצורך לעשות זאת כמעט בזמן אמת. החדשות ברשתות החברתיות מתפשטות במהירות, ולעיתים קורה שעד שעובדה מתגלה כשקרית, הנזק כבר נעשה ופעולת ההשפעה מתקדמת לעבר מטרתה. כך, למשל, הפצת חדשות כוזבות או כוזבות למחצה על מועמד ימים ספורים לפני הבחירות, עשויה לשנות את התוצאות.

לאחר שזיהינו מבצע השפעה בסייבר, בדרך כלל נרצה לדעת מי עומד מאחוריו ולאסוף הוכחות לכך. הקושי במקרה זה נובע מכך שהאנשים או הארגון שמאחורי מבצעי ההשפעה מסווים את עקבותיהם. הם מסתירים את זהותם האמיתית באמצעות שימוש בבוטים ובפרופילים מזויפים ברשתות החברתיות ועל ידי הסתרת פרטי התקשורת שלהם (כמו ה־IP) בעזרת דפדפנים ייעודיים לגלישה אנונימית או שרתי פרוֹקְסי.

פרמטרים לזיהוי מְבצעי השפעה בסייבר

כדי לזהות מבצעי השפעה בסייבר, יש לנטר ולנתח את התכנים המתפרסמים ברשתות החברתיות השונות – טקסטים, תמונות וסרטוני וידאו – באמצעות חקר ביצועים ואלגוריתמים מתקדמים ותוך שקלול פרמטרים רבים של תוכן ותקשורת. להלן פרמטרים אינדיקטיביים שעוזרים לזהות מבצע השפעה בסייבר:

- **שימוש באווטארים, בוטים וטרולים**. פעולת השפעה טובה תסתיר את מפעיליה כדי להגיע לתוצאות היעילות ביותר. ישנן מספר דרכים להגיע לאנונימיות של פעולת ההשפעה. שניים מהכלים הנפוצים ביותר הם אווטארים ובוטים. אווטארים הם זהויות וירטואליות ברשתות החברתיות שמסתירות את זהותו

9 Josh Wood, "How a Diplomatic Crisis among Gulf Nations Led to a Fake News Campaign in the United States", *PRI*, July 24, 2018, https://www.pri.org/stories/2018-07-24/how-diplomatic-crisis-among-gulf-nations-led-fake-news-campaign-united-states.

האמיתית של המפעיל. בוטים הם סוכנים קטנים שמתוכנתים להגיב אוטומטית לפוסטים ספציפיים או לפרסם פוסטים אוטומטיים כדי לקדם את הרעיון/המוצר שאליו תוכנתו. יש טקטיקות רבות לזיהוי בוטים. חוקרים מצאו מספר תכונות המאפשרות לזהות בוט, כמו למשל חשבון פעיל ללא הפסקה, נפח גבוה של שיתוף ציוצים, תגובות לתוכן המכיל מילות מפתח מסוימות, שימוש בתמונות פרופיל גנובות, שם פרופיל מומצא, פערים משמעותיים בפעילות בחשבון, ועוד.[10]

- **פרסום פוסטים וחדשות שמקורם בגורמים מחוץ למדינה**. כאשר אנשים מנסים לשכנע אנשים אחרים ולקדם את רעיונותיהם או אמונותיהם, הדבר מהווה פעולה לגיטימית, כל עוד הם עושים זאת בתוך מדינתם או פועלים ממדינה אחרת ללא הסתרת זהותם. אבל אם איש ממדינה אחרת מתחזה לאזרח מקומי, זוהי פעילות חשודה המחייבת בדיקה. דוגמה טובה לכך תהיה ניסיון להשפיע על תוצאות הבחירות במדינה אחרת. ראוי לציין שלא פשוט לגלות את המקור האמיתי לתוכן שפורסם. מפעילים יכולים להשתמש בשרת VPS (שרת וירטואלי פרטי) הממוקם במדינת היעד, וכך להסוות את המיקום האמיתי של המעורבים. הם גם יכולים להשתמש בחשבונות דוא"ל הממוקמים במדינת היעד ומקושרים לזהויות מזויפות או גנובות, כדרך לגבות את הזהויות המקוונות. זהויות כאלו יכולות לשמש גם להלבנת תשלומים דרך חשבונות PayPal ומטבעות דיגיטליים.
- **פרסום ידיעות כוזבות**. זוהי אחת השיטות היעילות ביותר להשפעה על דעת הקהל, כפי שניתן היה לראות במקרים של הבחירות בארצות הברית ובצרפת. חוקרים מאוניברסיטת סטנפורד גילו כי 62 אחוזים מהאמריקאים הבוגרים צורכים את החדשות שלהם דרך רשתות חברתיות, כי סיפורי החדשות הכוזבות הפופולריים ביותר זכו לשיתוף רב ב־"פייסבוק", וכי מספר גבוה של אנשים שנחשפו לחדשות כוזבות דיווחו כי הם מאמינים להן.[11] פירוש הדבר הוא שהפצת חדשות כוזבות ברשתות חברתיות היא טקטיקה טובה למבצעי השפעה, ולכן אינדיקטור טוב לזיהוי שלהם.
- **פרסום מספר רב של פוסטים בנושא ספציפי**. כדי להגיע לכמה שיותר אנשים וכדי להגדיל את ההשפעה, יש צורך לפרסם מספר רב של פוסטים בנושא שבו רוצים להשפיע. לדוגמה, אם מדינה מסוימת מתכננת פעולה צבאית נגד מדינה אחרת, המדינה המותקפת יכולה לפרסם מספר רב של פוסטים וציוצים נגד

10 Bill Fitzgerald and Kris Shaffer, "Spot a Bot: Identifying Automation and Disinformation on Social Media", *Data for Democracy*, June 5, 2017, https://medium.com/data-for-democracy/spot-a-bot-identifying-automation-and-disinformation-on-social-media-2966ad93a203.

11 Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election", *Journal of Economic Perspectives* 31, no. 2 (Spring 2017): 211-236, https://web.stanford.edu/~gentzkow/research/fakenews.pdf.

הפעולה, שיתייחסו לנזקים האפשריים לכלכלה, יפריזו במספר הנפגעים, יתמקדו בפגיעה בזכויות האדם, וכדומה.

- **שינוי פתאומי בדעת הקהל**. כאשר מסתכלים על קבוצות ספציפיות בפורומים וברשתות חברתיות ומגלים שינויים שהתרחשו בדעת הקהל בתוך פרקי זמן קצרים, הדבר יכול לרמוז על התערבות זרה, מכיוון ששינויים בדעת הקהל נוטים מִטְבעם להיות הדרגתיים. לדוגמה, אם מועמד מוביל בתקופת בחירות מאבד לפתע את ההובלה בתוך יום או יומיים, יש בכך אינדיקציה להתערבות חיצונית אפשרית.
- **פרסום ביטויים שליליים קיצוניים**. יש נטייה להשתמש בביטויים שליליים, במיוחד בקבוצות או בפורומים רלוונטיים, כדרך להשיג שינוי מהיר ויעיל בדעת הקהל. לכן, ביטויים כאלה עשויים להצביע על קיומה של פעולת הסתה. לדוגמה, אם קבוצה פוליטית מושמצת על ידי הטלת ספק בלגיטימיות ובאמינות שלה, תוך שימוש בביטויים שליליים במיוחד, הדבר צריך להדליק נורה אדומה.

תרשים 3 מתאר את הפרמטרים האינדיקטיביים לזיהוי מבצעי השפעה בסייבר. פרמטר בודד אינו מספיק כדי להצביע על מבצע השפעה, אך שילוב של מספר פרמטרים יכול ללמד על קיומו של מבצע כזה. ניתן גם לבצע אוטומציה של התהליך בעזרת אלגוריתם שישלב את כל האינדיקטורים, אם כי אלה עשויים להשתנות בהתאם למצב. נכון יהיה להקנות לפרמטרים האינדיקטיביים משקל שונה בהתאם להֶקשר שלהם.

תרשים 3. פרמטרים אינדיקטיביים לזיהוי מבצעי השפעה בסייבר

מקרה בוחן: התערבות רוסיה בבחירות לנשיאות ארצות הברית ב־2016

בשנים האחרונות נחשפו מקרים רבים של מבצעי השפעה בסייבר, אך אין ספק שאחד הידועים שבהם הוא ההתערבות הרוסית בבחירות לנשיאות ארצות הברית בשנת 2016. ניתוח המקרה מעלה כי כמעט כל הפרמטרים שהוזכרו לעיל רלוונטיים לזיהוי ההשפעה הרוסית באותן בחירות:

- **רוסים המפרסמים פוסטים בארצות הברית**: ב־7 באוקטובר 2016 יצאו משרד מנהל המודיעין הלאומי (ODNI) והמשרד לביטחון המולדת (DHS) של ארצות הברית בהצהרה משותפת, לפיה קהילת המודיעין האמריקאית קובעת בביטחון כי ממשלת רוסיה הורתה על פריצה לשרתי הדוא"ל של המפלגה הדמוקרטית האמריקאית במטרה להתערב בתהליך הבחירות בארצות הברית.[12] שני דוחות שהוגשו לוועדת המודיעין של הסנאט האמריקאי על ידי חוקרים עצמאיים חשפו כי בין השנים 2013 ל־2017 הצליחו גורמי מודיעין רוסיים להגיע למיליוני משתמשים ברשתות החברתיות בארצות הברית.[13]
- **שימוש באווטארים וטרולים**: על פי דוח של מנהל המודיעין הלאומי של ארצות הברית, הקמפיין הרוסי היה רב־ממדים וכלל מדיה במימון ממשלת רוסיה, תעמולה גלויה ומשתמשים וטרולים בתשלום ברשתות החברתיות.[14] דוחות מראים כי הטרולים השתמשו באתרי אינטרנט רבים להפצת הנרטיבים שלהם,[15] וגורמים רשמיים ב־"פייסבוק" מסרו כי מאז יוני 2015 נוצרו 470 חשבונות מזויפים, אשר שימשו במהלך מערכת הבחירות האמריקאית ב־2016 חברה רוסית בשם Internet Research Agency (IRA). חברה זו ידועה בכך שהיא משתמשת בחשבונות טרולים כדי לפרסם פוסטים ברשתות החברתיות ותגובות (טוקבקים) באתרי חדשות.[16]

---

12 "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security", *Department of Homeland Security*, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

13 Alex Ward, "4 Main Takeaways from New Reports on Russia's 2016 Election Interference", *Vox*, December 17, 2018, https://www.vox.com/world/2018/12/17/18144523/russia-senate-report-african-american-ira-clinton-instagram.

14 "Assessing Russian Activities and Intentions in Recent US Elections", *Office of the Director of National Intelligence*, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

15 "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security".

16 Scott Shane and Vindu Goel, "Fake Russian Facebook Accounts Bought $100,000 in Political Ads", *The New York Times*, September 6, 2017, https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html.

- **ידיעות כוזבות**: בינואר 2017 העיד מנהל המודיעין הלאומי של ארצות הברית כי רוסיה התערבה בבחירות 2016 גם באמצעות הפצה וקידום של חדשות כוזבות ברשתות החברתיות.[17] חברת IRA כיוונה משתמשים שמרנים אל כמעט 110 פוסטים ב־"פייסבוק", לרבות תמונות מזויפות המראות הודעות על שגיאה במכונות ההצבעה או בפתקי ההצבעה, והציגה להם מידע כוזב על הונאת בחירות רחבה, שלכאורה נועדה לסייע למועמדת הילרי קלינטון לנצֵח.[18]
- **פרסום ידיעות רבות על המועמדים**: אחד מסיפורי הידיעות הכוזבות על הילרי קלינטון שותף 800,000 פעמים.[19] ב־"אינסטגרם" נרשמו כ־187 מיליון מעורבויות של כעשרים מיליון משתמשים בתכנים של חברת IRA שהיו קשורים לבחירות, וב־"פייסבוק" נרשמו 76.5 מיליון מעורבויות של כ־126 מיליון איש.[20]
- **ריבוי ביטויים שליליים על המועמדים**: על פי משרד מנהל המודיעין הלאומי של ארצות הברית, רוסיה העלתה את הסיכויים של דונלד טראמפ להיבחר לנשיא על ידי פגיעה באמינותה של הילרי קלינטון ויצירת תדמית ציבורית שלילית שלה.[21] כאשר נראה היה למוסקבה שקלינטון עשויה לזכות בנשיאות, קמפיין ההשפעה הרוסי החל להתמקד בערעור הלגיטימיות שלה ובכרסום סיכוייה להגיע לנשיאות, כולל הטלת חשדות בטוהר הבחירות. על פי "הפרויקט לחקר תעמולה ממוחשבת" ("Computational Propaganda Research Project"), חברת IRA הרוסית הפעילה טקטיקות רבות כדי לעצב דעת קהל בארצות הברית, ועשתה זאת על ידי הפצת מידע שגוי בפלטפורמות הרשתות החברתיות, ניצול פלטפורמות אלו לצורך מבצעי השפעה מבחוץ והעצמת דברי שטנה ותוכן פוגעני באמצעות חשבונות מזויפים או בוטים פוליטיים.[22]

---

17 Ellen Nakashima, Karoun Demirjian and Philip Rucker, "Top US Intelligence Official: Russia Meddled in Election by Hacking, Spreading of Propaganda", *The Washington Post,* January 5, 2017, https://www.washingtonpost.com/world/national-security/top-us-cyber-officials-russia-poses-a-major-threat-to-the-countrys-infrastructure-and-networks/2017/01/05/36a60b42-d34c-11e6-9cb0-54ab630851e8_story.html.

18 "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security".

19 Nakashima, Demirjian and Rucker, "Top US Intelligence Official: Russia Meddled in Election by Hacking, Spreading of Propaganda".

20 Ward, "4 Main Takeaways from New Reports on Russia's 2016 Election Interference".

21 Ibid.

22 Philip N. Howard, Bharath Ganesh and Dimitra Liotsiou, "The IRA, Social Media and Political Polarization in the United States, 2012-2018", *Computational Propaganda Research Project*, *2018*, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

מקרי בוחן נוספים

כאמור, בחירות 2016 בארצות הברית לא היו המבצע הידוע הראשון או האחרון של השפעה בסייבר. להלן כמה מבצעי השפעה נוספים:

- במאי 2014 שיגרו האקרים פרו רוסיים סדרה של מתקפות סייבר במשך מספר ימים במטרה לשבש את הבחירות לנשיאות אוקראינה. מתקפות אלו כללו פריצה לדוא"ל ופרסום תוכנו, ניסיון לשנות הצבעות ועיכוב בפרסום התוצאות הסופיות באמצעות מתקפות מניעת שירות.[23]
- בדצמבר 2016 טען חבר הפרלמנט הבריטי בן ברדשאו כי רוסיה התערבה בקמפיין שנערך לקראת משאל העם על ה־"ברקזיט" (יציאת בריטניה מהאיחוד האירופי).[24]
- במהלך הבחירות לנשיאות צרפת ב־2017, חשבונות אוטומטיים שיתפו בחדשות כוזבות על הבחירות, שחלק גדול מהן הגיע ממקורות שנחשפו להשפעה רוסית.[25] ההשפעה הרוסית חדרה לשיח הפוליטי בצרפת דרך תכנים הנוגעים לסוגיות בין־לאומיות. התכנים היו מכוונים לערער מקורות תקשורת מסורתיים, להפחית בחשיבותם של נושאים שהועלו נגד הפעילות הרוסית, ובאופן כללי להסיט את המוקד והאשמה לעֵבר שחקנים אחרים. התכנים גם נועדו לרכך את הביקורת על רוסיה ולקדם תמיכה בעמדותיה הפוליטיות, ובעקיפין לקדם לנשיאות מועמדים הדוגלים באותן עמדות.

מִבצעי השפעה בסייבר יכולים לזהם גם את המרחב המסחרי. חברת "נייקי" מצאה עצמה תחת מתקפה דיגיטלית (קמפיין מבצעי מתואם) לאחר שיצאה בספטמבר 2018 בקמפיין הפרסומי עם קולין קפרניק.[26] היעדים של מתקפת הסייבר על חברת "נייקי" כללו פגיעה במכירותיה ובשווי המניה שלה. ניתן היה לזהות את המבצע בעזרת הפרמטרים האינדיקטיביים הבאים:

- **שימוש באווטארים ובבוטים**: קבוצות מסוימות קידמו חרם נגד חברת "נייקי" בכך שארגנו "תיבות תהודה" אשר נועדו לגייס ציוצים או לייצר תעבורה ממוחשבת

23 Mark Clayton, "Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers", *Christian Science Monitor*, June 17, 2014, https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

24 Joe Watts, "Labour MP Claims It's Highly Probable Russia Interfered with Brexit Referendum", *Independent*, December 13, 2016, https://www.independent.co.uk/news/uk/politics/russian-interference-brexit-highly-probable-referendum-hacking-putin-a7472706.html.

25 Pierre Haski, "Patterns of Disinformation in the 2017 French Presidential Election", *Bakamo*, 2017, https://www.bakamosocial.com/frenchelection/.

26 Jay Solomon and Aftan Snyder, "Lessons for Brands from the anti-Nike-Kaepernick Social Effort", *PRNEWS*, February 22, 2019, https://www.prnewsonline.com/social+media-Nike-Kaepernick-APCO-bots-Twitter.

(בניגוד לתעבורה אנושית) באמצעות בוטים. בדיקת המשתמשים הפעילים העלתה כי 426 מתוך 668 המשתמשים שתקפו את "נייקי" ונדגמו היו אווטארים.

- **פרסום מספר רב של פוסטים נגד "נייקי"**: אחד הקמפיינים המתואמים כלל 300 משתמשים והפיק 2,133 ציוצים ושיתופים בתוך פרק זמן קצר.
- **שימוש במספר רב של ביטויים שליליים**: המשתמשים פרסמו לפחות עשרה ציוצים שליליים או מילות מפתח חוזרות במהלך הקמפיין.
- **שינוי פתאומי בדעת הקהל**: שווי המניה של "נייקי" נפל ב־3.2 אחוזים יום לאחר שהקמפיין החל לפעול.

מסקנות

הרשתות החברתיות, הנמצאות בשימוש רחב של אנשים רבים בכל רחבי העולם, הן גם דרך יעילה להשפיע על התנהגות חברתית ולעצב דעת קהל. מבצעי השפעה בסייבר עושים שימוש בכלים ובשיטות של סייבר כדי לתמרן את דעת הקהל. מדינות רבות משתמשות כיום במרחב הסייבר, ובמיוחד ברשתות החברתיות, כדי להוציא לפועל מבצעי השפעה בסייבר, כחלק מלוחמת מידע כוללת שמתנהלת ברובה באופן חשאי. מבצע השפעה שמנסה להתערב בענייניה הפנימיים של מדינה אחרת עלול לפגוע באמון שיש לאזרחים בממשלתם. בנוסף, הוא ינסה לעורר שיח, פעולות והפגנות נגד הממשלה ולפגוע במורל הציבורי. מכאן החשיבות שממשלות וגופי ביטחון יידעו לזהות מבצעי השפעה בסייבר ולמנוע אותם, או לפחות לצמצם את השפעתם השלילית. למרות שידוע כיצד מבצעי השפעה בסייבר מתנהלים ובאילו טקטיקות הם משתמשים, הזיהוי שלהם אינו משימה קלה, שכן מפעילי ההשפעה משתמשים בטקטיקות הסוואה שונות.

מאמר זה ביקש להציג מספר פרמטרים אינדיקטיביים לזיהוי מבצעי השפעה בסייבר שמתבססים על פרסום תכנים, בעיקר ברשתות החברתיות. עצם מציאת הפרמטרים שנדונו במאמר הוא אתגר בפני עצמו. כל פרמטר בנפרד אינו אינדיקציה מספקת לקמפיין השפעה, אך ביחד הם מעניקים נקודת פתיחה טובה לניתוח מצבים, ושימוש משולב בו־זמני בהם יכול לספק אינדיקציה טובה לקיומו של מבצע השפעה.

מקרה הבוחן של מבצע ההשפעה הרוסי בבחירות 2016 לנשיאות ארצות הברית הוא דוגמה מושלמת, שכן הוא עונה על כמעט כל הפרמטרים האינדיקטיביים המסייעים לזיהוי, אפילו בשלב המוקדם ביותר. הדבר מאפשר ללמוד שהפרמטרים האינדיקטיביים שהוזכרו לעיל יכולים לשמש כדרך שיטתית לגילוי מבצעי השפעה בסייבר. גישה מעשית כזו מציעה אפשרות לגילוי מוקדם של המבצע הבא של השפעה בסייבר באמצעות ניטור מתמיד של אמצעי התקשורת הרלוונטיים, וזאת אפילו על ידי אנליסטים שאינם מומחים.

ברמה הלאומית, "תמונת מצב הסייבר" כוללת את מצב התשתיות הלאומיות הקריטיות של המדינה, את מצב הסייבר של גופי הביטחון והממשל, אירועי סייבר ישירים, לרבות ניסיונות למתקפות סייבר, וכן מתקפות סייבר שנעשו בפועל, כולל הנזק שנגרם מהן. יחד עם זאת, עליה לכלול גם פעולות סייבר עקיפות, כמו מבצעי השפעה בסייבר שהוציאו לפועל מדינות אחרות. יש לראות במבצעים אלה מלחמות חשאיות ולטפל בהם בהתאם, לרבות על ידי הקצאת משאבים לזיהוים וסיכולם. בכל מקרה, מומלץ לערוך מחקרים נוספים, שינסו לזהות עוד פרמטרים אינדיקטיביים, יתרמו לאוטומציה של תהליכי זיהוי של מבצעי ההשפעה ויציעו דרכים להתגונן מפני פעולות אלו.

פעילותה של איראן במרחב הסייבר: זיהוי דפוסים והבנת האסטרטגיה

גבי סיבוני, לאה אברמסקי וגל ספיר

מאמר זה מציג את פעילות הסייבר המתפתחת של איראן, מתוך מטרה לזהות את הדפוסים העומדים מאחורי אסטרטגיית הסייבר שמיישם המשטר האיראני נגד איומים חיצוניים ופנימיים כאחד. המאמר פותח בתיאור פעולות הסייבר האיראניות, תוך התבססות על מידע שפרסמה הרפובליקה האסלאמית של איראן ועל דיווחים של חברות לאבטחת סייבר. לאחר מכן הוא מנתח את פעולות הסייבר של איראן. המאמר משרטט את המאפיינים והדינמיקה של פעולות הסייבר ההגנתיות וההתקפיות שלה, הן בזירה הפנימית והן בזירה החיצונית, ומציג ארבעה דפוסים נפוצים של פעילות הסייבר האיראנית שזוהו. לבסוף הוא מנתח את הממצאים העיקריים.

מילות מפתח: איראן, ביטחון סייבר, אסטרטגיית סייבר לאומית, בניין כוח, איומים פנימיים וחיצוניים, פעולה הגנתית והתקפית.

מבוא

המידע המוגבל על יכולות הסייבר של איראן עשוי היה להיות הגורם לכך שמשקיפים בין־לאומיים העריכו יכולות אלו בעשור האחרון בצורה שגויה. עם זאת, לאחרונה חל שינוי בתפיסת האיום האיראני. במהלך שבוע הסייבר 2019 שנערך בישראל, אישר יגאל אונא, ראש מערך הסייבר הלאומי, כי האיראנים נמנים על חמשת השחקנים המדינתיים הפעילים ביותר בתחום הסייבר. עוד ציין אונא כי "האיראנים פעילים ברציפות מזה זמן רב ביזימת מתקפות רחבות היקף, כולל מתקפות לאיסוף

פרופ' גבי סיבוני הינו ראש תוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי. לאה אברמסקי היא מתמחה במכון למחקרי ביטחון לאומי. גל ספיר היא עוזרת מחקר בתוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.

מודיעין ומִבצעי השפעה, וכן מתקפות שנועדו להסב נזק והרס למערכות. איראן היא אחת המדינות היחידות שמוציאה לפועל מתקפות הרסניות".[1]

השינוי שהתרחש לאחרונה בדרך שבה נתפס האיום האיראני על ידי מדינות המערב מעורר תהיות לגבי העלייה ברמתן של היכולות האיראניות. לאור זאת, רצוי להגדיר את האיום האיראני ולתאר את המאפיינים של אסטרטגיית הסייבר הלאומית של איראן, אותה היא מיישמת נגד אויביה. מומחים אכן זיהו התעצמות בפעילות הסייבר האיראנית, והיא גם תועדה היטב על ידי חברות לאבטחת סייבר. על פי סקר של חברת "מיקרוסופט", שפורסם במארס 2019, קבוצות סייבר איראניות תקפו במהלך השנתיים האחרונות אלפי אנשים ויותר ממאתיים חברות ברחבי העולם, וגרמו לנזקים משמעותיים המוערכים במאות מיליוני דולרים.[2]

מאז ראשית המאה ה־21 הִשקיעה איראן חלק ניכר מתקציבה בשיפור יכולות הסייבר שלה. בשלוש השנים הראשונות לכהונתו הראשונה של הנשיא רוחאני (2013־2017) עלה תקציב הביטחון האיראני ב־1,200 אחוזים.[3] פרנק צ'ילופו, מנהל המרכז לביטחון הסייבר והמולדת וסגן נשיא אוניברסיטת ג'ורג' וושינגטון, הצהיר בשנת 2017 כי "בשנים האחרונות השקיעה איראן רבות בבניית יכולות למתקפת רשתות מחשב ולפריצה למחשבים. תקציב הסייבר של איראן קפץ תחת הנשיא רוחאני פי 12, והפך את איראן לאחת מחמש מעצמות הסייבר המובילות. איראן משלבת מבצעי סייבר גם באסטרטגיה ובדוקטרינה הצבאית שלה".[4]

שני אירועים בולטים מרכזיים היו בהתפתחות הפעילות האיראנית במרחב הסייבר. הראשון היה המחאה האזרחית שהתעוררה באיראן בשנת 2009 תחת השם "התנועה הירוקה", שקיבלה בכלי התקשורת הזרים את הכינוי "מהפכת הטוויטר". לאחר הבחירות לנשיאות איראן ב־2009 והניצחון של אחמדינג'אד על יריבו הראשי מוסאווי, יצאו המונים להפגין ברחובות איראן במחאה על תוצאות הבחירות.[5] המוחים לבשו ירוק – צבע הקמפיין של מוסאווי, שגם נתן את השם

1 The Israel National Cyber Directorate, "Iran Is a Main Cyber Threat on the Middle East", *Israel National Cyber Directorate*, June 26, 2019, https://www.gov.il/en/departments/news/unna_cyber_week_2019.

2 Robert McMillan, "Iranian Hackers Have Hit Hundreds of Companies in Past Two Years", *The Wall Street Journal*, March 6, 2019, https://www.wsj.com/articles/iranian-hackers-have-hit-hundreds-of-companies-in-past-two-years-11551906036.

3 Ben Schaefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism", *Georgetown Security Studies Review*, March 11, 2018, https://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/.

4 Sam Cohen, "Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests", *Cyber, Intelligence and Security* 3, no. 1 (2019): 71-94.

5 "Editorial: Iran's Twitter Revolution", *The Washington Times*, June 16, 2009, https://www.washingtontimes.com/News/2009/Jun/16/Irans-Twitter-Revolution/.

לתנועת המחאה – וטענו לזיוף תוצאות הבחירות. למרות ניסיונות הדיכוי של המשטר, המפגינים נותרו פעילים עוד חודשים רבים לאחר מכן. הם ריכזו את מאמציהם בערוצי הרשתות החברתיות, כמו "טוויטר", "פייסבוק" ו"יוטיוב", הן למטרות ארגוניות והן כפלטפורמה להעברת עדכונים ומידע בתוך המדינה ומחוצה לה. השימוש יוצא הדופן שנעשה בטכנולוגיות מידע ותקשורת (ICT) עזר לחזק את התנועה, תוך שהממשלה נאבקת לסכל את פעילותה. התוצאה הייתה שהמשטר האיראני נאלץ לשפר את היכרותו עם מרחב הסייבר ואת מיומנותו לפעול בתוכו. פיתוח אסטרטגיית סייבר הפך מאז לצורך חיוני עבורו.

האירוע המרכזי השני היה מתקפת "סטקסנט" (Stuxnet), שנתפסת כגורם מכריע בחתירתה של איראן לגיבוש תוכנית לאומית לבניית יכולות הסייבר שלה. התוכנה הזדונית "סטקסנט" נחשפה בשנת 2010, לאחר שתקפה מערכות מחשב איראניות.[6] הפעילות המדויקת של "סטקסנט" נותרה בלתי ברורה – דבר שמלמד על תקופת פעילות ארוכה עד לחשיפתה.[7] היא גרמה להרס עצמי של כמעט אלף צנטריפוגות – כחמישית מכלל הצנטריפוגות שהיו פעילות במתקן ההעשרה הגרעיני של נתנז – ולעיכוב ניכר בתוכנית הגרעין האיראנית.[8] השפעת התוכנה הזדונית חשפה את הפגיעות שמדינות חוות לנוכח התחזקות הקישוריות בין מגזרים קריטיים. הופעתן של הטכנולוגיות החדשות גם הדגישה את הצורך בשיפור האבטחה, כדי לשמור ולהגן על מדינות במרחב הסייבר.

שני אירועים מרכזיים אלה, לצד הלחץ הכלכלי והעיכוב בתוכנית הגרעין האיראנית, עודדו את טיפוח החוסן החברתי והכלכלי במדינה. נראה כי השיטה האיראנית לטיפוח החוסן הייתה באמצעות "כלים היברידיים", כולל פעילויות סייבר. במובן זה, ניתן לראות בפיתוח יכולות הסייבר גם אמצעי של המשטר האסלאמי להתמודד עם יריבים מבית ומחוץ.

בחלק הבא של המאמר נבחן עובדות, אירועים, נתונים והצהרות רשמיות במטרה לזהות דפוסים נפוצים בפעילות הסייבר האיראנית ולהבין אותה. מאפיינים אלה יאפשרו לנו לאחר מכן לנתח ולהבין את מה שנתפס כאסטרטגיית הסייבר של איראן.

---

6 Josh Fruhlinger, "What Is Stuxnet, Who Created It and How Does It Work?", *CSO*, August 22, 2017, https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

7 The Israel National Cyber Directorate, "Iran is a Main Cyber Threat on the Middle East".

8 Taylor Armerding, "Whatever Happened to Stuxnet", *Synopsys*, January 17, 2019, https://www.synopsys.com/blogs/software-security/whatever-happened-to-stuxnet/.

התמודדות עם אויבים חיצוניים

המשטר האיראני הקים במהלך השנים מערך סייבר, הכולל קבוצות האקרים מאורגנות שפועלות תחת ארגוני הביטחון השונים של המדינה, וכן ארגונים עצמאיים הפועלים לטובת המשטר. בנוסף לכך, מספר ארגונים ומדינות במזרח התיכון זוכים לתמיכה איראנית ומתפקדים כשליחים יעילים של האינטרסים האיראניים בתחום הסייבר. מטרת חלק זה של המאמר היא להכיר את פעילות הסייבר של איראן ואת האופן שבו היא תומכת באסטרטגיית הסייבר של המשטר.

מבצע "אבָּאבִּיל" נחשב לאחת מההתקפות ההרסניות ביותר של איראן, והוא חלק מאסטרטגיית ההגנה שלה נגד ארצות הברית. המבצע, שהחל בשנת 2012, עדיין פעיל, וכולל גרסאות שונות וגלים של מתקפות מניעת שירות מבוזרת (DDoS).[9] הגל הראשון של המתקפה התמקד במערכת הפיננסית של ארצות הברית ותקף בנקים אמריקאיים, שבשעתם לא היו מוכנים לנֶפַח התנועה הפתאומי. המתקפה חסמה את האתרים והשרתים של אותם בנקים ומנעה מלקוחותיהם את היכולת להשתמש בשירותי בנקאות מקוונים. לוחמי סייבר על שם עז א־דין אל־קסאם, הקשורים ככל הנראה לממשלת איראן, קיבלו את האחריות למתקפה זו. במקרה זה השתמשה איראן בכוח הסייבר שלה באמצעות שחקן הנתון לחסותה כדי לתקוף את אחד מאויביה העיקריים – הממסד הפיננסי האמריקאי.

בשנת 2012 חדרה תוכנה זדונית הרסנית בשם "Shamoon" למערכות המחשב של ענקית הנפט הסעודית "ארמקו" וגרמה לנזקים רבים ולעלויות התאוששות גדולות. יש לראות בהתקפות נגד יעדים אסטרטגיים של ערב הסעודית ובעלות בריתה באזור, כמו RasGas בקטר, חלק מהאסטרטגיה ההגנתית האיראנית במרחב הסייבר.[10] גרסאות נוספות של התוכנה הזדונית תקפו ב־2016 יעדים חדשים, בעיקר משרדי ממשלה כמו משרד העבודה הסעודי, וכן חברות בערב הסעודית, כמו הבנק המרכזי של המדינה.[11] ב־2018 תקפו גלים חדשים של התוכנה הזדונית תעשיות קריטיות (נפט, אנרגיה, טלקומוניקציה) וארגונים ממשלתיים בכל רחבי האזור.

במאי 2016 דווח כי ארגון הממומן על ידי איראן השתמש באתרים ובשרתים כדי לתקוף כ־120 ארגונים ומוסדות ישראליים.[12] קבוצת ההאקרים, שבהמשך

9 "Operation Ababil DDoS Attack", *Radware*, https://security.radware.com/ddos-experts-insider/expert-talk/ddos-attacks-operation-ababil/.

10 "Operation Cleaver", *Cylance*, 2014.

11 Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage and Revenge* (Washington DC: Carnegie Endowment for International Peace, 2018), pp. 1-57.

12 "Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford", *ClearSky*, January 5, 2017, https://www.clearskysec.com/oilrig/.

זוהתה בשם "OilRig",[13] פעלה בשמה של ממשלת איראן מאז שנת 2015. במאי 2017 תקפה אותה קבוצת האקרים מערכות מחשבים של קבלן ביטחון אמריקאי, הפעם תוך שימוש בכלי תקיפה שמקורם ברוסיה.[14] מומחי האבטחה של החברה האמריקאית ציינו כי מדובר במקרה הראשון של שיתוף פעולה בין האקרים איראניים להאקרים רוסיים שמוכרים את שירותיהם לכל המרבה במחיר. המתקפה חשפה גם את השדרוג המשמעותי ביכולותיהם של ההאקרים האיראניים. חודשים ספורים לאחר מכן הגיש משרד האוצר האמריקאי כתב אישום נגד חברת Ajily Software Procurement Group בגין היותה ארגון פשע בין־לאומי. הארגון האיראני השתמש בהאקרים כדי לגנוב מארצות הברית וממדינות מערביות אחרות תוכנות הנדסיות שניתן להשתמש בהן כדי לתכנן נשק מונחה GPS.[15] מתקפה זו הייתה חלק מיוזמות ההגנה של איראן בתגובה לסנקציות הכלכליות שהטילה עליה ארצות הברית. בניגוד למקרים הקודמים שנדונו כאן, מקרה זה עירב גניבה וריגול עיסקי והמחיש כיצד ממשלת איראן מגייסת את יכולותיה במרחב הסייבר כדי לעקוף את הסנקציות האמריקאיות ולייבא טכנולוגיה צבאית על ידי שכירת שירותיהם של האקרים.

ביוני 2014 נחשף כי ארגון טרור סייבר איראני, המזוהה עם משמרות המהפכה האיראניים, תקף מאות יעדים בישראל ובמזרח התיכון במשך כשנה. קבוצת ההאקרים, שנקראה "Ajax Team" או "Rocket Kitten", פעלה בשנים האחרונות במסגרת ארגוני הביטחון האיראניים.[16] המתקפה הרב־שלבית שמה לה כמטרה מגוון של יעדים, ובהם מדענים ישראלים, צוותי שגרירות, פקידי נאט"ו, מתנגדי משטר באיראן, משפחת המלוכה הסעודית ואחרים. מטרת המתקפה הייתה להשיג גישה למידע קריטי ולגנוב אותו. מומחים העריכו כי מדובר במערכת התקפית ממוקדת, מתוחכמת, קבועה ושיטתית, המבוססת על איסוף מודיעין ומידע ממוקד על היעדים. בנובמבר 2015 פרצו משמרות המהפכה לשרתי הדוא"ל והרשתות החברתיות של חברי הממשל של נשיא ארצות הברית לשעבר ברק אובמה, וחברת "פייסבוק" אישרה כי זיהתה ניסיונות להשתלט על פרופילים של עובדי ממשל אמריקאים.

13 Bryan Lee, Robert Falcone, "Behind the Scenes with Oil Rig", *Unit 42*, April 30, 2019, https://unit42.paloaltonetworks.com/behind-the-scenes-with-oilrig/.

14 Nicole Perlroth, "Web Defenders Detect Russian Hand in Iranians' Hacking Attempt", *The New York Times*, May 15, 2017, https://www.nytimes.com/2017/05/15/technology/web-defenders-detect-russian-hand-in-iranians-hacking-attempt.html.

15 "Ajily Software Procurement Group", *Iran Watch*, August 8, 2017, https://www.iranwatch.org/iranian-entities/ajily-software-procurement-group.

16 "Rocket Kitten: A Campaign with 9 Lives", *Check Point*, 2015.

ביולי 2017 פרסמה חברת מודיעין הסייבר ClearSky דוח על מבצע מודיעין סייבר איראני המכונה "Wilted Tulip".[17] בפעולה זו הצליחו האקרים איראניים, המכונים "CopyKittens", להשיג גישה למידע של מספר סוכנויות ממשלתיות בישראל.[18] ההאקרים השתמשו במגוון שיטות, ובכלל זה במתקפת Watering Hole, שכללה פריצה לאתרי חדשות, הדבקה שלהם ושליחת קישורים לשורה של קורבנות במסווה של מאמרים לגיטימיים, במטרה להשתלט על המחשבים שלהם. הרצון לזכות באמון הקורבנות ולגרום להם ללחוץ על הקישורים לאתרים הנגועים הביא את הקבוצה להשתמש ברשת מורכבת ואמינה יחסית של פרופילים ב"פייסבוק", שחלקם קיימים כבר שנים. כדי לחזק את האותנטיות של אותם פרופילים, הוקמו ברשת החברתית מספר אתרים (שנבנו בפלטפורמת בניית אתרים איראנית) וכן דפים עיסקיים. הקורבנות כללו סוכנויות ממשלתיות וחברות פרטיות במספר מדינות במזרח התיכון, כמו ישראל, ערב הסעודית וטורקיה, וכן במדינות מערביות, כמו ארצות הברית וגרמניה.

בשנת 2018 תקפה איראן יעדים ישראליים, תוך שימוש בתוכנה זדונית המכונה "מאדִי", וכן מכוני מחקר אמריקאיים וחברות ומוסדות אקדמיים, במטרה לגנוב מידע ומסמכים מיוֹתר מ־800 קורבנות.[19] בנובמבר 2019 הצהירה חברת "מיקרוסופט" כי זיהתה פעילות סייבר אינטנסיבית מצד קבוצת האקרים בשם "Phosphorous", שקשורה כנראה לממשלת איראן.[20] פעולת הסייבר כוונה נגד בכירי ממשל אמריקאים בהווה ובעבר, עיתונאים, אירנים המתגוררים מחוץ לאיראן, וכן מועמדים פוטנציאליים לבחירות לנשיאות ארצות הברית בשנת 2020 (אם כי לא צוין מי מהם). ההתקפה כללה יותר מ־2,700 ניסיונות לזהות חשבונות דוא"ל השייכים ליעדים הספציפיים, ולאחר מכן פגיעה ב־241 חשבונות כאלה.[21] מבצע מסוג זה, שמטרתו להתערב במערכות בחירות זרות, הפך למקור מרכזי לדאגה מאז שהממשל האמריקאי הגיע למסקנה שרוסיה הצליחה לשבש את תהליך הבחירות לנשיאות בשנת 2016. הניסיון לשבש בחירות זרות ולתקוף אנשים מחוץ לאיראן הוא חלק מהפעילות ההתקפית של איראן.

---

17 Eduard Kovacs, "Iranian CopyKittens Conduct Foreign Espionage", *Security Week*, July 25, 2017, https://www.securityweek.com/iranian-copykittens-conduct-foreign-espionage.

18 "Operation Wilted Tulip", *Clearsky Security and Trend Micro*, July 2017.

19 GReAT, "The Madi Campaign – Part I", *Kaspersky*, July 17, 2012. https://securelist.com/the-madi-campaign-part-i-5/33693/.

20 "Microsoft: Iranian Hackers Targeted a US Presidential Campaign", *Asharq Al-Awsat*, October 4, 2019, https://aawsat.com/english/home/article/1931446/microsoft-iranian-hackers-targeted-us-presidential-campaign.

21 Ibid.

התמודדות עם אויבים פנימיים

בעוד שלאחרונה נשמעו קריאות להגביל את הגישה לאינטרנט, למעשה איראן נקטה זה מכבר אמצעים המאפשרים למשטר לשלוט בגישתם של אנשים לקישוריות. ממשלת איראן משתמשת בשליטה שיש לה על הגישה לאינטרנט כאמצעי לשיבוש התקשורת במדינה, במיוחד בתקופות של תסיסה עממית. מאז 2009, כל מחאה המונית הובילה את המשטר להטיל מגבלות על הגישה לאינטרנט.[22] בנובמבר 2019, לאחר שהממשלה הודיעה על העלאה ניכרת במחירי הדלק, פרצו מחאות אזרחיות בטהראן ובערים איראניות אחרות. כוחות הביטחון האיראניים הגיבו בדיכוי אלים של המהומות ובהשבתה ארצית של האינטרנט למשך כמעט שבוע – מהלך שניתק לחלוטין את האזרחים מהרשת. מחאה זו הייתה דוגמה רלוונטית לשימוש שאיראן עושה בכוחה במרחב הסייבר למטרות פנימיות: למנוע מהאוכלוסייה לתקשר, להתארגן, לשתף מידע ולהפגין.[23]

מאמצי הרשויות לחסום את האינטרנט ולהגביל את הגישה של אנשים לפלטפורמות תקשורת באופן כללי, או לפתח פרויקט אינטרנט לאומי, הלכו והתגברו ומצאו את ביטוים בניסיונות להגביל את השימוש ב־VPN (רשת פרטית וירטואלית) בקרב האוכלוסייה. כך, למשל, ממשלת איראן חייבה את נותני שירותי האינטרנט לחתום על התחייבות הקובעת כי "הקמה והפצה של שירותי VPN ושירותי פרוקסי" אסורות.[24] בנוסף לניסיון למנוע מאנשים להשתמש ברשתות VPN, איראן מנסה ככל הנראה ליצור רשת VPN לאומית שתפקח על הגישה לאינטרנט של כל אזרח בהתבסס על מקצועו. כך עולה מהצהרה מ־11 בנובמבר 2019 של חמיד פאתחי, מנכ"ל "חברת תשתיות טלקומוניקציה" (TIC), שהיא חברה בבעלות ממשלתית.[25]

מאז שנת 2005 תמך המשטר האיראני, תחת הנהגתו של הנשיא ח'אתמי, ברעיון של רשת לאומית סגורה.[26] ב־2010 הוצג הפרויקט של יצירת רשת "אינטרנט חלאל"

22 Borzou Daragahi, "Massive Iranian Internet Shutdown Could Be Harbinger of Something Even Darker to Come, Experts Warn", *The Independent*, November 30, 2019, https://www.independent.co.uk/news/world/middle-east/iran-internet-shutdown-protests-communications-tehran-a9226731.html.

23 Amy Slipowitz, "The True Depth of Iran's Online Repression", *Freedom House*, December 2, 2019, https://freedomhouse.org/blog/true-depth-iran-s-online-repression.

24 "State-Developed VPN Would Determine Iranians' Internet Access Based on their Job", *Center for Human Rights in Iran*, November 21, 2019, https://iranhumanrights.org/2019/11/state-developed-vpn-would-determine-iranians-internet-access-based-on-their-job/.

25 Ibid.

26 Julie Kebbi, "Internet: l'Autre repression du régime iranien", *L'Orient-le-jour*, November 22, 2019, https://www.lorientlejour.com/article/1195979/internet-lautre-

באיראן, שנועד לשמור על ערכים איראניים ולמנוע חדירה של איומים זרים. רשת כזאת גם תאפשר לרשויות לשלוט על גורמים פנימיים ולעקוב אחרי מתנגדים פוטנציאליים.[27] היוזמה הופיעה זמן קצר לאחר חשיפת מתקפת "סטקסנט", והיא נתפסה כחלק מהצורך לתת מענה לסיכונים ולאיומים החדשים שהחלו להתעורר מול איראן. למרות הספקנות של משקיפים בנוגע להצלחתו של פרויקט כזה, מדינות נוספות החליטו לאמץ טקטיקה דומה. כך, למשל, רוסיה העבירה בנובמבר 2019 חוק שמאפשר למדינה ליצור אינטרנט למשתמשים רוסיים בלבד, שיהיה סגור לחלוטין בפני שחקנים חיצוניים ויישלט על ידי הרשויות הרוסיות, מה שמלמד על המניע האמיתי לקידומו של פרויקט כזה.[28]

הרעיון של "אינטרנט חלאל", המכוּנה גם "רשת המידע הלאומית של איראן" (SHOMA), התפתח על רקע הגברת המעקב באינטרנט אחר האוכלוסייה המקומית.[29] ואכן, שוב ושוב נשמעות קריאות של גורמי ממשל איראניים להגברת הפיקוח וההגבלות באינטרנט, והנשיא רוחאני נאלץ לספוג מתקפות תכופות של שמרנים, המאשימים אותו שהוא חלש ואינו מגיב בצורה מספקת לאיום הנובע מהאינטרנט.[30] לדוגמה, במאי 2019 קרא התובע הכללי של איראן, מוחמד ג'עפר מונתזרי, לחיזוק הפיקוח וההגבלות על האינטרנט. הוא הזהיר ישירות את שר התקשורת וטכנולוגיות המידע, מוחמד ג'וואד אזָרי ג'הרוֹמי,[31] שככל הנראה נתפס כרפורמיסט גדול מדי, כי יהיה עליו לתת את הדין על העיכובים ביישום ההגבלות החדשות ועל כך ש"האינטרנט הלאומי" לא הושק כפי שרצה המנהיג העליון עלי ח'מנאי.

במקביל למגבלות המרובות שאיראן מטילה על ענקיות תקשורת זרות, כמו "טלגרם" (אפליקציית מסרים מיידיים), המשטר מסייע בפיתוח פלטפורמות חלופיות על ידי מתן תמיכה טכנית ומשאבים כספיים לאפליקציות המסרים המיידיים האיראניות "סוֹרוּש" ו"בֵּייל", הפועלות ברמה הלאומית. אינדיקציה לכך שאיראן

---

repression-du-regime-iranien.html.

27 Christopher Rhoads and Farnaz Fassihi, "Iran Vows to Unplug Internet", *The Wall Street Journal*, May 28, 2011, https://www.wsj.com/articles/SB100014240527487048894045762773914490020 16.

28 Lucie Bras, "Russie: à quoi va ressembler le « Runet », le nouvel internet 100% russe contrôlé par Moscou?", *20Minutes*, November 5, 2019, https://www.20minutes.fr/high-tech/2644575-20191105-russie-quoi-va-ressembler-runet-nouvel-internet-100-russe-controle-moscou.

29 Slipowitz, "The True Depth of Iran's Online Repression".

30 "En Iran, la justice appelle à davantage de surveillance sur Internet", *Le Monde*, May 4, 2019, https://www.lemonde.fr/keyhani/article/2019/05/04/en-iran-la-justice-appelle-a-davantage-de-surveillance-sur-internet_5994643_5470831.html.

31 "Iran Prosecutor Warns Minister to Tame Social Media or Face Consequences", *Radio Farda*, May 5, 2019, https://en.radiofarda.com/a/iran-prosecutor-warns-minister-to-tame-social-media-or-face-consequences-/29922128.html.

מוכנה לעודד יצירת אפליקציות מקומיות ניתנה ב־2017, כאשר המדינה הציעה מענקי תמריץ של יותר מ־200,000 דולר למפתחי תוכנה שיצליחו להגיע למיליון משתמשים בפלטפורמת התקשורת שלהם.[32] גופים ממשלתיים נהנים מהמדיניות הרופפת בשאלת הפרטיות, המאפשרת להם לאסוף ולאחסן את נתוני המשתמשים – מצב שמהווה סכנה פוטנציאלית ללקוחות.[33] מכיוון שהמשטר האיראני משתמש בכוחו כדי לפקח על השימוש באינטרנט, הוא גם מצנזר את האינטרנט הקיים וגם מייצר חלופות שיאפשרו לו לממש שליטה רבה יותר ברשת.

ניתוח מבצעי הסייבר ובניין הכוח של איראן

מאז סוף העשור הראשון של המאה ה־21 מוכתבים האינטרסים האיראניים במרחב הסייבר על פי התפתחות סיכוני הסייבר והאיומים על המשטר האסלאמי. איראן השקיעה כמות רבה של משאבים כדי לפעול במרחב הסייבר, אותו היא רואה כשדה קרב פעיל נגד ארצות הברית ובעלות בריתה. היא עושה זאת תוך התקדמות בערוצים מרובים במקביל, הן כדי להגן על המשטר מפני התקפה מצד תרבות המערב והן כדי להשמיד פיזית תשתיות מערביות.[34] המשטר מוביל פעולות תגמול נגד אויבים המנסים לכאורה לתקוף את איראן, עורך מבצעי ריגול בסייבר שנועדו להשיג מידע על פעילותו ויכולותיו של האויב, וכן מקיים פעולות התקפיות שמטרתן להסב נזקים לאותם אויבים. בפורום השמיני להגנה אזרחית לאומית, שהתקיים בטהראן בנובמבר 2019, הודיע ראש ארגון ההגנה האזרחית של איראן, הגנרל גולאם רזה ג'לאלי, כי איראן מאמצת גישה הגנתית חדשה נגד האיומים ההיברידיים והרב־שכבתיים החדשים, ומפתחת מוצרי הגנה שישמשו אותה במרחב הסייבר.[35]

היעדים למתקפות הסייבר האיראניות הם מתנגדי המשטר במדינה, כמו גם יריביה של איראן במערב ובמזרח התיכון, ובהם ישראל וערב הסעודית. רבים מהיעדים הם ארגונים עם שיוך אזרחי, כמו מערכות אבטחה, חברות פרטיות, גורמים אקדמיים, פקידי ממשל ותשתיות ציבוריות. כמו בשנים קודמות, מתקפות הסייבר האיראניות ממשיכות להיות אפקטיביות הודות לרמה הגבוהה של תכנון המבצעים והגישה המערכתית שבה הם מוצאים לפועל. למרות שהמתקפות

32 "In Iran, State-Sanctioned Messaging Apps Are the New Hallmark of Internet Nationalization", *Global Voices*, October 24, 2018, https://advox.globalvoices.org/2018/10/24/in-iran-state-sanctioned-messaging-apps-are-the-new-hallmark-of-internet-nationalization/.

33 "Pressure on Web Service Providers in Iran to Ban Proxies", *BBC Persia*, November 23, 2019, https://www.bbc.com/persian/iran-50531178.

34 דעת המחברים בהתבסס על המחקר.

35 "Iran Opts for New Civil Defense Approach to Confront US Threats", *Fars News Agency*, November 5, 2019, https://en.farsnews.com/newstext.aspx?nn=13980814000432.

האיראניות אינן מתוחכמות מבחינה טכנולוגית, הרמה הטכנית שלהן עלתה בצורה ניכרת בשנים האחרונות.[36]

פיתוח תחום הסייבר מהווה ביטוי לחדשנות טכנולוגית ומחזק את מעמדה של איראן במערכת הבין־לאומית כמעצמה טכנולוגית אזורית. המשאבים הרבים שמשקיע המשטר בטהראן בסייבר נשאו פירות גם במגזר האזרחי, לאחר שתשתיות התקשורת במדינה הורחבו לאזורים הכפריים ומהירות הגלישה באזורים העירוניים עלתה.

בחלק הבא של המאמר יוצגו ארבע תבניות עיקריות המאפיינות את האסטרטגיה האיראנית במרחב הסייבר. הראשונה היא האסטרטגיה של "מידה כנגד מידה" בפעולות הסייבר ההגנתיות וההתקפיות, שמותאמת להתפתחויות הגיאו־פוליטיות ומציגה דפוס של פעולות התקפיות נגד אויבים חיצוניים; השנייה היא פיתוח יכולות סייבר פנימיות במטרה לבנות חוסן כלכלי, כלומר כדי להיות חלק מהכלכלה העולמית למרות הסנקציות הבין־לאומיות ולקחת חלק בחדשנות טכנולוגית. ניתן לסווג תבנית זאת כדפוס של האסטרטגיה האיראנית במרחב הסייבר בזירה הפנימית, הכוללת יוזמות התקפיות והגנתיות גם יחד; המאפיין השלישי של אסטרטגיית הסייבר האיראנית הוא התאמה למערך הערכים, הדת והתרבות של המשטר, הן באסטרטגיה ההתקפית וההגנתית והן כלפי פנים וכלפי חוץ; המאפיין הרביעי והאחרון הוא הניצול המלא של ערכת הכלים של הסייבר והיעדר מסגרת חוקית שתבדיל את הסייבר מתחומי פעילות אחרים. מצב זה מאפשר לאיראן לחזק את האסטרטגיה ההתקפית שלה נגד יריבים פנימיים וחיצוניים כאחד.

אסטרטגיית "מידה כנגד מידה" תוך התאמתה להקשר הגיאו־פוליטי

איראן האיצה את פעילותה במרחב הסייבר זמן קצר לאחר שנחשף וירוס "סטקסנט". שנתיים לאחר מכן, הסנקציות הכלכליות שהטילה ארצות הברית הובילו את הרפובליקה האסלאמית להשתמש בסייבר לתקיפת יריבתה האמריקאית. אפשר לכנות את האסטרטגיה האיראנית במרחב הסייבר כאסטרטגיה של "מידה כנגד מידה", מכיוון שהיא מתאימה את תגובותיה למתחים הגיאו־פוליטיים ברמה האזורית או הבין־לאומית כחלק מהאסטרטגיה ההתקפית שלה במרחב הסייבר נגד אויבים חיצוניים. השימוש בפעילות התקפית במרחב הסייבר כדי להגיב על אירועים גיאו־פוליטיים הוא מנגנון קבוע באיראן. משמעות הדבר היא שאסטרטגיית הסייבר האיראנית קשורה, שלא לומר תלויה, באינטרסים הגיאו־פוליטיים של איראן ומותאמת אליהם. זהו מרכיב מעניין המאפיין את אסטרטגיית הסייבר האיראנית,

36 Schaefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism".

שכן מדינות אחרות (כמו סין או רוסיה) אינן מתכננות את אסטרטגיית הסייבר שלהן במיוחד כתגובה להתפתחויות גיאו־פוליטיות.[37]

ארצות הברית ראתה במבצע "אבאביל" את ההתקפה המשמעותית ביותר שאיראן ביצעה בתגובה לסנקציות הכלכליות הבין־לאומיות שהממשל האמריקאי כפה להטיל עליה בעקבות פיתוח תוכנית הגרעין האיראנית. התקפה זו הייתה משמעותית ברמתה ובעוצמתה, ומשרד החוץ האמריקאי הגיש ב־2016 כתב אישום נגד שבעה אזרחים איראניים שהיו קשורים למשמרות המהפכה, בגין חלקם באותה מתקפה.

המאפיין של התאמת אסטרטגיית הסייבר של איראן להתפתחויות גיאו־פוליטיות ניכר כבר במשא ומתן על הסכם הגרעין ("תוכנית הפעולה המשותפת"). גורמים רשמיים בארצות הברית ציינו כי בשנים 2013 ו־2014 – התקופה שקדמה להסכם – ביצעה איראן פעולות סייבר שהסבו נזק ניכר לחברות במערב ולאויביה של איראן במזרח התיכון.[38] כאשר הוטלו סנקציות על איראן ניתן היה להבחין בעלייה ברורה במספר המתקפות האיראניות במרחב הסייבר, בעוד שהסכם הגרעין השפיע ממשית על אסטרטגיית הסייבר של איראן, מכיוון שעם החתימה עליו ירדו תדירות המתקפות והיקפן. כאשר הנשיא טראמפ הודיע במאי 2018 על החלטתו לפרוש מהסכם הגרעין, חלה השפעה הפוכה: פחות מ־24 שעות לאחר מכן פתחה איראן בקמפיין אגרסיבי של מיילים מסוג "פישינג", שנשלחו לבעלות בריתה של ארצות הברית בחו"ל. היקף ההכנות הדרוש למתקפה כזאת מעיד על כך שהכוחות האיראניים הכינו אותה עוד לפני הכרזתו של טראמפ, ובחרו להוציאה אל הפועל בתגובה להחלטתו. ואמנם, מומחים זיהו אז עלייה מחודשת בפעולות הסייבר ההתקפיות שהגיעו מאיראן, מה שביטא שינוי של ממש במדיניות האיראנית.[39] על פי מומחי אבטחת סייבר, המאמצים האיראניים לתקוף מתקנים ואזרחים אמריקאיים במרחב הסייבר התגברו לאחר 2018 ובעקבות נסיגת ארצות הברית מהסכם הגרעין.[40]

---

37 Mark Pomerleau, "DoD Releases First New Cyber Strategy in Three Years", *Fifth Domain,* September 18, 2018, https://www.fifthdomain.com/dod/2018/09/19/department-of-defense-unveils-new-cyber-strategy/.

38 Kate Brannen, "Abandoning Iranian Nuclear Deal Could Lead to New Wave of Cyber Attacks", *Foreign Policy*, October 2, 2017, https://foreignpolicy.com/2017/10/02/abandoning-iranian-nuclear-deal-could-lead-to-new-wave-of-cyberattacks/.

39 Nicole Perlroth, "Without Nuclear Deal, U.S. Expects Resurgence in Iranian Cyberattacks", *The New York Times*, May 11, 2018, https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html.

40 "Iranian Hackers Wage Cyber Campaign amid Tensions with US", *Asharq Al-Awsat,* June 22, 2019, https://aawsat.com/english/home/article/1779921/iranian-hackers-wage-cyber-campaign-amid-tensions-us.

האסטרטגיה של "מידה כנגד מידה" כוללת גם את הפעילות שאיראן מבצעת מחוץ לגבולותיה באמצעות שליחים (by proxy). הגל השני של מבצע "Shamoon", בשנים 2016־2017, כלל התייחסויות לתימן ותמונה של הילד הסורי אלן כורדי, שהופיעה במכשירים מותקפים ונתפסה כנקמה על פעולות סעודיות בסוריה ובתימן. ביוני 2019 הודיעו החברות CrowdStrike ו־FireEye על התגברות פעולות הסייבר ההתקפיות של איראן.[41] פעילות התקפית זו באה זמן קצר לאחר שממשל טראמפ הטיל סנקציות חדשות על ענף הפטרוכימיה האיראני. על פי CrowdStrike, קבוצת ההאקרים "Refined Kitten", שמתקפת הסייבר מיוחסת לה, מנסה כבר שנים לפגוע בתעשיות הביטחון והאנרגיה האמריקאיות. בספטמבר 2019 הואשמה איראן בביצוע המתקפה נגד "ארמקו", אם כי היא הכחישה את הדברים והאשימה במתקפה את החותים (שיעים זיידים בתימן).[42] מתקפה זו הייתה בעלת השפעה משמעותית על יצרנית הנפט הגדולה בעולם ועיכבה את ייצור הנפט. עיתויה היה מיד לאחר שגורמים אמריקאיים רשמיים הצהירו כי תקפו את איראן במערכה סמויה ביוני 2019.

בניית חוסן: עקיפת הלחץ הכלכלי והובלת מהפכה בסייבר

בנוסף להקמתם של גופי סייבר חדשים והנהגת פיקוח על מרחב הסייבר, נראה כי ממשלת איראן משקיעה גם בחינוך הדור הבא,[43] וזאת כחלק מאסטרטגיה התקפית שמטרתה לבנות יכולות סייבר בזירה הפנימית. איראן השקיעה באופן מסיבי בתחום הסייבר באמצעות הקמת ארגונים רשמיים ותשתיות חדשות, וחלק ניכר מההשקעה מוקדש לחינוך. נראה כי גם הממשלה וגם גורמים לא מדינתיים מכירים בחשיבות לימודי הסייבר. כך, למשל, כמה אוניברסיטאות איראניות מציעות קורסים ללימוד פצחנות (האקינג).[44] לימוד רחב היקף של טכנולוגיות סייבר צפוי לסייע לפיתוח הענף, ואולי גם לשפר את מחויבות האזרחים למדינה בתחום זה.[45] מכיוון שקשה לבצע ייחוס נכון במרחב הסייבר, קבוצות לא רשמיות הקשורות למדינה יכולות לפעול לקידום האינטרסים המדינתיים. מקבלי ההחלטות באיראן הבינו את החשיבות שיש להשקעת סכומי כסף גדולים בלימוד התחום, מתוך ציפייה שבעקבות זאת יפתחו אנשים מחויבות לתמוך במדינה. אמנם,

41 Ibid.

42 Bruce Riedel, "Who are the Houthis, and Why Are we at War with them?", *Brookings*, December 18, 2017, https://www.brookings.edu/blog/markaz/2017/12/18/who-are-the-houthis-and-why-are-we-at-war-with-them/.

43 Veronika Netolická and Miroslav Mareš, "Arms Race 'in Cyberspace' – A Case Study of Iran and Israel", *Comparative Strategy* 37, no. 5 (2017): 414-429.

44 "Threat Intelligence Briefing Episode 11", *HP Security Research,* February 2014.

45 Netolická and Mareš, "Arms Race 'in Cyberspace'".

ההשקעה בחינוך לא תתורגם ישירות לתוספת של עובדי ציבור חדשים, אך היא תוכל להוביל להקמת קבוצות בעלות מוטיבציה עצמאית. בנוסף, הממשלה מראה עניין בתמיכה בחברות סטארט־אפ וחדשנות באיראן. בספטמבר 2019 החליטה ממשלת איראן להשקיע 225 מיליון דולר ב"קרן החדשנות האיראנית" מתוך כוונה לתמוך בחדשנות ולעודד חברות סטארט־אפ.[46]

ההשקעה בפיתוח יכולות סייבר כאמצעי להפוך למובילה בתחום זה מצביעה גם על כך שאיראן עוסקת בריגול סייבר במטרה לגנוב טכנולוגיה מיריבים ולהשיג מידע על יכולותיהם. התוכנה הזדונית "Madi" שהופעלה בשנת 2012, הפעילויות של "Rocket Kitten" בשנת 2014 והניסיונות של Ajily Software Procurement Group לייבא לאיראן תוכנות אמריקאיות גנובות באופן לא חוקי, הם כולם דוגמאות רלוונטיות לפעילות הריגול בסייבר של איראן. הפעילות האיראנית להשגת עוצמה טכנולוגית מלווה בדרך כלל בפעילות משבשת שנועדה לתקוף תשתיות קריטיות זרות, במיוחד בתחום האנרגיה והביטחון, כפי שמוכיח מזה שנים רבות האיום APT33 (המכונה גם "Elfin").[47]

פיתוח יכולות סייבר עשוי לשמש גם כאמצעי לעקיפת הלחץ הכלכלי על איראן ולגיוון מגזרי המשק, כחלק מאסטרטגיה הגנתית. בנייה ושיפור של יכולות הסייבר פירושם גם פיתוח של כלים טכנולוגיים חדשים. מטבעות וירטואליים, שהם דיגיטליים לחלוטין, עשויים לגלם את הכלים הכלכליים של מרחב הסייבר. נכון לעכשיו, המסחר במטבעות וירטואליים עדיין אסור ברפובליקה האסלאמית של איראן, אך לאחרונה הותרה שם כריית מטבעות וירטואליים כפעילות תעשייתית חוקית.[48] למשרד התעשייה, המסחר והכרייה של איראן יש את הסמכות המלאה לתת אישורים לכרייה מקומית, וכללים להסדרת פעילות זו אכן נוסחו בחוק. החוק החדש התקבל באיראן בתקופה שבה האיראנים כבר הפעילו כריית מטבעות וירטואליים, כדרך לעקוף את הסנקציות הכלכליות. החוק אמנם מגביל את האזורים הגיאוגרפיים שבהם מותר לכרות ומחייב אנשים לשלם עבור החשמל הנצרך, אך סגן שר האנרגיה האיראני, הומאיון חארי, כבר הצהיר כי הממשלה תאשר מהלך להחלת תעריפי חשמל נמוכים יותר על חוות כרייה, מה שצפוי לעודד את פעילות

46 "Iran Gov't Invests $225m in Innovation Fund", *Financial Tribune*, September 6, 2019, https://financialtribune.com/articles/sci-tech/99750/iran-gov-t-invests-225m-in-innovation-fund.

47 "Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.", *Symantec*, March 27, 2019, https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage.

48 Marie Huillet, "Iranian Gov't Authorizes Cryptocurrency Mining as Industrial Activity", *CoinTelegraph*, July 29, 2019, https://cointelegraph.com/news/iranian-govt-authorizes-cryptocurrency-mining-as-industrial-activity.

הכרייה באיראן. יחד עם זאת, הצהרתו של השר האיראני נשמעת חשודה, מכיוון שהבנק המרכזי של איראן המליץ לאסור על תשלום במטבעות וירטואליים בתוך המדינה. זאת, בשעה שגורמי החברה האזרחית וחברות פרטיות מנסים לקדם שימוש במטבעות וירטואליים ברמה המקומית.

יתר על כן, בדצמבר 2019 הציע הנשיא רוחאני ליצור מטבע וירטואלי מוסלמי כדרך להילחם בהגמוניה הכלכלית האמריקאית. הייתה זו הפעם הראשונה שהמשטר האיראני הודיע באופן פומבי על כוונתו לייצר מטבע וירטואלי במטרה להימנע משימוש בדולר האמריקאי, וזאת כחלק מאסטרטגיה פיננסית הגנתית.[49]

בעוד שאיראן מפתחת כלי זה כחלק מהניסיון להתמודד עם הסנקציות הכלכליות הבין־לאומיות, ארצות הברית כבר נקטה פעולה נגד שני איראנים שלכאורה השתתפו בהעברת תשלומים לתוכנת הזדונית "SamSam". המשרד לבקרת נכסים זרים של משרד החוץ האמריקאי הכניס את השניים לרשימת הסנקציות שלו בגין פעילות בתחום הביטקוין. פירוש הדבר הוא שהם נכללים ברשימה השחורה ואינם יכולים לשלוח או לקבל כסף מיחידים או מנותני שירותים.[50]

שמירה על יציבות המשטר והפצת ערכיו

לאחר אירועי "התנועה הירוקה" של שנת 2009 הבינה איראן את הסכנה הטמונה בטכנולוגיות החדשות מבחינת יכולת ההתארגנות להבעת התנגדות ולהתקוממות פוטנציאלית. כחלק מתגובת המדינה לתופעה זאת, פיתחה איראן אסטרטגיה הגנתית והתקפית במרחב הסייבר, שיושמה הן בזירת הבית והן בחוץ. במסגרת הפעולות ההגנתיות בתוך המדינה ניסה המשטר לפקח על הפעילות במרחב הסייבר ולשלוט בתכנים המשותפים. על פי סקר שפורסם בשנת 2012, 27 אחוזים מאתרי האינטרנט היו אז חסומים באיראן,[51] מכיוון שנחשבו כנוגדים את הערכים המוסלמיים. יתר על כן, איסור כלל־ארצי מוּחָל למעשה על רוב הרשתות החברתיות, כולל "פייסבוק" ו"טוויטר".[52]

---

49 Helen Partz, "Iran Wants to Create Crypto to Confront 'Economic Hegemony' of US", *CoinTelegraph*, December 19, 2019, https://cointelegraph.com/news/iran-wants-to-create-crypto-to-confront-economic-hegemony-of-us.

50 "US Regulators Tie Two Bitcoin Addresses to Iranian Ransomware Plot", *CoinDesk*, November 28, 2018, https://www.coindesk.com/us-regulators-tie-two-bitcoin-addresses-to-iranian-ransomware-plot.

51 "Current State of Internet Censorship in Iran", *View DNS.info*, March 23, 2012, https://viewdns.info/research/current-state-of-internet-censorship-in-iran/.

52 Leyla Khodabakhshi, "Why Ordinary Iranians Are Turning to Internet Backdoors to Beat Censorship", *BBC News*, January 10, 2018, https://www.bbc.com/news/blogs-trending-42612546.

על פי ראיון עם התובע אחמד עלי מונתזרי, שמכהן כראש ועדת הצנזורה באינטרנט, איראן סגרה ב־2016 14,000 אתרי אינטרנט וחשבונות ברשתות מדי שבוע.[53] מונתזרי הסביר כי תוכן האתרים הללו, שהתנגדו לערכים איראניים ולדת, הצדיק את סגירתם, והוסיף כי המדינה נתונה למתקפה של תקשורת זרה ועוינת. טקטיקת ההתקרבנות הזו משמשת באיראן מפעם לפעם לצורך הטלת צנזורה והפצת תעמולה. בשנים 2017, 2018 ו־2019, במהלך ההפגנות העממיות באיראן, חסם המשטר כמה אתרים ופלטפורמות תקשורת, ובמקומות מסוימים הרשויות אפילו ניתקו את הגישה לאינטרנט.[54] כך, לדוגמה, הממשלה חסמה את "טלגרם", שהיא אחת מאפליקציות התקשורת הפופולריות ביותר באיראן. גורמים איראניים רשמיים, שככל הנראה הפיקו לקחים מאירועים קודמים, היו מעוניינים למנוע מהחברה האזרחית את הדרך לתקשר, ליידע ולהתארגן באמצעות פלטפורמה זו.

חלק מהמאמץ האיראני לפתח יכולות סייבר נובע מהרצון לשמור על התרבות האיראנית – מניע שהוא דפוס חוזר באסטרטגיה של איראן. הגורם התרבותי בא לידי ביטוי גם בפעילות הסייבר של איראן, ורבות מהמתקפות שהובילו גורמים איראניים נקשרו בצורה כזו או אחרת להצדקות דתיות או תרבותיות. אחת הסיבות לכך שאיראן מעוניינת להיות מובילה אזורית ובין־לאומית מבחינת חדשנות טכנולוגית היא הגאווה הלאומית.[55]

ראש ארגון ההגנה האזרחית של איראן, ג'לאלי, הדגיש בנובמבר 2019 את התפקיד הבולט שיש לאיראן בתחום הסייבר והוסיף כי המשטר פיתח יכולת הגנה בסייבר לפני כל מדינה אחרת, כולל ארצות הברית. לדבריו, מדינות רבות, כמו רוסיה וצפון קוריאה, מעוניינות לקבל הדרכה מכוחות הסייבר של איראן.[56] תחושת הגאווה הלאומית, הנקשרת לתפקיד של ההובלה הטכנולוגית, חיונית להבנת האסטרטגיה של איראן במרחב הסייבר. ואכן, מאז שנת 2010 הצליחה איראן להרחיב את הגישה לאינטרנט לאזורים כפריים ולשפר את הקישוריות

53 "Iran Bans 14 Thousand Websites and Accounts Weekly", *Al Arabiya*, December 8, 2016, https://english.alarabiya.net/en/media/digital/2016/12/08/Iran-bans-14-thousand-websites-and-accounts-weekly-.html.

54 "In Response to Protests, Iran Cuts Off Internet Access, Blocks Apps", *NPR*, January 3, 2018, https://www.npr.org/2018/01/03/575252552/in-response-to-protests-iran-cuts-off-internet-access-blocks-apps.

55 Gawdat Bahgat and Anoushiravan Ehteshami, "Iran's Defense Strategy: The Navy, Ballistic Missiles and Cyberspace", *Middle East Policy Council* 24, no. 3 (2017): 89-103.

56 "Iran Opts for New Civil Defense Approach to Confront US Threats", *Fars News Agency*, November 5, 2019, https://en.farsnews.com/newstext.aspx?nn=13980814000432.

בערים,[57] והפכה בכך לאחת המדינות המזרח תיכוניות עם המספר הגדול ביותר של משתמשים באינטרנט.

המשטר האיראני מחויב להפצת ערכיו גם מחוץ למדינה, וזאת כחלק מפעילות התקפית נגד "האויב". ב־2018 זיהתה חברת אבטחת הסייבר FireEye קמפיין לקידום נרטיבים פוליטיים איראניים.[58] המבצע כלל שימוש באתרי חדשות לא לגיטימיים וניצול זדוני של רשתות חברתיות. לפי הניתוח של חברת אבטחת הסייבר, היה זה שכפול של הניסיון הרוסי להשפיע על דעת הקהל הזרה בבחירות 2016 לנשיאות ארצות הברית. בספטמבר 2019 הודיע גולאם רזה סולימאני, מפקד ארגון הבסיג', על הקמת אלף גדודי סייבר ברחבי המדינה, באמצעות חשבונות של משתמשים תומכי משטר ברשתות החברתיות.[59] כל גדוד כזה מורכב מכ־500 חיילים. פירוש הדבר הוא שהמשטר שיגר כנראה לרשתות למעלה מחצי מיליון חשבונות התומכים במשטר. סולימאני לא אמר דבר ביחס לאמצעים ולתקציב ששימשו את ארגון הבסיג' כדי לממש פרויקט זה, אך הוסיף והצהיר כי "האויב הביע במספר הזדמנויות דאגה מנוכחותו המאורגנת של הנוער המהפכני במרחב הסייבר, מה שמשקף את המומנטום שנוצר. הנוכחות הזו רק תתרחב ותשתפר". עם זאת, חרף היוזמה החדשה להפצת דעות תומכות משטר באינטרנט, איראן צפויה להתמודד גם עם קשיים, לאחר ש"טוויטר" הסירה לאחרונה אלפי חשבונות שפעלו בגיבוי המדינה (כולל חשבונות שהוערכו כמקושרים לממשלת איראן).

מעֵבר לנחישות של איראן להגן על מערכת הערכים שלה, המשטר גם מנסה להילחם ברעיונות זרים וגם להפיץ את התעמולה שלו באמצעות מתקפות סייבר. לדוגמה, במסגרת מבצע "אבאביל" תבעו האקרים להסיר את "תמימות המוסלמים" – סרט שהופץ בשנת 2012 ונחשב כפוגע בכבוד המוסלמים.[60] מתקפת הסייבר לוּותה בהצדקה תרבותית, שהתבססה על העלבון שנגרם לתדמיתה של איראן. דוגמה נוספת להפצת תעמולה באמצעות הסייבר הייתה מתקפת התוכנה הזדונית "Shamoon" בשנת 2016, שבמהלכה הופצו במכשירים שנפגעו תמונות אנטי מערביות, כמו תמונה של שריפת דגלה של ארצות הברית. בהמשך צצה גרסה

57 Anoushiravan Ehteshami, "Iran: Stuck in Transition", *Journal of International and Global Studies* 9, no. 2 (2017): 186-188.

58 Ed Parsons and George Michael, "Understanding the Cyber Threat from Iran", *MWR Info Security*, April 17, 2019, https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-iran.

59 "Nouveaux cyber-brigades en Iran", *PressTV*, September 7, 2019.

60 Brannen, "Abandoning Iranian Nuclear Deal Could Lead to New Wave of Cyber Attacks".

נוספת של "Shamoon", שהפיצה את התוכנה הזדונית למכשירים באמצעות פסוק של הקוראן.[61]

ניצול המאפיינים של הסייבר

מרחב הסייבר הוא תחום שבו יש לאיראן ולמדינות לא ליברליות הפריווילגיה לשחק שלא לפי הכללים של מדינות דמוקרטיות כמו ארצות הברית וישראל. ואכן, נראה שאיראן מנצלת את העובדה שאינה כפופה לאותם כללים כדי ליישם את האסטרטגיה ההתקפית שלה נגד אויבים מבית ומחוץ. מכיוון שמדובר במערכת ערכים שונה, איראן רואה חלק מהמעשים כמקובלים ואחרים כאסורים מבחינה אתית ומוסרית. לעומת זאת, המדינות המערביות, הדמוקרטיות והמפותחות פועלות בהתאם למערכת המשפטית שלהן, וגם נוטות לאמץ ולכבד את המשפט הבין־לאומי כחלק מהחשיבות הרבה שהן מייחסות לדעת הקהל.

בהיותה משטר לא ליברלי, איראן מרשה לעצמה להסדיר ולצנזר את מרחב הסייבר באופן מגביל ביותר, ושוללת מאזרחיה כלים בסיסיים להתחבר לעולם. גם המידע הנוגע לפעולות שהיא מבצעת בתחום הסייבר ברמה הלאומית מוסתר מהציבור. בעוד שמדינות דמוקרטיות נוטות להימנע מעמימות מתוך מחויבות לעקרונות משפטיים, במשטרים סמכותניים כמו איראן העמימות היא אמצעי נפוץ. איראן רחוקה מלהיות שקופה בכל הנוגע לפעילותה בנושא אבטחת סייבר ומידע, בעוד שמדינות דמוקרטיות מחויבות לשקיפות ברמה גבוהה ונושאות באחריות לכל החלטה שיקבלו. בכירי הממשל האיראני דוחים את תפיסת האחריותיות ונהנים מחופש פעולה רחב, מבלי לחשוש יתר על המידה מפני חוסר הסכמה מצד האוכלוסייה. מקרה מייצג היטב הוא הניסיון של איראן, שנחשף על ידי חברת "מיקרוסופט" בספטמבר 2019, לחדור לרשתות אמריקאיות ואירופיות באמצעות מבצע שהוביל הארגון "Phosphorous". בדומה לפעילות הרוסית בשנת 2016, איראן ניסתה, ככל הנראה, להשפיע על בחירות במדינות אחרות ולתקוף מועמדים פוטנציאליים לבחירות לנשיאות ארצות הברית בשנת 2020.

העמימות ויכולת ההכחשה של מתקפות הסייבר מאפשרות לתוקפים להשתמש בלוחמת סייבר בצורה סמויה. הדבר הופך את מרחב הסייבר לזירה מועדפת להתעמתות עם אויבים מבלי לחשוש מתגמול ישיר. סוגיה אחרת בהקשר זה היא הפעילות של קבוצות האקרים שהזיקה שלהן למשטר האיראני הינה מעורפלת. תופעה נוספת ההולכת ומתפתחת בפעילות הסייבר של איראן ומאפשרת לה את יכולת ההכחשה היא שיתוף פעולה עם קבוצות זרות. השימוש שעשו "OilRig"

61 Charlie Osborne, "Shamoon Data-Wiping Malware Believed to Be the Work of Iranian Hackers", *ZDnet*, December 20, 2018, https://www.zdnet.com/article/shamoons-data-wiping-malware-believed-to-be-the-work-of-iranian-hackers/.

בכלי סייבר רוסיים כדי לתקוף יעד אמריקאי בשנת 2017 הוא דוגמה לתיאום בין האקרים רוסיים להאקרים איראניים. היבט נוסף של יכולת ההכחשה בסייבר הוא החשיבות שיש לשליחים (proxies), קרי שחקנים מדינתיים או לא מדינתיים הנתמכים על ידי איראן ומבַצעים פעולות עצמאיות שעולות בקנה אחד עם האינטרסים האיראניים. שליחים כאלה של איראן פזורים בכל רחבי האזור, גם בקרב השיעים וגם בקרב הסונים (החותים בתימן, חמאס ברצועת עזה, חיזבאללה בלבנון וכן הלאה). העמימות שיוצרת פעולה הנעשית באמצעות שליחים מאפשרת לאיראן להכחיש בקלות את מעורבותה במבצעי סייבר. דוגמה לכך היא ההכחשה של איראן את ההאשמה נגדה כאילו היא זו שתקפה את מתקני הנפט הסעודיים בספטמבר 2019, וטענתה שמי שאחראים למבצע זה הם החותים

הדפוס האחרון שזוהה באסטרטגיית הסייבר הלאומית של איראן הוא היכולת שלה להכחיש את היותה יעד למתקפות. הצהרות פומביות של גורמים רשמיים באיראן, הטוענים כי הרפובליקה האסלאמית חסינה בפני מתקפות סייבר, הן דבר שכיח. דוגמה אחרונה להצהרות כאלו ניתן לראות בראיון עם ג'לאלי שפורסם בנובמבר 2019, בו אמר כי ניסיונות זרים לתקוף את איראן במרחב הסייבר לא צלחו בשנתיים האחרונות בזכות יעילותם של מנגנוני הביטחון האיראניים בתחום הסייבר.[62] דבריו באו במקביל להצהרות של גורמים רשמיים בארצות הברית על הצלחתו של מבצע סייבר סמוי באיראן, אשר השפיע על יכולתו של המשטר לתקוף מכליות נפט במפרץ הפרסי ביוני 2019.[63] שר התקשורת וטכנולוגיית המידע של איראן, מוחמד ג'וואד אזָרי ג'הרומי, אף הגדיל לעשות והצהיר שארצות הברית "ודאי חלמה" את המבצע.[64]

סיכום ומסקנות

איראן מציבה כיום איום סייבר משמעותי על המערכת הבין־לאומית. פעולותיה והאסטרטגיה שמאחוריהן הביאו גורמים מערביים רשמיים, יחד עם מומחים מהמגזר הפרטי, להאמין שאיראן מבקשת להציב את עצמה בשורה אחת עם מעצמות סייבר כמו רוסיה וסין. מומחים גורסים כי אם יכולותיה של איראן ימשיכו להתפתח, יש לצפות בסבירות רבה למתקפת סייבר איראנית שתפגע בתשתיות פיזיות.

ניתן לתאר את אסטרטגיית הסייבר ההתקפית של איראן כאסטרטגיה של "מידה כנגד מידה", הנשענת על הצדקה תרבותית, גאווה לאומית ויתרונות ייחודיים במרחב הסייבר. איראן צמחה להיות אחת משחקניות הסייבר המובילות בעולם.

62 "Iran Opts for New Civil Defense Approach to Confront US Threats".

63 Julian E. Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say", *The New York Times*, August 28, 2019, https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html.

64 Ibid.

המוניטין שהיא רכשה משרת את האסטרטגיה שלה ואת מאמציה להפעיל לוחמה אסימטרית נגד אויביה מבחוץ. המשטר האיראני משקיע משאבים רבים בפיתוח יכולות סייבר במגוון תחומים כדי לחזק את ההגנה שלו. תחום הסייבר גם נהנה מהשקעות אזרחיות, ומוסדות איראניים, כמו אוניברסיטת שריף, זוכים להערכה רבה.

האסטרטגיה ההגנתית של איראן מובלת על ידי הצורך לבנות חוסן כלכלי וטכנולוגי, וכן על ידי נחישותה לנטרל איומים פנימיים וחיצוניים. המשטר מכיר בחשיבות בנייתן של יכולות הגנה, לצד יכולות התקפה. בנוסף לכך, הוא משקיע מאמצים רבים ברכישת יכולות מעקב וניטור אחרי פעילות באינטרנט כדי להגן על עצמו, ומסתייע לשם כך בתוקפים מומחים מקרב השותפות הטבעיות שלו – סין, רוסיה וצפון קוריאה.

מניתוח מתקפות הסייבר האחרונות שיוחסו לאיראן עולה כי המשטר האיראני שם על הכוונת טווח רחב של אויבים, וביניהם מתנגדי משטר בתוך המדינה ומחוצה לה, שכנות קרובות כמו ישראל וערב הסעודית, ומדינות רחוקות כמו ארצות הברית ומדינות אירופה. איראן שיפרה את יכולות הסייבר שלה, גם אם לא ניתן עדיין להשוות אותן לאלו של ארצות הברית או ישראל. התקפות הסייבר של איראן הפכו ממוקדות יותר בשנתיים האחרונות. הן עושות שימוש במגוון רחב של כלים ושיטות, שתוכננו ובוצעו ברמה גבוהה של מקצועיות וסבלנות, ומאפשרים לה לגשר על הפערים הטכנולוגיים ולהגביר את היעילות. השאלה אם איראן הרוויחה או הפסידה ממאמציה ההתקפיים נגד יריביה החיצוניים מותנית במידת הקונצנזוס הפנימי, כאשר אינדיקטורים לו הם התשתית הלאומית וההגנתית והרטוריקה הציבורית.

גישת העמימות – כל גוני האפור

ראז'ה לזוביץ'

מטרתו של מאמר זה היא לעמוד על טיבם של העימותים המתרחשים ב"אזור האפור". המאמר מחולק לשלושה חלקים. החלק הראשון מתאר את "האזור האפור" ומגדיר את גישת העמימות הקשורה אליו. המאמר טוען כי המרכיבים הקריטיים של גישת העמימות הם השימוש באמצעים שאינם חוצים את סף המלחמה, בהדרגתיות בכפייה ובעמימות מכוונת; החלק השני דן בגישת העמימות כמשתנה תלוי, ומצביע על היעדר הכוח והיעדר הלגיטימיות לשימוש בכוח כמניעים העיקריים לאימוץ מדיניות של עמימות; החלק השלישי והאחרון בוחן כיצד שחקנים יכולים לשבש את ההערכה האסטרטגית של יריביהם באמצעות יצירת עמימות סביב מרכיבי מפתח במשחק: השחקנים עצמם, פעולותיהם, תוצאות של אינטראקציות והמידע הרלוונטי לקבלת החלטות.

מילות מפתח: אזור אפור, גישת העמימות, יריבות שאינה חוצה סף מלחמה, הדרגתיות בכפייה, עמימות אסטרטגית.

מהם "האזור האפור" וגישת העמימות

האתגרים האסטרטגיים של העת הנוכחית מטשטשים את ההבחנות הברורות והמקובלות שהיו עד כה בין המושגים מלחמה ושלום.[1] מתברר כי הכוח הצבאי אינו מספיק עוד כדי להתמודד עם אתגרי הביטחון האסימטריים העכשוויים, ובמקביל מתברר כי יכולתם של מקבלי ההחלטות להבין מהו הסף שחצייתו תוביל לעימות צבאי מלא נפגעת והופכת לבלתי מעשית.[2] התוצאה היא התפשטות התחרות הפראית בין מי שהם כמעט שווים ביכולותיהם לעבר מרחב מעורפל הנמצא

ראז'ה לזוביץ' עובד במשרד ההגנה של סרביה. הדעות המובאות במאמר זה הן של המחבר ואינן משקפות את הדעות או העמדות של ממשלת סרביה.

1 Nathan Freier and others, *Outplayed: Regaining Strategic Initiative in the Gray Zone* (Carlisle: SSI and US Army College Press, 2016).

2 Ben Connable, Jason H. Campbell and Dan Madden, *Stretching and Exploiting Thresholds for High-Order War: How Russia, China and Iran Are Eroding American*

בין מלחמה לשלום, מרחב המכונה "האזור האפור". שינויים מתמשכים בסביבה האסטרטגית הגלובלית יוצרים תנאים נוחים לעימותים באזור זה.

הן אלה המבקשים לאתגר את המצב הקיים והן אלה המעוניינים לשמור עליו תופסים את "האזור האפור" כמגרש משחקים ראוי שבו ניתן לבחון מחדש התחייבויות ולקיים תחרות גיאו־פוליטית, שכן הוא מאפשר להימנע מהסיכונים והמחירים של מלחמה כוללת.[3] ואכן, כמה מחקרים מעלים את האפשרות כי עימותים מהסוג הזה צפויים להפוך לצורת הלוחמה השלטת בין מדינות בשנים הקרובות.[4]

המאמר משתמש במונח "כוח הסטטוס קוו" ("status quo power") כדי לתאר את ארצות הברית, בעוד שהמונחים "רביזיוניסטים" ו"מאתגרי הסטטוס קוו" משמשים לתיאור מעצמות גלובליות מתעוררות או כאלו שחזרו למעמדן הקודם, כמו גם למדינות השואפות להגמוניה אזורית ואינן מרוצות מהַסדר העולמי הקיים ולהוטות לאתגר את כוחות הסטטוס קוו ברמה האזורית או הגלובלית.

עליונות הצבא האמריקאי מעודדת את הרביזיוניסטים לבחור ב"אזור האפור" כחלופה לזירה הצבאית המסורתית בתחרות הגיאו־פוליטית.[5] משחק לפי הכללים שנקבעו על ידי כוחות הסטטוס קוו אינו הדרך שבה הכוחות המאתגרים יוכלו לשנות את מאזן הכוחות הקיים. מבחינתו של הצד החלש, הרציונל העיקרי בהעתקת העימות ל"אזור האפור" הוא הרצון לשנות את כללי המשחק העומדים בבסיס הסדר העולמי הנוכחי, ולהשיג בדרך זו רמה של חופש פעולה. הרביזיוניסטים מבקשים לשחוק את כוח ההרתעה של הסטטוס קוו, לשתק את תהליך קבלת ההחלטות של המחזיקים בו וליצור דה־לגיטימציה לפעולותיו של היריב, וכל זאת כדי לאזן את הפערים ביחסי הכוחות.

כוח הסטטוס קוו נדרש להתמודד בו־זמנית עם שני איומים: האיום המציב אתגר של ממש לכללים שהגדירו את הסדר העולמי, והאיומים הנגרמים על רקע העולם שהסדר שלו הופר.[6] על ידי גרירת העימות ל"אזור האפור", כוח הסטטוס קוו שואף לשמר או לבנות מחדש את חופש הפעולה שלו, ובמקביל – לצמצם

Influence Using Time-Tested Measures Short of War (Santa Monica: RAND Corporation, 2016), https://www.rand.org/pubs/research_reports/RR1003.html.

3 USSOCOM, "The Gray Zone", *Public Intelligence*, May 15, 2016, https://info.publicintelligence.net/USSOCOM-GrayZones.pdf.

4 Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle: SSI and US Army War College Press, 2015); Hal Brands, "Paradoxes of the Gray Zone", *SSRN*, 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2737593.

5 Freier and others, *Outplayed: Regaining Strategic Initiative in the Gray Zone*.

6 Kevin D. Scott, "Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World", *Joint Chiefs of Staff*, July 14, 2016, https://www.jcs.mil/Doctrine/Joint-Concepts/JOE/.

את חופש הפעולה של הרביזיוניסטים. מהלך כזה יאפשר לכוחות הסטטוס קוו להיות מעורבים בתחרותיות שתתנהל מתחת לסף של עימות מזוין, תוך גיוס כל העוצמה הלאומית במגמה לשמור על היוזמה, להימנע ממאמץ יתר אסטרטגי ולחזק את ההרתעה.

אין שם מקובל למערכות המתנהלות ב"אזור האפור". במאמר זה נשתמש במונחים "גישת העמימות/מדיניות העמימות" או "עימות עמום" כדי לתאר תחרותיות שנשארת מתחת לסף של עימות מזוין ועושה שימוש באמצעים מעורפלים במתכוון שהם פחות ממלחמה, המיושמים בתחומים רבים, במטרה לערער, להחליש ולבצע דה־לגיטימציה ליריב, ובכך לקדם אינטרסים לאומיים או לעצב את הסביבה לקראת עימות עתידי. שלושה מושגים מרכזיים אלה המאפיינים את גישת העימות יידונו בהמשך מאמר זה.

ראשית, מדיניות העמימות עושה שימוש משולב באמצעים שמתחת לסף המלחמה כדי ליצור מערכה מגובשת. אמצעים כאלה כוללים כל פעולה עוינת, אלימה או לא אלימה, שמפעילים שחקנים זה נגד זה כדי להשיג יעדים אסטרטגיים ולשמור עליהם מבלי להיכנס למלחמה של ממש. ג'ורג' קֶינן (Kennan) חילק את סוגי הפעולות האלו לשתי קטגוריות כלליות: אמצעי הסתגלות ואמצעי לחץ.[7] בעוד שאמצעי ההסתגלות הם כולם חלק מהרפרטואר הדיפלומטי הרחב, אמצעי הלחץ חורגים מהנוהג הרגיל והמקובל ביחסים בין מדינות. אמצעי לחץ יכולים ללבוש צורות רבות, לרבות הפחדה, חתרנות, לוחמה פסיכולוגית, לחץ כלכלי, ניסיון להשפיע על בחירות, תמיכה באופוזיציה פוליטית, פעילות סייבר התקפית, שימוש בשליחים (proxies), חיסול ממוקד ועוד. חשוב להדגיש כי מדיניות של עמימות מחייבת שילוב של כל האמצעים האלה לכדי מערכה מגובשת, כדי שניתן יהיה להשיג אפקט אסטרטגי מצטבר.[8] אחרת, סביר להניח כי הם ישיגו יעדים טקטיים בלבד.

שנית, מדיניות העמימות נועדה לערער, להחליש ולבצע דה־לגיטימציה הדרגתית של היריב, ובדרך זו ליצור תנאים נוחים לעימותים עתידיים, כשהמאמץ נועד להשיג יעדים שישמרו על האינטרס הלאומי ויקדמו אותו. הדרגתיות בכפייה היא סוג של תוקפנות, שבה השחקן חותר להשיג את האינטרסים שלו בשלבים, במקום במהלך של מתקפת פתע אחת נגד מדינה אחרת והאינטרסים שלה. שחקנים המיישמים הדרגתיות בכפייה לאורך זמן מפעילים כלים שונים שעומדים לרשות המדינה, תוך שהם מנצלים את ההשפעה ההדרגתית שיש למעשים המצטברים כדי לבנות

7 George Kennan, Giles Harlow and George Maerz, *Measures Short of War* (Washington DC: National Defense University Press, 1991), p. 3.

8 Ibid., p. 16.

תמונה אסטרטגית חדשה.[9] דוגמאות בנות זמננו להדרגתיות בכפייה הן "שיטת הסלמי" או "קביעת עובדות מוגמרות".[10]

תומס שֶלינג (Schelling) מציין כי הרעיון המרכזי של "שיטת הסלמי" הוא שרוב ההתחייבויות הן מעורפלות. הדבר מאפשר לשחקנים לאתגר את רצינות ההתחייבות של היריב באמצעות טקטיקות של שחיקה. האתגור יהיה בדרך כלל ברמה נמוכה או מעורפלת מספיק כדי שלא יהיה צורך לחצות את הסף של היריב. אם היריב אינו מגיב למהלך, השחקן יעשה את הצעד הבא, ובסופו של דבר ישיג שינוי משמעותי בסטטוס קוו באמצעות לחץ מצטבר קבוע.[11] התפיסה הסינית של "שלוש מלחמות" ויישומה בים סין הדרומי הם דוגמה אופיינית ל"שיטת הסלמי". הסינים מבקשים להשיג תוצאה אסטרטגית מבלי לעורר תגובה אלימה, ועושים זאת על ידי הפעלת לחץ מצטבר קבוע על פני תחומים שונים לאורך זמן.

מנגד, שחקן יכול ליישם גישה של "עובדה מוגמרת". במקרה כזה סביר להניח שיזכה ברווח חד־צדדי מוגבל לפני שמישהו יספיק להגיב, ויכריח את היריב לבחור בין ויתור ובין תגובה מסלימה.[12] דניאל אלטמן מציין כי מילות המפתח במקרה זה הן "מוגבל" ו"חד־צדדי": ראשית, הרווח צריך להיות קטן מספיק כדי שלא להצית עימות צבאי גלוי; שנית, "עובדה מוגמרת", מעצם הגדרתה, היא פעולה חד־צדדית היוצרת מציאות חדשה בשטח.[13] בשלב זה ההרתעה כבר נכשלה, וליריב אין דרך לחזור לסטטוס קוו אנטה מבלי להסלים את הסכסוך.

הן "שיטת הסלמי" והן שיטת "העובדה המוגמרת" בגרסתה המוגבלת עלולות לגלוש להסלמה בלתי מבוקרת, ובסופו של דבר למלחמה כוללת. עם זאת, במקרה שבו לתוקפן יש שליטה על ההסלמה המקומית, ההחלטה להסלים תהיה מורכבת יותר עבור המדינה המותקפת.[14] סיפוח חצי האי קרים על ידי רוסיה הוא הדוגמה הקלאסית ל"עובדה מוגמרת" הלכה למעשה.[15]

---

9 William G. Pierce, Douglas G. Douds and Michael A. Marra, "Understanding Coercive Gradualism", *Parameters* 45, no. 3 (2015): 51.

10 Mazarr, *Mastering the Gray Zone.*

11 Thomas C. Schelling, *Arms and Influence* (Westport, Greenwood Press, 1977), pp. 66-69.

12 Daniel W. Altman, "Red Lines and Faits Accomplis in Interstate Coercion and Crisis" (PhD diss., Massachusetts Institute of Technology, 2015), https://dspace.mit.edu/bitstream/handle/1721.1/99775/927329080-MIT.pdf?sequence=1.

13 James J. Wirtz, "Life in the Gray Zone: Observations for Contemporary Strategists", *Defense & Security Analysis* 33, no. 2 (2017): 108.

14 Alexander Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe", *International Affairs* 92, no. 1 (2016): 189.

15 Steven Metz, "In Ukraine, Russia Reveals Its Mastery of Unrestricted Warfare", *World Politics Review*, April 16, 2014, http://www.worldpoliticsreview.com/articles/13708/in-ukraine-russia-reveals-its-mastery-of-unrestricted-warfare.

לבסוף, ערפול מכוון הוא מאפיין מרכזי של גישת העמימות. למרות שכל עימות מתאפיין מטבעו באי־ודאות, מערכות המתקיימות ב"אזור האפור" נועדו להיות מעורפלות במתכוון כדי לשבש את החישובים האסטרטגיים של היריב ולשתק את תהליך קבלת ההחלטות שלו. עמימות אסטרטגית אינה רעיון חדש; מטרתה העיקרית היא ליצור חוסר ודאות במעשים ובאמונות (ובאמונות על האמונות) של אחרים.[16] העמימות האסטרטגית נשענת על הרעיון שהשחקן שומר במכוון על מדיניות לא ברורה, כדי ליצור איזון בין האינטרסים השונים שלו ולהשאיר את כל האופציות פתוחות.[17] המטרה היא לאלץ את היריב, בבואו לשקול את שיקוליו האסטרטגיים, לקחת בחשבון שקיימת אי־ודאות לגבי כוונותיו, יכולותיו ופעולותיו האפשריות של השחקן. המחיר הגבוה של הערכה שגויה ירתיע את היריב מלנקוט פעולה.

המדיניות של ארצות הברית כלפי טייוואן ומדיניות הנשק הגרעיני של ישראל הן דוגמאות אופייניות לעמימות אסטרטגית. השימוש בערפול מכוון בגישת העמימות מתאים להיגיון זה. פעולותיו של הצד התוקפן מעורפלות במתכוון כדי להסתיר את מקור האיום, את כוונת התוקפן או את המוטיבציה שלו.[18] אירן היא רב האומן במשחק זה; חולשתה הקריטית בזירה הקונבנציונלית הביאה אותה לפתח את "דוקטרינת המוזאיקה", שנועדה להתמודד עם יריבים חזקים ממנה ולהגדיל את מרחב הלוחמה שלה מעֵבר לתחום המסורתי של עימות מלא.[19] בהיותה נתונה ללחץ מתמיד, אירן מבינה שההגנה הטובה ביותר שלה טמונה "ביצירת דילמות מרובות למתנגדיה".[20] שימוש אסטרטגי חדשני בעמימות הוא הגורם המכריע שמאפשר לשמור סכסוך מתחת לסף ההסלמה ולהבטיח את הדה־לגיטימציה של שימוש בכוח צבאי מצד היריב, ובכך להימנע מעימות ישיר.[21]

---

16 Stephen Morris and Hyun Song Shin, "Measuring Strategic Uncertainty", *ResearchGate,* July 2002, https://www.researchgate.net/publication/228609097_Measuring_strategic_uncertainty.

17 Brett Benson and Emerson Niou, "Comprehending Strategic Ambiguity: US Policy toward the Taiwan Strait Security Issue", *ResearchGate*, April 2000, https://www.researchgate.net/profile/Brett_Benson2/publication/229051924_Comprehending_strategic_ambiguity_US_policy_toward_the_Taiwan_Strait_security_issue/links/0f31752fcbf8ac873c000000.pdf.

18 Freier and others, *Outplayed: Regaining Strategic Initiative in the Gray Zone.*

19 Anthony H. Cordesman and Abdullah Toukan, "Analyzing the Impact of Preventive Strikes Against Iran's Nuclear Facilities", *Center for Strategic and International Studies*, September 6, 2012, https://csis.org/files/publication/120906_Iran_US_Preventive_Strikes.pdf.

20 Freier and others, *Outplayed: Regaining Strategic Initiative in the Gray Zone.*

21 Erik Reichborn-Kjennerud and Patrick Cullen, "What is Hybrid Warfare?", *NUPI Policy Brief* 1, 2016, https://nupi.brage.unit.no/nupi-xmlui/handle/11250/2380867.

מדוע עימותים מגיעים ל"אזור האפור"?

חלק זה של המאמר יבחן את גישת העמימות כמשתנה תלוי, כמו למשל היותה תוצאה של אינטראקציה אסטרטגית בין שחקנים. כדי לנתח מדוע עימותים בני זמננו מסתיימים ב"אזור האפור", עלינו לזהות את התמריצים העיקריים לאימוץ מדיניות של עמימות ואת התנאים להצלחתה. נראה כי התמריצים המרכזיים לניהול סכסוכים ב"אזור האפור" הם היעדר כוח והיעדר לגיטימיות להשתמש בכוח אלים.

עימותים אלימים היו חלק מחיי האנושות משחר ימי ההיסטוריה המתועדת.[22] בעוד שטבעם של העימותים נותר ללא שינוי, אופיים עבר שינויים רבים בהתאם לסביבה האסטרטגית.[23] מלחמת צללים הייתה חלק מהרצף מלחמה–שלום מאז ימי קדם, ועימותים ב"אזור האפור" גם הם אינם סוג חדש של מלחמה.[24] עם זאת, ניתן לומר שהסביבה האסטרטגית העכשווית תורמת יותר מבעבר ליכולת ליזום עימותים מסוג זה ולהתמיד בהם.

ארצות הברית נהנתה לאחר סיום המלחמה הקרה מסביבה נוחה שלא אתגרה את עוצמתה.[25] היא שאפה לשמור על עליונותה הטכנולוגית ולהגדיל את רשת הבריתות והשותפויות הגלובליות שלה כדי לשמור על יתרונה מול מתחרים פוטנציאליים דומים לה. עם זאת, המשבר הכלכלי בשנת 2008 והמלחמות הבלתי מוכרעות בעיראק ובאפגניסטן דחפו את ארצות הברית למתוח את עצמה כמעט מעֵבר ליכולותיה. כוחה הלך והתפזר מול תהליך הגלובליזציה, עד כדי שיֵש הסבורים שהיא נמצאת בשקיעה יחסית, במקביל לעלייתם של כוחות אחרים. עם זאת, לדברי ג'וזף ניי (Nye), תפיסה זו אינה מדויקת ואף מטעה, שכן ארצות הברית תישאר חזקה מספיק כדי לעצב את עתיד העולם.

למרות הנאמר, כוח הוא "משאב סכום אפס", ואפילו התפיסה של דעיכת כוחות הסטטוס קוו די בה כדי לתמרץ רביזיוניסטים לאתגר את הַסדר הקיים, במיוחד ברמה האזורית.[26] סין, רוסיה ואיראן מאזנות באופן פעיל את ארצות הברית. למרות שכל אחת מהן משתמשת ב"אזור האפור" בצורה שונה, יש להן כמה מאפייני התנהגות משותפים. כך, למשל, הן מבקשות ליצור לעצמן את היכולת לשלוט בהסלמות מקומיות; הן מרחיבות באופן יזום את מרחב ההשפעה שלהן על ידי

22 Henry Kissinger, *World Order: Reflections on the Character of Nations and the Course of History* (London: Penguin, 2015), p. 331.

23 Freier and others, *Outplayed: Regaining Strategic Initiative in the Gray Zone*.

24 US Department of State, International Security Advisory Board, "Report on Gray Zone Conflict", June 30, 2017, https://2009-2017.state.gov/t/avc/isab/266650.htm.

25 Thomas J. Wright, *All Measures Short of War: The Contest for the Twenty-First Century and the Future of American Power* (Yale University Press, 2017), p. 4.

26 Lawrence Freedman, "A Subversive on a Hill", *National Interest*, no. 101 (2009): 46.

התמקדות במדינות חלשות; הן מנצלות קשרים היסטוריים וחברתיים עם המדינות המסומנות על ידן כיעד, וזאת כדי ליצור לגיטימציה למעשיהן.[27] המאמץ העיקרי של הכוחות הרביזיוניסטיים הוא לשחוק את אמינותם של כוחות הסטטוס קוו ולהעמיד למבחן את התחייבותם לספק הרתעה מורחבת לבעלות הברית ולשותפות שלהם. אם הרביזיוניסטים יצליחו לשנות את שיווי המשקל ברמה האזורית, הסדר העולמי הליברלי לא יוכל להמשיך להתקיים במתכונתו הנוכחית.[28] העליונות הצבאית של ארצות הברית מאלצת את הכוחות המאתגרים למצוא דרך אחרת כדי להשיג את יעדיהם – כזו שלא תחשוף אותם לפעולת תגמול ישירה מצידם של כוחות הסטטוס קוו. "האזור האפור" מאפשר לאותם גורמים מאתגרים לעקוף את האסימטריה בכוחות ולשוב ולקחת חלק בתחרות הגיאו־פוליטית המוכרת.[29]

חיוניות הסדר הבין־לאומי תלויה באיזון הרגיש בין כוח ללגיטימציה.[30] המשפט והנורמות הבין־לאומיים מגבילים את השימוש בכוח כדרך לפתרון סכסוכים. בנוסף, כוחות צבא כבר אינם מסוגלים להשיג "ניצחון מכריע" בסכסוכים אסימטריים בני ימינו, בין היתר בגלל היעדר מטרות צבאיות לגיטימיות. לאמיתו של דבר, התוצאות נטולות ההכרעה של מערכות צבאיות והנזק שנגרם לנפגעים חפים מפשע הפחיתו עוד יותר מהלגיטימיות שיש להפעלת כוח אלים. מרבית העימותים הללו מוכיחים את העובדה שכוח צבאי אינו מספיק עוד כדי להשיג יעדים פוליטיים בני קיימא. אם כוחות הסטטוס קוו ימשיכו להפעיל כוח ללא לגיטימציה, הדבר יחזק את ההתנגדות בתוך המערכת, יעודד אחרים לנהוג בצורה דומה ויפגע בסמכותם של אותם כוחות. מצד שני, אם הכוחות הרביזיוניסטיים יורשו לעשות שימוש בכוח צבאי מבלי שייענשו על כך, הדבר יערער את האמינות של המערכת הבין־לאומית ושל כוחות הסטטוס קוו גם יחד. עימותים עמומים מטשטשים במתכוון את ההבחנה בין פעולות חוקיות ובלתי חוקיות ומאפשרים לשחקנים להמשיך בתחרות ביניהם מבלי להצית עימות צבאי ישיר.

היעדר הלגיטימיות לשימוש בכוח מספק תמריצים לשחק ב"אזור האפור" לא רק לרביזיוניסטים; ישראל היא כוח סטטוס קוו אזורי, עם עליונות צבאית מוחצת באזור. עם זאת, יכולתה להשתמש בכוח היא מוגבלת בשל הלגיטימיות החלשה שלה לעשות כן. מול איומים היברידיים ייחודיים והאשמות בלתי פוסקות של שימוש מופרז בכוח, אין לישראל ברירה אלא להילחם במתנגדיה ב"אזור האפור". דוקטרינת "המערכה בין מלחמות" שאימצה נועדה להאריך את פרקי הזמן בין מלחמות באמצעות מאמץ מתמיד להחלשת האויב ופגיעה ביכולתו להתחזק,

27 Lanoszka, "Russian Hybrid Warfare".
28 Wright, *All Measures Short of War*, p. 34.
29 Wirtz, "Life in the Gray Zone", p. 111.
30 Kissinger, *World Order*, p. 66.

יצירת תנאים אופטימליים למלחמה הבאה ובניית לגיטימציה לפעולה ישראלית במקביל לצמצום הלגיטימיות של האויב.[31]

ברמה הגלובלית, ארצות הברית היא בעלת ניסיון רב כשחקנית משמעותית בעימותים המגיעים עד פחות מסף המלחמה.[32] מאז תפיסת השליטה באזור תעלת פנמה ועד סוף המלחמה הקרה, הוכיחה ארצות הברית שהיא מתחרה מובילה במשחק זה. עם זאת, לאחר הניצחון במלחמה הקרה נראה היה כי ארצות הברית מאבדת עניין בפעילות אסטרטגית ב"אזור האפור". כמעצמת־על יחידה, הדרך הפשוטה יותר למימוש האינטרסים האמריקאיים הייתה השימוש החד־צדדי בכוח צבאי. מנגד, התערבויות צבאיות חד־צדדיות פגעו בלגיטימיות של ארצות הברית והעניקו לכוחות המאתגרים אותה תירוץ לאמץ שיטות דומות ברמה האזורית.

ארצות הברית היא כוח סטטוס קוו עולמי, ולכן חיוני שתצליח לשמור על האיזון הנכון בין כוח ובין לגיטימציה, מכיוון שיש לה אינטרס מושקע שהַסדר העולמי הליברלי יישמר באופן יציב ואיתן.[33] כדי להחזיר את האמון בסדר עולמי המונהג על ידי ארצות הברית, וושינגטון צריכה להרגיע את בעלות בריתה ושותפותיה האזוריות כי היא תגן עליהן מפני איומים עמומים.[34] מנגד, יש הסבורים כי ארצות הברית צריכה להישען יותר על הכוח שיש לה כדי לכפות את רצונה על הכוחות הרביזיוניסטיים, אך מבלי להצית עימות מזוין גלוי. לשיטתם, האמצעים היעילים ביותר שאינם חוצים את סף המלחמה הם סנקציות כלכליות ומסחריות, אמברגו צבאי, מניפולציות בשוק האנרגיה, פעילויות סייבר התקפיות, הפעלת שליטה בים ותמיכה באופוזיציה פוליטית במדינות עוינות.[35]

הסביבה האסטרטגית הנוכחית

תנאי הכרחי לגיבוש אסטרטגיה נכונה הוא הבנה מעמיקה של הסביבה האסטרטגית.[36] התנאים הטכנולוגיים, הכלכליים והחברתיים הנוכחיים יוצרים סביבה המעודדת עימותים שאינם מגיעים לכלל מלחמה.

---

31 "Deterring Terror: How Israel Confronts the Next Generation of Threats", Belfer Center Special Report (Cambridge: Belfer Center for Science and International Affairs, 2016), (במקור: **אסטרטגיית צה"ל**, לשכת הרמטכ"ל, 13 באוגוסט 2015).

32 Freier and others, *Outplayed: Regaining Strategic Initiative in the Gray Zone*.

33 Wright, *All Measures Short of War*, p. 188.

34 Ibid., p. 197.

35 David C. Gompert and Hans Binnendijk, *The Power to Coerce, Countering Adversaries Without Going to War* (Santa Monica: RAND Corporation, 2016), https://doi.org/10.7249/RR1000.

36 Timothy L. Thomas, "China's Concept of Military Strategy", *Parameters* 44, no. 4 (2014): 42.

ההבדל המכריע בתפיסת הלוחמה של ימינו הוא הפוטנציאל ההרסני של הנשק הגרעיני.[37] מכיוון שמלחמה כוללת כבר אינה אפשרות רציונלית, שחקנים מדינתיים מנצלים חלופות אחרות, כגון מלחמה קונבנציונלית מוגבלת, מלחמה תת־קונבנציונלית, שימוש בכוח ללא מלחמה ואיום להשתמש בכוח.[38] עם זאת, אף אחת מהאפשרויות הללו לא יכולה לשלול לחלוטין את הסיכון שיש בה להסלמה לא מכוונת שתגלוש עד כדי עימות גרעיני. ארצות הברית כופה אמצעים רחבי היקף, לרבות אמברגו על נשק וטכנולוגיה, כדי לא לאפשר תפוצת נשק להשמדה המונית ולמנוע ממדינות סוררות גישה לטכנולוגיה צבאית מתקדמת. אדרבא, מדינות הנמצאות בתהליך של הפיכתן למעצמות גלובליות, או מעצמות לשעבר החוזרות למעמדן, ממתנות את הסיכון להסלמה בלתי מבוקרת של עימותים עמומים על ידי הדגשת נכונותן להשתמש בנשק גרעיני כדי להגן על האינטרסים שלהן.[39] בנוסף לכך, מעצמות החותרות לעליונות אזורית מבקשות לפתח נשק גרעיני ואמצעי שיגור כדרך להגן על עצמן מפני התערבות צבאית מצידם של כוחות הסטטוס קוו.[40]

בעידן המהפכה הטכנולוגית הרביעית, כוחות הסטטוס קוו צריכים לשמור על מעמדם המוביל במרוץ לעליונות טכנולוגית. הכוחות המאתגרים אותם מבקשים לגשר על הפער הטכנולוגי ביניהם באמצעות רכישת נשק "משַנה כללי משחק", כגון יכולות התקפה בליסטיות ומדויקות, מערכות מניעת גישה/חדירה לשטח (A2AD), נשק אנטי־לווייני (ASAT), נשק אנרגיה מכוּונת (Directed Energy) ונשק אנטי־לווייני קינטי. למרות שבעימותים עמומים הממד הלא קינטי הוא השליט, לכוח צבאי אמין יש עדיין תפקיד משמעותי, הן עבור כוחות הסטטוס־קוו והן עבור הכוחות הרביזיוניסטיים. הגורמים המאתגרים חייבים להשיג דומיננטיות צבאית מקומית כדי להרתיע את כוחות הסטטוס קוו מפני התערבות צבאית.[41] מנגד, על כוחות הסטטוס קוו להפגין נכונות להשתמש בכוח צבאי כדי שאסטרטגיית ההשפעה שלהם תִפעל.

התפתחות טכנולוגיית המידע מאפשרת כיום לצד התוקפן לשלוט בסיכון של הסלמה בלתי מבוקרת, להשפיע ברמה חסרת תקדים על דעת הקהל במדינה המותקפת ולנצל את מרחב הסייבר הפתוח לכל. הן ארצות הברית והן הכוחות הרביזיוניסטיים מקדישים תשומת לב רבה להשפעה על העמדות, ההתנהגות וההחלטות של היריב, ועושים זאת דרך ערוצי תקשורת שונים. קמפיינים של מידע

37 Schelling, *Arms and Influence*, p. 21.
38 Jasjit Singh, "Dynamics of Limited War", *Strategic Analysis* 24, no. 7 (2000):1208.
39 Andrew Monaghan, "The 'War' in Russia's Hybrid Warfare", *Parameters* 45, no. 4 (2015): 69.
40 Scott, "Joint Operating Environment 2035".
41 Lanoszka, "Russian Hybrid Warfare", p. 189.

ממלאים תפקיד מכריע בעימותים עמומים ומשמשים כמכפיל כוח עבור אמצעים שהם פחות ממלחמה.[42] לארצות הברית יש רשת תקשורת גלובלית, המאפשרת לה להפיץ את הנרטיב שלה כדי לגייס בעלות ברית ולבודד יריבים. לעומת זאת, הכוחות הרביזיוניסטיים נוקטים גישה אחרת; הם משקיעים מאמצים ומשאבים ניכרים בזריעת בלבול, בהסחת דעת, בפילוג ובדמורליזציה בקרב יריביהם, תוך שהם חוסמים זרימת מידע חיצוני אליהם.[43] מטרתם היא לשחוק את דומיננטיות המידע ולהרתיע את כוחות הסטטוס קוו מפני התערבות, וזאת באמצעות יצירת דה־לגיטימציה לשימוש בכוח ברוטלי. מצב כזה מאפשר לרביזיוניסטים לנהל "מלחמת נרטיבים" עם כוחות הסטטוס קוו.

ארצות הברית היא בעלת יתרון מבני ניכר בעולם הסייבר.[44] כמעצמת סייבר, יש לה יכולות ללא תחרות לנטר, להגן ולנהל פעילויות התקפיות במרחב הסייבר. עם זאת, לוחמת סייבר כוללת אינה אופציה מבחינתה, מכיוון שהיא לא תצא ממנה כמנצחת.[45] האינטרס הגדול ביותר של ארצות הברית הוא לשמור על אינטרנט חופשי ופתוח. סין ורוסיה אינן מרוצות מהתפקיד הדומיננטי של ארצות הברית במרחב הסייבר, והן נוקטות גישות שונות כדי לאזן את היתרון האמריקאי במרחב זה. רוסיה פיתחה תשתית אינטרנט לאומית המסוגלת לבודד את עצמה מהתנועה התקשורתית החיצונית, ואילו סין אימצה שורה של אמצעים טכנולוגיים וחקיקתיים, המכונים "חומת האש הגדולה של סין", במטרה לפקח על הגישה לאינטרנט בתוך המדינה.

הן כוחות הסטטוס קוו והן הכוחות הרביזיוניסטיים בוחנים את האפשרות לפעולות סייבר התקפיות כדרך לנצל את נקודות התורפה של יריביהם, התלויים תלות הולכת וגוברת במחשבים. מרחב הסייבר מציע הזדמנויות זולות יחסית להוציא לפועל פעולות התקפיות אנונימיות, כמו ריגול, חבלה וחתרנות.[46] חוסר היכולת לייחס את הפעולה לתוקף מסוים הוא מאפיין מכריע של הפעילות החשאית במרחב הסייבר. הוא מאפשר לתוקפים יכולת הכחשה סבירה, שהיא חיונית כדי להימנע מפעולת תגמול. למרות שהאנונימיות מועילה לאלה המבקשים לחצות קווים אדומים, היא יכולה להוות גם חיסרון, שכן פעולת כפייה מחייבת חשיפת

42 Rod Thornton, "The Changing Nature of Modern Warfare: Responding to Russian Information Warfare", *RUSI Journal* 160, no. 4 (2015): 40.

43 Scott, "Joint Operating Environment 2035".

44 Wright, *All Measures Short of War*, p. 147.

45 Gompert and Binnendijk, "The Power to Coerce".

46 Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies* 35, no. 1 (2012): 27.

הייחוס. כדי להשיג יעדים פוליטיים, יש לוודא שפעולות הסייבר ישולבו עם אמצעים אחרים שהם פחות ממלחמה, ויתבססו על רציונל אסטרטגי אחד ויחיד.[47]

הגלובליזציה הכלכלית יצרה סביבה של תלות הדדית, המעודדת את השחקנים להשתמש בכלים כלכליים ופיננסיים למטרות כפייה. המוסדות המערביים הסדירו את הפיקוח על הפיננסים והסחר העולמי מאז תום מלחמת העולם השנייה, והדולר האמריקאי הוא מטבע העתודות של העולם. דבר זה מאפשר לכוחות הסטטוס קוו להשתמש באמצעים כלכליים ופיננסיים, דוגמת מניפולציות על השוק, מלחמות סחר וסנקציות, כדרך להפעלת לחצים גיאו־פוליטיים. ההשפעות של הסנקציות הכלכליות והפוליטיות שמטילה ארצות הברית על הרביזיוניסטים תלויות ביכולתה של וושינגטון לשכנע מדינות נוספות לכבד את הסנקציות הללו, אלא שהתיאום עם אותן מדינות הוא לעיתים תהליך איטי ומסובך. ידוע כי הכוחות הרביזיוניסטיים משקיעים מאמצים ניכרים ליצירת פילוג בין ארצות הברית ובין בעלות בריתה ושותפותיה, כדי לצמצם את השפעת הסנקציות. מעֵבר לכך, הגלובליזציה העלתה את התלות ההדדית הכלכלית בין המדינות לרמה יוצאת דופן. רייט סבור שהתלות ההדדית מרסנת את התוקפנים, ובמקביל מגבילה את התגובות האפשריות נגדם.[48] קשה יהיה להטיל סנקציות כלכליות ומסחריות על סין, מכיוון שהיא ממלאת תפקיד קריטי בכלכלה העולמית. מאותה סיבה ממש, מלחמת סחר בין ארצות הברית לסין עלולה לפגוע בשתי המדינות כאחת ולסכן את יציבותה של הכלכלה העולמית.

הפגיעוּת של הכלכלה העולמית וקיומם של שחקנים רבי־עוצמה בעלי אינטרסים מנוגדים מגבירים את ההזדמנות לאינטראקציות עוינות.[49] הרביזיוניסטים מפתחים מערכת מכשירים כלכליים משלהם כדי שיוכלו לכפות על יריבים ולהרתיע את כוחות הסטטוס קוו מפני הטלת סנקציות.[50] החלשת הרגולציה הפיננסית והמשבר הכלכלי העולמי של שנת 2008 הביאו למשבר אמון במודל הכלכלי המערבי ונתנו הזדמנות למעצמות כלכליות עולות לקדם מוסדות חלופיים, כמו הבנק האסייתי להשקעה בתשתיות.[51] בנוסף לכך, סין מקדמת באופן פעיל את מטבע הרֶנְמִינְבִּי כחלופה אזורית לדולר, ובדרך זו מבקשת לצמצם את יכולתה של ארצות הברית

47 Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth", *Quarterly Journal: International Security* 38, no. 2 (2013): 57.

48 Wright, *All Measures Short of War*, p. 143.

49 Jeffry A. Frieden, David A. Lake and Kenneth A. Schultz, *World Politics: Interests, Interactions, Institutions* (New York: W. W. Norton, 2009), p. 529.

50 Wright, *All Measures Short of War*, p. 145.

51 John Baylis, Steve Smith and Patricia Owens, eds., *The Globalization of World Politics: An Introduction to International Relations*, 6th edition (Oxford and New York: Oxford University Press, 2013), p. 525.

לנצל את הדולר האמריקאי להפעלת לחץ.[52] סין מציעה להשקיע בשווקים זרים ללא תנאים פוליטיים מוקדמים, דבר מושך מאוד עבור מדינות רבות. התוצאה היא השקעות סיניות מעבר לים שמגבירות את ההשפעה הגלובלית של סין.

מבחינה חברתית, ההשפעה הגוברת של דעת הקהל על קבלת ההחלטות הפוליטיות מספקת מוטיבציה נוספת לעשות שימוש במדיניות העמימות. בסביבת מידע המתקבל כמעט בזמן אמת, דעת הקהל המקומית הופכת למשתתפת ישירה בעימותים צבאיים המתרחשים במדינות זרות. החברה המערבית פיתחה ציפיות לא מציאותיות מכל עימות. דרישת הציבור לכמעט אפס נפגעים והשמירה הקפדנית על זכויות אדם יוצרות כללי התנהגות במלחמה, שהופכים ליותר ויותר מורכבים. במקביל, הנוכחות התקשורתית המתמדת יוצרת לחץ נוסף. "המלחמה המתמשכת בטרור" והמעורבות הצבאית היקרה והבלתי מוכרעת בעיראק, באפגניסטן ובלוב ערערו את האמון של הציבור המערבי ופגעו בנכונותו לתמוך במלחמות מעבר לים. בנסיבות שנוצרו, ארצות הברית תוכל לשלב פעילויות לא צבאיות עם פעולות צבאיות במאמץ להשיב לידיה את היוזמה ב"אזור האפור". יחד עם זאת, לתרבות האסטרטגית יש השפעה על האופן שבו הצדדים יחליטו לפעול במצבי עימות. לפיכך, גם אם יש לארצות הברית פוטנציאל עצום להצליח ב"אזור האפור", היבטים מסוימים בתרבות האסטרטגית האמריקאית אינם עולים בקנה אחד עם רעיון העימות העמום, ולכן ארצות הברית נוטה להשתמש באמצעים שהם על סף מלחמה ברמה הטקטית בלבד.[53] סטיבן מץ (Metz) גורס כי ארצות הברית מעדיפה מצבים נטולי עמימות פוליטית, בהם היא יכולה להשתמש בכוחה הצבאי האולטימטיבי, בתמיכה של בעלות בריתה.

לעומת ארצות הברית, התרבות האסטרטגית הסינית, וכן האיראנית, דוגלות בהימנעות מסכסוכים צבאיים מלאים שלא לצורך.[54] במקום זאת, כל אימת שהדבר ניתן, סין ואיראן מעדיפות גישה מתוחכמת ועקיפה יותר. גם לתרבות האסטרטגית הרוסית יש מסורת ארוכה של פעילויות חתרניות והיסטוריה מוכחת של תיאום וביצוע פעילויות כאלו ברמה האסטרטגית.[55] בסיכומו של דבר, התרבויות האסטרטגיות של סין, רוסיה ואיראן מספקות בסיס איתן לפיתוח גישה של עמימות לעימותים המתרחשים ב"אזור האפור".

---

52 Wright, *All Measures Short of War*, p. 145.

53 Connable, Campbell and Madden, "Stretching and Exploiting Thresholds for High-Order War".

54 Mazarr, *Mastering the Gray Zone*.

55 Randal G. Bowdish, "Military Strategy: Theory and Concepts" (PhD diss. University of Nebraska, Lincoln, 2013), http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1026&context=poliscitheses.

מניפולציות על תפיסת הסיכון של היריב

ערפול מכָוון הוא מאפיין המייחד את גישת העמימות. יריבות שנשמרת מתחת לרף של עימות צבאי היא משחק רב־פנים, שנועד ליצור כמה שיותר אי־ודאות אצל היריב.[56] שחקנים במגרש זה יכולים לייצר עמימות סביב ארבעה מרכיבים מרכזיים של האינטראקציה המתקיימת בעימותים: (1) השחקנים המעורבים בעימות; (2) פעולותיהם; (3) התוצאות האפשריות; (4) המידע העומד לרשות השחקנים.

העמימות ביחס לזהות השחקנים נועדה להסתיר את מקור האיום. היכולת של התוקפן להסתיר את זהותו או להכחיש מעורבות היא חלק מכריע בגישת העמימות.[57] אם הצד התוקף יצליח להישאר סמוי, לא יהיה לצד המותקף יעד לפעולת התגמול שלו. התוקפן הלא מזוהה גם יוכל לחמוק מעונש או מסנקציות מצד כוחות הסטטוס קוו על הפרתו את הנורמות והכללים הבין־לאומיים. שחקנים יכולים לערפל את חלקם בעימות באמצעות שימוש בשליחים (proxies), בסוכנויות או בארגונים אזרחיים, או באמצעות פעולות סמויות, לרבות פעולות סייבר התקפיות. בחלק מהמקרים יצליח התוקף להסתיר את זהותו זמן מספיק, שיאפשר לו להעמיד את הצד המותקף בפני "עובדה מוגמרת". באופן דומה, מידת ההכחשה הסבירה שהתוקפן יידרש לה תלויה בהקשר המסוים, ויהיו מקרים שאי־הבהירות לגבי זהות התוקף תהיה חיונית כדי לאפשר ליריב לשמור על כבודו.

יש מטרה כפולה ליצירת עמימות ביחס למעשיו של התוקף: לחמוק מקווים אדומים שהציב המותקף ולהקשות על זיהוי, ייחוס או הגדרה פומבית של פעולות התוקף כמי שהפעיל כוח כפייה. מדיניות של עמימות נועדה לפגוע באסטרטגיית ההרתעה של היריב.[58] המנגנון שבבסיס ההרתעה הוא המניפולציה הנעשית על שיקולי עלות–סיכון של היריב,[59] דבר המחייב הצבת סף לתגובה צבאית. סף כזה אינו קיים במציאות האובייקטיבית, אלא במוחם של מקבלי ההחלטות.[60] משום כך, מרכז הכובד של המערכה ליצירת ערפול שייך לעולם המידע והפסיכולוגיה.

לתוקפן יש שתי אפשרויות עיקריות לעקוף את הקווים האדומים של היריב: ראשית, הוא יכול למתוח את הסף על ידי העמָדה למבחן של התחייבות היריב לתגובה והתקדמות הדרגתית בקנה מידה קטן מכדי לגרות תגובה.[61] ההיגיון הוא

56 Mazarr, *Mastering the Gray Zone*.

57 Frans-Paul van der Putten, Minke Meijnders and Jan Rood, *Deterrence as a Security Concept against Non-Traditional Threats* (The Hague: Cingendael, 2015).

58 Wirtz, "Life in the Gray Zone", p. 107.

59 Van der Putten, Meijnders and Rood, *Deterrence as a Security Concept.*

60 Forrest E. Morgan and others, *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica: RAND Corporation, 2008), p. 11.

61 Connable, Campbell and Madden, "Stretching and Exploiting Thresholds for High-Order War".

פשוט; אם התוקף ייענה בתגובה, הוא תמיד יוכל להעמיד פנים שהפעולה הייתה בלתי מכוונת או בלתי מורשית, אבל אם המותקף ייכשל באכיפת הסף אליו התחייב, המשמעות היא שהסף זז והתוקפן יכול לעבור לשלב הבא.[62] המטרה היא לשחוק את ההרתעה של היריב, תוך הימנעות מחצייה בוטה של הקווים האדומים.

האפשרות השנייה היא לנצל נקודות תורפה בסף שקבע היריב, כמו למשל אי־רצון שלו להשתמש בכוח אלים או מיסקלקולציה שלו לגבי הסף.[63] אולם, גישה כזו מתאימה רק במקרים שבהם הקו האדום סובל מנקודות תורפה, כמו שרירותיות, חוסר דיוק, חוסר יכולת לאמת אותו או היותו בלתי שלם.[64] ניצול הסף בצורה כזו מחייב הבנה מעמיקה של נקודות התורפה שלו. כפי שאיראן הפגינה בהצלחה בעיראק, כאשר חותרים להשגת יעדים אסטרטגיים, ניתן לשלב גם מתיחת הסף וגם שימוש בקווים האדומים.[65]

מטרה מרכזית נוספת ביצירת עמימות היא להקשות על היכולת לסווג את הכוונה שמאחורי מעשי התוקף כרצון להתעמת עם היריב או להשית עליו כפייה. הדרך היעילה ביותר ליצור עמימות מסוג זה היא לדאוג לכך שמכלול האמצעים שהם פחות ממלחמה ישולב ויגויס למטרה אחת ותחת רציונל אסטרטגי אחד. שחקנים בעלי כוח ריכוזי יצליחו טוב יותר לשלב את כל אמצעי הכוח של המדינה ביצירת עימות שאינו חוצה את הסף של מלחמה קונבנציונלית.[66] תיאום אפקטיבי של האמצעים שהם פחות מסף מלחמה יאפשר לתוקף להוציא לפועל פעולות בממדים שונים (צבאיים ולא צבאיים), וכך לטשטש את פעולותיו וכוונותיו ולצמצם את הסיכון לפעולת תגמול אלימה.

בדומה למתרחש במלחמות המסורתיות, גם כאן הסלמה אנכית כרוכה בעלייה בעוצמת הפעולה.[67] עם זאת, יש להדגיש כי הסלמה אנכית בעימותים עמומים תנסה לא לחצות את "נקודת השיא של הכפייה".[68] מנגד, הסלמה אופקית בעימותם עמומים כרוכה בסנכרון ההשפעה שיש לאלמנטים צבאיים ולא צבאיים העומדים לרשות המדינה.[69] בהתחשב בכך שתפיסת היריב היא מרכז הכובד של מדיניות

62 Schelling, *Arms and Influence*, pp. 67-69.
63 Connable, Campbell and Madden, "Stretching and Exploiting Thresholds for High-Order War".
64 Altman, "Red Lines and Faits Accomplis in Interstate Coercion and Crisis".
65 Connable, Campbell and Madden, "Stretching and Exploiting Thresholds for High-Order War".
66 Thornton, "The Changing Nature of Modern Warfare: Responding to Russian Information Warfare", pp. 40-48.
67 Morgan and others, *Dangerous Thresholds*.
68 Dmitry (Dima) Adamsky, "From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture", *Journal of Strategic Studies* 41, no. 1-2 (2018): 56.
69 Reichborn-Kjennerud and Cullen, "What is Hybrid Warfare?"

העמימות, ממד המידע ממלא את התפקיד הדומיננטי ביותר. גישת העמימות מנצלת את כל הממדים של הסלמת הסכסוך ב"אזור האפור", מעמידה למבחן זהיר את התחייבויותיו של היריב ומנצלת נקודות תורפה בסף שהציב כדי להשיג את האפקט האסטרטגי הרצוי. הרמן קאהן (Kahn) מכנה את השילוב של הסלמה אנכית ואופקית בשם "הסלמה מורכבת".[70]

האפשרות להסלמה לא מכוונת של עימות המתרחש ב"אזור האפור" לכדי מלחמה בהיקף מלא קיימת תמיד, במיוחד בהתחשב בכך שהתוקפן חייב להכיל את הסכסוך מבחינה גיאוגרפית, תוך מניעת התערבות חיצונית. עם זאת, אם המדינה המותקפת מוכנה להסתכן בעימות צבאי, התוקפן יתקשה לשלוט בהסלמה, ללא קשר לדומיננטיות הצבאית המקומית שלו.[71]

התחום הבא שבו שחקנים יכולים לייצר עמימות מכוונת הוא במערך התוצאות האפשריות. פעולה עמומה שתוכננה היטב אמורה לאפשר ליריב להתעלם מתוצאת פעולתו של שחקן, בין אם משום שהיריב רוצה "לשמור על כבודו" ובין משום שהוא לא מודע להשלכות מסוימות. כמו כן, שחקן יכול לנצל את העובדה שהתגמול שיקושר לפגיעות שספג היריב יכול להיות רב־ממדי, אך הדבר מחייב היכרות מעמיקה עם התרבות האסטרטגית של היריב. במקרה כזה, מערכת כפייה חוצת־תחומים תוכל להשפיע על רצונו של היריב ועל בחירותיו ולמנוע הסלמה לא מכוונת. ככלל, פעולות עמומות מרחיבות את מערך התוצאות האפשריות של העימות. שחקן יכול להסתיר את התוצאה אליה כיוון או להימנע מלחשוף את גבולות כוונותיו. בשני המקרים, המטרה היא להקשות על החישובים האסטרטגיים של היריב.

היכולת לעצב את האופן שבו היריב תופס את הסביבה האסטרטגית היא משתנה קריטי כשמדובר בעימותים ב"אזור האפור": מידע מעורפל ישפיע על האסרטיביות ויכולת התגובה של היריב. חוסר בהירות לגבי העובדות ייצור בלבול עמוק לגבי הסיכונים וישבש את חישוביו האסטרטגיים של היריב.[72] כאשר מקבלי ההחלטות עומדים בפני איום עמום, הם נוטים "להתעלם ולהפחית ממידת הסיכון ולנקוט גישה של 'נמתין ונראה'".[73] גם אם הם מודעים לאופי האיום, חוסר הבהירות לגבי סף הסיכון של התוקפן והחשש מהסלמה עשויים להוביל אותם לבחור בחוסר מעש על פני פעולה. שיתוק החלטות כתוצאה ממידע עמום יכול להיות קטלני

70 Herman Kahn, *On Escalation: Metaphors and Scenarios* (New Brunswick: Routledge, 2009), pp. 4-6.

71 Jan Angstrom and Magnus Petersson, "Weak Party Escalation: An Underestimated Strategy for Small States?", *Journal of Strategic Studies* 42, no. 2 (2019): 282-300.

72 Freier and others, *Outplayed: Regaining Strategic Initiative in the Gray Zone*.

73 Michael Roberto, Richard M. J. Bohmer and Amy C. Edmondson, "Facing Ambiguous Threats", *Harvard Business Review*, November 1, 2006.

מבחינה אסטרטגית. מדיניות העמימות מיועדת לזרוע בלבול סביב אחד או יותר מהאלמנטים שתוארו לעיל, וזאת בהתאם להקשר הרחב ולנסיבות הספציפיות.

סיכום ומסקנות

לוחמה שמתנהלת ב"אזור האפור" פועלת על פי ההיגיון של גישת העמימות. המאמר ביקש לטעון כי גישת העמימות מתבססת על שלושה מרכיבים חיוניים: ראשית, סנכרון ותיאום בין כל האמצעים האסטרטגיים שאינם חוצים את סף המלחמה; שנית, חשיפה של האינטרסים של מדינות אחרות להדרגתיות בכפייה; ושלישית, עימותים ב"אזור האפור" המתוכננים במתכוון לשמור על ערפול.

היעדר הסימטריה בין כוחה של ארצות הברית לזה של יריבותיה המתקרבות לרמתה, בשילוב עם הירידה בלגיטימיות של שימוש בכוח אלים ביחסים הבין־לאומיים, מַספקים תמריצים משמעותיים לשחקנים השונים להעתיק את העימות ל"אזור האפור". במקביל, היכולת של השחקנים לפעול ב"אזור האפור" גוברת בזכות ההתקדמות הטכנולוגית, הגלובליזציה הכלכלית והתנאים החברתיים השוררים כיום.

ניתן ליצור עמימות מכוונת סביב הצדדים לעימות, פעולותיהם, התוצאות האפשריות והמידע שיהיה ליריב. ההשפעה המצטברת של העמימות המכוונת היא שיבוש תהליך קבלת ההחלטות של היריב ויצירת הזדמנות לשחקן כלשהו למתוח או לנצל את הקווים האדומים שקבע היריב, תוך מניעת היכולת לייחס את הפעילות אל אותו השחקן ואי־חצייתּ הסף שיביא את היריב לנקוט תגובה הצבאית.

מדיניות של עמימות מאפשרת לשחקנים לעצב את תפיסת הסיכון של היריב ואת התיאבון שלו לסיכונים. עם זאת, עימותים ב"אזור האפור", כמו כל שאר העימותים, נותרים דיאלקטיקה של רצונות מנוגדים, העלולים לעורר הסלמה בלתי נשלטת עד כדי מלחמה כוללת או תוצאות בלתי רצויות אחרות. בין אם תהיה זו הערכה שגויה או בחירה אסטרטגית רציונלית של אחד הצדדים, התוצאה יכולה להיות הסלמה שתוציא את העימות מ"האזור האפור".

ביטחון סייבר וביטחון מידע: מודרניזציה של מבנה הכוח בצבא הסיני

מירנדה באס

מאז 2012 מבצעת סין בראשות הנשיא שי ג'ינפינג מהלכים שימצבו אותה כמעצמה עולמית. בין המהלכים – מודרניזציה גורפת של "צבא השחרור העממי" (PLA) של סין, במטרה להופכו לצבא בעל יכולת הקרנת כוח. בולט במיוחד המהלך שנעשה ב־2015 להקמת "כוח התמיכה האסטרטגי" כחיל נפרד המרכז תחתיו את כל הכוחות המבצעיים האחראים על לוויינים ורשתות, לרבות הכוחות העוסקים במבצעי סייבר, לכדי ארגון אחד רב־סמכויות. ההחלטה המדינית לארגן מחדש את מבנה הכוח של הצבא הסיני משקפת את המקום שתופסים מבצעי המידע בביטחון הלאומי של סין, שרובם המכריע מתרחשים במרחב הסייבר, ומחזקת אותם.

מילות מפתח: סין, צבא, סייבר, מבנה הצבא, מודרניזציה, מבצעי מידע, ביטחון לאומי

מבוא

כל צבא נדרש להתפתח במקביל להתפתחויות הטכנולוגיות הצבאיות וליעדים האסטרטגיים והפוליטיים של החברה שבה הוא פועל. הצבא הסיני, ובשמו המלא "צבא השחרור העממי" (PLA), נולד כזרוע צבאית של המפלגה הקומוניסטית של סין. מאז ועד היום הוא נותר צבאה של המפלגה ולא עשה את המעבר לצבא של מדינה. מאמציו הראשונים של הצבא הסיני לעבור מודרניזציה החלו תחת מנהיגותו של דנג שיאופינג בשנת 1979, כחלק מתנועת "הרפורמה והפתיחות" הכלל־חברתית שהנהיג הנשיא ובעקבות ההפסד הכואב במלחמת סין–וייטנאם. עליית מעמדה של סין למעצמה גלובלית בעשרים השנים האחרונות הביאה גם את צבאה לחתור לשינוי, ובמסגרת זו להפוך מצבא המושתת על מגויסים בלבד

סגן משנה מירנדה באס (Bass), צבא היבשה של ארצות הברית, היא תלמידה לתואר מ.א. באוניברסיטת תל אביב.

ועל יכולת נמוכה והתמקדות פנימית, לכוח אזורי אדיר ממדים. תחת הנהגתו של הנשיא שי ג'ינפינג, שנכנס לתפקידו בשנת 2012, הואצו קידום מעמדה הגלובלי של סין וקידום המודרניזציה של צבאה – שתי מטרות הכרוכות זו בזו.

חלק בלתי נפרד מהמיקוד ומהיכולות של צבא הוא מבנה הכוח שלו, שגם הוא מתפתח עם תהליך המודרניזציה. מבנה הכוח הוא היבט מהותי בהרכב הצבא, אך גם תחום מאתגר כאשר מנסים להכניס לתוכו מערכות חדשות, וזאת בעיקר בשל התנגדות ביורוקרטית. לפיכך, כל התפתחות בתחום זה מחייבת מאמץ ייעודי ומחויבות ארוכת טווח בדרגים הגבוהים ביותר.

מאז תחילת המאה ה־21, ובמיוחד בחמש השנים האחרונות, נקטו הצבא הסיני וממשלת סין צעדים משמעותיים כדי לגבש ולמסד מדיניות סייבר מקיפה. מהלכים אלה הגיעו לשיאם בשנת 2015 במודרניזציה בהיקף נרחב במבנה הכוח הצבאי, לרבות ארגון מחדש מלא של כוחות הצבא המעורבים בפעילות סייבר. הדחף העיקרי לארגון מחדש היה הקמת "כוח התמיכה האסטרטגי" (SSF) ב־31 בדצמבר 2015. מאמר זה מפרט את השינויים שחלו בצבא הסיני ומתאר כיצד ההחלטה על הקמת "כוח התמיכה האסטרטגי" קשורה קשר הדוק למטרותיה של סין במרחב הסייבר וניהול המידע.

מרחב הסייבר, מתקפות סייבר והגנת סייבר

מרחב הסייבר הוא מונח קשה מאוד להגדרה מדויקת, בגלל השימוש המגוון שנעשה בו בשיח העכשווי. התפיסה הרווחת מקשרת בין מרחב הסייבר ובין האלקטרוניקה. זוהי אמנם תפיסה נכונה, אבל אינה מבטאת את התמונה במלואה. הגדרה מועילה של מרחב הסייבר מנקודת מבט ביטחונית תתבסס על מרכיביו, שהם שלוש שכבות המונחות זו על גבי זו: השִכבה הפיזית, השכבה התחבירית והשכבה הסמנטית.[1] כדי שמרחב הסייבר יתקיים כשלם, עליו לכלול את כל שלוש השכבות; בהיעדר אחת מהן המערכת כולה צפויה להיעלם, אם כי באופן זמני בלבד.

השכבה הפיזית של מרחב הסייבר מורכבת מהתשתית המוחשית של המדיום, ובכלל זה הכבלים והקופסאות עמוסות האלקטרוניקה שמצויים פיזית באתרים שונים בעולם. מנקודת מבט ביטחונית, הבולטות של מרכיבי השכבה הפיזית מהווה יעד פוטנציאלי לתקיפה של היריב, המסוגל בדרך זו לפגוע ביכולתם של אנשים ומכונות לפעול במרחב הסייבר. השכבה התחבירית אינה גלויה, וכוללת את המחשבים והפרוטוקולים המאפשרים את כלל החילופים והפעולות במרחב הסייבר. שכבה זו היא הממלכה שבה מתרחשת האינטראקציה בין מחשבים, כולל ניתוב ומיתוג. מרבית הפריצות – שהן אינטראקציה במרחב הסייבר שבמהלכה

1 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), p. 39.

צד אחד משלים פעולה לתועלתו האישית באמצעות הסטת נתיבים קיימים לרעת צדדים אחרים – מתרחשות ברמה התחבירית.

השכבה הסמנטית מכילה את הרוב המכריע של הנתונים והממשקים שהמשתמש הטיפוסי נוטה לראותם כמרחב הסייבר, וזאת עקב היותם קיימים בנפרד מהעולם המציאותי (אם כי לעיתים קרובות בסמוך אליו). שלא כמו השכבה התחבירית, השכבה הסמנטית מתבטאת בעיקר בשפה אנושית טבעית.

הגדרת עבודה זו של מרחב הסייבר מאפשרת לפנות לטיפול בתופעת הפריצה (hacking), שהיא ניצול הנתיבים של המדיום למטרות אחרות מהמטרות הייעודיות שלהם. המטרה הנפוצה של פריצה היא גניבת נתונים, בדרך כלל ממחשב של משתמש או ממערכת של אחרים.[2] מבחינה אבטחתית, פעילויות אלו במרחב הסייבר מכונות "ניצול רשת מחשבים" (CNE) ויכולות להתרחש בין כל סוגי השחקנים. מדינה עשויה (ולעיתים קרובות אף עושה זאת) לגנוב נתונים מארגון, מאדם או ממדינה אחרת למען מטרותיה הלאומיות; תאגידים גונבים קניין רוחני האחד מהשני; אנשים גונבים נתונים מישויות שונות כחלק מגניבת זהות, ממניעים אידיאולוגיים, או לכל מטרה אחרת.

כדי לדון בהשלכות של "ניצול רשת מחשבים" על מבנה הכוח הממשלתי והצבאי, רצוי לרכוש הבנה בסיסית במתווה הכללי של "ניצול רשת המחשבים". בשונה מגניבת אובייקט מוחשי כמו משגר טילים, גניבת נתונים היא מעשה לא תחרותי (non-rivalrous), כלומר עצם גניבת הנתונים אינה משפיעה על יכולת השימוש בהם, וייתכן שאלה העוסקים בניטור המערכת המארחת את הנתונים כלל לא יידעו שהגניבה התרחשה.[3] "ניצול רשת מחשבים" מתחיל בכך שהגורם הפורץ מקבל גישה בלתי מורשית למערכת היעד ומשתלט על הרשאות ורמת גישה של משתמש או של מנהל באותה מערכת. בהמשך ינסה הפורץ לגנוב את הנתונים המבוקשים, תוך שהוא חומק מלהיחשף כדי להבטיח את סיכויי ההצלחה הגבוהים ביותר. אופייה הלא תחרותי של תופעת "ניצול רשת מחשבים" מגביר את סיכויו של הפורץ להשיג את מטרותיו.

"ניצול רשת מחשבים" הוא למעשה פעולת ריגול, שקודם להתפתחות מרחב הסייבר מדינות נהגו לא לראות בה צעד מלחמתי. למעשה, "ניצול רשת מחשבים" אינו מונע מהמשתמש את השימוש המלא בציוד שלו, ולמעט אובדן המידע, המשתמש אינו סופג נזק ממשי. יתר על כן, דיני המלחמה אינם מכירים בריגול כעילה למלחמה (קאזוס בֶּלי), קרי כסיבה מספקת לפתוח במלחמה.[4]

2 Ibid., p. 14.
3 Ibid., p. 15.
4 Ibid., pp. 23-24.

מתקפת סייבר דומה בדרך כלל ל"ניצול רשת מחשבים" בשלבים המוקדמים שלה, וזאת בגלל אופי הפעילות במרחב הסייבר; עם זאת, יש לה מטרה שונה: במתקפת סייבר התוקף (בדרך כלל מדינה) מבקש במתכוון להפריע או להשחית מערכת חשובה של מדינה אחרת. בדומה ל"ניצול רשת מחשבים", לאחר שהצד התוקף משיג את ההרשאות הנדרשות, הוא ממשיך להתקדם לעֵבר שיבוש המערכת עד שזו לא תתַפקד כראוי, ובכך גורם להשלכות דרסטיות, ברורות ומיידיות. הוא גם עשוי לפעול להשחתת המערכת בדרכים מתוחכמות ואפילו בלתי מורגשות, שאפשר שישפיעו אחרי זמן מה או שיתרחשו בגלים.[5]

במקביל למתקפות סייבר צמחה הגנת הסייבר, אם כי בצורה פחות בולטת, כפי שקורה לא פעם כשעולם הביטחון עוסק בשאלות של הגנה. מטרתה של הגנת הסייבר היא להפוך את המערכת לעמידה ככל האפשר בפני חדירה בלתי רצויה מכל סוג שהוא, בין אם מדובר ב"ניצול רשת מחשבים" או במתקפת סייבר. מנהלי מערכות עושים מאמצים רבים כדי להשיג דרגת אבטחה גבוהה למערכת, אך מצב זה אינו המצב הרצוי מבחינתם של המשתמשים בה. הבעיה הקלאסית של אבטחה במרחב הסייבר היא עיסקת החליפין בין אבטחה ובין נגישות. מערכות מרושתות נועדו להקל על המשתמשים את הפעולה והאינטראקציה עם מחשבים אחרים ועם האינטרנט. הפתיחות ההכרחית, בשילוב עם התפיסה והתכנון המקוריים של האינטרנט כמרחב נטול גבולות וכמעט ללא אמצעי אבטחה, יצרו מצב שבו הגנות סייבר הפכו לחיסרון.

מדינות הן לא השחקניות היחידות המשתתפות במתקפות סייבר או בהגנות סייבר, אך מדינות שמשקיעות רבות בתחום זה הן, ללא ספק, השחקניות מהסוג המתוחכם ביותר, וזאת הודות לגודלן, למשאביהן ולמטרות שהן מבקשות לקדם. היכולות של ביטחון סייבר ברמה הלאומית כוללות את היכולת לתקוף, להתגונן ולהוציא לפועל פעולות ריגול. יכולות אלו שונות מאוד ממדינה למדינה, בהתאם לעדיפות שהממשלה המקומית נתנה לפיתוח הכלים החדשים.

על אף שהמדינות העשירות הן המתקדמות ביותר ביכולותיהן (כפי שהן מתקדמות בחידושים טכנולוגיים אחרים), פעולות סייבר מצריכות פרדיגמה שונה מזו שפותחה עבור מה שהיה החידוש ההיסטורי הגדול האחרון בטכנולוגיה הצבאית – הטכנולוגיה הגרעינית. בניגוד להתפתחות הטכנולוגיה הגרעינית, שהייתה יקרה מאין כמותה לרובן המכריע של המדינות, ובוודאי עבור שחקנים לא מדינתיים, יכולות הסייבר נגישות עד מאוד לכל שחקן, כולל אנשים פרטיים. בשל המשאבים האדירים והיעדים המורכבים יחסית של מדינות, הן אלו שמחזיקות ביכולות הסייבר המתוחכמות ביותר, אבל התחום בכללותו כבר אינו מוגבל למדינות העשירות בלבד. אפילו מדינות עניות, כמו צפון קוריאה, מצליחות לצבור השפעה

5 Ibid., pp. 15-16.

מעבר לגודלן היחסי. במצבים קיצוניים, גם שחקנים לא מדינתיים עשויים לפעול באופן עצמאי ואפקטיבי.

מרחב הסייבר אינו רק טכנולוגיה. זהו כלי בידי המשתמשים בו. כלומר, מקור האיום אינו במחשב, אלא באנשים שמתכננים ומפעילים את המחשב.[6] גם כיום, מרחב הסייבר מזכיר עדיין את המערב האמריקאי הישן, דהיינו מקום רחב ידיים, לא ממופה, עם עמימות תרבותית ומשפטית, קשה לניווט, ובאופן כללי פתוח לראשון שישתלט עליו.[7] סביבה כזו היא קרקע פורייה לחדשנות בכל הקשור לאופן שבו יעוצב העולם, לקביעה מי יהיו השחקנים והקטגוריות בעלי הכוח, לצורה שבה התקשורת צריכה להיראות, לשאלה מהי אמת ומה המשמעות של חירות. למרות או בגלל אפשרויות אלו, מרחב הסייבר נותר עדיין השתקפות של העולם הרחב – זה שאינו סייבר – ושל יחסי הכוחות בו.

תרומתו העיקרית של מרחב הסייבר למבנה הכוח ולחלוקתו היא הנמכת סף הכניסה בפני שחקן המבקש להשיג רלוונטיות ברמה הגלובלית – ואין זה חידוש של מה בכך. בנוסף להנמכת סף הכניסה, שחקנים במרחב הסייבר נהנים מחוסר הרלוונטיות הכמעט מוחלט של המרחק, ממהירויות רשת המתקרבות למהירות האור ומהקושי הגובר לייחס בוודאות פעולה מסוימת לשחקן מסוים. תכונה פחות אינטואיטיבית של מרחב הסייבר היא שכמעט בלתי אפשרי לדעת מי יהיו העדים לאירוע נתון, היכן ומתי הם עשויים לראות אותו, או כיצד הם עשויים לפרשו.[8]

קטגוריות של עוצמת סייבר בביטחון הלאומי

ישנם כמה סוגים של עוצמת סייבר בתפיסה הביטחונית הלאומית.[9] הסוג הנפוץ ביותר הוא עוצמת סייבר פרודוקטיבית, כלומר בניית שיח במרחב הסייבר הכוללת גם את חיזוק השיח הקיים וגם המצאה והפצה של שיח חדש. למרחב הסייבר תרומה ייחודית לשיח ולהגברתו בזכות החסמים המזעריים שהוא מציב. עוצמת סייבר **מבנית** היא היכולת לשמור על מבני כוח קיימים ולאפשר לשחקנים לפעול בתוך מבנים אלה, או לחילופין להגבילם. עוצמת סייבר מבנית נוטה לכיוון האנרכי, במיוחד כשהיא מאפשרת לביקורת סרקסטית ומרושעת ולטינה לשגשג ולהכפיל את עצמן.

עוצמת סייבר **ממוסדת** היא השליטה במרחב הסייבר באמצעות מוסדות, כמו "תאגיד האינטרנט להקצאת מספרים ושמות" (ICANN) – עמותה אמריקאית ללא מטרות רווח, האחראית על ניהול מאגרים של כתובות שמיות ומספריות

6 David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power* (London: International Institute for Strategic Studies, 2011), p. 13.

7 Ibid., p. 14.

8 Ibid., p. 40.

9 Ibid., pp. 45-50.

באינטרנט. סוג כזה של עוצמת סייבר מתרחב גם למוסדות בלתי פורמליים, כלומר לנורמות הנבנות על ידי התנהגות השחקנים במרחב הסייבר ומשפיעות עליהם.

הסוג המצומצם ביותר של עוצמת סייבר הוא עוצמת סייבר **כופה**. סוג זה כולל "ניצול רשת מחשבים" ומתקפות שנועדו לשלוט בהתנהגות של מחשב או של רשת ולמנוע משחקן לפעול במרחב הסייבר, ועוד.

כל סוגי עוצמות הסייבר הללו רלוונטיים לצבא, שהוא גוף מרכזי, אם כי בהחלט לא היחיד, המעורב בפעולות ובמדיניות הקשורות לביטחון הסייבר הלאומי של המדינה. הַקשר בין צבא ובין עוצמת סייבר כופה הוא מובן מאליו, מכיוון שברוב המקרים הצבא הוא זה שמוציא את הכפייה אל הפועל. הַקשר בין צבא ובין עוצמת סייבר מבנית הוא בכך שעוצמת סייבר מבנית מרחיבה את אפשרויות האיום של מי שהם בעיקר שחקנים מדינתיים, אך גם שחקנים לא מדינתיים המאורגנים ומיומנים ברמה גבוהה ביותר, לעבר צמתים מרושתים יחידים שחסמי הכניסה אליהם נמוכים. כלומר, מרחב הסייבר מצמצם את המגבלות הקיימות על מבני הכוח הקיימים בכל מה שנוגע לשאלה מי מהשחקנים יהיה בעל גישה לאינטראקציות גלובליות בעלות השפעה. גם עוצמת סייבר ממוסדת רלוונטית לכוח הצבאי, במיוחד כשהנורמות לפעולות צבאיות במרחב הסייבר עדיין נמצאות בשלב של כתיבה. לפיכך, צבא המבקש לגבש את כללי המשחק כך שיפעלו לטובתו (וזה המצב בכל מדינה שיש לה יכולת או שאיפה להשפעה בין־לאומית), יבקש להרחיב את עוצמת הסייבר המבנית שלו ושל המדינה בכלל. עוצמת סייבר פרודוקטיבית היא ייחודית יותר, בכך שהיא קושרת את המרחב הצבאי של המלחמה לממד הפוליטי שלה ומאפשרת לשחקן לעצב את השיח לפי היתרון האסטרטגי שלו. למרות שמדובר במקרה זה בהשפעה של המרחב הפוליטי ולא הצבאי, ארגונים צבאיים עדיין יכולים לבצע פעולות ברוח זו וגם להתעצב על פיהן.

ההגדרה המסורתית של קלאוזביץ קובעת שמטרת המלחמה היא לגרום לקריסת האויב, כלומר להשארת היריב במצב של חוסר אונים. על סמך הבנה זו, עוצמת סייבר היא מכפיל כוח, אך אינה מהווה תחליף לעוצמה פיזית.[10] אמנם, כשמתייחסים אל המלחמה לפי תפיסת "העוצמה הרכה" בהתאם למודל של ג'וזף ניי (Nye), מטרת העימות היא שכנוע, ואז עוצמת הסייבר יכולה להיות גורם אסטרטגי מכריע. אלא שהגדרה כזאת אינה מועילה ביותר: עוצמת סייבר היא מרכיב משלים ליכולות אחרות, קינטיות יותר, ולמרות שהיא צוברת מעמד של גורם משלים קריטי, היא עדיין לא מבטלת את החשיבות של היכולות הקינטיות ולא משנה את אופייה של המלחמה. מה שעוצמת הסייבר עושה, ובצורה משמעותית, הוא לתת נשק בידי אלה שמבחינה היסטורית היו חלשים צבאית ופוליטית.

10 Ibid., p. 86.

במאות השנים האחרונות שמר המערב על כוחו הצבאי והפוליטי באמצעות מעגל חוזר של התרחבות כלכלית ופוליטית. עם זאת, מאז הדה־קולוניזציה, עוצמתו הצבאית של המערב והשימוש שלו בנשק קינטי השיגו תוצאות פחות אפקטיביות ומכריעות. כדי להתמודד עם מצב זה, מדינות המערב החלו לשנות את הטקטיקה שלהן ולנצל את כוח המשיכה של הרעיונות, ברוח "העוצמה הרכה" של ניי, כשיטה שרשמה הצלחות.[11] מציאות זו הביאה לכך ששחקנים המתנגדים להגמוניה המערבית, ובמיוחד משטרים לא ליברליים, תופסים כיום את האינטרנט החופשי ואת השיח והמידע שבו כסכין המונחת על צווארם.[12] זו גם הסיבה לכך שמשטרים סמכותניים ובעלי מערכת פוליטית לא ליברלית רואים את שליטתם בזרימת הרעיונות ככורח של הביטחון הלאומי. אף גורם מדיני מוביל לא הבין זאת טוב יותר ולא היטיב לפעול בהתאם לכך יותר מאשר המפלגה הקומוניסטית של סין, בעיקר משום שהיא התפתחה מתוך מערכת טוטליטרית בעיצומן של תהפוכות המאה העשרים, וכן בשל דבקותה מאז הקמתה בטהרנות אידיאולוגית ובהשלטת השיח המרקסיסטי.

השאלה כיצד מפלגת השלטון בסין החלה לשלוט באינטרנט, במרחב הסייבר ובמידע בכללותו היא מעֵבר לגבולות הדיון של מאמר זה. נציין רק כי מפלגת השלטון הסינית רואה בפוטנציאל של האינטרנט מנוע להתפתחות כלכלית, כלי המסייע ליצירה ולהפצה של תרבות, פלטפורמה ל"ממשל חברתי", הן על ידי שיפור זכויות הפרט והן על ידי הקלת השליטה הממשלתית, וטריטוריה המחייבת השלטת הריבונות הלאומית, בדיוק כשם שהיבשה, הים, השמיים והחלל מחייבים זאת.[13] לצד היתרונות, המפלגה רואה בחדירת הסייבר איום על הביטחון הפוליטי של סין – שלתפיסתה הוא חיוני להתפתחות הלאומית ולאושרו של העם הסיני – בשל גרימתו לתסיסה חברתית. לפי תפיסה מפלגתית זו, מתקפות סייבר מאיימות על הביטחון הכלכלי, וכל מידע המאיים על התרבות המסורתית הוא מידע מזיק.[14]

להלן יוסבר מבנה הכוחות המבצעיים של הצבא הסיני בתחום הסייבר והמידע, ובעיקר פרויקט המודרניזציה של הצבא שהחל ב־2015. בנוסף לכך, יובהר תפקידה של המודרניזציה בעיצוב מחדש של אותם כוחות וכיצד השינוי במבנה הכוח תומך ביעדים הצבאיים של המפלגה הקומוניסטית הסינית.

לפני הדיון בצד הטכני של ארגון הצבא, חשוב להבין את התפיסה הסינית לגבי ביטחון סייבר, שכמו דברים רבים נוספים בחשיבה הסינית, שונה מההבנה

11 Ibid., p. 132.

12 Ibid.

13 Office of the Central Cyberspace Affairs Commission, "Guo jia wang luo kong jian an quan zhan lue", *Zhongguo Wangxinwang*, December 27, 2016, http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.

14 Ibid.

המערבית הרווחת. הרעיון המערבי של ביטחון סייבר נקרא בסין "ביטחון רשת". רעיון זה חוסה תחת הרעיון הסיני הרחב יותר של "ביטחון מידע", המתמקד בעיקר בניהול תוכן. המשמעות היא שצנזורה ושליטה בהפצת מידע הן חלק מהשכבה הסמנטית של מרחב הסייבר ולא חלק מאבטחת הרשת או משמירה על שלמות הרשת עצמה.[15] מי שעמד בשעתו בראש הארגון שניסח את המסמך הראשון של סין בנושא מדיניות ביטחון הסייבר טען כי ביטחון מידע "הכרחי ליציבות חברתית ולפיתוח תרבותי ואידיאולוגי סוציאליסטי".[16] מילים אלו אינן רטוריקה ריקה; הן הבסיס לתפיסת הביטחון הלאומי של מפלגת השלטון בסין, ובעיקר לתפיסתה מהו ביטחון מרחב הסייבר.

אינפורמטיזציה בצבא הסיני

"אינפורמטיזציה" (Informationization) היא התרגום הקרוב ביותר למונח הסיני *xinxihua* 信息化, שהוא עיקרון מנחה במודרניזציה של הצבא הסיני ובהפיכתו מצבא איכרים המכוון פנימה לצבא בעל יכולת להקרין כוח כלפי חוץ. אם יש חברה אזרחית בסין, הרי שהיא קיימת באינטרנט.[17] עצם נוכחותה מהווה איום קריטי על היציבות הפנימית בסין, שלפי מפלגת השלטון נשענת על היעדר מוחלט של התנגדות לשלטון או של חוסר שביעות רצון ממנו.

מדיניות הסייבר הסינית החלה להתגבש בתחילת המאה ה־21 בעזרת שני ארגונים – "הארגון הראשי למידע ממלכתי" (SILG) ו"לשכת המידע של מועצת המדינה" – שעסקו לפני כן בביטחון מידע. החלק החשוב ביותר במסמך מדיניות הסייבר הסינית הוא חוות הדעת של "הארגון הראשי למידע ממלכתי" משנת 2003, המכונה "מסמך 27", שניסחה לראשונה את מדיניות ביטחון הסייבר של סין במונחים הגנתיים.[18] סבך ביורוקרטי צפוף של משרדים ומוסדות היה אחראי בעשור שלאחר מכן להיבטים השונים של גיבושה וניהולה של מדיניות ביטחון הסייבר הסינית. בתקופה זו נעצרה ההתקדמות בנושא, שכן תשומת ליבה של ממשלת סין הוסטה אז לעדיפויות אחרות, ובראשן ההיערכות לאולימפיאדת בייג'ינג ב־2008, ואחר כך למשבר הכלכלי העולמי שפרץ באותה שנה.

---

15 Jon R. Lindsay, "Introduction – China and Cybersecurity: Controversy and Context", in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (Oxford: Oxford University Press, 2015), p. 11.

16 Qu Weizhi, *China's Path to Informationization*, cited in Jon R. Lindsay, "Introduction – China and Cybersecurity: Controversy and Context", *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, p. 11.

17 Ibid., p. 1.

18 Ibid., p. 8.

בשנת 2012 נכנס שי ג'ינפינג לתפקידו כנשיא, ומפלגת השלטון החלה לפעול להגברת השליטה בחברה הסינית ולצמצום הפתיחות החברתית, במקביל לשאיפה להפוך למעצמה עולמית מובילה. מיד עם כניסתו לתפקיד החל הנשיא שי לארגן מחדש את משרדי הממשלה על פי סדר העדיפויות החדש של המדיניות הסינית, ובמסגרת זו הפך בשנת 2014 "הארגון הראשי למידע ממלכתי" ל"ארגון הראשי לביטחון סייבר ואינפורמטיזציה" (CILG). שי עצמו עמד בראש הארגון, והוא עדיין ממשיך להוביל אותו ביחד עם אישים בכירים ורמי דרג נוספים במפלגה. תוצאה ישירה מכך היא מתן עדיפות גבוהה ביותר לסוגיות הנוגעות למדיניות האינפורמטיזציה בצבא הסיני.

הדוקטרינה הצבאית של הצבא הסיני נוטה כיום להיות התקפית ברמה המבצעית (לרבות מכות מנע), אך הגנתית ברמה האסטרטגית־פוליטית.[19] מבחינה פונקציונלית, משמעותה של דוקטרינה זו היא שכוחות הסייבר של הצבא הסיני הם פעילים ואגרסיביים מאוד, שכן הם מעורבים במבצעי סייבר המתקרבים עד לסף של מלחמה. ואכן, הדוקטרינה הספציפית של סין לפעולות סייבר מדגישה את חשיבות המכה הראשונה בכל עימות מזוין באמצעות מתקפות סייבר, שמטרתן היא שיתוק מערכות הפיקוד והלוגיסטיקה של היריב.[20]

מבנה הכוח הסיני לפני תהליך המודרניזציה

עד המחצית הראשונה של העשור הנוכחי, מפלגת השלטון בסין כבר הספיקה לפתח מערך משלים גדול של כוחות פעולה וכוחות תמיכה בסייבר. המטה הכללי של הצבא הסיני (GSD), הכפוף לסמכות הפיקודית העליונה – הוועדה הצבאית המרכזית של המפלגה הקומוניסטית של סין – היה אז אחראי על מבצעים משותפים שוטפים, מודיעין, תכנון אסטרטגי, דרישות מבצעיות, אימונים, גיוס, דיפלומטיה צבאית ואבטחת מנהיגים בכירים, כך שהפך למוביל החדשנות בצבא הסיני.[21] המטה הכללי כלל את המחלקות השנייה, השלישית והרביעית, שקיבלו בהתאמה את השמות "המשרד השני" (PLA/2), "המשרד השלישי" (PLA/3) ו"המשרד הרביעי" (PLA/4).[22]

---

19 Kevin Pollpeter, "Chinese Writings on Cyberwarfare and Coercion", in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, p. 141.

20 Lindsay, "Introduction – China and Cybersecurity: Controversy and Context", in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, p. 18.

21 Mark Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure", in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, p. 164.

22 Ibid., p. 10.

"המשרד השני" שימש כארגון המודיעין האנושי (HUMINT) של סין, שביצע איסוף מודיעין זר ממקורות אנושיים. הפעולות הגלויות של "המשרד השני" נעשו על ידי הרשת העולמית של נספחי ההגנה של סין, שנבחרו בזכות יכולות אנליטיות וכישורי שפה, ובדרך כלל נעדרו ניסיון צבאי קונבנציונלי.[23] "המשרד השלישי" היה ארגון מודיעין האותות (SIGINT) של סין, שמקורו במודיעין האותות המסורתי של טרום עידן האינטרנט, אולם עד המאה ה־21 כבר ידע להתמודד עם כל צורות ה־SIGINT. משימותיו ופעולותיו כללו בעיקר משימות מעקב בסייבר (cyber reconnaissance) וניצול רשתות מחשב (CNE).[24] "המשרד הרביעי" היה גוף הרבה יותר חשאי, וביצע פעילות משבשת בתחומי הלוחמה האלקטרומגנטית, לוחמת מידע ומבצעי מידע, וכן מתקפות על רשתות מחשב (CNA).[25]

הצבא הסיני מקיים שלוש קטגוריות של מִבצעי סייבר, שאותן הוא מכנה "לוחמת רשת מחשבים": הקטגוריה הראשונה כוללת משימות ניצול של רשתות מחשבים ומעקב אחריהן; הקטגוריה השנייה היא תקיפת רשתות מחשבים; הקטגוריה השלישית עוסקת בהגנת רשתות מחשבים (CND).[26] לוחמת הרשת כוללת, על פי הדוקטרינה הסינית, פעולות תקיפה כמו הרס מערכות רשת ומידע של היריב ופגיעה באפקטיביות המבצעית שלו. פעולות ההגנה כוללות הגנה על מערכות הרשת והמידע של סין ועל היכולת לבצע פעולות – בעיקרון, כל מה שהוא ההיפך מפעולות תקיפה.[27]

"המשרד השלישי" של המטכ"ל הסיני מעניין במיוחד בשל פעילות הסייבר הניכרת שלו. נכון ל־2014, "המשרד השלישי" עסק במחשוב, הצפנה ופענוח והיה המעסיק הגדול ביותר בסין של בלשנים בכירים.[28] המטה שלו היה ממוקם במחוז חיידיאן (Haidian) בבייג'ינג, בקרבת רוב משרדי הממשלה החשובים. מפקדת "המשרד השלישי" כללה יחידת מטה, מחלקה פוליטית, מחלקת לוגיסטיקה, לשכה מודיעינית למדע וטכנולוגיה, לשכה לציוד מדעי וטכנולוגי, ואת מכון המחקר מספר 56, שהוא מכון המחקר והפיתוח בתחום מדעי המחשב הוותיק והגדול ביותר של הצבא הסיני.[29] במסגרת "המשרד השלישי" נמצא גם "מרכז המחשבים הצפוני של בייג'ינג" (BNCC) – יחידה סודית האחראית על תכנון הארכיטקטורה של

23 Nigel Inkster, "The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace", in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, p. 33.

24 Ibid.

25 Ibid.

26 Pollpeter, "Chinese Writings on Cyberwarfare and Coercion", p. 143.

27 Ibid., p. 139.

28 Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure", p. 164.

29 Ibid., pp. 166-167.

מעקבי סייבר, על פיתוח טכנולוגיה ועל הנדסת מערכות ורכש. "מרכז המחשבים הצפוני של בייג'ינג" הוא אחד הארגונים הראשונים של הצבא הסיני, שהיה אחראי על מבצעי סייבר עוד בראשיתם במאה העשרים, וכפופות אליו עשר חטיבות שאחראיות על מבצעי רשתות מחשב (CNO) מכל הסוגים, ובכלל זה מתקפות על רשתות מחשב, ניצול רשתות מחשב והגנת רשתות מחשב.[30] הצוותים המבצעיים ומומחי הבלשנות של "המשרד השלישי" רכשו את הכשרתם באוניברסיטאות מתמחות של הצבא הסיני.[31]

בנוסף ל"משרד השלישי" הוקמו במסגרת הצבא הסיני נכסים וכלים מבצעיים נוספים בתחום הסייבר, שקיבלו את השם "לשכות מעקב טכני" (TRB). חיל האוויר, חיל הים וכוח הארטילריה השני (או "כוח הרקטות האסטרטגי") החזיקו כל אחד "לשכת מעקב טכני" משלהם, וכך גם כל אחד משבעת הפיקודים הצבאיים האזוריים. לחיל האוויר הסיני היו שלוש "לשכות מעקב טכני" שניטרו את פעילותם של חילות אוויר סמוכים וביצעו משימות סיגינט מוטסות ומבצעי רשתות מחשב שתמכו ישירות בפעולות חיל האוויר. לחיל הים הסיני היו שתי "לשכות מעקב טכני" – אחת לים הצפוני ואחת לים הדרומי – שככל הנראה עסקו באיסוף סיגינט מספינות. גם לכוח הארטילריה הייתה "לשכת מעקב טכני" משלו. כל "לשכת מעקב טכני" של פיקוד אזורי תמכה במבצעי אותו פיקוד.

להלן תיאור מפורט של הלשכות המבצעיות של "המשרד השלישי" ושל פעילותן, ובכלל זה פירוט מדויק של המבצעים שבהם השתתפו וממשיכים להיות מעורבים כוחות הסייבר המבצעיים. ל"משרד השלישי" הייתה סמכות ישירה על 12 לשכות מבצעיות – שמונה מתוכן בבייג'ינג, שתיים בשנגחאי, אחת בצ'ינגדאו ואחת בווּהָאן. כאמור, "לשכות מעקב טכני" אלו הוקמו ופעלו במנותק מהלשכות שהוכפפו לחילות הצבא ולפיקודים האזוריים שלו. ל"משרד השלישי" היה גם משרד ייעודי להונג קונג ומקאו.[32] מפקד היחידה היה בעל דרגה מקבילה למפקד קורפוס, ומנהלי "לשכת המעקב הטכני" והקומיסרים הפוליטיים (שהשתוו להם בסמכותם) היו בעלי דרגות ברמת מפקד אוגדה, עם שליטה על בין שישה ל־14 משרדים:

- הלשכה הראשונה, שהמטה שלה נמצא בחיידיאן יחד עם המטה של "המשרד השלישי", הייתה אחד הגופים הממלכתיים המובילים בתחום מבצעי רשתות מחשב וביטחון המידע.
- הלשכה השנייה, שפעלה בעיקר בשנגחאי, התמקדה בארצות הברית ובקנדה, כחלק מהניסיון להשיג מודיעין מדיני, כלכלי וצבאי, ובמקביל שמרה על קשרים מקצועיים ומחקריים עם מוסדות אקדמיים רבים באזור.

30 Ibid., p. 168.
31 Ibid., p. 169.
32 Ibid., pp. 170-172.

- ללשכה השלישית, שבסיסה היה בבייג'ינג, היו כפופות לפחות 13 יחידות בפריסה גיאוגרפית רחבה, מה שמלמד שהיא עסקה ככל הנראה באיסוף תשדורות רדיו בקו ראייה (line-of-sight), איכון כיוונים ובקרה ואבטחה של שידורים.
- הלשכה הרביעית שכנה בעיר הנמל צ'ינגדָאו והתמקדה ביפן ובחצי האי הקוריאני, עם משרדים לכל אורך החוף.
- הלשכה החמישית ישבה גם היא בבייג'ינג, עם משרדים בהיילונג־ג'יאנג – אחת הפרובינציות הצפוניות ביותר של סין – ומשימתה הייתה רוסיה.
- הלשכה השישית שכנה בוואהאן שבמרכז סין, עם משרדים פרוסים בכל האזור, מה שמעיד שהייתה מופקדת על טייוואן ודרום אסיה.
- הלשכה השביעית הייתה בחיידיאן והעסיקה כמה מתרגמים לאנגלית. היא נטלה חלק במבצעי רשתות מחשב, אך קשה לדעת בברור מה הייתה המשימה שלה.
- הלשכה השמינית הייתה צמודה למטה "המשרד השלישי" והתמקדה באירופה ואולי גם במזרח התיכון ובאמריקה הלטינית.
- הלשכה התשיעית, שבסיסה היה בפאתי בייג'ינג, הייתה החשאית ביותר ואחראית על מחשוב, ניתוח מודיעין אסטרטגי, ניהול מסדי נתונים וטכנולוגיה אור־קולית.
- הלשכה העשירית ישבה בבייג'ינג ומשימתה הייתה מרכז אסיה או רוסיה, ייתכן בעיקר בתחומי הטלמטריה ומעקב אחרי טילים וניסויים גרעיניים.
- הלשכה ה־11 שכנה גם היא בבייג'ינג והופקדה על רוסיה.
- הלשכה ה־12 הייתה ממוקמת בשנגחאי והופקדה על משימה לווינית שהתמקדה בסיגינט מהחלל.

ל"משרד השלישי" היה תפקיד מרכזי בניצול רשתות מחשב ובהגנה על רשתות מחשבים, אולם הארגון המוביל במתקפות על רשתות מחשבים היה, ככל הנראה, המחלקה הסודית יותר – "המשרד הרביעי" – שהחזיק בשם הרשמי "המחלקה למכ"ם ואמצעי נגד אלקטרוניים". "המשרד הרביעי" היה אחראי על פיתוח הדרישות המבצעיות המשותפות (צי"ח) בתחומי המכ"ם ואמצעי הנגד האלקטרוניים, כולל חסימת לווינים ומערכות מכ"ם לאיתור מטוסים חמקנים.[33] גוף זה כלל לפחות ארבע לשכות, קבוצה מייעצת ואת מכון המחקר מספר 54. הלשכה לאמצעי נגד אלקטרוניים תכננה, תכנתה ותקצבה מערכות של אמצעי נגד אלקטרוניים, ולשכת הציוד הטכני עסקה ברכש. כוח האדם שהוקצה ל"משרד הרביעי" קיבל הכשרה מיוחדת באוניברסיטה ייעודית של הצבא הסיני. ידוע על לפחות שתי חטיבות מבצעיות של אמצעי נגד אלקטרוניים, שככל הנראה היו אחראיות על תחנות קליטה קרקעיות של לווייני סיור וריגול אלקטרוניים וסייעו בקביעת מטרות ובביצוע חסימות של לווינים.

33. Ibid., p.174.

מבנה הכוח לאחר המודרניזציה

הארגונים הללו הוחלפו בעקבות החלטה שנכנסה לתוקף ב־1 בינואר 2016. במקום ריבוי הארגונים שפעלו תחת המטה הכללי, כל הנכסים המבצעיים בתחומי המידע והסייבר רוכזו תחת "כוח התמיכה האסטרטגי" (SSF). שבעת הפיקודים האזוריים אורגנו מחדש לחמישה פיקודים מרחביים, והמרחבים החדשים קיבלו את סמכות הפיקוד שהייתה שייכת בעבר לחילות הנפרדים, במטרה להקל על ביצוע פעולות משותפות (כמו במרבית כוחות המשלוח).[34] במסגרת מבנה הכוח החדש, "לשכות המעקב הטכני", שהיו כפופות ישירות לחילות ולפיקודים האזוריים, עברו לסמכותו של "כוח התמיכה האסטרטגי". מדובר בכוח משותף ללוחמת מידע, המשולב במלואו בצבא הסיני ומספק לו מידע אסטרטגי, בעיקר בזכות יכולות הרשת ויכולות החלל שלו, המוצאות את ביטוין בשתי היחידות העיקריות הכפופות לו.[35] יכולות אלו כוללות תקשורת, ניווט ואיכון, מודיעין, מעקב וסיור והגנה על תשתית המידע של הצבא הסיני.[36] "כוח התמיכה האסטרטגי" מוציא לפועל מבצעי מידע בחלל ובסייבר, לוחמה אלקטרונית ולוחמה פסיכולוגית. לפיכך, לא מדובר בכוח ייעודי למִבצעי סייבר בלבד, אלא בכוח ייעודי למִבצעי מידע שפועל בעיקר במרחב הסייבר, אך גם בסביבות נוספות, באופן המתיישב עם התפיסה הסינית של ביטחון מידע ומרחב הסייבר. המטה הכללי וארגונים אחרים, שכללו בתוכם כוחות עם מערכי משימה דומים, פורקו כולם עד סוף שנת 2015.

בנוסף לשתי המחלקות המבצעיות – האחת למערכות החלל והשנייה למערכות רשת (SSD ו־NSD בהתאמה) – יש ל"כוח התמיכה האסטרטגי" גם מחלקת מטה שאחראית על מבצעים, תכנון, הדרכה, ניהול ובקרת פרויקטים וניהול כוח אדם.[37] הוא גם כולל מחלקה לפעילות פוליטית, המהווה חלק אינטגרלי של כל גוף בצבא הסיני: מכיוון שהצבא כפוף למפלגה ולא למדינה, על כל גוף של הצבא לוודא שהחשיבה הפוליטית והמשימות ישמרו על הקו האידיאולוגי של המפלגה.

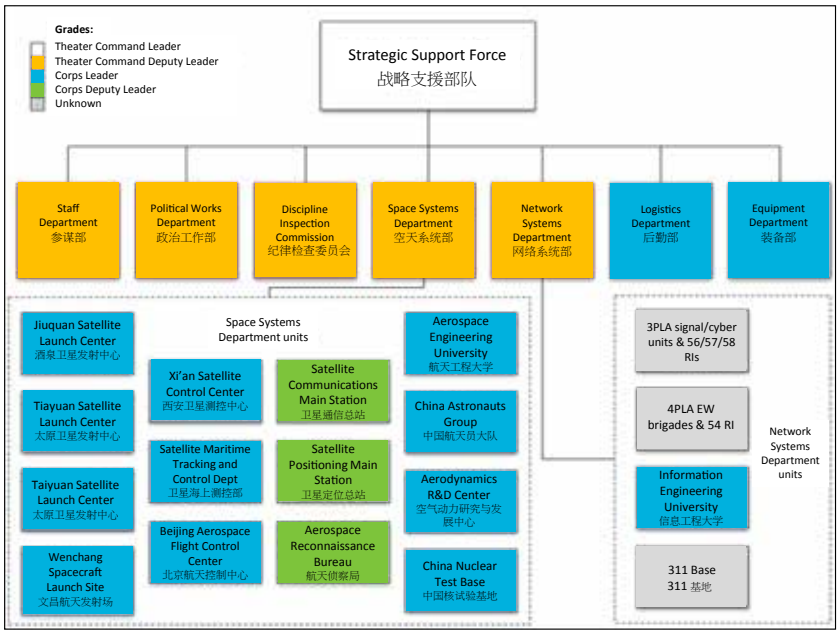
המחלקה למערכות חלל מטפלת כמעט בכל היבט של פעולות החלל של המדינה, והמחלקה למערכות רשת לקחה לידיה את כל מה שבעבר היה משימות הרשת של "המשרד השלישי" ו"המשרד הרביעי", לרבות סיגינט, ריגול סייבר, מבצעי רשתות מחשב, לוחמה אלקטרונית ולוחמה פסיכולוגית. "כוח התמיכה האסטרטגי" החדש אינו מבצע, אפוא, פעולות השונות באופן משמעותי מאלו שעשו "המשרד

34 Xinhua News, "Xin shi dai de zhong guo guo fang", *Xinhuanet*, July 24, 2019, http://www.xinhuanet.com/politics/2019-07/24/c_1124792450.htm.

35 Adam Ni and Bates Gill, "The People's Liberation Army Strategic Support Force: Update 2019", *Jamestown Foundation China Brief*, May 29, 2019, https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/.

36 Ibid.

37 Ibid.



תרשים 1. כוח התמיכה האסטרטגי (מקור: Adam Ni and Bates Gill, "The People's Liberation Army Strategic Support Force: Update 2019", *Jamestown Foundation China Brief*, May 29, 2019, https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/).

השלישי" ו"המשרד הרביעי" במשך השנים, אך הוא הפך לזרוע צבאית מן המניין, שוות ערך לכוח הארטילריה השני, מה שמלמד על העלייה בחשיבותם של מבצעי המידע לרמה הגבוהה ביותר.

המקורות הסיניים מחזקים ברטוריקה המדויקת שלהם את השיח הרשמי, לפיו "כוח התמיכה האסטרטגי" הוא סוג חדש של כוח קרבי לוחם (新型作战力量 *xinxing zuozhan liliang*). פירוש הדבר הוא שמפלגת השלטון רואה ב"כוח התמיכה האסטרטגי" ובמבצעי המידע תחום בפני עצמו בביטחון הלאומי הסיני.[38] לפי גורמים סיניים רשמיים, מבצעי המידע של "כוח התמיכה האסטרטגי" ועצם הקמתו הם ביטוי ל"מודרניזציה צבאית בעלת מאפיינים סיניים" (中国特色强军 *zhongguo tese qiangjun*) – ביטוי שמתכתב עם הביטוי בן עשרות השנים "סוציאליזם בעל מאפיינים סיניים" (中国特色社会主义 *zhongguo tese shuhuizhuyi*), שהיה

38 Liu Shangjing, ed., "Guo fang bu zin wen fa xin ren jiu shen hua guo fang he jun dui gai ge you guan wen ti jie shou mei ti zhuan fang", *Ministry of National Defense of the People's Republic of China*, January 1, 2016, http://www.mod.gov.cn/info/2016-01/01/content_4637926.htm.

וממשיך להיות עיקרון מנחה בביצוע "הרפורמות הלאומיות והפתיחות" (改革开放 *gaige kaifang*). אותם מקורות סיניים רשמיים מתארים את "כוח התמיכה האסטרטגי" כגוף שעוזר להגשמת "החלום הסיני" וחלום המודרניזציה הצבאית, ומוסיפים כי על כל הקצינים והחיילים להסתגל לכללי המדיניות החדשים.[39]

למעשה, המודרניזציה מתבטאת לא רק בהקמת "כוח התמיכה האסטרטגי", אלא במבנה ובארגון הכוללים של הצבא הסיני, העוברים תהליך של מודרניזציה במטרה לשפר את הביטחון הלאומי. "כוח התמיכה האסטרטגי" הוא חלק מתהליך זה, ומהווה כוח לוחמה קרבי להגנת המולדת.[40]

סיכום ומסקנות

הארגון מחדש של כוחות הסייבר בתוך "צבא השחרור העממי" של סין הוא חלק מפרויקט המודרניזציה בכלל הצבא הסיני, שהחל בשנת 2015. "הספר הלבן" של סין בנושא ביטחון והגנה, משנת 2019, הגדיר את שני היעדים של סין לשנת 2020 כמכניזציה, קרי מודרניזציה פיזית של הציוד הטקטי, ואינפורמטיזציה, שמתייחסת ליחידות בצבא הסיני המופקדות על ביטחון המידע, ובתוכו ביטחון הסייבר.[41] המטרה המוצהרת של הצבא הסיני היא להשלים את המודרניזציה הצבאית במלואה עד שנת 2035 וליישר קו עם הצבאות המובילים בעולם. מטרת־על זו כוללת מודרניזציה של התיאוריה הצבאית, של המבנים הארגוניים ומבני הכוח ושל הנשק והציוד.[42] "כוח התמיכה האסטרטגי" הוא פרי המאמצים של בניית האינפורמטיזציה, וסביר להניח שיישאר מבנה הכוח העיקרי לפעולות הסייבר של הצבא הסיני בעשור הקרוב. כפי שצוין ב"ספר הלבן", עד שנת 2035 צפויים להתרחש שינויים נוספים במבנה הכוח הצבאי הסיני מתוך כוונה להשלים את פרויקט המודרניזציה שלו, אולם "כוח התמיכה האסטרטגי" יישאר הגורם השולט על כוחות מבצעי הסייבר, וגם המודרניזציה העתידית לא צפויה לשנות באופן דרמטי את מבנהו הנוכחי. אם יחולו שינויים משמעותיים, סביר להניח שהם יהיו בשרשרת הפיקוד שתחתיה פועל "כוח התמיכה האסטרטגי", ולא בארגון עצמו.

הארגון מחדש של מבנה הכוח, שנעשה בצורה גורפת ב־2016 והביא להקמת "כוח התמיכה האסטרטגי", גם הכניס שינויים במערכי המשימה הקודמים של "המשרד השלישי" ו"המשרד הרביעי", יחד עם עלייה במעמדם. לצד זאת, הארגון

---

39 Xinhua News, "Lu jun ling dao ji gou huo jian jun zhan lve zhi yuan bu dui cheng li da hui zai jing ju xing xi jin ping xiang zhong guo ren min jie fang jun lu jun huo jian jun zhan lve zhi yuan bu dui zhi xu jun qi bing zhi xun ci", *Xinhuanet*, January 1, 2016, http://www.xinhuanet.com//politics/2016-01/01/c_1117646667.htm.

40 Ibid.

41 Ibid.

42 Xinhua News, "Xin shi dai de zhong guo guo fang".

מחדש מייצג ומשקף שינוי מהותי באסטרטגיה הצבאית של סין ובסדרי העדיפויות שלה. לפי שינוי זה, מבצעי מידע הפכו לתחום לוחמה חדש וקריטי לשמירה על השקט בתוך המדינה – מטרה שמפלגת השלטון רואה כחיונית לשימור הסמכות והלגיטימיות שלה ולתפיסתה כשלטון היחיד שמסוגל לנהל בצורה שלווה ומשגשגת מדינה מאוכלסת וגדולה כל כך. זוהי הסיבה שמפלגת השלטון, בהנהגתו הריכוזית והאפקטיבית של הנשיא שי, הוציאה את תחום הסייבר מהסבך הביורוקרטי ומהמעמד הנמוך שאפיינו אותו, והקימה אותו מחדש תחת המטריה של מבצעי מידע. המשימה החדשה נועדה לתמוך באופן ישיר במטרותיה של מפלגת השלטון – אחדות אידיאולוגית וחוסר סובלנות כלפי כל דעה אחרת – כחלק מהדרך להבטיח את הביטחון הלאומי. הארגון מחדש של מבנה הכוח הוא שיקוף אפקטיבי של המדיניות החדשה לביטחון סייבר וביטחון מידע, ושיפורה, מתוך הבנה כי שני התחומים כרוכים זה בזה.

ההשקעות הסיניות בסרי־לנקה: משמעויות לישראל

שלומי יאס

מאמר זה עוסק בפרויקטים סיניים בסרי־לנקה, חלקם במסגרת יוזמת "חגורה ודרך", במטרה לגזור מהם תובנות לזירה הישראלית. זאת ועוד, המאמר ינסה להשיב על השאלה האם, ועד כמה, היוזמה הסינית "שייכת לעולם", כפי שנכתב באתר הרשמי שלה[1], או שמדובר בביטוי לשאיפה סינית להשפעה, העלולה להביא לסדר עולמי סיני חדש.[2] המאמר מציג את היוזמה לצד טיעונים נגדה, ובהמשך הוא מתאר את יחסי סין-סרי־לנקה ומפרט ארבעה פרויקטים סיניים המתקיימים באי. בעקבות זאת בוחן המאמר את יחסי ישראל-סין על רקע המעורבות הסינית בפרויקטים אסטרטגיים בישראל, תוך התמקדות בפרויקט של נמל המפרץ בחיפה. בסיום מציג המאמר תובנות לישראל כפועל יוצא של יוזמת "חגורה ודרך", תוך שהוא בוחן את ההיתכנות לנזקים מדיניים, לסיכונים ביטחוניים ולהשפעה על פוליטיקאים ישראלים כתוצאה מיוזמה זו.

מילות מפתח: סין, סרי־לנקה, ישראל, אסטרטגיה, פרויקטים, היוזמה, היוזמה הסינית

מבוא

זמן קצר לאחר שנבחר לנשיאות סין בשנת 2013, הכריז שי ג'ינפינג על מה שנראה כפרויקט הכלכלי הגדול ביותר בהיסטוריה: יוזמת "חגורה ודרך" ("Belt and Road Initiative" – BRI). היוזמה הסינית היא אסטרטגיה רבתי של נשיא סין לחידוש

שלומי יאס הוא מתמחה במכון למחקרי ביטחון לאומי וכותב אורח בפורום לחשיבה אזורית.

1 "The Belt and Road Initiative Progress, Contributions and Prospects", *Belt and Road Portal*, April 22, 2019, https://eng.yidaiyilu.gov.cn/zchj/qwfb/86739.htm.

2 Mark Melton, "China's Plan for a New World Order: Review of Maçães' Belt and Road", *Providence*, September 12, 2019, https://providencemag.com/2019/09/chinas-new-world-order-book-review-bruno-macaes-belt-road-initiative.

דרך המשי היבשתית העתיקה[3] באמצעות בניית רשת של מסילות רכבת וכבישים מהירים בין־מדינתית, לצד הקמת מערכת של נמלים ימיים היוצרים נתיב מסחר ימי שישתרע על פני מספר אוקיינוסים. במסגרת אסטרטגיה זו מתכוונת סין גם להרחיב הסכמים קיימים לתובלה אווירית ולבנות מגוון מתקני אנרגיה, תקשורת, תעשייה ועוד.[4]

התקדמות משמעותית ביישום היוזמה הושגה ביוני 2015, כאשר 57 מדינות (ללא יפן וארצות הברית) הצטרפו כחברות מייסדות של בנק חדש בבייג'ינג – "הבנק האסייתי להשקעה בתשתיות" (AIIB) – שההון ההתחלתי שלו נקבע למאה מיליארד דולר.[5] נכון לאוקטובר 2019, סין מחזיקה ב־31 אחוזים מסך ההון של הבנק, מה שמקנה לה כוח הצבעה של 26.6 אחוזים, כלומר, זכות וטו בכל החלטה הדורשת רוב מיוחד (של לפחות 75 אחוזים מהמצביעים).[6] גם ישראל הצטרפה אל "הבנק האסייתי להשקעה בתשתיות" כמדינה מייסדת, מתוך הנחה שהדבר יסייע לחברות ישראליות להשתתף בפרויקטים של הבנק.[7]

הפורום הראשון של יוזמת "חגורה ודרך" התכנס ב־2017. ארצות הברית נטלה חלק בכינוס, אם כי בנוכחות מצומצמת של המנהל הבכיר לענייני אסיה ב"מועצה לביטחון לאומי".[8] באפריל 2019 התקיים הפורום השני של היוזמה, בהשתתפות 36 ראשי מדינות וממשלות.[9]

3 Mai Phan, "A Mixed Reality of The Belt and Road Initiative in Southeast Asia", *Journal of International Relations*, July 22, 2019, http://www.sirjournal.org/op-ed/2019/7/22/a-mixed-reality-of-the-belt-and-road-initiatives-in-southeast-asia.

4 Martin Hart-Landsberg, "A critical look at China's One Belt, One Road Initiative", *CADTM*, October 10, 2018, http://www.cadtm.org/A-critical-look-at-China-s-One-Belt-One-Road-initiative.

5 "Founding 57 members of China-led AIIB investment bank sign up in Great Hall ceremony", *Deutsche Welle*, June 29, 2015, https://www.dw.com/en/founding-57-members-of-china-led-aiib-investment-bank-sign-up-in-great-hall-ceremony/a-18546332.

6 Jason Kirk, "China and the Asian Infrastructure Investment Bank", *Observer Research Foundation*, November 1, 2019, https://www.orfonline.org/expert-speak/china-and-the-asian-infrastructure-investment-bank-55693.

7 Hagai Shagrir, *Israel-China Relations: Innovative Comprehensive Partnership*, Memorandum No. 194 (Tel Aviv: Institute for National Security Studies, 2019), p. 21.

8 Matt Spetalnick, David Brunnstrom, "Trump Asia expert to become new deputy national security adviser: sources", *Reuters*, September 20, 2019, https://www.reuters.com/article/us-usa-trump-adviser/trump-asia-expert-to-become-new-deputy-national-security-adviser-sources-idUSKBN1W523F.

9 Shannon Tiezzi, "Who Is (and Who Isn't) Attending China's 2nd Belt and Road Forum?", *The Diplomat*, April 27, 2019, https://thediplomat.com/2019/04/who-is-and-who-isnt-attending-chinas-2nd-belt-and-road-forum.

מספר המדינות המעורבות ביוזמה האסטרטגית הסינית הוא מרשים. נכון למארס 2019, סין חתמה 173 הסכמי שיתוף פעולה עם 125 מדינות ועם 29 ארגונים בין־לאומיים. בנוסף לכך, סין חתמה על הסכמים בילטרליים לתעבורה אווירית עם 126 מדינות והרחיבה הסכמים קיימים בתחום התעבורה האווירית עם מדינות שונות (כולל ישראל). בחמש השנים האחרונות פתחה סין יותר מאלף נתיבי תעופה בין־לאומיים חדשים.[10] באפריל 2019 חתמה איטליה על מזכר הבנות עם סין במסגרת היוזמה "חגורה ודרך", ולאחרונה הצטרפה גם רוסיה לאותה יוזמה, כשנתנה אור ירוק לבניית אוטוסטרדה בין־מדינתית עם סין.[11] הבנק העולמי העריך, נכון לאוגוסט 2019, כי פרויקטים של מסילות רכבת, כבישים, נמלים ועוד, בשווי של כ־575 מיליארד דולר, היו או נמצאים בתהליך של בנייה במסגרת היוזמה הסינית.[12]

בהקשר זה ראוי להזכיר "דרכי משי" נוספות שסין בונה כיום: "דרך המשי הדיגיטלית" – רשת כבלים ימיים תת־קרקעיים לאינטרנט – "דרך המשי בחלל" (Beidou), שהיא מערכת ניווט סינית החותרת להחליף את רשת לווייני הג'י.פי.אס האמריקאים,[13] ו"דרך המשי בקוטב", שמטרתה לטפל בנתיבי ספנות, במחקר מדעי, בשינויי אקלים, ובמשאבים ארקטיים.[14]

אתגרים ליוזמת "חגורה ודרך"

ההשפעה וההשלכות הגלובליות הנרחבות של יוזמת "חגורה ודרך" גוררות גם ביקורות וחושפות חסרונות וחולשות שלה. סין מקדמת נרטיב של "אי־התערבות", לפיו כל התערבות בפוליטיקה או במדיניות של המדינות השותפות ליוזמה חייבת להיראות כאילו הוזמנה על ידי ממשלותיהן.[15] למעשה, הפרויקטים הסיניים במסגרת היוזמה פתוחים רק בהיקף מצומצם להשתתפות בין־לאומית. נכון ל־2018, מתוך כלל הקבלנים המשתתפים בפרויקטים של היוזמה, 89 אחוזים שייכים לחברות

10 "The Belt and Road Initiative Progress, Contributions and Prospects", *Belt and Road Portal*, April 22, 2019, https://eng.yidaiyilu.gov.cn/zchj/qwfb/86739.htm.

11 Alice Scarsi, "Russia and China agree 5000-mile 'Moscow bypass' road to strengthen economic ties, *Express*, July 10, 2019, https://www.express.co.uk/news/world/1151662/russia-news-china-Russia-Western-China-highway-Belt-and-Road-Initiative-bri.

12 "China's Belt and Road Gets a Reboot to Boost Its Image", *Bloomberg*, August 14, 2019, https://www.bloomberg.com/news/articles/2019-08-14/china-s-belt-and-road-is-getting-a-reboot-here-s-why-quicktake.

13 Matthew Johnson, "China's International Partnerships: Pakistan, CPEC and Central Asia", *Tibet Digest*, Foundation for Non-violent Alternatives, August 2019, p. 98.

14 Qiyang Niu, "China's Evolving Arctic Policy: Two Geopolitical Threats", *Tibet Digest*, Foundation for Non-violent Alternatives, August 2019, p. 116.

15 Nicholas Crawford, "China and instability in developing countries", *The International Institute for Strategic Studies*, October 28, 2019, p. 3, https://www.iiss.org/blogs/research-paper/2019/10/china-and-instability.

סיניות, 7.6 אחוזים שייכים לחברות מקומיות (חברות שהמשרדים הראשיים שלהן נמצאים באותה המדינה בה הפרויקט מתבצע), ו־3.4 אחוזים שייכים לחברות זרות. בין הפרויקטים הרבים הנכללים ביוזמת "חגורה ודרך" גם כאלה שהחלו שנים לפני השקתה.[16]

בשנה וחצי האחרונות (נכון לאוקטובר 2019), הואט באופן משמעותי הגידול בהיקף היוזמה. ב־2018 ירד הערך של פרויקטים חדשים ב־61 מדינות המעורבות ביוזמה ב־13 אחוזים בהשוואה ל־2017, וב־6.7 אחוזים נוספים עד לאוגוסט 2019. בשמונת החודשים הראשונים של 2019 חלה ירידה של 4.2 אחוזים בחוזים הקיימים. אחדות מהמדינות השותפות ביוזמה צמצמו הלוואות מתוכננות ואף ביטלו פרויקטים, בין היתר מטעמים כלכליים ופוליטיים.[17] לפחות שבע מדינות, ביניהן פקיסטן, מיאנמאר, האיים המלדיביים, קניה וסרי־לנקה, נתקלו בבעיות עם פרויקטים של היוזמה או ביקשו לשקול אותה מחדש.[18] ההשקעה הסינית הזרה, ובייחוד הפרויקטים של היוזמה, מעלים סוגיות הנוגעות לחוב, לאיומים על הריבונות, לתפיסת קרקעות, לעקירה, לניצול זכויות אדם באזורי סכסוך, להשפעות סביבתיות, לחששות לבריאות הציבור ולהפרות של תנאי תעסוקה.[19]

מספר טיעונים מועלים נגד היוזמה. הטיעון הראשון רואה בה יותר מיוזמה כלכלית, ובעצם כלי מרכזי לקידום שאיפות גיאו־פוליטיות סיניות. יש הסבורים כי מדובר בתגובת נגד סינית להתמקדות האמריקאית המחודשת באסיה ("Pivot to Asia"), שהחלה ב־2011 בתקופת ממשל אובמה, ואשר רבים בבייג'ינג רואים בה ניסיון לבלום את סין באמצעות הרחבת הקשרים הכלכליים של ארצות הברית בדרום־מזרח אסיה. ארצות הברית וחלק מבעלות בריתה מזהירות כי היוזמה הסינית עשויה להיות "סוס טרויאני" שנועד לקדם השפעה אזורית של סין ולאפשר התרחבות צבאית ומוסדית סינית.[20] טיעון שני רואה ביוזמה הסינית סוג של "מלכודת חוב דיפלומטית" כנגד מדינות מתפתחות. על פי טיעון זה, סין משעבדת את המשאבים

16 Jonathan E. Hillman, "China's Belt and Road Initiative: Five Years Later", *Center for Strategic and International Studies*, January 25, 2018, https://www.csis.org/analysis/chinas-belt-and-road-initiative-five-years-later-0.

17 Cissy Zhou, "China slimming down Belt and Road Initiative as new project value plunges in last 18 months, report shows", *South China Morning Post*, October 10, 2019, https://www.scmp.com/economy/global-economy/article/3032375/china-slimming-down-belt-and-road-initiative-new-project.

18 "China's Belt and Road Is Getting a Reboot. Here's Why".

19 "The Belt and Road Initiative: Chinese agribusiness going global", *GRAIN*, February 18, 2019, https://www.grain.org/en/article/6133-the-belt-and-road-initiative-chinese-agribusiness-going-global.

20 Andrew Chatzky and James McBride, "China's Massive Belt and Road Initiative", *Council on Foreign Relations*, May 21, 2019, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

והנכסים האסטרטגיים של מדינות מתפתחות בתמורה למימון ולבניית תשתיות באותן מדינות וחותרת להשיג נגישות מועדפת לנכסיהן הטבעיים. בדרך זו משיגה סין גם חדירה כלכלית וגם מינוף אסטרטגי.[21] טיעון שלישי רואה ביוזמה גורם לנזק סביבתי בקנה מידה עולמי. מדובר בחשש לגיטימי מפני ההשפעות הסביבתיות של היוזמה, במיוחד נוכח הניסיון המועט שיש בניתוח ההשפעות הסביבתיות של פיתוח תשתיות מסיביות בקנה מידה כמו זה של היוזמה הסינית.[22]

ביוני 2019 פורסם מחקר של הבנק העולמי, המנסה לענות על שלושת הטיעונים דלעיל. כותבי המחקר אינם פוסלים את היוזמה הסינית כשלעצמה, אך ממליצים על הכנסת שורה של שינויים עמוקים בה: "היוזמה הסינית עשויה להאיץ את הפיתוח הכלכלי ולהקטין את העוני בעשרות מדינות מתפתחות, אולם היא מוכרחה להיות מלווה ברפורמות מדיניות עמוקות שיגדילו את השקיפות ויביאו לשיפור במאזן החובות וכן לצמצום הסיכונים הסביבתיים, החברתיים ואלה הקשורים בשחיתות".[23]

יחסי סין-סרי־לנקה נוכח המערכת הפוליטית באי

ההתעניינות הסינית בסרי־לנקה נובעת במידה רבה ממיקומה האסטרטגי, המהווה מזה שנים רבות צומת מסחר ימי גדול במרחב האירו־אסייתי. ספציפית לאינטרסים הסיניים, סרי־לנקה יכולה לספק שער כניסה נוח ומהיר לשווקים המתפתחים בתת־היבשת ההודית.[24] ההתקרבות האסטרטגית בין סין לסרי־לנקה החלה בתקופת כהונתו של נשיא סרי־לנקה דאז, מהינדה רג'פקסה (Rajapaksa), שכיהן בשנים 2005־2015 – תקופה בה סין הפכה לספקית הנשק העיקרית של סרי־לנקה. בשעה שארצות הברית עצרה את הסיוע הצבאי הישיר לסרי־לנקה ב־2007, סין הגדילה את הסיוע לאי בכמיליארד דולר והפכה לתורמת הגדולה ביותר לכלכלתו ולצבאו. במסגרת זו היא סיפקה אמצעי לחימה מתוחכמים, ובכלל זה שישה מטוסי קרב סיניים מדגם F-7, ועודדה את פקיסטן למכור נשק לסרי־לנקה ולאמן את טייסיה.

21 Ronak Gopaldas, "Lessons from Sri Lanka on China's 'debt-trap diplomacy'", *Institute for Security Studies*, February 2, 2018, https://issafrica.org/amp/iss-today/lessons-from-sri-lanka-on-chinas-debt-trap-diplomacy.

22 Hoong Chen Teo, Alex Mark Lechner, Grant W. Walton, Faith Ka Shun Chan, Ali Cheshmehzangi, May Tan-Mullins, Hing Kai Chan, Troy Sternberg and Ahimsa Campos-Arceiz, "Environmental Impacts of Infrastructure Development under the Belt and Road Initiative", *MDPI*, June 19, 2019, p. 1.

23 "Millions Could Be Lifted Out of Poverty, but Countries Face Significant Risks", *World Bank*, June 18, 2019, https://www.worldbank.org/en/news/press-release/2019/06/18/success-of-chinas-belt-road-initiative-depends-on-deep-policy-reforms-study-finds.

24 Marcello Rossi, "Next Hambantota? Welcome to the Chinese-funded US$1.4 billion Port City Colombo in Sri Lanka", *South China Morning Post*, May 12, 2019, https://www.scmp.com/week-asia/geopolitics/article/3009731/next-hambantota-welcome-chinese-funded-us14-billion-port-city.

סין סייעה לסרי־לנקה גם בזירה המדינית, ואף הטילה וטו על הצעת החלטה של מועצת הביטחון של האו"ם לערוך דיון על סרי־לנקה לאחר מלחמת האזרחים באי, ואולי גם לשלוח פקחים של הארגון לשם.[25] גם היחסים הכלכליים בין שתי המדינות העמיקו, עד שב־2013 תפסה סין את המקום הראשון במקורות ההשקעה הזרה הישירה בסרי־לנקה.[26] הנשיא רג'פקסה הסתמך יותר ויותר על הסינים לצורך בניית פרויקטים לאחר סיום מלחמת האזרחים, וסרי־לנקה לוותה מסין לצורך זה יותר משישה מיליארד דולר.[27]

המעורבות הסינית בסרי־לנקה הפכה לסוגיה חשובה במהלך מערכת הבחירות לנשיאות באי ב־2015. מהינדה רג'פקסה הפסיד ובמקומו נבחר מייטריפלה סיריסנה (Sirisena), שהבטיח לכונן "יחסים שווים" עם הודו, סין, פקיסטן ויפן ולשנות לחלוטין את מדיניות החוץ של האי. סיריסנה ביקש להתרחק מסין, בעלת בריתו של קודמו רג'פקסה, ולהתקרב להודו ולמערב, תוך בחינה מחדש של הפרויקטים הסיניים.[28] למעשה, ממשלתו הייתה עסוקה בעיקר בצמצום הנזקים של הממשלות הקודמות.

כ־95 אחוזים מההכנסות של ממשלת סרי־לנקה הופנו עד שנת 2015 לתשלום החוב לסין, מה שהביא אותה לנהל עם סין משא ומתן על החוב.[29] החוב לסין עמד ב־2016 על שמונה מיליארד דולר (קרוב לעשרה אחוזים מהתמ"ג), ונבע בעיקר מהלוואות לבניית פרויקטים, שמרביתם אושרו בתקופת ממשלות רג'פקסה.[30] ממשלת סרי־לנקה בראשות סיריסנה אישרה באותה שנה להמשיך בפרויקטים,

25 "How Beijing won Sri Lanka's civil war", *The Independent*, May 23, 2010, https://www.independent.co.uk/news/world/asia/how-beijing-won-sri-lankas-civil-war-1980492.html.

26 N.P. Ravindra Deyshappriya, "China is Sri Lanka's biggest source of FDI, but there is room for more", *London School of Economics*, September 12, 2017, https://blogs.lse.ac.uk/southasia/2017/09/12/china-is-sri-lankas-biggest-source-of-fdi-but-there-is-room-for-more.

27 "Moving away from China, Sri Lanka puts Chinese 'mega-projects' on hold", *AsiaNews/Agencies*, January 20, 2015, http://www.asianews.it/news-en/Moving-away-from-China,-Sri-Lanka-puts-Chinese-mega-projects-on-hold-33240.html.

28 Heather Timmons, "Sri Lanka's election upset just destroyed a linchpin of China's foreign policy", *Quartz Daily Brief*, January 9, 2015, https://qz.com/323718/how-sri-lankas-surprising-election-results-could-destroy-a-lynchpin-of-chinas-foreign-policy.

29 Jonathan E. Hillman, "Game of Loans: How China Bought Hambantota", *Center for Strategic and International Studies*, April 2, 2018, https://www.csis.org/analysis/game-loans-how-china-bought-hambantota.

30 Karthik Sivaram, "'Locked-In' to China: The Colombo Port City Project", *Freeman Spogli Institute for International Studies*, Stanford University, https://fsi.stanford.edu/publication/locked-china-colombo-port-city-project.

אך בכפוף לשינויים.[31] ב־2017 דווח כי סין הפכה למלווה הגדולה ביותר לבניית פרויקטים של תשתיות בסרי־לנקה (21.5 אחוזים מסך ההלוואות שסרי־לנקה לקחה לבניית פרויקטים של תשתיות) ואחריה יפן, הבנק העולמי והבנק האסייתי לפיתוח (ADB).[32] במאי 2019 נפגש הנשיא סיריסנה עם נשיא סין, שי ג׳ינפינג, ועם ראש ממשלתו, לי קה־צ׳יאנג, במהלך ועידה בין־לאומית.[33]

בנובמבר 2019 נערכו בסרי־לנקה פעם נוספת בחירות לנשיאות. הנשיא היוצא סיריסנה לא התמודד בהן, וגוטבאיה רג׳פקסה, אחיו הצעיר של הנשיא לשעבר מהינדה רג׳פקסה, ששימש כשר ההגנה בממשלתו בשנים 2005־2015, נבחר לנשיא החדש. דובר משרד החוץ הסיני מיהר לברך אותו, והוסיף: ״אנחנו מוכנים... לעבוד עם ההנהגה והממשלה החדשה כדי לשתף פעולה ברמה גבוהה סביב היוזמה הסינית, יחד עם התקדמות גדולה יותר בקשרים הבילטרליים, על מנת להביא לרווחים מוחשיים ונוספים יותר לשתי המדינות ולעמיהן״.[34] עוד במהלך מסע הבחירות הודיעו מקורביו של המועמד גוטבאיה כי הוא מתכוון ״להשיב את היחסים על כנם״ עם נשיא סין שי ג׳ינפינג.[35] זאת ועוד, עם היבחרו לנשיא, מיהר גוטבאיה רג׳פקסה למנות את אחיו, הנשיא לשעבר מהינדה רג׳פקסה, לראש הממשלה ולשר האוצר החדש.[36] מהלכים אלה עשויים להצביע על התקרבות אסטרטגית מחודשת בין סרי־לנקה לסין, גם אם היא עשויה להתפתח באופן זהיר מאשר בעבר.

סין-סרי־לנקה: ארבעה פרויקטים מרכזיים

כאמור, מרבית ההלוואות הסיניות לפרויקטים בסרי־לנקה ניתנו בתקופת הנשיא מהינדה רג׳פקסה. להלן יפורטו ארבעה פרויקטים מרכזיים במדינה שבוצעו במימון

---

31 Shihar Aneez, Ranga Sirilal, “Sri Lanka to allow Chinese port city project after delay”, *Reuters*, January 12, 2016, https://www.reuters.com/article/sri-lanka-china-portcity-idUSL3N14W42G20160112.

32 Nilanthi Samaranayake, “China’s Engagement with Smaller South Asian Countries”, *United States Institute of Peace*, April 2019, p. 6.

33 “Li Keqiang Meets with President Maithripala Sirisena of Sri Lanka”, *Ministry of Foreign Affairs of the People’s Republic of China*, May 19, 2019, https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1664297.shtml.

34 “China ready to work with new Sri Lankan President”, *Ada Derana*, November 18, 2019, http://www.adaderana.lk/news_intensedebate.php?nid=59134.

35 Shihar Aneez, Ranga Sirilal, “Record number of candidates to contest Sri Lanka’s presidential election”, *Reuters*, October 7, 2019, https://www.reuters.com/article/us-sri-lanka-elections/record-number-of-candidates-to-contest-sri-lankas-presidential-election-idUSKBN1WM1FB.

36 “Sri Lanka president pledges election at ‘earliest opportunity’”, *Al Jazeera*, November 22, 2019, https://www.aljazeera.com/news/2019/11/sri-lanka-president-pledges-election-earliest-opportunity-191122084348262.html.

סיני: נמל הַמְבַּנְטוֹטָה (Hambantota); אצטדיון הקריקט הבין־לאומי; שדה התעופה הבין־לאומי בהמבנטוטה; עיר הנמל של קולומבו. כל הפרויקטים האלה התבססו על מימון סיני ונבנו על ידי קבלנים סינים. לפחות שניים מהפרויקטים הם בעלי השלכות אסטרטגיות ארוכות טווח לסרי־לנקה (נמל המבנטוטה ועיר הנמל של קולומבו).

נמל המבנטוטה

נמל המבנטוטה הוא דוגמה לְמה שמכונה "מלכודת חוב דיפלומטית" סינית. הנמל, השוכן באחד מהנתיבים הימיים האסטרטגיים העמוסים בעולם, נבנה בעזרת הלוואה סינית בסך של כ־1.3 מיליארד דולר – אחת היוזמות הגדולות ביותר במימון ממשלתי סיני – ונפתח בשנת 2010. עם זאת, ולמרות שחלק גדול מהסחר מזרח–מערב עובר דרך נתיבי הים באוקיינוס ההודי, מרבית הספינות עוקפות את נמל המבנטוטה ופונות לנמל קולומבו.[37] עד מהרה התברר כי הנמל החדש אינו רווחי: בשנת 2012 עברו בו 34 ספינות בלבד. סרי־לנקה, שלא יכלה לעמוד בתשלומי ההלוואה שקיבלה מסין לצורך בניית הנמל, ביקשה להקל בתנאי ההלוואה, אולם נענתה בשלילה. המשא ומתן הממושך והלחץ הכספי הכבד הביאו את ממשלת סרי־לנקה להיענות, בדצמבר 2017, להעברת הנמל לשליטה סינית ולהסכם חכירה של שישים קמ"ר מהקרקע של הפרויקט לסין למשך 99 שנים. החכירה אפשרה לסין לשלוט על טריטוריה המרוחקת מאות קילומטרים ספורים מחופי יריבתה הודו, והעניקה לה דריסת רגל אסטרטגית לאורך מעבר מים מסחרי וצבאי בעל חשיבות מכרעת.[38]

אצטדיון הקריקט הבין־לאומי

ב־2011 נפתח בקרבת העיירה המבנטוטה אצטדיון הקריקט הבין־לאומי על שם מהינדה רג'פקסה, שבנייתו באה במטרה לארח את תחרות גביע העולם בקריקט שהתקיימה באותה שנה בסרי־לנקה. זהו האצטדיון השני בגודלו בסרי־לנקה, ותפוסתו היא 32,000 מקומות ישיבה. עלות בנייתו הגיעה לכ־3.8 מיליון דולר. לא עבר זמן רב מאז פתיחתו, עד שהחלו להישמע ביקורות נגדו. בראשן הייתה הביקורת על עלות האחזקה הגבוהה שלו, ולצידה ביקורת על כך שמאז הקמתו

37 Lu-Hai Liang, "Sri Lanka hands over port to China to pay off debt", *The National*, December 14, 2017, https://www.thenational.ae/world/asia/sri-lanka-hands-over-port-to-china-to-pay-off-debt-1.684606.

38 Maria Abi-Habib, "How China Got Sri Lanka to Cough Up a Port", *The New York Times*, June 25, 2018, https://www.nytimes.com/2018/06/25/world/asia/china-sri-lanka-port.html.

התקיימו בו תחרויות בין־לאומיות ספורות.[39] כיום מדובר ב"פיל לבן", המשמש בית לציפורים ולבעלי חיים משוטטים, ולפי הפרסומים גם לאירועים פרטיים, ביניהם חתונות.[40]

ראוי להדגיש כי במקרה של אצטדיון הקריקט הבין־לאומי אין מדובר באינטרס גיאו־פוליטי סיני. זאת, לעומת ההשקעה הסינית בנמל המבנטוטה, שמעניקה לסין הישגים גיאו־פוליטיים ברורים.

שדה התעופה הבין־לאומי בהמבנטוטה

ב־2013 נפתח לטיסות מסחריות שדה התעופה הבין־לאומי על שם מהינדה רג'פקסה בעיירה המבנטוטה. עלות ההקמה של השדה הגיעה ל־209 מיליון דולר, מתוכם 190 מיליון דולר הלוואה סינית. העומס בשדה התעופה הבין־לאומי על שם בנדרנייקה בקולומבו והרצון לצמצם פערים עם אזורים אחרים בסרי־לנקה היו המניעים העיקריים לבניית שדה התעופה הבין־לאומי הנוסף באי. אלא שהמבנטוטה חסרה אוכלוסייה במספרים משמעותיים ותשתית תעשייתית, שיהוו מוקד משיכה לזרים. לא עבר זמן רב והשדה החדש זכה לכינוי "שדה התעופה הריק ביותר בעולם".[41] כמו כן, התברר כי הוא גורם נזק לסביבה, שכן הוא שוכן בלב שמורת טבע. כך, במקרה אחד דווח על מאות חיילים, שוטרים ומתנדבים שפעלו להברחת בעלי חיים מאזור השדה, וגורם רשמי אף אישר כי הם מפריעים לטיסות. יתר על כן, בנחיתה הראשונה בשדה התעופה החדש התנפץ חלון של מטוס עקב פגיעה של ציפור.

גם שדה התעופה הבין־לאומי בהמבנטוטה הפך, כמו אצטדיון הקריקט, ל"פיל לבן", ובשלב מסוים החל לשמש לאחסון אורז.[42] המצב השתנה ב־2018, כאשר הודו הודיעה כי תפעיל את השדה בהסכם חכירה לארבעים שנה ובהשקעה של

---

39 Nirmala Kannangara, "Hambantota White Projects Eat Up Economy", *The Sunday Leader*, June 28, 2015, http://www.thesundayleader.lk/2015/06/28/hambantota-white-projects-eat-up-economy.

40 Hafsa Sabry, "Attempts To Revive Another 'White Elephant'", *The Sunday Leader*, October 16, 2016, http://www.thesundayleader.lk/2016/10/16/attempts-to-revive-another-white-elephant.

41 Wade Shepard, "The Story Behind The World's Emptiest International Airport", *Forbes*, May 28, 2016, https://www.forbes.com/sites/wadeshepard/2016/05/28/the-story-behind-the-worlds-emptiest-international-airport-sri-lankas-mattala-rajapaksa/#3e385ee67cea.

42 "Troops clear wild animals from Sri Lanka's white-elephant airport", *The Phuket News*, March 27, 2016, https://www.thephuketnews.com/troops-clear-wild-animals-from-sri-lanka-white-elephant-airport-56780.php#fiXboQ2cffE7AXhv.97.

225 מיליון דולר בשיפוצו, המהווים 70 אחוזים מעלות השיפוץ. סרי־לנקה תשקיע את הסכום הנותר.[43]

עיר הנמל של קולומבו

בשנת 2014 החלה יציקת היסודות לבניית הנמל המלאכותי בקולומבו, שנועדה להיעשות באמצעות שאיבת חול ים מחופים סמוכים. הנמל החדש צפוי לקום על שטח של 2.69 קמ"ר לצד הנמל המרכזי של בירת סרי־לנקה.[44] מדובר בהשקעת החוץ הישירה הגדולה ביותר בהיסטוריה של סרי־לנקה, שכללה הלוואה של 1.4 מיליארד דולר מענקית הבנייה הסינית CCCC, הנמצאת בבעלות ממשלתית. בפרויקט צפויים להיבנות מגדלי מגורים, מלונות יוקרה, קניונים יוקרתיים, פארקים מרווחים ו־80,000 דירות. זאת, בנוסף להעסקה של כרבע מיליון עובדים סרי־לנקים על בסיס יומי עם סיום הפרויקט.[45]

מאחר ומדובר בנמל אסטרטגי נוסף שנבנה ביוזמה סינית, קיים חשש אמיתי שגם הוא, כמו נמל המבנטוטה, ייפול בעתיד תחת השפעה סינית. התבטאותו של השר הסרי־לנקי הממונה על פרויקט הנמל כי השטח שבו מתבצעת שאיבת חול ים על ידי הסינים לא יאיים על ריבונותה של סרי־לנקה ולא יחתור תחת האינטרסים של הודו,[46] לא הרגיעה את המצב, במיוחד כשכבר בשנת 2014 עגנו בנמל קולומבו צוללות ואוניות מלחמה סיניות חרף התנגדות הודית. יתר על כן, מאות אוניות קרב ממדינות שונות עוגנות בנמל קולומבו לצורך תדלוק והתרעננות, אלא שתדירות הביקורים הסיניים במקום והעובדה שצוללות סיניות עגנו בנמל הממוקם באזור האוקיינוס ההודי, כחלק ממבצע של צבא סין למלחמה בפירטיות במפרץ עדן, אינן דבר שבשגרה.[47] אם לא די בכך, בניית פרויקט עיר הנמל של קולומבו לוותה

43 Meera Srinivasan, "'Mattala project with India is on'", *The Hindu*, August 3, 2018, https://www.thehindu.com/news/international/mattala-project-with-india-is-on/article24595483.ece.

44 "Feature: Hearts bound together, city built together – China, Sri Lanka co-develop Colombo Port City", *Xinhua*, May 15, 2018, http://www.portcitycolombo.lk/press/2018/05/23/hearts-bound-together-city-built-together-China-sri-lanka-co-develop-colombo-port-city.html.

45 Rossi, "Next Hambantota? Welcome to the Chinese-funded US$1.4 billion Port City Colombo in Sri Lanka".

46 "Chinese firm completes US$1.4 billion land reclamation works for Sri Lanka's Colombo Port City project", *South China Morning Post*, January 17, 2019, https://www.scmp.com/news/asia/south-asia/article/2182461/chinese-firm-completes-14-billion-land-reclamation-works-sri.

47 Shihar Aneez, Ranga Sirilal, "Chinese submarine docks in Sri Lanka despite Indian concerns", *Reuters*, November 2, 2014, https://www.reuters.com/article/sri-lanka-china-submarine/chinese-submarine-docks-in-sri-lanka-despite-indian-concerns-idINKBN0IM0LU20141102.

גם בנזק סביבתי: שאיבת החול לצורך בניית הנמל המלאכותי יצרה סחף ושיבשה את המערכת האקולוגית הימית, אשר בתורה הזיקה לתעשיית הדיג באזור.[48]

יחסי ישראל-סין: אינטרסים כלכליים

ישראל הייתה המדינה הראשונה במזרח התיכון שהכירה בסין העממית כבר בינואר 1950, אולם רק בינואר 1992 כוננו יחסים דיפלומטיים בין שתי המדינות. מאז נוצר שיתוף פעולה בתחומים מגוונים, שבשנים האחרונות הגיע לשיאים חדשים. הנציגויות הישראליות בסין מקדמות את דימויה של ישראל כמדינה טכנולוגית וחדשנית, ושתי המדינות מקדמות פרויקטים משותפים בתחומי החדשנות במחקר, במדע, באקדמיה, בחקלאות ובבריאות.[49]

בשנת 2014 הוקם המנגנון הבין־ממשלתי המרכזי בין ישראל לסין – ועידת החדשנות. מדובר בפלטפורמה בין־ממשלתית (G2G) עליה חתמו ראש הממשלה בנימין נתניהו וסגנית ראש ממשלת סין ליו יַנדונג, בעת ביקורה בישראל באותה שנה. הוועידה מתכנסת אחת לשנה לסירוגין בבייג'ינג ובירושלים, ואת עבודתה מובילים 13 משרדי ממשלה וסוכנויות ממשלתיות בישראל, לצד שרים ממשרדי ממשלה סיניים. הוועידה מקדמת שיתופי פעולה בין גורמי הממשל בשתי המדינות, פרויקטים משותפים המשלבים את המגזר הפרטי, מחקרים משותפים בתחומי המדע והתעשייה, מתן מלגות לימוד לסטודנטים משתי המדינות ועוד.[50]

סין רכשה חברות ישראליות, כגון "תנובה", "אדמה" ו"אהבה", והשקיעה בחברות הזנק ישראליות ובקרנות הון סיכון.[51] לצד זאת, סין מעורבת בבניית מנהרות הכרמל, קו הרכבת עכו־כרמיאל, הרכבת הקלה בתל אביב, הפרטת נמלי אשדוד וחיפה, מסילת הרכבת תל אביב–ירושלים ומסילת הרכבת המתוכננת בין תל אביב לאילת.[52]

---

48 Rossi, "Next Hambantota? Welcome to the Chinese-funded US$1.4 billion Port City Colombo in Sri Lanka".

49 "25 שנה לכינון היחסים הדיפלומטיים בין ישראל לסין", משרד החוץ, 23 בינואר 2017, https://mfa.gov.il/MFAHEB/PressRoom/Spokesman/2017/Pages/25-years-Israel-China-diplomatic-relations-230117.aspx.

50 "ביקור סגן נשיא סין – המפגש ה־4 של ועדת החדשנות ישראל–סין", משרד החוץ, 18 באוקטובר 2018, https://mfa.gov.il/MFAHEB/PressRoom/Spokesman/2018/Pages/ Visit_of_Vice_President_of_China_181018.aspx.

51 Dan Catarivas, *Israel-China Relations: Ideal and Reality*, Memorandum No. 194 (Tel Aviv: Institute for National Security Studies, 2019), p. 30.

52 Yossi Melman, "Cause for concern? Chinese investment and Israel's national security", *The Jerusalem Post*, April 7, 2018, https://www.jpost.com/Jerusalem-Report/Chinese-TAKEAWAY-546692.

התקדמות נוספת ביחסים בין ישראל לסין נרשמה בביקורו של ראש הממשלה בנימין נתניהו בסין ב־2017, וכן במיתוג המחודש של מסגרת שיתוף הפעולה בין שתי המדינות, שנקבע על ידי נשיא סין שי ג'ינפינג – "שותפות כוללת בחדשנות" ("Innovative Comprehensive Partnership").[53] שדרוג היחסים התאפשר בחלקו הודות לחיזוק הקשר והדיאלוג בין גורמים וגופים ממשלתיים, ובחלקו נבע מאינטרסים, כמו רצון להשיג נגישות לטכנולוגיות אזרחיות ישראליות מצד אחד, ושאיפה ישראלית לנגישות אל השוק הסיני מצד שני. זאת, בנוסף לחיזוק הקשר האקדמי והמחקרי ולעידוד תנועת אנשים משתי המדינות.[54]

קשרי הסחר שישראל מנהלת כיום עם סין הם מהגדולים והחשובים ביותר עבור ישראל בהשוואה לשאר מדינות העולם. בעשור האחרון חל גידול חד בהיקף הסחר בין שתי המדינות (גם אם באופן לא שוויוני), וסין היא מקור הייבוא הגדול ביותר לישראל ויעד הייצוא השלישי בגודלו שלה (אם מתייחסים לאיחוד האירופי כגוף אחד). הדבר מתבטא בעלייה בייצוא ובייבוא כאחד: ב־2018 עמד היקף הסחר בין ישראל לסין על כ־15.7 מיליארד דולר (עלייה של כ־30 אחוזים לעומת שנת 2017). ב־2018 הגיע הייצוא לסין ל־4.7 מיליארד דולר (זינוק של כ־50 אחוזים לעומת שנת 2017, ואילו הייבוא מסין הגיע לכ־11 מיליארד דולר (עלייה של כ־20 אחוזים לעומת שנת 2017). הדומיננטיות של הייבוא מסין במאזן הסחר בין שתי המדינות מביאה לכך שישראל נמצאת בגירעון סחר מתמשך מול סין.[55]

נמל חיפה

ישראל החלה ב־2004 בתהליך של הפרטת שלושת הנמלים המסחריים שלה – אשדוד, אילת וחיפה. בסופו של התהליך הוחלפה רשות הנמלים בארבע חברות ממשלתיות, שמטרתן הייתה להפריד בין תפעול הנמלים, ניהולם ופיתוחם העתידי, ובין הפעילויות השוטפות בהם. נקבע כי חברת נמלי ישראל תספק את התשתית ותהיה אחראית לפיתוחה, בשעה שהחברות הפרטיות יספקו את שירותי הובלת המטענים, תוך שימוש במתקנים ובציוד שלהן.[56]

ב־2014 זכתה חברת SIPG (חברה בת של "צ'יינה הארבור" הסינית, בעצמה חברה בת של חברת CCCC, הנמצאת, כאמור, בבעלות ממשלתית סינית) במכרז

---

53 "חיזוק שיתוף הפעולה בין סין לישראל בתחום החדשנות והטכנולוגיה", משרד הכלכלה והתעשייה, 19 באוגוסט 2018, https://www.gov.il/he/departments/news/a-billion-chinese-are-not-mistaken.

54 Shagrir, *Israel-China Relations: Innovative Comprehensive Partnership*, p. 14.

55 "ישראל–סין: סקירת סחר כלכלית", מכון היצוא – היחידה הכלכלית, 2018, https://www.export.gov.il/economicreviews/article/israelchinacom2018.

56 Oded Eran, "China Has Laid Anchor in Israel's Ports", *Strategic Assessment*, 19 no. 1, April 2016, p. 56.

לבניית נמל חדש באשדוד במשך שבע שנים ובעלות של 3.6 מיליארד שקל. ב־2015 זכתה קבוצת SIPG גם במכרז להפעלת נמל המפרץ שעתיד לקום בחיפה למשך 25 שנה, וזאת בתמורה לדמי שימוש שוטפים שתעביר למדינה. עלות בניית הנמל הוערכה בשני מיליארד דולר, והוא צפוי להתחיל לפעול בשנת 2021.[57] בחברת נמלי ישראל נאמר כי המפעילים הבין־לאומיים יתכננו, יממנו ויקימו את השטח התפעולי, כולל השלמת מערכות תשתית שונות.[58]

הנמל החדש בחיפה הוא דוגמה למעורבות סינית אסטרטגית־ביטחונית בתחום התשתיות בישראל. מדובר באחת מגולות הכותרת במגמה הפרו־סינית שהוביל שר התחבורה והבטיחות בדרכים לשעבר, ישראל כץ. כחלק מהמגמה הגיע לישראל במאי 2017 צוות חדשות סיני, והשר כץ העניק לו ראיון אישי. בתקשורת הסינית גם פורסם כי שר התחבורה דאז קידם באופן פעיל, מאז נבחר לתפקידו, פרויקטים של תשתיות בין שתי המדינות וכי התבטא בזכות המעורבות הסינית בבניית הנמל החדש באשדוד ובהפעלת הנמל החדש במפרץ חיפה. כמדווח, השר כץ כינה מעורבות זו "צעד בעל חשיבות אסטרטגית לחברות סיניות".[59]

ביוני 2019 הגישה עיריית חיפה לבית המשפט המחוזי עתירה מינהלית למניעת המשך בניית הנמל החדש בעיר, בטענה ששדה התעופה העירוני ייפגע וכי בניית הנמל מונעת את הארכת מסלול ההמראות והנחיתות בו. ראשת עיריית חיפה, עינת קלישׁ־רותם, קבלה כי לא נעשה מחקר מעמיק כדי להבין את ההשלכות של המהלכים החד־צדדיים על קידום הספנות והתעופה בעיר.[60] באוגוסט 2019 צייצה עינת קלישׁ־רותם בעמוד הטוויטר שלה כי הגיעה להסכמות עם משרד התחבורה על הארכת מסלול שדה תעופה חיפה ל־2100 מטר, משיכת העתירות נגד נמל המפרץ והסדרת שחיקת חופי הים.[61]

נמל חיפה החדש, על התשתית הצבאית והאזרחית שלו, הוא נכס אסטרטגי של ישראל. לכן, מעורבות סינית בבנייתו ובהפעלתו עשויה ליצור אפשרות להשפעה

57 "Haifa container terminal deal with China's SIPG under review", *PortSEurope*, December 23, 2018, https://www.portseurope.com/haifa-container-terminal-deal-with-chinas-sipg-under-review.

58 ליאור גוטמן, "SIPG הסינית זכתה במכרז להפעלת הנמל החדש בחיפה", **כלכליסט**, 23 באפריל 2015, https://www.calcalist.co.il/local/articles/0,7340,L-3655245,00.html.

59 Dubi Ben-Gedalyahu, "Israeli minister's Chinese romance provokes US", *Globes*, December 20, 2018, https://en.globes.co.il/en/article-israeli-ministers-chinese-romance-provokes-us-1001265841.

60 מיכל רז־חיימוביץ, דניאל שמיל, "עיריית חיפה נגד המשך בניית הנמל: 'יהרוס את התעופה בעיר'", **גלובס**, 16 ביוני 2019, https://www.globes.co.il/news/article.aspx?did=1001289748

61 מתוך עמוד הטוויטר של עינת קליש רותם, 14 באוגוסט 2019, https://twitter.com/EINATkalisch/status/1161648831894872064?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1161648831894872064&ref_url=https%3A%2F%2Fwww.themarker.com%2Fdynamo%2Fcars%2F1.7684086.

עתידית של ממשלה זרה על רציפות תנועת הסחורות מהנמל ואליו, ובדרך זו עלולה להוות כלי להשפעה על ישראל.[62] עם זאת, בחינת המעורבות הסינית בנמל חיפה בישראל מול המעורבות הסינית בנמל המבנטוטה בסרי־לנקה מעלה הבדל משמעותי בין שני המקרים: במקרה של ישראל, הרחבת נמל חיפה ותפעולו אינה תלויה בהלוואה סינית, ואילו במקרה של סרי־לנקה, בניית נמל המבנטוטה התבססה על הלוואה סינית גדולה, על כל ההשלכות שנבעו מכך.

סיכונים ומסקנות

בכירים בממשלת ישראל מעריכים כי ישראל היא המדינה היחידה שבה תאגידים סיניים השקיעו או קיבלו גישה לפרויקטים בשווי של כ־15 מיליארד דולר.[63] אחת הסיבות לכך היא הרגולציה הישראלית, המבוזרת מבחינת השקעות ורכישות זרות בתחומים אזרחיים, כאשר כל גוף או משרד ממשלתי מפעיל באופן עצמאי רגולטור משלו.[64] חבר הכנסת עפר שלח אמר בעניין זה כי יש צורך ב"מדיניות מתכללת", במיוחד בנוגע לסין, אחרת כל משרד ממשלתי "יקבע את המדיניות בעצמו".[65] ראש "המטה לביטחון לאומי" לשעבר, יעקב נגל, הציע להקים ועדה רגולטורית בין־משרדית בהשתתפות כל הצדדים המעורבים, שתהיה "בעלת סמכויות, ולא בגדר מתן המלצות בלבד".[66]

לאחרונה החליט הקבינט המדיני־ביטחוני על הקמת ועדה מייעצת בראשות משרד האוצר לבחינת היבטי ביטחון לאומי בתהליך האישור של השקעות זרות בישראל, כנהוג במדינות כגון ארצות הברית, קנדה, בריטניה, גרמניה, אוסטרליה ועוד.[67] עם זאת, ובניגוד לוועדות הפועלות באותן מדינות, הוועדה בישראל תקום על בסיס וולונטרי ולא כחלק מחקיקה העוסקת בהשקעות זרות; היא תייעץ לרגולטורים, אך לא לדרגים פוליטיים בכירים, והדיווח אליה יהיה על בסיס וולונטרי ולא בגדר

---

62 Galia Lavi and Rotem Nusem, *The Rising Tension between China and Australia: Lessons for Israel*, Memorandum No. 194 (Tel Aviv: Institute for National Security Studies, 2019), pp. 36-37.

63 Yossi Melman, "Over U.S. objections, Chinese firms step up their involvement in Israel", *The Jerusalem Post*, July 13, 2019, https://www.jpost.com/Jerusalem-Report/Over-US-objections-Chinese-firms-step-up-their-involvement-in-Israel-595325.

64 Doron Ella, *Regulation of Foreign Investments and Acquisitions: China as a Case Study*, Memorandum No. 194 (Tel Aviv: Institute for National Security Studies, 2019), p. 61.

65 Melman, "Cause for concern? Chinese investment and Israel's national security".

66 Jacob Nagel, "Ex-national security advisor to 'Post': Israel needs to review China deals", *The Jerusalem Post*, January 10, 2019, https://www.jpost.com/Opinion/Ex-national-security-advisor-to-Post-Israel-needs-to-review-China-deals-576891.

67 "הודעת ועדת השרים לענייני ביטחון לאומי", *משרד ראש הממשלה*, 30 באוקטובר 2019, https://www.gov.il/he/departments/news/spoke_national_security301019.

חובה. בנוסף לכך, טכנולוגיות שונות בהיי־טק, שהן סוגיה "חמה" בין ארצות הברית לישראל, לא יחויבו בפיקוח הוועדה.[68] חסרונות אלה של הוועדה עשויים להוות פתח לנזקים מדיניים, לסיכונים ביטחוניים ולהשפעה על פוליטיקאים בישראל.

נזקים מדיניים אפשריים כתוצאה ממעורבות סינית בפרויקטים אסטרטגיים בישראל עלולים לנבוע גם מניגוד האינטרסים בין ארצות הברית לסין, כשישראל מצויה בתווך. הפוטנציאל לפגיעה ביחסים ההדוקים בין ישראל לארצות הברית על רקע המעורבות הסינית בישראל מוצא ביטוי במחקר של "המרכז לביטחון אמריקאי חדש" (CNAS), הקובע כי בניית נמל המפרץ בחיפה עלולה להיות מסוכנת מבחינה גיאו־פוליטית. בנוסף לכך, היועץ לשעבר לביטחון לאומי של ארצות הברית, ג'ון בולטון, הביע חשש מפני שליטה עתידית סינית על תפעול הנמלים בישראל, תוך שהוא מדגיש במיוחד את העובדה שנמל המפרץ בחיפה מארח תמרונים ימיים בין ישראל לארצות הברית על בסיס קבוע ומשמש גם נקודת עגינה לצי השישי האמריקאי הפועל בים התיכון.[69] בנוסף לכך נשמעו אזהרות מפורשות מפיו של סגן שר האנרגיה של ארצות הברית, דן ברויט, שאמר כי "אם ישראל תעמיק את שיתוף הפעולה הזה, יתכן ולא נחלוק איתה מידע מודיעיני".[70]

עיקר הסיכונים הביטחוניים משיתוף הפעולה המתהדק עם סין נובע מההשקעה הסינית בתשתיות ישראליות אסטרטגיות ומהחדירה הסינית אליהן ואל חברות טכנולוגיה ישראליות שונות. ראש השב"כ, נדב ארגמן, התריע בהקשר זה כי "יש פיגור של החוק בישראל לעומת הצרכים הביטחוניים, מבחינת פיקוח על השקעות של מדינות זרות", ואף הזהיר כי "ההשפעה הסינית בישראל מסוכנת, במיוחד בכל הקשור לתשתיות אסטרטגיות וחברות גדולות במשק".[71] ראש המוסד לשעבר, אפרים הלוי, התבטא גם הוא בעניין זה, ואמר כי למרות שאינו מתנגד ליחסי מסחר עם סין, הוא מתנגד "לכל פעולה שתביא לשליטה סינית על עורק תחבורה ראשי

---

68 Doron Ella, "A Regulatory Mechanism to Oversee Foreign Investment in Israel: Security Ramifications", *INSS Insight* No. 1229, November 19, 2019, https://www.inss.org.il/publication/a-regulatory-mechanism-to-oversee-foreign-investment-in-israel-security-ramifications.

69 Daniel Kliman, Rush Doshi, Kristine Lee and Zack Cooper, "grading china's belt and road", *Center for a New American Security*, April 8, 2019, p. 14, https://www.cnas.org/publications/reports/beltandroad.

70 **גלי צה"ל**, טוויטר, 15 בינואר 2019, https://twitter.com/glzradio/status/1085404578122776576.

71 "Shin Bet chief said to warn Chinese investment in Israel poses security threat", *The Times of Israel*, January 10, 2019, https://www.timesofisrael.com/shin-bet-chief-said-to-warn-chinese-investment-in-israel-poses-security-threat.

אסטרטגי בישראל". הלוי גם הזהיר כי אם סין תשלוט במסילת הרכבת בקו אשדוד–אילת, תהיה לה שליטה על "נקודות שליטה פוליטיות וכלכליות" בתוך ישראל.[72]

לעומת המסתייגים, יש הסבורים כי הסיכון העיקרי בריבוי ההשקעות הסיניות בישראל אינו נובע מההשלכות של השקעה בתשתיות אסטרטגיות, אלא מההשקעה בחברות טכנולוגיה ישראליות. לפי טענה זאת, השקעה בחברות כאלו עלולה לאפשר לסין לפתח בעתיד טכנולוגיות שבסיסן בישראל, להזיק בכך ליחסי ישראל עם ארצות הברית ולחבל ביכולת התחרותית הכלכלית של ישראל בזירה הבין־לאומית.[73]

סיכון נוסף של ריבוי השקעות הוא ההשפעה הפוטנציאלית על פוליטיקאים. השפעה כזו עלולה להתרחש, למשל, כתוצאה ממעורבות סינית (או אחרת) בלתי מוסדרת. למרות שחוק מימון מפלגות משנת 1973 וחוק המפלגות משנת 1992 אוסרים על מפלגות ישראליות לקבל תרומות מגורמים שאינם בעלי זכות בחירה לכנסת, אין הם מונעים מתן תרומות ישירות לפוליטיקאים.[74]

בעניין זה, קבע מחקר של CNAS כי פרויקטים שבוצעו במסגרת היוזמה הסינית במדינות שונות ברחבי העולם שבהן מתקיימת קלפטוקרטיה (kleptocracy), היו משולבים במתן שוחד לפוליטיקאים ולביורוקרטים.[75] כך, למשל, שר האוצר של סרי־לנקה האשים ב־2016 את ממשלת רג'פקסה כי שווי הבנייה האמיתי של האצטדיון בהמבנטוטה היה כרבע מהסכום שזו פרסמה בשעתה[76] (למרות שהאצטדיון אינו פרויקט בעל חשיבות אסטרטגית סינית). בנוסף דווח כי חברות סיניות העבירו שוחד למשפחתו של נשיא סרי־לנקה לשעבר, רג'פקסה. גם במלזיה נחתמו, כמדווח, פרויקטים עם חברות סיניות בעלות מנופחת, ונמסר כי חלק מהכספים עבר לידי פוליטיקאים. בנגלדש הכניסה את החברה הסינית "צ'יינה הארבור" לרשימה השחורה בגין ניסיון לשחד פוליטיקאי בכיר בממשלה. עוד דווח כי חברות סיניות

---

72 "Former Mossad chief Efraim Halevy warns against China's role in Israeli rail", *The Economic Times*, October 5, 2013, https://economictimes.indiatimes.com/former-mossad-chief-efraim-halevy-warns-against-chinas-role-in-israeli-rail/articleshow/23579256.cms.

73 Yoram Evron, "Chinese Investments in Israel: Opportunity or National Threat?", *INSS Insight* No. 538, April 8, 2014, https://www.inss.org.il/publication/chinese-investments-in-israel-opportunity-or-national-threat.

74 Lavi and Nusem, "The Rising Tension between China and Australia: Lessons for Israel", p. 39.

75 Daniel Kliman, Rush Doshi, Kristine Lee and Zack Cooper, "grading china's belt and road", *Center for a New American Security*, April 8, 2019, p. 6, https://www.cnas.org/publications/reports/beltandroad.

76 "Ravi K Says Actual Cost of Hambantota Cricket Stadium Is Rs. 852 Million, And Not Rs. 4.5 Billion As Claimed By Rajapaksa", *Colombo Telegraph*, July 23, 2016, https://www.colombotelegraph.com/index.php/ravi-k-says-actual-cost-of-hambantota-cricket-stadium-is-rs-852-million-and-not-rs-4-5-billion-as-claimed-by-rajapaksa.

העניקו לבן הנשיא ולסגן הנשיא בגינאה המשוונית תשלומים במיליוני דולרים. פקיסטאן עצרה פרויקטים של היוזמה הסינית מחשש לשחיתות, ובאקוודור נתון סגן הנשיא לשעבר בחקירה על האשמות לקבלת שוחד מסין.

הנכונות הסינית לשלם לפוליטיקאים בכדי להקל על ביצוע פרויקטים, ונכונותם של אלה לקבל שוחד מביאות לפגיעה במוסדות הדמוקרטיים, וזאת בניגוד מוחלט לאינטרס הציבורי.[77] הדבר מעורר חשד במיוחד כשתנאי העסקאות הנחתמות בפרויקטים המבוצעים במסגרת היוזמה הסינית אפופים חשאיות, מה שמעורר את החשש שפוליטיקאים מקומיים ירוויחו מהם יותר מאשר האזרחים.[78]

מצב כזה עלול להתרחש לא רק בדמוקרטיות המאופיינות בקלפטוקרטיה. מתברר כי גם פוליטיקאים באוסטרליה קיבלו תרומות מאנשי עסקים סינים בתמורה לתמיכה במדיניותה של סין.[79] בנסיבות שתוארו לעיל אין, לפיכך, להוציא מכלל אפשרות השפעה עתידית סינית (ואחרת) גם על פוליטיקאים ישראלים ועל פקידים במערכת הביורוקרטית, המעורבים בקביעת מדיניות ובקבלת החלטות במדינת ישראל.

77 Daniel Kliman, Rush Doshi, Kristine Lee and Zack Cooper, "grading china's belt and road", *Center for a New American Security*, April 8, 2019, pp. 6-7, https://www.cnas.org/publications/reports/beltandroad.

78 "China's belt-and-road plans are to be welcomed – and worried about", *Economist*, July 26, 2018, https://www.economist.com/leaders/2018/07/26/chinas-belt-and-road-plans-are-to-be-welcomed-and-worried-about.

79 A. Odysseus Patrick, "This Chinese mogul made powerful friends in Australia. Now he's a case study on worries over Beijing's influence", *The Washington Post*, October 7, 2019, https://www.washingtonpost.com/world/asia_pacific/this-chinese-mogul-made-powerful-friends-in-australia-now-hes-a-case-study-on-worries-over-beijings-influence/2019/10/05/c5f7f1e6-dea9-11e9-be7f-4cc85017c36f_story.html.

הדין הפלילי ככלי להתמודדות עם תופעת האלימות המקוונת בקרב בני נוער

לימור עציוני

מאמר זה מבקש לבחון האם הדין הפלילי ערוך להתמודד עם תופעת האלימות המקוונת בקרב קטינים. במקרים רבים הדין הפלילי אינו דרך ההתמודדות המיטבית עם תופעת האלימות המקוונת, ולכן הפנייה אליו צריכה להיות מוצא אחרון, תוך נקיטת זהירות מיוחדת, בפרט כשאותה אלימות נובעת לעיתים לא מאופי "עברייני", אלא ממאפייניה של הרשת, הסוחפים קטינים נורמטיביים לבצע מעשים אסורים. הדרך העדיפה היא התמודדות מלכתחילה, כלומר התמקדות בחינוך ובמניעה ולא בענישה בדיעבד. מדובר בנושא חברתי מן המעלה הראשונה, אשר הורים, ילדים ומחנכים צריכים להיות מודעים לו.

מילות מפתח: בריונות, אלימות רשת, נוער, קטינים, סייבר, משפט פלילי, חינוך ומניעה.

מבוא

ההגנה על ילדים ובני נוער מפני פגיעה מקוונת צריכה להיעשות בכמה מישורים: הראשון והעיקרי שבהם הוא המישור החינוכי, שהפעילות במסגרתו אמורה להיות מכוונת כלפי מורים, ילדים והורים. יש לפתח שיטות ואמצעים חדשים להתמודדות עם התופעה, וכל המערכת המקיפה את התלמיד – משפחה, חברים וצוות חינוכי – צריכה להיות שותפה לפיתוח תוכניות התמודדות ולהפעלתן. המקרה של אלימות ברשת מאפשר ומזמין שיתוף פעולה הדוק במיוחד בין הצוות החינוכי ובין ההורים.

חשוב שגם הצוות החינוכי וגם ההורים יבינו ויכירו את המרחב המקוון ואת הסכנות הטמונות בו. גם חשוב לזכור שאלימות שמתחילה במרחב הבית־ספרי ממשיכה לא פעם למרחב המקוון, ובריונות ואלימות במרחב הווירטואלי גולשות

ד"ר לימור עציוני היא מרצה בכירה במרכז האקדמי שערי מדע ומשפט וחוקרת בכירה בתוכנית לביטחון סייבר במכון למחקרי ביטחון לאומי. להרחבה בנושא המאמר ראו ספרה **נוער במשפט הפלילי**, הוצאת נבו, 2019.

לעיתים למרחב הפיזי הבית־ספרי. המערכת הבית־ספרית נדרשת, אפוא, להיערכות שתחרוג משעות הפעילות בבית הספר. זאת ועוד, יש לנהל שיחות בנושא זה עם הילדים כדי להעלות את המודעות שלהם לתופעה, להביאם להבין את ההשלכות של מעשיהם ולפנות לעזרה בעת הצורך.

מישורים נוספים שבהם צריך להתמודד עם תופעת האלימות המקוונת הם מישור הרגולציה הציבורית. זו צריכה לקבוע את כללי המשחק והאמצעים להגנה על קטינים שייפגעו מהפרת אותם כללים, וכן פעולות להסְדרה עצמית שייעשו בהסכמה ובאופן וולונטרי באתרים וברשתות החברתיות.

בעשור האחרון התרחב השימוש באינטרנט במידה כזאת, שכיום הוא חלק בלתי נפרד מחיינו במישורים רבים: המישור המקצועי, התנהלותנו כצרכנים, מגענו עם הרשויות, מקורות הידע שלנו, וגם המרחב החברתי לניהול מערכות יחסים. אחד משימושי האינטרנט הפופולריים ביותר בשנים האחרונות בקרב בני נוער בארץ ובעולם הוא הפעילות ברשתות החברתיות. מחקרים שנערכו בארצות הברית ובאירופה מצאו כי 60־75 אחוזים מן הילדים בני תשע או יותר משתמשים ברשתות חברתיות, ושיעורם עולה ליותר משמונים אחוזים בגיל ההתבגרות. מחקר של חברת "בזק" שנערך בישראל בשנת 2018 מלמד כי 95 אחוזים מבני הנוער בישראל בגילאי 13־18 משתמשים ברשת "וואטסאפ", 88 אחוזים פעילים ב"אינסטגרם" ו־65 אחוזים – ברשת "פייסבוק"; 43 אחוזים מההורים לא הגבילו באותה שנה את זמן השימוש, בעוד שבשנת 2017 חמישים אחוזים מהם הגבילו אותו לשעתיים ביום.[1]

האינטרנט, ובפרט הרשתות החברתיות, הפכו לחלק מסדר יומם של רוב בני הנוער, ואף של קטינים צעירים יותר. לשימוש ברשת על ידי קטינים יש כמובן יתרונות רבים: ללמידה ולהרחבת אופקים, להיחשפות לתכנים ולעולמות חדשים, לצורכי יצירה וביטוי עצמי, ואף לצורך בניית קשרים חברתיים ופיתוח תחושת שייכות. עם זאת, השימוש באינטרנט עלול לחשוף את הקטינים לסכנות: הוא עלול להוות מקור להשפעה שלילית, להתנהגויות מסַכנות ומסוכנות, לחציית גבולות ולחשיפה לתכנים פוגעים ומזיקים. השפעותיו השליליות של האינטרנט על קטינים הן נושא רחב ביותר. ניתן לדון בו בשלל הקשרים, החל בחשיפת קטינים לחומר פורנוגרפי וכלה בשידול קטינים במרחב האינטרנטי בידי עבריינים מין המבקשים לנצלם. מאמר זה יתייחס רק לאחת התופעות השליליות של חשיפת קטינים לאינטרנט, והיא תופעת האלימות בקרב קטינים ברשת.

התנהגות אלימה המתקיימת באינטרנט מציבה שלל אתגרים, ובהם חינוכיים, חברתיים ומשפטיים, שגם המשפט הפלילי נדרש להתמודד איתם. להלן תיבחן תופעת האלימות המקוונת תוך התמקדות באותם מקרים שבהם שני הצדדים

1 https://www.bezeq.co.il/media/PDF/doh_2018.pdf.

– התוקף והנפגע – הם קטינים. הדיון ייסוב סביב השאלה האם הדין הפלילי הישראלי ערוך להתמודד עם תופעה זו.[2]

הגדרה

ניתן להגדיר "אלימות מקוונת", המכונה גם "בריונות מקוונת" (Cyber-Bullying),[3] כשימוש של פרט או קבוצה במידע ובטכנולוגיה כדי לתמוך בהתנהגות מכוונת ותוקפנית חוזרת ונשנית במטרה לפגוע באחרים. האלימות ברשת היא סוג חדש של אלימות, עשויה לבוא לידי ביטוי בשימוש במגוון אמצעים אלקטרוניים, כמו טלפונים ניידים חכמים ומחשבים, ומתבטאת בעיקר דרך שימוש ברשתות חברתיות, כגון "ווטסאפ", "פייסבוק", "אינסטגרם" ו"סנאפצ'ט". היא מתרחשת בכל מקום – בבית הקטין, בבית הספר, במסיבה או בעת בילוי, ויכולה לכלול הצקות, רכילות, מסרים טורדניים, מעליבים, משפילים ואף מאיימים, התחזות, הפצה ברבים של חומר הקשור בצנעת הפרט, סחיטה ושימוש במצלמות אינטרנט להעברת תכנים פוגעניים, כגון תמונות או סרטוני וידאו. יעד הפעילות יכול להיות אדם "מציאותי" (אמיתי), או אדם "וירטואלי" הקיים רק במרחב המקוון.

הגדרת אלימות מקוונת כ"מכוונת ותוקפנית במטרה לפגוע באחרים" יוצרת קושי, במיוחד כשהדיון נוגע לקטינים. במקום אחר ציינתי בעניין זה: "הואיל ומדובר לרוב בשימוש במילים ובתמונות, הגבול שבין הצקה פשוטה, שלצערנו מאפיינת קשרים בין בני אדם בכלל וילדים בפרט, לבין התנהגות 'מכוונת ותוקפנית במטרה לפגוע', אינו ברור. בנוסף, התנהגות יכולה להיות גם התעלמות או נידוי ממסגרת או ממרחב מסוים. תופעות כגון חרם ומניעת השתתפות הן בעלות עוצמה רבה".[4] ברור כי מן הקושי בהגדרת התופעה נובע גם הקושי להתמודד עימה היטב, ואולם אין להסיק מקושי זה אי־יכולת של הדין הפלילי להתמודד עם המקרים המהווים עבירה.[5]

---

2 במאמר אחר התייחסתי בהרחבה לשאלת האלימות במגרש המשחקים המקוון, תוך הדגשת אחריותן של ספקיות התוכן ומפעילות האתרים לנעשה בשטחן. ראו: לימור עציוני, "בריונות במגרש המשחקים המקוון – אחריות ספקיות התוכן ומפעילות האתרים על הנעשה בשטחן", **המשפט**, יז, 463 ,2013.

3 אני מבכרת את המושג "אלימות מקוונת" ולא "בריונות מקוונת", מאחר שלמונח "בריונות" מתלווה קונוטציה של מעשים שאינם חמורים, המבוצעים על ידי קטינים כחלק ממשובת נעורים ותו לא, ואילו המעשים שאדון בהם כאן אינם כאלה כלל ועיקר.

4 עציוני, "בריונות במגרש המשחקים המקוון", עמ' 470.

5 יתרה מזו, בפסקי דין רבים שניתנו בשנים האחרונות נראה כי משתרשת ההבנה שבעת המודרנית, שבה המרחב הווירטואלי הוא חלק בלתי נפרד מחיי החברה, יש להכיר בעבירות הנעשות במרחב זה ולהעניש בגינן בחומרה. ראו, למשל, את דברי השופטת דפנה ברק־ארז בע"פ 7725/11, **פלוני נ' מדינת ישראל**: "כאשר מביאים בחשבון את הדרכים החדשות ליצירת קשר בין אנשים, תוך שימוש באמצעים השונים שמעמידה לרשותנו הטכנולוגיה המודרנית, מעשה מגונה יכול להיעשות גם תוך שימוש במסרים אלקטרוניים, תמונות

דרכי הביטוי המוכרות ביותר של אלימות באינטרנט בקרב קטינים

שלל ההתנהגויות האלימות הוא אינסופי – כיד הדמיון. ההתנהגויות הפשוטות והנפוצות ביותר הן שליחת דוא"ל, מסרונים והודעות ברשתות חברתיות, כגון "פייסבוק" או "ווטסאפ", בכמות גדולה למי שאינו מעוניין בכך.[6] התוכן יכול לכלול איומים לפגוע, התייחסויות מיניות, ביטויי שנאה וכדומה. ניתן לסווג מכלול התנהגויות זה של אלימות מקוונת בין קטינים לכמה דרכי ביטוי עיקריות:

- **הטרדה** – שליחה חוזרת ונשנית של מסרים רבים ופוגעניים (קללות, העלבות, איומים) לקורבן באמצעות מסרים מיידיים, מסרונים בטלפון הנייד, מסרונים רבים ובלתי פוסקים או הודעות ברשת החברתית.[7]
- **התלהמות** – החלפת דברים פוגעניים, בוטים ומעליבים בדיונים בפורומים, בחדרי שיחות (צ'ט) ובקבוצות "ווטסאפ". המעורבים בעניין נגררים, בדרך כלל, להתנהגות מתלהמת, והאווירה הופכת ללוחמנית ופוגענית.[8]
- **השמצה** – הפצת סיפורים שקריים ומידע כוזב באמצעות שליחת מידע כזה למספר רב של מכרים. המטרה בהשמצה היא הריסת התדמית של הקורבן ופגיעה בקשריו ובמעמדו החברתי.
- **התחזות** – שימוש בפרטיו האישיים של הקורבן כדי להתחזות אליו ולבצע פעולות בשמו. לדוגמה, נער נכנס לרשת בתור נער אחר וכותב בשמו הודעות דוא"ל פוגעניות לכמה חברים.[9]

במחשב ועוד. בעולם שניתן לקיים [בו] קשר בין אנשים באמצעות חוטים, תדרים ומסרים אלקטרוניים, מעשה מגונה יכול להיעשות 'באדם' באותם אמצעים ממש", ע"פ 7725/11, **פלוני נ' מדינת ישראל** (פורסם בנבו, 24.1.2013).

6 דוגמה למקרה קיצוני כזה היא של הנער דוד־אל מזרחי, שהתאבד לאחר מסכת התעללויות ב"פייסבוק" שכללה קללות, השפלות והצקות, אשר הובילו אותו למעשה קיצוני זה. עוד דוגמה היא של הנערה רבקה אן סדוויק מארצות הברית, שהתאבדה לאחר שקיבלה הודעות נאצה ברשת חברתית משתי נערות שהאיצו בה להתאבד. למקרים נוספים ראו: ענת ליאור, "בריונות ברשת – קריאת השכמה למחוקק הישראלי", **אתר משפט ועסקים**, 2013 idclawreview.org/2013/11/17/blogpost-20131117-lior.

7 ע"פ 9152/06 **פלוני נ' מדינת ישראל** (פורסם בנבו, 19.2.2007), שבו מתואר מקרה של קטינים שהטרידו קטינה אחרת, בין היתר באמצעות מסרים מאיימים במשיבון הקולי ובמחשב; עפ"ג (מחוזי מרכז) 11–01–25892 **חורי נ' מדינת ישראל** (פורסם בנבו, 9.2.2011), שם מתואר מקרה שבו המערער והמתלוננת הכירו באתר היכרויות באינטרנט, ולאחר כמה פגישות ביקשה המתלוננת להפסיק את הקשר. בעקבות זאת החל המערער להטריד אותה בכך שהתקשר אליה פעמים רבות וקילל אותה.

8 יצוין כי משחקי מחשב הכוללים משחקי לחימה מאפשרים לעיתים להתנכל לדמות וירטואלית של קטין, למשל באמצעות התאגדות נגדו או תקיפות כלפיו החורגות ממטרת המשחק הרשמית.

9 בש"פ 4820/15 **מדינת ישראל נ' פלוני** (פורסם בנבו, 14.7.2015) תואר מקרה שבו פרץ המערער לחשבון ה"פייסבוק" של קטין כדי ליצור קשר עם קטינות אחרות.

- **החצנה והולכת שולל** – חשיפת מידע אינטימי ופרטי על הקטין. למשל, חשיפת בלוג אנונימי וזיהויו עם אדם מסוים (תופעה האופיינית לתכנים הקשורים לנטיות מיניות), או הפצת תמונות וסרטונים אישיים ברשת.[10]
- **מניעה** – חרם אינטרנטי. זהו מצב שבו קבוצה שלמה מנדה קטין מזירות חברתיות. למשל, כאשר כיתה שלמה מחרימה ילד מסוים או אינה מאשרת אותו כחבר ב"פייסבוק".
- **מעקב** – התחקות אחר קטין לשם השגת פרטים ומידע אישי כדי לפגוע בו, לסחוט אותו או להטיל עליו אימה.
- **איומים** – משלל סוגים הנאמרים בהקשר האישי, כמו איום בפגיעה עצמית או על חיי אדם אחר. איומים ברשת יכולים להתבצע בתוכנות למסרים מיידיים, בדואר האלקטרוני, ברשת החברתית ועוד.[11]

המאפיינים הייחודיים של אלימות ברשת

"מסך המחשב, שהוא הכלי המציג לנו באופן חזותי את האותות החשמליים המתקבלים מהמחשב, משקף במידה רבה את הדו־קוטביות המאפיינת את הרשת. הזגוגית השקופה הניצבת בקדמת המסך פותחת לפנינו צוהר למידע רחב ועשיר ועולמות חדשים. חלקו האחורי של המסך, לעומת זאת, אטום וסגור ויכול לדַמות את העלטה בה אנו מצויים ביחס לזהות האמיתית של האנשים המצויים מצידה השני של הרשת".[12]

השימוש ברשת הוא בעל מאפיינים ייחודיים, וגם לאלימות המבוצעת בה ייחוד משלה.[13] האנונימיות מאפשרת לקטין לשתף את האחר או לגלות לו פרטים אישיים מבלי להיחשף. מרבית הקורבנות של אלימות ברשת אינם מכירים את התוקף,

---

10 ע"פ 2656/13 **פלוני נ' מדינת ישראל** (פורסם בנבו, 21.1.2014), שם מתואר כי המערער צילם קטינות ללא ידיעתן במהלך התכתבויות ביניהם ואיים לפרסם את התמונות אם לא יבצעו את שביקש. להרחבה בנושא הפצת תצלומים בקרב בני נוער ברשת ראו: אתי וייסבלאי, "הפצת צילומים פוגעניים ברשת האינטרנט על ידי ילדים ובני נוער", *הכנסת, מרכז המחקר והמידע*, 2010; ראו גם ע"פ 6357/11 **ברברמן נ' מדינת ישראל** (פורסם בנבו 26.12.2013), שם מדובר במערער שהורשע בשורה של עבירות מין כלפי קטינות, שאותן הכיר ברשתות החברתיות. המערער נהג לפתות את הנערות באמצעות שימוש ברשתות החברתיות השונות.

11 ע"פ 538/13 **סבח נ' מדינת ישראל** (פורסם בנבו,26.12.2013) , שם מדובר במערער שאיים על כמה קטינות כי אם לא יבצעו את בקשותיו, יפגע בעצמו ויספר למשפחותיהן על מעשיהן המיניים עימו. הוא אף איים בהתאבדות.

12 השופט הנדל בע"פ 2656/13 **פלוני נ' מדינת ישראל** (פורסם בנבו 21.01.14).

13 עידית אבני ואברום רותם, "פגיעה מקוונת", **מתקוונים לאתיקה**, 3, 2009, /ianethics.com wp-content/uploads/2009/10/cyberBullying_IA_oct_09.pdf.

ולתוקפים יש יכולת לשמור על זהות בדויה ולהישאר אנונימיים.[14] האנונימיות המוחלטת משחררת עכבות, ויש אנשים מסוימים שבהם היא מעוררת רוע של ממש. יתרה מזו, האנונימיות המוחלטת אף יכולה להביא להבעה מוגזמת של רגשות שליליים, מבלי להתחשב בנורמות ובמגבלות של "העולם האמיתי".[15]

זאת ועוד, ב"עולם האמיתי" אלימות והצקה מתרחשות בזירה תחומה – בגבולות בית הספר, בקרב חברים, בחוג או בקבוצת נוער – ואילו האינטרנט מאפשר תפוצה רחבה ומהירה למספר רב של משתמשים.[16] למעורבים באלימות ברשת יש יכולת להפיץ הודעות, תמונות או כל חומר אחר לקהל רב ומגוון, מבלי שהתוקף מודע, פעמים רבות, לכדור השלג שגִלגל.[17]

תופעת האלימות המקוונת מתייחדת גם בנגישותו של האינטרנט בכל מקום ובכל שעה, כאשר הגבול בין מקום הימצאותו של הפוגע ובין מקום הימצאות הקורבן מטושטש לחלוטין. אם בעבר היה לקורבן מקום מפלט מההטרדה בביתו, בהטרדה האינטרנטית אין לו לאן לברוח, וההצקות חודרות למרחב הפרטי ואינן מותירות לו מקום מפלט.[18]

התמודדות במישור הדין הפלילי

למרות הסייגים הקיימים באשר לשימוש בדין הפלילי לצורך התמודדות עם אלימות מקוונת, ייתכן שיהיו מקרים שהזירה הראויה להתמודדות עימם תהיה זירת הדין הפלילי. בהכללה ניתן לומר שמקרים אלה נחלקים לשני סוגים עיקריים: הסוג

---

14 Wannes Heirman & Michel Walrave, "Assessing Concerns and Issues about the Mediation of Technology in Cyberbulling", *Cyberpsychology, Journal of Psychosocial Research on Cyberspace*, vol. 2, no. 2 (2008).

15 ליאור, "בריונות ברשת – קריאת השכמה למחוקק הישראלי": "מחקרים רבים שנערכו בארצות הברית ובאיחוד האירופי מצביעים על כך שיש סיכוי גבוה שבני נוער בעלי פרופיל ברשתות חברתיות יהיו מעורבים באירועי פגיעה מקוונים. המחקרים מעידים כי השיעור הגדול ביותר של פגיעה מקוונת, כ־41%, הוא בבנות בגילאי 15–17".

16 כך, למשל, בקבוצות שונות ב"פייסבוק", בני הנוער משתמשים ברשת כדי להקניט ולהעליב נערים אחרים. ראו, למשל, את המקרה של הקטינה שנערה החלה להתעלל בה ברשתות החברתיות השונות. בין היתר היא הפיצה סרטונים פורנוגרפיים שעליהם הדביקה את ראשה של הקטינה. הפרסום בוצע בקבוצה שבה חברים כ־90,000 בני נוער וגרר אחריו קללות, איומים והשפלות מצד נערים ונערות שאינם מכירים כלל את הקטינה. להרחבה בנושא זה ראו: לירון שמם, "הכתובת על הקיר", *Mako*, 11 באפריל 2013, www.mako.co.il/nexter-weekend/Article-6554514438eed31006.htm.

17 Michele L. Ybarra & Kimberly J. Mitchell, "Online Aggressor/Targets, Aggressor and Targets: A Comparison of Youth Characteristics", *Journal of Child Psychology and Psychiatry* 45:7 (2004): 1308-1316.

18 Janis Wolak, Kimberly J. Mitchell & David Finkelhor "Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-Only Contacts", *Journal of Adolescent Health*, 41 (2007): S51–S58.

הראשון כולל מקרים שבהם ברור מאליו כי אילו האלימות התרחשה ב"עולם האמיתי" ולא בעולם המקוון, לא היה ספק שהם מהווים עבירה פלילית. דוגמה מובהקת ופשוטה לכך היא צילום קטין בסיטואציה אינטימית ללא ידיעתו וללא אישורו והפצת התצלום באמצעות האינטרנט; הסוג השני של מקרים כולל מעשים אלימים המבוצעים בין קטינים וייחודיים לעולם הווירטואלי, אלא שתוצאות המעשים (או פוטנציאל התוצאות) חמורות במיוחד ולכן יחייבו תגובה עונשית.

בישראל אין חקיקה ספציפית נגד אלימות ברשת ("בריונות רשת"), על אחת כמה וכמה לא חקיקה פלילית. בהיעדר הסדר מיוחד, מעשים המבוצעים במרחב הווירטואלי יצטרכו להיבחן בהקשר הפלילי על פי הכלים הקיימים היום – בדיקה אם מתמלאים יסודות העבירה העובדתיים והנפשיים. לעומת זאת, ישנה בישראל חקיקה העוסקת בהעמדה לדין פלילי של קטין שהפיץ סרטונים בעלי תוכן מיני. בשנת 2014 קבע המחוקק סעיף חדש בחוק למניעת הטרדה מינית,[19] הידוע בתקשורת כ"חוק הסרטונים". הסעיף קובע כי הטרדה מינית תהיה גם "פרסום תצלום, סרט או הקלטה של אדם, המתמקד במיניותו, בנסיבות שבהן הפרסום עלול להשפיל את האדם או לבזותו, ולא ניתנה הסכמתו לפרסום...". החוק קובע עונש של חמש שנות מאסר על עבירה זו.

התיקון לחוק נועד להתמודד עם התגברות התופעה של פרסום תמונות, סרטונים או הקלטות בעלי אופי מיני ברשתות חברתיות ובאמצעות אפליקציות סלולריות להעברת מסרונים, כאשר הפרסום לא נעשה בהסכמת המצולמים. בהנחיית פרקליט המדינה[20] נאמר כי קיים אינטרס ציבורי ממשי באכיפת החוק על מבַצעי העבירה, גם כאשר מדובר בחשודים שהם קטינים ונעדרי עבר פלילי. זאת, נוכח פגיעתה הקשה של העבירה והשלכותיה מרחיקות הלכת על קורבנותיה, ובשל הצורך להטמיע את האיסור הפלילי גם בקרב בני נוער.

כאמור, כשמדובר באלימות ברשת, מערכת אכיפת החוק נאלצת להתמודד עם התופעה באמצעות הכלים הקיימים היום בדין הפלילי. דבר זה דורש מן הגורמים העיקריים המטפלים בנושא – המשטרה, הפרקליטות ובתי המשפט – זהירות המשולבת ביצירתיות; במילים אחרות, עליהם לבחון אם מעשה מסוים בלבוש חדש נופל להגדרה של עבירה קיימת, או אם מדובר בחידוש שאין ביכולתו של הדין הפלילי להסדירו. מנגד, על אותם גורמים להפעיל אמת מידה של זהירות בבואם להחיל את הדין הפלילי על קטינים. "זהירות יצירתית" זו היא מחויבת המציאות משני טעמים עיקריים: הטעם הראשון הוא שיש לפעול למניעת יצירתו של שטח חוץ־טריטוריאלי במרחב האינטרנטי, שבו קטינים מופקרים למעשי אלימות מצד חבריהם. כפי שתואר לעיל, אלימות מקוונת פורצת את רשתות ההגנה סביב

19 חוק למניעת הטרדה מינית, תשנ"ח–1998.

20 הנחיית פרקליט המדינה 2.29.

הקטינים, חודרת לחייהם הפרטיים ולביתם שאמור להיות מבצרם, ומביאה לפגיעה במישורים רבים. המחשבה שילדים אינם מוגנים בביתם קשה לעיכול, וקשה גם לעכל את המחשבה שקטינים נפגעים בחדרם ובביתם גם תחת עינם הפקוחה של הוריהם, וכי נגרם להם נזק שאת שיעורו קשה להעריך. קטינים אינם צריכים לצעוד בחשש, לא במסדרונות בית הספר ולא במסדרונות הרשת. לכן, גם אם עשויים להתעורר קשיים מסוימים בהוכחת הפגיעה או קשיים באיתור הפוגעים,[21] די בכלים המשפטיים הקיימים כדי להתגבר עליהם, ויש לפעול "ביצירתיות" המתבקשת לצורך הגנה על אותם קטינים. הטעם השני ל"זהירות היצירתית" הוא משום שמדובר בנושא חדש שטרם לובן, ומשום שמדובר בקטינים שנדרש משנה זהירות בעניינם ובהעמדתם לדין.

שאלת תחולתן של נורמות פליליות במרחב הווירטואלי היא סוגיה נכבדה, אלא שבמקרים רבים תופעות של אלימות מקוונת אינן מעוררות אותה למעשה. אמנם, יכולים להיות מקרים שבהם מבוצעות עבירות וירטואליות בעולם המקוון, ואולם במקרים רבים אחרים מדובר בעבירות ברורות המבוצעות בעולם הממשי אך משודרות באינטרנט. דוגמה פשוטה המבהירה את הדבר היא זו של קטין המפרסם ברשת חברתית תמונות של קטין אחר בסיטואציה אינטימית (למשל, ללא לבוש) בלי לבקש את רשותו. במקרה זה הפרסום אמנם אינו נעשה בדרך של הדפסת התמונה והפצתה בין חברי כיתתו, אולם אין בכך כדי לשנות את טיב המעשה ומהותו – פרסום הפוגע בפרטיות, ללא הסכמה.

חלק מן המעשים שהם בגדר אלימות מקוונת מבוצעים בעולם הממשי, הפיזי, והאינטרנט אינו אלא אמצעי להעברה מיידית ובו־זמנית של המעשה לידיעת הקהל הרחב; במקרה כזה, המעשים אינם וירטואליים, ולכן אין חשיבות למדיה שבאמצעותה הם מופצים. הדבר יהיה רלוונטי בעיקר בנוגע למעשי אלימות מקוונת הפוגעים בפרטיות, אך לא רק להם. דוגמה לכך היא מצב שבו כמה קטינים משוחחים בחדר צ'ט (או בקבוצת "ווטסאפ"), והדינמיקה הפנימית ביניהם גורמת להשמעת איומים הממוקדים בקטין אחד. למרבה הצער, השמעת איומים בין קטינים הפכה לדבר שבשגרה גם בעולם הממשי וגם בעולם הווירטואלי, ולכן הבחינה צריכה להיות זהה בשני העולמות: האם מדובר ב"איום" כהגדרתו בחוק, והאם הוא מגיע לכלל עבירה פלילית שיש להעמיד בגינה לדין. הרשת במקרה זה משמשת אמצעי להעברת האיומים מיד ובעת ובעונה אחת.

כאשר מובאת לידיעת אנשי המשטרה ואנשי הפרקליטות ידיעה בדבר מעשה החשוד כעבירה הנעשה על ידי קטין בזירה האינטרנטית, עליהם לשאול את עצמם ביושר: מה ההבדל מבחינתנו אם הפעולה האלימה מבוצעת באמצעות רשת

21 יש לזכור כי האנונימיות המתקיימת ברשת היא במרבית המקרים למראית עין, ומעטות ההתקשרויות שאי אפשר לנטר את מקורן בעזרת צו מבית המשפט.

חברתית, דואר אלקטרוני או טלפון? מה שקובע אינו מתכונת הפעולה – וירטואלית או ממשית – אלא אופי המעשים. כשמהות הפעולה היא איום, פרסום הפוגע בפרטיות או הקנטות המגיעות עד כדי הטרדה, המדיום אינו מעלה ואינו מוריד.

פעילות ברשת מקבלת פעמים רבות ביטוי גם בפעולות ממשיות ב"עולם האמיתי", אותן מבָצעים קטינים (למשל, צילום קטין כשהוא ברשות הפרט, או חדירה לדואר אלקטרוני של קטין אחר). הדבר מחזק עוד יותר את המסקנה שאין ליצור הפרדה דיכוטומית בין העולם הממשי לעולם הווירטואלי. יתרה מזו, הזיקה בין התנהגות וירטואלית ובין נזקים ב"עולם האמיתי" חוזרת ומתגלה בתחומים רבים. כך, למשל, איום המבוצע ברשת חברתית יכול להביא לידי פגיעה פיזית בקטין, והטרדה חוזרת ונשנית באינטרנט עלולה להביא קטין לידי התאבדות.[22]

דומה שהרוב המוחלט של ההתנהגויות הפוגעניות הנכללות באלימות המקוונת עונה על הגדרת החוקים הקיימים בדין הפלילי, וייתכן שלא ראוי ליצור הפרדה בין העולם המקוון ובין פגיעות שאינן מקוונות. עם זאת, יש לנקוט משנה זהירות בטרם נפנה לדין הפלילי במקרים אלה. היסוד הנפשי המאפיין בני נוער כשהם מפעילים אלימות מקוונת הוא עמום; לעיתים הוא מהווה אדישות לפגיעה ולעיתים הפגיעה נעשית בקלות דעת והגבול בין לחץ חברתי, שעשוע וגחמות של בני נוער ובין זדון ורצון לפגוע הוא מטושטש. ילד המפרסם דבר מה, לא תמיד מודע להיקף התפוצה של דבריו ולכוחם ההרסני. יתרה מזו, הזמינות הרבה של אמצעי התקשורת, בשילוב מאפייני הקשרים החברתיים בין בני הנוער, מביאים לכך שהטלת אחריות פלילית נראית במקרים מסוימים בלתי מידתית, גם אם מדובר בהגנה על ערכים מוגנים זהים – שמו הטוב ובריאותו הפיזית והנפשית של הקורבן. חוסר המידתיות נובע מכך שייתכן שאותם בני נוער פעלו מתוך גחמה זמנית וללא מודעות ברורה להשלכות מעשיהם. זאת ועוד, גם כאשר התוצאה והנזק הם הרסניים, ייתכן שההתנהגות המקורית של התוקף הייתה שולית, כגון במצב של התייחסות מקניטה לתמונה, שבשל החשיפה הנרחבת והמהירה באינטרנט, התנפחה אחר כך לממדים מזיקים.

הזמינות והקלות שבהן קטינים יכולים לבצע את מרבית העבירות הפליליות ב"עולם האמיתי" הן נמוכות יחסית, ולכן הגבולות הנורמטיביים של מותר ואסור, טוב ורע, הם ברורים יותר. לעומת זאת, כל אלה עמומים יותר במרחב המקוון. גם מכך נובע הקושי לקבל החלטה בדבר העמדה לדין פלילי. יחד עם זאת, אין בקשיים אלה כדי להביא להפקרת הזירה האינטרנטית; בסופו של דבר, יש לזכור כי עשיית המעשים בדוא"ל או ברשת חברתית, ולא פנים מול פנים, אינה מפחיתה כהוא זה מחומרתם, וניתן לומר כי במידת מה אף מגבירה את חומרתם.

---

22 ראו בהקשרים אחרים ע"פ 512/13 **פלוני נ' מדינת ישראל** (פורסם בנבו, 4.12.2013); אסף הרדוף, **הפשע המקוון**, הוצאת נבו, 2010.

סיכום

ביתו של קטין הוא מבצרו והטלפון הנייד או המחשב הם שלוחת ביתו. הפלישה לביתו של הקטין אינה חייבת להיות פיזית. גם פלישה טכנולוגית יכולה לזכות להגנת החוק הפלילי הרלוונטי. אסור לאפשר לנאשמים, קטינים כבגירים, לנצל את הנגישות וקלות הביצוע הכרוכות במעשים הנעשים באמצעות האינטרנט – כאלה שככל הנראה הם לא היו מעזים לעשות פנים אל פנים, שהרי אז הם היו מהווים עבירה פלילית. הרשת מקנה לקטינים מעין תחושת ריחוק והגנה רבה יותר ומאפשרת להם לחצות גבולות, לעומת התנהגותם כשהם ניצבים פנים מול פנים. דרך המלך לטיפול באמור היא חינוך והסברה מדוע מדובר בחציית גבולות ומדוע אין לעשות כן. יחד עם זאת, אסור למשפט הפלילי להתעלם ולאפשר את חציית הגבולות, ובמקרים המתאימים עליו לומר את דברו. אין לאפשר לקטינים לבצע מעשים שהיו מהססים לבצעם ב"עולם האמיתי", רק משום שהאינטרנט מאפשר להם אנונימיות לכאורה לנהל מניפולציות על חשבון חבריהם, שלוותם ובריאותם הנפשית; אין להפוך את האינטרנט לעיר מקלט לביצוע עבירה בחסות האנונימיות והיעדר המגע הפיזי. מדובר בתופעה מגונה ופסולה, הראויה לאכיפה פלילית מחמירה יותר.

ההבחנה בין מילים למעשים, בין התנהגות וירטואלית להתנהגות אמיתית, הולכת ומיטשטשת. עלינו להיזהר מפני יצירת מציאות שבה העולם הווירטואלי, בהיעדר אכיפה פלילית, יעניק מחסה לפושעים של ממש. יש לוותר על הרעיון שלפיו אלימות כרוכה בקרבה פיזית. קטינים עלולים לנהוג באלימות גם ללא קרבה פיזית. יתר על כן, קטינים מבצעים מעשים בזירה הווירטואלית שבגירים היו מהססים לבצע, ולעיתים נדרשת תגובה ברורה וחד־משמעית של הדין הפלילי על מעשים אלה. יש להחיל את החקיקה הפלילית הקיימת, בשינויים המחויבים, כלומר באופן שלא כל פרסום מגנה ומגונה באינטרנט יהווה עילה להעמדה לדין, למשל בגין לשון הרע או פגיעה בפרטיות. יש אמנם להכיר במאפיינים המיוחדים של השיח האינטרנטי, אולם אין לוותר מראש על השימוש באמצעים קיימים רק בשל האתגרים המלווים את השיח הזה.

האתגרים שהעולם הווירטואלי מציב בפנינו מחייבים את רשויות אכיפת החוק לנקוט גישה זהירה. ייתכן שבמקרים כאלה יש מקום לדרוש חוות דעת של שירות המבחן לנוער לפני הגשת כתב אישום בעניינו של קטין, יהיה גילו אשר יהיה, וזאת כדי לקבל תמונת מצב רחבה יותר באשר לקטין עצמו. פתרון נוסף הוא שבשלב ראשון מי שירכז את נושא ההעמדה לדין בגין עבירות כאלו יהיו יחידה אחת במשטרה וגורם אחד בפרקליטות המדינה. כך תגובש נקודת מבט כללית בנושא ויהיה יישום שוויוני והוגן של הדין הפלילי במקרים ספציפיים. יתרה מזו, הכלים המשמשים את הקטינים באופן תדיר יכולים בקלות להפוך את התנהגותם לכזו

שעשויה לגרור הטלת אחריות פלילית – מצב שלא אליו פילל המחוקק כשניסה להגדיר מהי פגיעה בפרטיות או הטרדה. ריכוז הנושא בידי גורם מטפל אחד, בעל ראייה רחבה, יאפשר בחינה ביקורתית מתמשכת באשר למידת התאמתו של הדין הפלילי לטיפול בסוגיה זו.

אסטרטגיות לביטחון סייבר בתחום הבריאות בישראל ובהולנד: סקירה השוואתית

סטפן ווינק

הקצב המהיר של החידושים הטכנולוגיים יצר שורה של הזדמנויות לשינויים בתחום הבריאות. שינויים אלה משפרים את איכות החיים, אך גם יוצרים זירת הזדמנויות לפושעי סייבר. שירותי הבריאות מופקדים על בריאותם של האזרחים, אולם במקביל הם גם אחראים לא פעם לחלק משמעותי מהתפוקה הכלכלית הלאומית. הגברת הסיכונים בתחום ביטחון הסייבר בענף הבריאות המשתייך למערכת התשתיות הקריטיות, מציבה איום על הביטחון הלאומי ומחייבת תגובה ממשלתית. מאמר זה משווה בין האסטרטגיות והתקנות הלאומיות לביטחון סייבר של ישראל ושל הולנד, כחלק מאסטרטגיית ההגנה שלהן על ענף הבריאות מפני איומי סייבר, ומביא המלצות לאסטרטגיות ותקנות עתידיות בתחום זה.

מילות מפתח: ענף שירותי הבריאות, טכנולוגיה, תקנות ואסטרטגיה לאומית לביטחון סייבר, האינטרנט של הדברים הרפואיים (IoMT), תשתיות קריטיות

מבוא

תחום שירותי הבריאות נמנה על המגזרים הנהנים מההתפתחויות הטכנולוגיות המואצות.[1] ייעודו ופעילותו חיוניים לבריאותם של אנשים, ובמקרים מסוימים גם אחראים לחלק ניכר מהתפוקה הכלכלית הלאומית.[2] הטכנולוגיות המתפתחות

סטפן ווינק סיים תואר ראשון בלימודי ניהול אבטחה באוניברסיטת סאקסיון למדעים יישומיים בהולנד, ובעבר התמחה בתוכנית לביטחון סייבר של המכון למחקרי ביטחון לאומי.

1 Sanjay Poonen, "Health Care Innovation Harnessing New Technology to Benefit Patients", *Forbes*, April 2, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/04/02/health-care-innovation-harnessing-new-technologies-to-benefit-patients/#4d7afdf45a88.

2 "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities", *KPMG*, September 2015, pp. 1-6; "Critical Infrastructure Sectors", *US Department of Homeland Security (CISA)*, February 2, 2019, https://www.dhs.gov/cisa/critical-

והדיגיטציה ממלאות תפקיד מרכזי בפיתוח מוצרים, שירותים ומחקרים, לטובת החולים והספקים גם יחד. לשילוב של הגנטיקה והביולוגיה עם נתוני עתק (Big Data) ובינה מלאכותית, שזכה לכינוי "מהפכת האוטומציה והמידע הרפואיים", הייתה השפעה רבה על המחקר. שילוב זה חולל מהפכה בייצור תרופות, ברפואה מותאמת אישית ובסביבת העבודה הקלינית, ושינה את אופן האבחון והטיפול בחולים.[3]

בריאות דיגיטלית מגבירה את היעילות והאפקטיביות של מערכות רפואיות ומשפרת את ניהול המרשמים, את שירותי הבריאות מרחוק, את הפיקוח והמעקב ואת הפעולות הקליניות עצמן.[4] לדיגיטציה של מערכת הבריאות יש ערך מוסף, בכך שהיא מאפשרת את הגדלת המרחק הגיאוגרפי לטיפול בחולים. דוגמאות לכך הן המערכת הכירורגית "דה וינצ'י" ומערכות רובוטיות המסייעות למנתחים לבצע פעולות עדינות ממקומות שונים.[5] השילוב של טכנולוגיות מתפתחות, מערכות מידע, רשתות רפואיות ומכשור רפואי, המחוברים ביניהם בְּמה שמכונה "האינטרנט של הדברים הרפואיים" (Internet of Medical Things – IoMT), מתפתח באופן שהוא קריטי למערכות הבריאות ובה בעת עלול לשבש את פעילותן.[6]

סיכוני אבטחת סייבר בענף שירותי הבריאות

תוצר לוואי של ההתקדמות בתחום הבריאות הדיגיטלית הוא הסיכון המשותף למכשור רפואי, ל"אינטרנט של הדברים הרפואיים", ליישומים רפואיים דיגיטליים, לתוכנות, למערכות מידע ולהתקני אבטחה ("חומות אש" ואנטי וירוס).[7] התוצאה של סיכון כזה יכולה להיות פגיעה בנתונים, ובכלל זה בקניין רוחני של הארגון,

---

infrastructure-sectors; "Critical Infrastructure Sectors*", European Cooperation Network on Critical Infrastructure Protection (euconcip)*, March 15 2019, https://www.euconcip.org/; Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats", *Military and Strategic Affairs* 3, no. 2 (2011): 61-78.

3 "2018-2019 Innovation in Israel Overview", *Israel Innovation Authority*, January 14, 2019, pp. 60-62; Poonen, "Health Care Innovation Harnessing New Technology to Benefit Patients".

4 "Connected Health, How Digital Technology Is Transforming Health and Social Care", *Deloitte Center for Health Solutions*, London, 2015, pp. 1-40; "2018-2019 Innovation in Israel Overview".

5 ראיון עם אליאב נ., 25 בנובמבר 2018.

6 Safi Oranski, "Obstacles on the Path to Comprehensive IoMT Security", *Cyber MDX*, November 26, 2018, https://www.cybermdx.com/blog/obstacles-on-the-path-to-comprehensive-iomt-security.

7 Aurore Le Bris and Walid El Asri, "State of Cybersecurity & Cyber Threats in Healthcare Organizations", *Journal of Strategic Threat Intelligence,* January 10, 2017,https://blogs.harvard.edu/cybersecurity/2017/01/10/cybersecurity-cyber-threats-in-healthcare-organizations/; Barbara Filkins, "Health Care Cyberthreat Report",

כמו מחקרים רפואיים, ניסויים וממצאים; פגיעה במידע כספי ובחיובים הקשורים להעברות כספים אלקטרוניות (EFT); פגיעה בפרטי מטופלים ובהיסטוריה הרפואית שלהם, הקשורים לרשומות רפואיות ממוחשבות (EHR) או לתיק רפואי ממוחשב (EMR).[8] בסופו של דבר, תהיה בכך פגיעה בפעילות של שירותי הבריאות ובשירות שהם נותנים, דבר שיגרום לעלויות נוספות כתוצאה מנזקים ומתביעות, וכל זאת תוך פגיעה ברווחת המטופלים.[9]

כדי להמחיש את פגיעויות האבטחה בתשתיות הרפואיות, פיתחו חוקרים במרכז לאבטחת סייבר באוניברסיטת בן גוריון תוכנה זדונית המנצלת פגיעויות של מכשירי הדמיה רפואיים, כגון מכונות CT ו־MRI, ושל הרשתות המעבדות את ההדמיות. במחקר נמצא כי סריקות ה־CT שעברו שינוי מכוון (המציג ממצאים סרטניים) הובילו רדיולוגים מנוסים לאבחן את המצב הרפואי בצורה שגויה.[10] ככל הידוע, תרחיש כזה טרם התממש במציאות ולא גרם נזקים או מוות. מרבית התקפות הסייבר על ענף הבריאות עד היום כללו פריצות לנתונים של רשומות רפואיות ממוחשבות, וזאת כתוצאה מנקודות תורפה ברשתות של בתי החולים, של ספקי שירותי בריאות כמו חברות ביטוח, או של גורמים הקשורים בשרשרת האספקה.[11]

רבע מכלל הפריצות למאגרי נתונים בארצות הברית מתרחש, לפי ההערכות, בענף הבריאות.[12] אחד המקרים הבולטים היה חשיפתה של קבוצה חדשה של האקרים, שזכתה לכינוי "תולעת כתומה" ("Orangeworm"). החשיפה נעשתה על ידי חברת Symantec בתחילת 2015, לאחר שההאקרים שתלו תוכנה זדונית מותאמת – Kwampirs – שכוונה נגד מחשבים של ספקי שירותי בריאות וספקים של צדדים שלישיים במספר מגזרים הנותנים שירותים לענף הבריאות. בדרך זו השיגה קבוצת ההאקרים גישה בלתי מורשית לרשומות רפואיות ממוחשבות ולמכשירי הדמיה רפואיים, כגון MRI וציוד רנטגן.[13]

SANS Institute and Norse, March 2014, pp. 1-42; "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities".

8 Ibid.

9 Ibid.

10 Kim Zetter, "Hospital Viruses: Fake Cancerous Nodes in CT Scans, Created by Malware, Trick Radiologists", *The Washington Post*, April 3, 2019, https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/.

11 Filkins, "State of Cybersecurity and Cyber Threats in Healthcare Organizations"; "Health Care Cyberthreat Report".

12 "Health Care Innovation Harnessing New Technology to Benefit Patients".

13 Jessica Davis, "New Hacking Group Targeting Healthcare Infects Mri, X-Ray Machine", *Healthcare IT News,* April 24, 2018, https://www.healthcareitnews.com/news/new-hacking-group-targeting-healthcare-infects-mri-x-ray-machine; Security

מתקפת "דיוג", שהתרחשה בשנת 2018 נגד חשבונות דוא"ל של עובדי חברת UnityPoint Health שבוויסקונסין, גרמה לפריצה לנתונים של 16,000 מטופלים. מתקפה עוקבת על המערכות העיסקיות של החברה הביאה לפריצה לנתונים של 1.4 מיליון מטופלים.[14] בשנת 2018 גם נפרץ מחשב של עובד בחברת Med Associates בניו יורק – ספקית של תביעות בנושאי בריאות – ונחשפו למעלה מ־270,000 רשומות של מטופלים.[15] באותה שנה נפגעו במיזורי Blue Springs Family Care, Cass Regional Medical Center, וכן LabCorp מהתקפות של תוכנות כופר, שמנעו מהמשתמשים גישה למערכות התקשורת שלהם ולרשומותיהם הממוחשבות.[16]

בשנים 2015־2018 פרצו האקרים, ששמו על הכוונת את מאגר הבריאות הממלכתי של סינגפור, לרשומות של 1.5 מיליון מטופלים, ובתוכם לפרטיו של ראש הממשלה לי סיאן לונג.[17] ביוני 2017 דווח על פריצה לרשתות המחשבים של שניים עד שלושה בתי חולים בישראל, אם כי מערך הסייבר הלאומי שלה אישר רק את דבר קיומן של שתי מתקפות. האירוע הביא להחלפת חמישים מחשבים מיושנים וחשופים לפגיעה.[18]

Response Attack Investigation Team, "New Orangeworm Attack Group Targets the Healthcare Sector in the U.S., Europe and Asia", *Symantec*, April 23, 2018, https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia.

14 Jessica Davis, "1.4 Million Patient Records Breached in Unitypoint Health Phishing Attack", *Healthcare IT News*, July 13, 2018, https://www.healthcareitnews.com/news/14-million-patient-records-breached-unitypoint-health-phishing-attack.

15 Jessica Davis, "270,000 Patient Records Breached in Med Associates Hack", *Healthcare IT News,* June 20, 2018, https://www.healthcareitnews.com/news/270000-patient-records-breached-med-associates-hack.

16 Jessica Davis, "Update: Ransomware Attack on Cass Regional Shuts down HER," *Healthcare IT News*, July 11, 2018, https://www.healthcareitnews.com/news/update-ransomware-attack-cass-regional-shuts-down-ehr; Jessica Davis, "Ransomware, Malware Attack Breaches 45,000 Patient Records," *Healthcare IT News,* July 26, 2018, https://www.healthcareitnews.com/news/ransomware-malware-attack-breaches-45000-patient-records.

17 Jessica Davis, "Hackers Breach 1.5 Million Singapore Patient Records, Including the Prime Minister's," *Healthcare IT News*, July 20, 2018, https://www.healthcareitnews.com/news/hackers-breach-15-million-singapore-patient-records-including-prime-ministers.

18 Globes Correspondent, "Cyber Attack Hits Israeli Hospitals", *Globes*, June 29, 2017, https://en.globes.co.il/en/article-cyber-attack-hits-israeli-hospitals-1001194803 ; Judy Siegel-Itzkovich and Sharon Udasin, "Cyber Attacks Hit Israeli Hospitals as Globe Battles New Computer Virus", *The Jerusalem Post*, June 29, 2017, https://www.jpost.com/Israel-News/Israel-thwarts-hackers-from-cyber-attack-on-hospitals-498256.

הרגולציה בענף הבריאות בישראל ובהולנד

ביטחון הסייבר של מערכות הבריאות בישראל היה אחד הנושאים שנדונו במהלך סמינר ה"סייבר־מד", שהתקיים במסגרת כנס "סייבר־טק" בתל אביב בינואר 2019. מסקנת הדיון הייתה כי ביטחון הסייבר של מערכות הבריאות בישראל נמצא "מתחת לקו הבריאות" וכי אינו מוכן לאיום המתפתח על רשתות התקשורת, המכשור הרפואי והארגונים המספקים שירותים רפואיים. לדברי מנהל בית החולים האוניברסיטאי "הדסה", התשתיות הקריטיות החיוניות מותאמות לתקנים, אולם מרכיבים אחרים, כגון התקנים מרחוק, זוכים לאבטחת סייבר ברמה שהיא פחות חסינה. המעבר לבריאות דיגיטלית, הנובע מהטכנולוגיות החדשות ומהאפשרות ליצור שילוביות, הציב אתגרים חדשים רחבי היקף, המאיימים על המוניטין של ארגוני הבריאות.[19]

לשם השוואה, 56 אחוזים מבתי החולים בהולנד עמדו בשנת 2015 בתקנים לאבטחת מידע בענף הבריאות (NEN–7510120).[20] אמצעי האבטחה הפכו למחייבים מאז מאי 2017, וציות להם הוא תנאי הכרחי לקבלת גישה למספרי השירות של אזרחים בכל ענף הבריאות ההולנדי.

מספרן העולה של מתקפות סייבר נגד רשתות והתקנים בכל תחום התשתיות הקריטיות מסַכן את השירותים גם בתחום הבריאות ואת האמון בספקים של שירותי הבריאות. מתקפות אלו הובילו ליוזמות לשיפור החוסן והעמידות של הארגונים בכל תחומי הבריאות, כולל בארגונים המשרתים את ענף הבריאות, ולגיבושה של אסטרטגיה לאומית לביטחון סייבר.

אסטרטגיות לאומיות לביטחון סייבר

ביטחון סייבר הפך לחלק אינטגרלי מהאבטחה הארגונית ומוגדר על ידי תאגיד הטכנולוגיה CISCO כ"שיטה להגנה על מערכות, רשתות ותוכניות מפני התקפות דיגיטליות".[21] בשנת 2011 הוצג בכנס הבין־לאומי לביטחון תשתיות של מידע קריטי (CRITIS) מחקר השוואתי בין עשר אסטרטגיות לאומיות לביטחון סייבר. לפי המחקר, חסרה הגדרה משותפת לביטחון סייבר ברמה האירופית והבין־לאומית.[22]

19 Ami Rojkes Dombe, "CyberMed: Cyber Threats and Challenges in Healthcare", *Israel Defense*, January 28, 2019, https://www.israeldefense.co.il/en/node/37255.

20 "Cyber Security Risk Assessment (CSRA) for the Economy", *CPB Netherlands Bureau for Economic Policy Analysis*, 2017.

21 "What is Cybersecurity", *CISCO*, December 2, 2018, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

22 H.A.M. Luiijf, Kim Besseling, Maartje Spoelstra and Patrick de Graaf, "Ten National Cyber Security Strategies: A Comparison", in *Critical Information Infrastructure Security,* ed. Sandro Bologna, Bernhard Hämmerli, Dimitris Gritzalis and Stephen Wolthusen (Berlin: Springer, 2013), pp. 1-17.

גיבוש אסטרטגיות ביטחון לאומי במסגרת האיחוד האירופי הוא תופעה חדשה יחסית, וראשיתה בתחילת שנות האלפיים. קביעת אסטרטגיות לאומיות כאלו מעודדת קובעי מדיניות להגדיר יעדים אסטרטגיים ולנסח הנחיות כיצד להגיע אליהם. אמירה ידועה בעולם האבטחה גורסת כי "חוזק ביטחון הסייבר הוא כחוזק החוליה החלשה ביותר".[23] ארגון יכול להיות בעל מערכת ביטחון סייבר מצוינת, ועדיין לסבול מחוסר יעילות אם אין לו מערכת ניהול סיכונים מקיפה בתחום זה.[24] ההתפתחויות בנושא ביטחון סייבר – שרשרת האירועים שזירזו את קבלת ההחלטות בנושאי הסייבר בהולנד ובישראל – זקוקות להבהרות כדי להבין טוב יותר את מהותן של אסטרטגיות ביטחון הסייבר בשתי המדינות. השוואת שתי האסטרטגיות שתובא להלן תתמקד באופן שבו הולנד וישראל מתמודדות עם אתגרי ביטחון הסייבר ובדרך שבה שתי המדינות מגדירות מהם הנכסים הרלוונטיים למדיניות ביטחון הסייבר שלהן.

הקריטריונים שלהלן מבוססים על הנושאים המרכזיים שמופיעים במדריך NCSS Good Practice Guide[25] ועל המחקר שנערך על ידי Luiijf ואחרים,[26] וישמשו להשוואת האסטרטגיות הלאומיות לביטחון הסייבר של ישראל והולנד. סוגיית המפתח הראשונה היא **משטר סיכונים ברמה האסטרטגית והלאומית,** כאשר אחת האסטרטגיות היא יצירת תוכנית־אב כוללת המפרטת כיצד יושגו המשימה והיעדים. סוגיית המפתח השנייה היא **הסביבה הרגולטורית הלאומית**, שהיא חלק מהאסטרטגיה הלאומית הכוללת של ממשלות. סוגיית המפתח השלישית היא **בעלי העניין העיקריים באסטרטגיות הלאומיות לביטחון סייבר**, וכוללת מידע על סביבת בעלי העניין המייצגים תחומים רבים ומעורבים בתהליך פיתוחה של האסטרטגיה הלאומית לביטחון הסייבר. סוגיית המפתח הרביעית היא **הגדרת תשתיות קריטיות ואובייקטים קריטיים**. סוגיית המפתח החמישית והאחרונה היא **מודיעין סייבר ומודעות לביטחון סייבר**. להלן יתייחס המאמר לפעילויות של סוכנויות ביון וגופים ממשלתיים בתחום הסייבר ולקשר שלהן למשאבים

23 Niels Nagelhus Schia, "'Teach a Person How To Surf': Cyber Security as Development Assistance", *Norwegian Institute of International Affairs,* Report no. 4, 2016, pp. 1-36.

24 Gabi Siboni and Hadas Klein, "Guidelines for the Management of Cyber Risks", *Cyber, Intelligence and Security* 2, no. 2 (2018): 23-38.

25 European Union Agency for Network and Information Security (ENISA), NCSS Good Practice Guide, *Designing and Implementing National Cyber Security Strategies* (Heraklion: ENISA, 2016), pp. 1-59.

26 H.A.M. Luiijf, Kim Beseling, Maartje Spoelstra and Patrick de Graaf, "Ten National Cyber Security Strategies: A Comparison", in: *Critical Information Infrastructure Security*, ed. Sandro Bologna, Bernhard Hammerli, Dimitris Gritzalis and Stephen Wolthusen (Berlin: Springer,2013), pp.1-17.

העומדים לרשותם של מוסדות הבריאות, במטרה להגביר את המודעות לביטחון סייבר ברמה הלאומית.

א. משטר ניהול סיכונים סיכונים ברמה אסטרטגית ולאומית

סוגיית המפתח הראשונה לניתוח אסטרטגיית ביטחון סייבר לאומית היא משטר סיכונים (Risk Governance). משטר ניהול סיכונים מציע לארגונים ולמדינות יתרונות והזדמנויות ומאפשר לארגונים ולסביבתם להשתנות, תוך צמצום התוצאות השליליות של הסיכונים הנלווים.

משטר ניהול סיכונים בישראל

משטר ניהול הסיכונים בישראל עבר במהלך העשור האחרון מהתמקדות ראשונית בהגנה על תשתיות מידע ומאגרי מידע ממוחשבים, כפי שקבעה הרגולציה, לגישה ישירה יותר של הגנה על מרחב הסייבר בעזרת אינטראקציות אסטרטגיות אזרחיות־צבאיות ושיתופי פעולה ציבוריים־פרטיים.[27] ארגונים מתמודדים עם אתגרים רבים במערכות הסייבר, ובמקביל יש תוכניות אקדמיות וממשלתיות שיוזמות ומפתחות פעולות ופתרונות טכניים חדשים לשיפור אמצעי הנגד והתגובה להתקפות סייבר.[28] כך, בשנת 2016 הטמיעו מערך הסייבר הלאומי ומשרד הבריאות את מערכת MedSOC – מרכז לפעולות אבטחה עבור תעשיית הרפואה. MedSOC עוקבת אחרי מתקפות בתחום הבריאות ומפרסמת מידע רלוונטי ברשת שלה. הפורטל של MedSOC נתמך על ידי צוות החירום לטיפול באירועי מחשב (CERT-IL), הכפוף למערך הסייבר הלאומי.[29]

הרגולציה המקומית בישראל מתבססת על תקנים בין־לאומיים, וזאת בהתאם להחלטת הממשלה 2443 "לקדם רגולציה לאומית והובלה ממשלתית בתחום ביטחון הסייבר". ככלל, כל הארגונים בישראל מתבקשים או נדרשים לעמוד בתקנים ISO/IEC 27001 ו־ISO 15408, החלים על "ארגונים ומערכות ניהול אבטחת מידע" ועל "מדדי הערכה לאבטחת טכנולוגיות מידע" בהתאמה.[30] ארגונים

27 Michael Raska, "Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defense Strategy", *S. Rajaratnam School of International Studies, Singapore*, January 2015, https://www.rsis.edu.sg/wp-content/uploads/2015/01/PR150108_-Israel_Evolving_Cyber_Strategy_WEB.pdf.

28 "Cyber Security Risk Governance", *International Risk Governance Council*, October 2015, pp 1-33.

29 ראיון עם אליאב נ., 25 בנובמבר 2018.

30 Eli Greenbaum, "Israel Chapter on Cybersecurity – Getting the Deal Through", *Yigal Arnon & Co. Law Firm*, February 1, 2018, https://www.arnon.co.il/member/4358/articles; "ISO/IEC 27001: 2013 Information technology – Security techniques – Information security management systems – Requirements", *ISO*, October 2013, https://

ייעודיים נדרשים לנקוט אמצעים נוספים, המבוססים על קריטריונים המתייחסים לתשתיות קריטיות ברמה הלאומית ולהנחיות הגוף הרגולטורי. בשנת 2012 פרסם משרד הבריאות חוזר מס' 18/2012, המורה לכל ארגוני הבריאות וספקי השירותים הנלווים לעמוד בתקן ISO 27799. החוזר הציג פרמטרים ביחס ל"סביבת סיכון אבטחת המידע" של הארגון בעת "בחירה, יישום וניהול בקרות" הנוגעים ל"תקני אבטחת מידע ארגוניים ושיטות ניהול אבטחת מידע".[31] משרד הבריאות פיתח, יחד עם מכון התקנים הישראלי, מערכת הסמכה מתקדמת בשירותי הבריאות, המאמצת קריטריונים נוספים של מכון התקנים.[32]

ציוד רפואי מיוצר עם מערכות נעולות, וכך מונע גישה למערכות ההפעלה שלו. מערך הסייבר הלאומי מנהל מעבדת מחקר רפואי, יחד עם בית החולים איכילוב, לבדיקת תקני איכות למכשור רפואי (לפי הנחיות ממשלתיות). המערך מספק את הידע והציוד, ואילו בית החולים איכילוב מספק את סביבת הבדיקות. הפעילות כוללת מבחני חדירה, קישוריות רשת וזיהוי פגיעויות וחולשות.[33]

משטר ניהול סיכונים בהולנד

בשנת 2018 הוקם בהולנד ארגון Z-CERT, כמענה להזדמנויות ולסיכונים שיתפתחו כתוצאה מהדיגיטציה של ענף הבריאות, וכן כמענה לאתגרים אחרים הנוגעים לפרטיות הנתונים ול"אינטרנט של הדברים" (IoT).[34] Z-CERT הוא חלק מיוזמה של איגוד בתי החולים בהולנד (Nederlandse Vereniging van Ziekenhuizen), הפדרציה ההולנדית של המרכזים הרפואיים האוניברסיטאיים (Nederlandse Federatie van Universitair Medische Centra), שירות הבריאות הכללי של הולנד והמרכז הלאומי לביטחון סייבר בהולנד (NCSC). Z-CERT מציע שירותי מומחים למוסדות הבריאות בהולנד ועושה זאת בעזרת אספקת ידע מעמיק על רשתות רפואיות, יישומים רפואיים ומכשירים רפואיים.[35] מכשירים רפואיים חייבים לעבור הערכה לפני הוצאתם לשוק בהולנד, במטרה לקבוע אם יוצרו בהתאם לדרישות

---

www.iso.org/standard/54534.html; "ISO/IEC 15408–1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model", *ISO*, January 2014, https://www.iso.org/standard/50341.html.

31 Greenbaum, "Israel Chapter on Cybersecurity – Getting the Deal through"; "ISO 27799:2008 Health informatics – information security management in health using ISO/IEC 27002", *ISO*, July 2008, https://www.iso.org/standard/41298.html; "ISO 27799:2016 Health informatics – Information security management in health using ISO/IEC 27002", *ISO*, July 2016, https://www.iso.org/standard/62777.html.

32 ראיון עם יניב פ., 6 בינואר 2019.

33 ראיון עם אליאב נ., 25 בנובמבר 2018.

34 ראיון עם הסל ב., 17 בדצמבר 2018.

35 שם.

של צו EEG/93/42 וצו EC/2007/47 העוסקים במכשור רפואי. פיתוח של מכשור רפואי מתוכנן ברובו כך שישמור על עקרונות הפרטיות והאבטחה. פירוש הדבר הוא שהחברה המַפתחת את המכשירים הרפואיים וגם הגורמים המשולבים בשרשרת האספקה צריכים להקדיש תשומת לב לאמצעים משפרי פרטיות, המכונים גם "טכנולוגיות משפרות פרטיות" (PET).[36] אבטחת המידע היא באחריות של כל מוסד בריאות. התקנים NEN 7510 ו־NEN 7512, שבתי החולים בהולנד חייבים לעמוד בהם, מבטיחים שיושגו הרמות הדרושות של אבטחת מידע ופרטיות. מלבד הַתקנים הסטטוטוריים, כל בית חולים צריך להחליט איזה תקן מתאים לסביבת הסיכון שלו.[37]

ב. הסביבה הרגולטורית הלאומית

ממשלות קובעות רגולציות שמחייבות את ענף הבריאות ליישם אמצעי ביטחון סייבר הולמים כדי להסדיר ולחזק את אמצעי ביטחון הסייבר בתחום הבריאות. יישום הרגולציות בענף הבריאות על ידי הטלת האחריות על הארגונים – תוצאה של עלייה במספר התביעות והקנסות של סוכנויות ממשלתיות על אי־ציות – מביא לשיתוף פעולה רחב יותר.

הרגולציה בישראל

כדי להבטיח שארגונים ציבוריים ופרטיים יוכלו לפעול לנוכח איומי ביטחון הסייבר, יש צורך להקים סביבה רגולטורית (בין־)לאומית ו/או מסגרת מדיניות מתאימה, שיבצעו לעיתים קרובות הערכות תכופות של אסטרטגיות ויעדים בתחום ביטחון הסייבר ויעדכנו אותם בהתאם. ישראל נקטה מאז 1981 מספר מהלכים וחוקקה חוקים להגנת הפרטיות וביטחון הסייבר, במטרה להתמודד באופן כללי עם בעיית ההגנה על הפרטיות. החוקים והמהלכים העיקריים בתחום זה הם חוק הגנת הפרטיות משנת 1981;[38] התיקון לחוק הגנת הפרטיות משנת 2001;[39] החלטת הממשלה 3611 לקידום יכולות הסייבר הלאומיות משנת 2011;[40] החלטת הממשלה 2444 לקידום המוכנות הלאומית לביטחון הסייבר משנת 2015.[41] בשנת 2018 פרסמה ממשלת ישראל טיוטה לחוק ביטחון סייבר והוציאה "קול קורא" לציבור לבקש

36 שם.

37 שם.

38 Ian Bourne, "A Guide to Data Protection in Israel", *Israeli Law, Information and Technology Authority (ILITA)*, January 2010.

39 Ibid.

40 "Resolution 3611 – Advancing National Cyberspace Capabilities", *Israel's Prime Minister's Office*, August 7, 2011, pp. 1-6.

41 Deborah Couriel-Housen, "Israel: Organization Security Cyber National", *Cyber Defense Center of Excellence NATO* 2. no, 4 (February 2017): 12-1.

את הערותיו לטיוטה. הצעת החוק מסכמת שנים של התייעצויות ודיונים בשאלת הגישה לביטחון סייבר בישראל ומשלבת מספר חידושים בחקיקה ובמדיניות בנושא זה.[42]

חוק הגנת הפרטיות מהווה את החקיקה העיקרית להגנת מידע בישראל. לחוק שני מרכיבים: הראשון הוא ההגנה על הפרטיות באופן כללי, והשני עוסק ספציפית במאגרי מידע וקרוב הרבה יותר לחוקי הגנת נתונים מסוג "מידע".[43] החוק התפתח עם הזמן ועבר, מאז שהתקבל לראשונה ב־1981, תשעה תיקונים. בשנת 2001 התווספו אליו תקנות ברוח המונחים האירופיים להגנת מידע, באופן שמגביר את התאמתו לתקנים האירופיים.

הרשות הישראלית למשפט, טכנולוגיה ומידע (רמו"ט, כיום הרשות להגנת הפרטיות) הוקמה בספטמבר 2006 כחלק ממשרד המשפטים, מכוח החלטת הממשלה 4660. משימת הרשות היא לחזק את ההגנה על מידע אישי, להסדיר את השימוש בחתימות אלקטרוניות ולהגביר את האכיפה בתחומי הגנת הפרטיות ועבירות הקשורות לטכנולוגיות מידע. הרשות להגנת הפרטיות פועלת גם כבסיס ידע מרכזי של הממשלה לחקיקה הקשורה לטכנולוגיה ולפרויקטים גדולים של IT, כמו eGov.[44] כאמור, בשנת 2011 קיבלה הממשלה את החלטה 3611 העוסקת בהקמת מערך הסייבר הלאומי, וזאת במטרה לחזק את ההגנה על תשתיות לאומיות קריטיות ולהסדיר סמכויות ותחומי אחריות בתחום הסייבר.[45]

כאמור, בשנת 2012 גם פרסם משרד הבריאות את חוזר 18/2012. החוזר מחייב את כל מוסדות הבריאות בישראל לקבל הסמכה של תקן ISO 27799, ואת כל ספקי השירות המחזיקים במידע רפואי, או במידע הנוגע לתשתית המוסד הבריאותי, לעמוד באותו תקן.[46]

הרגולציה בהולנד

כדי להבין את החוקים ההולנדיים העוסקים בפשעי סייבר ובאבטחת מידע, יש לסקור את ההיסטוריה של החקיקה ההולנדית שהובילה לסביבה הרגולטורית (הבין־) לאומית ו/או למדיניות הנוכחית של הולנד בנושאים אלה. החוקים המרכזיים הנוגעים לפשעי סייבר שנחקקו בהולנד הם חוק פשעי מחשב (Wet computercriminaliteit)

---

42 Deborah Housen-Couriel, "A Look at Israel's New Draft Cybersecurity Law", *Net Politics*, *Council on Foreign Relations*, August 5, 2018, https://www.cfr.org/blog/look-israels-new-draft-cybersecurity-law.

43 Bourne, "A Guide to Data Protection in Israel".

44 Greenbaum, "Israel Chapter on Cybersecurity – Getting the Deal Through".

45 "Resolution 3611 – Advancing National Cyberspace Capabilities".

46 ראיון עם אליאב נ„ 25 בנובמבר 2018; Greenbaum, "Israel Chapter on Cybersecurity – Getting the Deal Through".

משנת 1993[47] וחוק פשעי מחשב II (Wet computercriminaliteit II) משנת 2006, וכן התיקון האחרון לו, שהביא לחקיקת חוק פשעי מחשב III.[48]

לכאורה, ניתן להעמיד לדין בהולנד בגין הפרת פרטיות מידע או הפרת הגנה על מידע על בסיס התערבות בנתונים, לפי סעיף 350a של החוק הפלילי ההולנדי.[49] למעשה, אין בחוק הפלילי ההולנדי פירוט שמתייחס באופן ספציפי להפרות הקשורות להגנת מידע. חוק רלוונטי נוסף הוא חוק הגנת המידע (Wet bescherming persoonsgegevens) משנת 2000,[50] הנאכף בעיקר על ידי אמצעים מינהליים שקבעה הממשלה. החוק עודכן בשנת 2015 כדי להבטיח שארגונים ידווחו על דליפת נתונים, וכן כדרך להרחיב את הסמכות המינהלית של המועצה ההולנדית להגנת המידע (College bescherming persoonsgegevens).[51]

ברמה הבין־לאומית, הולנד, כחברה באיחוד האירופי, מיישמת את "החלטת המסגרת JHA/2005/222 של מועצת אירופה... בנושא התקפות על מערכות מידע", מפברואר 2005. ריבוי ההתקפות על מערכות מידע והתגברות האיומים של פשע מאורגן הביאו את האיחוד האירופי להחליף באוגוסט 2013 את "החלטת המסגרת" ב"דירקטיבה EU/2013/40... בנושא התקפות על מערכות מידע".[52]

החקיקה הראשונה של האיחוד האירופי שהתמקדה באופן ספציפי בביטחון סייבר נקראת "הדירקטיבה בנושא אבטחת מערכות מידע ורשת" (דירקטיבה NIS). היא כוללת אמצעים חוקיים להגברת הרמה הכוללת של ביטחון הסייבר ולסנכרון המדיניות בנושא ביטחון סייבר בין המדינות החברות באיחוד, כשהמטרה הסופית היא לתמוך בחברה ובכלכלה של אותן מדינות על ידי שיפור המוכנות הדיגיטלית וצמצום עד למינימום של אירועי סייבר.

---

47 "Computer Crime Act", *Government of the Netherlands: Ministry of Justice and Security*, October 28, 1993, pp. 1-33 (in Dutch).

48 "Computer Crime Act II", *The Government of the Netherlands: Ministry of Justice,* July 4, 2006, pp. 1-2 (in Dutch); "Computer Crime Act", *The Government of the Netherlands: Ministry of Justice and Security*; October 8, 2018, pp. 1-33 (in Dutch).

49 "Dutch Criminal Code", *Official Publication of the Kingdom of the Netherlands*, April 22, 2015, p. 165 (in Dutch).

50 "The Data Protection Act", *Official Publication of the Kingdom of the Netherlands*, July 6, 2000, pp. 1-25 (in Dutch).

51 "Amendment of the Data Protection Act", *Official Publication of the Kingdom of the Netherlands*, June 4, 2015, pp. 1-8 (in Dutch).

52 "Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems", *Official Journal of the European Union*, March 16, 2005, pp. 67-71; "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA", *Official Journal of the European Union*, August 14, 2013, pp. 8-14.

"הרגולציה הכללית להגנה על מידע" (GDPR) של האיחוד האירופי אושרה סופית בפרלמנט האיחוד ב־14 באפריל 2016, לאחר הכנות שנמשכו ארבע שנים. מטרת הרגולציה היא להגן על כל אזרחי האיחוד האירופי מפני הפרות של פרטיות ופריצות לנתונים. ההבדל העיקרי בין הרגולציה החדשה ובין הדירקטיבה הקודמת הוא בסמכות השיפוט המורחבת שנכללת ברגולציה ומתפרסת על פני כלל מדינות האיחוד האירופי, וכן הקנסות על ארגונים שיפרו אותה.[53]

כל גוף ממשלתי או ארגון ציבורי באיחוד האירופי, שעוסק בבקרה או בפיקוח, נדרש למנות קצין אבטחת מידע (DPO), וזאת במקרים שבהם הפיקוח כולל מעקב קבוע, שיטתי ובקנה מידה גדול אחר אנשים, או כאשר מתקיים פיקוח בהיקף נרחב על מידע אישי רגיש.[54] מינוי קצין אבטחת מידע בהולנד הוא חובה רק אם הארגון ההולנדי עומד בדרישות הרגולציה החדשה.

ג. בעלי עניין עיקריים באסטרטגיה לאומית לביטחון סייבר

יש חשיבות לדעת מיהם בעלי העניין הרלוונטיים בענף הבריאות המעורבים בתהליכים המרכזיים במוסדות הבריאות השונים. אסטרטגיות לאומיות לביטחון סייבר, המשכילות לערב בעלי עניין רלוונטיים, ישיגו מודעות אופטימלית למצב, וכתוצאה מכך יגדילו את התשואות של כל הגורמים המעורבים באותה אסטרטגיה.[55]

בעלי העניין בישראל

ישראל היא מחלוצות שיתופי הפעולה עם בעלי עניין בנושאי ביטחון סייבר. אלה כוללים מוסדות ממשלתיים, את האקדמיה וארגונים במגזר הפרטי. שיתוף פעולה בנושא ביטחון סייבר הוא הרחבה טבעית של דפוס שיתוף פעולה לאומי שכבר קיים בתחומים אחרים,[56] ובא לידי ביטוי באחת מיוזמות הדגל של ישראל – פרויקט "יוזמת החדשנות" (CyberSpark) בבאר שבע. תהליך זה כולל מספר רב של בעלי עניין ומאפשר להפגיש ביחד את השחקנים הרלוונטיים. ההקשר וההיקף של התהליך האסטרטגי, ובפרט הבמה שעליה הוא מתרחש, מסייעים מאוד לקביעת הפרופיל של בעלי העניין.

---

53 "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)", *Official Journal of the European Union*, May 4, 2016, pp. 1-88.

54 Global Legal Group, "The International Comparative Legal Guide to: Data Protection 2018", *Global Legal Group*, 2018.

55 Alexander Klimburg, ed. *National Cyber Security Framework Manual* (Tallinn: NATO CCD COE 2012).

56 Housen-Couriel, "A Look at Israel's New Draft Cybersecurity Law".

הארגון האחראי על פיתוח אסטרטגיות לביטחון סייבר בישראל הוא מערך הסייבר הלאומי, הכולל בעלי עניין משלוש קטגוריות: הרמה הלאומית, המרחב האזרחי וארגונים לאומיים ובין־לאומיים. כל אלה רלוונטיים למטרה אותה נועדה לשרת האסטרטגיה. הרמה הלאומית מורכבת ממשרדי ממשלה ומסוכנויות בעלי ידע וקשר לתעשיית הבריאות, לחקיקה ולביטחון הסייבר; בעלי עניין מהמרחב האזרחי כוללים את משטרת ישראל ויחידת הסייבר הלאומי שלה, לצד גורמים מהאקדמיה; המרחב הלאומי והבין־לאומי כולל, בין השאר, מוסדות בריאות, ארגונים לשירותי בריאות (קופות החולים) וארגוני תקינה בין־לאומיים. בעלי העניין "הפנימיים" כוללים מנהלי אבטחת מידע ראשיים (CISO), נציגים מחטיבות ה־IT ואת ההנהלה של מוסדות הבריאות.

ענף הבריאות הישראלי מתמודד עם כמה תקנים בין־לאומיים הקשורים לאבטחת מידע ברשת. משום כך, יש תועלת בעירוב שחקנים מתחומי אחריות וידע אחרים בעת הכנת אסטרטגיה לאומית לביטחון סייבר עבור תחום הבריאות.

בעלי העניין בהולנד

האסטרטגיה הלאומית של הולנד לביטחון סייבר 2 (NCSS2) גובשה על ידי הקבינט ההולנדי ביחד עם מגוון רחב של ארגונים ציבוריים ופרטיים, מוסדות ידע וארגוני חברה אזרחית. אסטרטגיית NCSS2 מאפשרת לממשלת הולנד לגבש גישה משולבת לפשעי סייבר, עליה היא התחייבה בהסכם הקואליציוני. ב־1 בינואר 2012 הוקמה בהולנד "המועצה לביטחון סייבר" (CSR), שהיא גוף מייעץ עצמאי, המורכב מהקבינט ההולנדי ומנציגים בכירים מארגונים ציבוריים ומהמגזר הפרטי.[57]

ממשלת הולנד יכולה כיום לסמוך על מגוון רחב של שותפויות ציבוריות־פרטיות שיגבשו אסטרטגיית ביטחון סייבר מקיפה לתחום שירותי הבריאות בעתיד. שני גופים – "המרכז ההולנדי לשיתוף וניתוח מידע בתחום הבריאות" (ISAC) ו־Z-CERT – מבטיחים כי ענף שירותי הבריאות בהולנד יהיה מוגן טוב יותר, וזאת בזכות שיתוף המידע, בין היתר בתחומים של התקפות סייבר בין־מגזריות ומגמות מתפתחות בתחום יכולות הסייבר.

יעד נוסף באסטרטגיית ביטחון הסייבר הלאומית של הולנד הוא "דיפלומטיית סייבר". מטרתה היא לפתח מרכז של מומחיות בתחום המשפט הבין־לאומי וביטחון הסייבר, שיקדם שימוש חיובי במרחב הדיגיטלי. המרכז יאגד מומחים וקובעי מדיניות בין־לאומיים, דיפלומטים, אנשי צבא וארגונים לא־ממשלתיים,

57 "The National Cyber Security Center (NCSC) bundles knowledge and expertise", *Government of the Netherlands*, January 12, 2012, https://www.government.nl/latest/news/2012/01/12/the-national-cyber-security-center-ncsc-bundles-knowledge-and-expertise.

וזאת במטרה לחלוק ידע עם גופים קיימים. המומחים הבין־לאומיים יכללו גם כאלה החברים ב"מרכז האירופי לפשעי סייבר" (EC3 – Europol) וב"קומפלקס הבין־לאומי לחדשנות של האינטרפול" (Interpol Global Complex for Innovation – IGCI), המשַמש לפיתוח מחקרים בתחום זה.[58]

ד. תשתיות קריטיות ואובייקטים קריטיים

זיהוי נכון של נכסי הארגון חשוב לא רק מנקודת מבט עיסקית אסטרטגית, אלא גם מהיבט של אבטחה, ובכלל זה אבטחה בסייבר. אפשר להגדיר נכסים כמשאבים וכיכולות מוחשיים ובלתי מוחשיים, המאפשרים לארגון להשיג את יעדיו האסטרטגיים.[59]

התשתית הקריטית בישראל

ביוני 2017 גיבשה "הרשות הלאומית להגנת סייבר" במשרד ראש הממשלה את "המתודולוגיה להגנת סייבר בארגונים". הגנה על ארגונים היא מרכיב בתפיסת ההגנה הלאומית של ישראל, המתמקדת בהגנה על הכלכלה הישראלית והמרכיבים החיוניים שלה כנגד כל הפרעה. המסמך של "הרשות הלאומית להגנת סייבר" מנחה ארגונים כיצד להגדיר ולמפות את נכסיהם, לבצע הערכת סיכונים ולבדוק את מערכות ביטחון הסייבר שלהם. האסטרטגיה הלאומית לביטחון סייבר בישראל מתמקדת בצורה ברורה במיפוי הנכסים הקריטיים והמשניים של ארגון והקשר שלהם לספקים. שרשרת האספקה היא אחד הסיכונים הגדולים ביותר עבור ארגון. מכיוון שהתלות בצדדים שלישיים הופכת לקריטית גם בענף הבריאות בישראל, ארגונים הקשורים לתחום זה חייבים לשפר ולהתאים את תהליכי ניהול הסיכונים שלהם.

מהערכת סיכונים של מוסדות הבריאות שערך משרד הבריאות עלה כי מוסדות מסוימים תלויים במערכות רבות, שכולן נתמכות על ידי ספק חיצוני אחד (צד שלישי או ספק). כמו כן מצא משרד הבריאות כי מרבית בתי החולים בישראל משתמשים במערכת של אותו ספק.[60] לפי נציג של "הרשות הלאומית להגנת סייבר", מערך הסייבר הלאומי מכין, ביחד עם מספר בעלי עניין, אסטרטגיית סייבר ספציפית לתחום הבריאות, כדי להתמודד עם האיום הגובר של התקפות סייבר בענף הבריאות".[61]

---

58 Annegret Bendiek, "The European Union's Foreign Policy Toolbox in International Cyber Diplomacy", *Cyber, Intelligence and Security* 2, no. 3 (2018): 57-71.

59 Mark Frigo and James Hurley, "Understanding Your Organization's Genuine Assets", *Strategic Finance*, February 2014.

60 ראיון עם יניב פ., 6 בינואר 2019.

61 ראיון עם אליאב נ., 25 בנובמבר 2018.

התשתית הקריטית בהולנד

אסטרטגיית ביטחון הסייבר הלאומית של הולנד פותחה כדי לגבש מודל משטר מוגדר היטב, שיהיה בו איזון דינמי בין ביטחון, חופש ותועלת חברתית־כלכלית. במקביל, ממשלת הולנד ביקשה להתאים את תחומי האחריות של אבטחה פיזית גם על אבטחת הסייבר, והיא מתכוונת לעשות זאת על ידי דו־שיח עם ארגונים המתמודדים עם איומי סייבר.

נכון להיום, ממשלת הולנד אינה פועלת ליצירת התנאים ולגיבוש האמצעים לביטחון סייבר בתחום של שרשרת האספקה לעסקים או לענף הבריאות. יחד עם זאת, הצעת החקיקה האירופית יוצרת את התנאים והאמצעים שיוכלו לחול על מוצרים ושירותים של טכנולוגיות מידע ותקשורת גם בהולנד.[62] יתרה מכך, נכון להיום אין בהולנד אסטרטגיית ביטחון סייבר ספציפית להגנה על מוסדות המספקים שירותי בריאות מפני מתקפות סייבר. למרות זאת, ניתן לסכם ולומר כי מנקודת מבט לאומית הולנדית, החקיקה, התקנים והרשויות להגנת המידע של הולנד ושל האיחוד האירופי יוצרים את שכבת ההגנה הנדרשת מפני איומי סייבר על ענף הבריאות ההולנדי.

ה. מודיעין סייבר ומודעות לאבטחת סייבר

הן ישראל והן הולנד מתמקדות במודיעין סייבר ובמודעות לביטחון סייבר בתשתיות קריטיות כחלק ממאמציהן להילחם באיומי סייבר ולהגביר את המודעות אליהם בקרב הארגונים. הסיבה לכך היא ששתי המדינות התחילו להפנים את המטרות שמאחורי התקפות סייבר מתוחכמות ומזיקות ואת השפעותיהן על תשתיות קריטיות.

מודיעין סייבר ומודעות לאבטחת סייבר בישראל

ענף הבריאות בישראל בכללותו לא הגיע לרמה המיטבית של מודעות לסכנות אליהן חשופים הרשתות והמכשור הרפואי בתעשיית שירותי הבריאות. למעשה, ההזנחה בטיפול בפגיעויות ובעדכוני תוכנה הופכת את מוסדות הבריאות בישראל למטרה מושלמת.[63] מודיעין הסייבר בתחום הבריאות מועבר בישראל בעיקר דרך מוסדות ממשלתיים: משרד הבריאות אוסף מידע על ביטחון סייבר באמצעות שלל מקורות, כמו גופי ממשל, ארגונים אזרחיים וארגונים בין־לאומיים.[64] המשרד

62 ראיון עם Tom S., 19 בדצמבר 2018.

63 Patricia Williams and Andrew Woodward, "Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem", *Dove Press Journal*, no. 8 (2015): 305-316.

64 ראיון עם יניב פ., 6 בינואר 2019.

גם מעודד את מוסדות הבריאות בישראל להתחבר לשירותי מודיעין הסייבר שלו ללא תשלום, כדי להשיג הגנה נוספת.

מערך הסייבר הלאומי של ישראל ומשרד הבריאות הקימו את מערכת MedSOC כדי לספק מידע על מתקפות סייבר בתחום שירותי הבריאות ולשתף מידע דרך רשת MedSOC. נכון להיום, רשת MedSOC מחוברת רק לבתי חולים, והיא צפויה להתחבר לכל מוסדות הבריאות בישראל במהלך חמש השנים הבאות.[65] בנוסף לכך, ממשלת ישראל התחייבה להשקיע משאבים ומאמצים בכל מוסדות החינוך בתחום סיכוני סייבר ולחזק את מאמצי ביטחון הסייבר במגזר הטכנולוגי.

מודיעין סייבר ומודעות לאבטחת סייבר בהולנד

הארגונים הגדולים במגזר הפרטי בהולנד מגלים, ככלל, מודעות מספקת לביטחון הסייבר, ורובם גם מודעים לכך שתקיפות סייבר עלולות לגרום נזק לנכסיהם. הבעיה היא שמתקפות סייבר יכולות לפגוע גם בתדמית הארגון. ממשלת הולנד קיימה מפגשים עם מדינות נוספות באיחוד האירופי כדי לדון בשאלה האם לחייב ארגונים לדאוג לביטחון סייבר בתחום החומרה והתוכנה.[66] למרות שהממשלה השקיעה רבות בהעלאת המודעות לאיומים דיגיטליים, יש צורך בגישה מחודשת, שתתמקד בתמרוץ ארגונים ובסיוע להם לנקוט פעולות לשיפור האבטחה המקוונת.

בסוף 2017 השיקו המשרד לכלכלה ומדיניות האקלים ומשרד המשפטים והביטחון של הולנד תוכנית משותפת שנקראת "מרכז אֵמון דיגיטלי" (DTC). חזון התוכנית הוא להגביר את חוסן העסקים מול איומי סייבר, תוך התמקדות בשתי משימות מפתח: הראשונה היא לספק לעסקים מידע אמין ועצמאי על נקודות תורפה דיגיטליות וייעוץ קונקרטי לגבי הפעולה שעליהם לנקוט; המשימה השנייה היא לטפח בריתות בין עסקים לאבטחת סייבר.[67]

ממצאים השוואתיים

שתי האסטרטגיות הלאומיות לביטחון סייבר של ישראל ושל הולנד הן בעלות מטרות דומות: להגן על מרחב הסייבר מפני אויבים ולהעצים את חוסן הסייבר. עם זאת, קיימים הבדלים בין שתי המדינות במרכיבים, כמו סביבת איומי הסייבר,

65 ראיון עם אליאב נ., 25 בנובמבר 2018.

66 Herna Verhagen, "De economische en maatschappelijke noodzaak van meer cyber security – Nederland digitaal droge voeten", *Nederland digitaal droge voeten, The Hague*, September 2016.

67 "Factsheet Digital Trust Center", *Government of the Netherlands: Ministry of Economic Affairs and Climate Policy*, August 6, 2018, pp. 1-4.

התנאים הסוציו־פוליטיים, מגמות הביטחון, המסורות ורמת המודעות לסייבר. אלה הביאו להבדלים משמעותיים בגישתן של שתי המדינות לביטחון הסייבר.[68]

משטר ניהול סיכונים

יש קווי דמיון וקווי שוני רבים בין הגישות של ישראל והולנד מבחינת משטר ניהול הסיכונים. לשתי המדינות יש גופים ממשלתיים (בהולנד – משרד הבריאות ו"המרכז הלאומי לביטחון סייבר" – NCSC; בישראל – משרדי הבריאות, הרווחה והספורט ומערך הסייבר הלאומי), המארגנים פגישות סדירות עם המוסדות המספקים שירותי בריאות, במטרה לשמור על הידע הנצבר בתעשייה ועל המודעות שלה לאתגרים ולתהליכים הרלוונטיים. עם זאת, עצם ההקמה של רשת MedSoc בישראל, התומכת באופן ספציפי במגזר השירותים הרפואיים, היא הוכחה ברורה לכך שממשלת ישראל מבינה כי איומי הסייבר מהווים כיום איום פוטנציאלי לרציפות העיסקית של ענף שירותי הבריאות. בהולנד פועל "המרכז הלאומי לביטחון סייבר", אך אין גוף המתמקד ספציפית בענף הבריאות.

הסביבה הרגולטורית

בנוסף למשטר ניהול הסיכונים, ממשלות ישראל והולנד חוקקו חוקים דומים בנושא סייבר ומידע, אם כי כל אחת משתי המדינות שומרת על המאפיינים הייחודיים שלה, שהם תוצאה של מיקומה ומצבה. שתי המדינות גם קבעו תקנות למינוי מנהלי אבטחת מידע ראשיים וקציני אבטחת מידע בארגונים. חוק הפרטיות בישראל מחייב את המחזיקים במידע למנות מנהלי מידע, אלא שלמרות החובה, החוק לא תמיד נאכף.

חרף הדמיון בין שתי המדינות, ישנם כמה הבדלים עיקריים ביניהן בתחום הרגולציה: בהולנד יש חוק ביטחון סייבר, שמתעדכן בימים אלה לפי תקנות "הרגולציה הכללית להגנה על מידע", ובכך הוא מציע שיטה טובה יותר להתמודדות עם נתונים אישיים. עדכון החוק גם הביא להקמת "הסוכנות להגנת נתונים" (DPA), כסמכות העיקרית בהולנד לנושא זה. בישראל, נכון להיום, אין חוק ביטחון סייבר (הוא נמצא עדיין בשלבי ניסוח). מצב זה מקשה על גופי הממשל בישראל לאכוף שימוש באמצעים או לקבוע תקנים מסוימים של ביטחון סייבר לענף שירותי הבריאות. עם זאת, שתי הסביבות הרגולטוריות בישראל ובהולנד דומות בכל הנוגע לביטחון סייבר ואבטחת מידע, וזאת מכיוון שישראל העתיקה

68 Martti Lehto, "The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies", *International Journal of Cyber Warfare and Terrorism* 3, no. 3 (2013): 1-18.

בצורה נרחבת את "הדירקטיבה האירופית להגנת מידע" כדי להבטיח התאמה רבה יותר עם התקנים האירופיים.[69]

בעלי העניין העיקריים באסטרטגיה

הולנד וישראל הן חלוצות בתחום ביטחון הסייבר, שכן שתיהן תומכות בשיתוף פעולה עם מומחים מכל מוסדות הממשלה, וכן מהמגזר האזרחי והתעשייתי, לצורך השגת ביטחון בסייבר. אמנם, מסמך האסטרטגיה הלאומית לביטחון סייבר של ישראל אינו מתמקד בשיתוף פעולה בין־לאומי כמו במקרה של האסטרטגיה ההולנדית, אך ריבוי השותפויות הפרטיות־ציבוריות הבין־לאומיות מלמד בבירור על האינטרסים של ממשלת ישראל בשיתוף פעולה בין־לאומי בנושא זה.

הגדרת תשתיות קריטיות ואובייקטים קריטיים

היבט משמעותי באסטרטגיה הלאומית לביטחון סייבר של שתי המדינות הוא הסודיות, השלמות והזמינות של המידע. האסטרטגיה של ישראל מדגישה שימוש בבקרות ספציפיות להגנה על מערכות וארגונים מפני פגיעה בסודיות, בשלמות ובזמינות של מידע ומערכות. מסמך האסטרטגיה ההולנדי אמנם מציין את הסודיות, השלמות והזמינות, אך אינו מספק תפיסה להתמודדות עם שאלת ביטחון הסייבר. שתי המדינות מכירות בכך שיש למפות את הנכסים הקריטיים והמשניים של מוסדות הבריאות, כדי להבין את האיומים על התהליכים המתקיימים בהם ואת נקודות התורפה שלהם.

יחד עם זאת, הגישה של ישראל להתמודד עם נקודות התורפה בשרשרת האספקה של ענף הבריאות היא יוצאת דופן בתחום ביטחון הסייבר: מערך הסייבר הלאומי ומשרד הבריאות הקימו מערכת מבוססת ציונים בכדי לבדוק עד כמה המערכות והשירותים של הספקים הם קריטיים לענף הבריאות, וכן כדי לבדוק את אמצעי ביטחון הסייבר אצל הספק, בהתבסס על קריטיות המוצרים ו/או השירותים.

מודיעין סייבר ומודעות לאבטחת סייבר

ישראל והולנד נמנות על המדינות היותר מפותחות מבחינת חדשנות בתחום הסייבר ואמצעי ביטחון הסייבר. מערך הסייבר הלאומי בישראל מגן באופן יזום על ענף הבריאות על ידי סריקת "הרשת האפלה" במטרה לאתר פושעי סייבר ושיטות חדשות של מתקפות סייבר. שירות המודיעין של הולנד הקים את "יחידת הסייבר המאוחדת" (Joint SigInt Cyber Unit – JSCU), המספקת מידע ומיומנות מקצועית לכלל התשתיות הקריטיות.

69 Bourne, "A Guide to Data Protection in Israel".

במקביל, ממשלת הולנד יצאה בתוכנית לשיפור המודעות לביטחון סייבר בחברה ההולנדית באמצעות פרסומות ומדיה. היוזמה הממשלתית מכוונת לכל אזרחי הולנד, תוך שהממשלה משנה בהדרגה את גישתה מגישה מבוססת־ידע לגישה של רכישת מיומנויות בביטחון סייבר.[70] בישראל אין יוזמה דומה להרחבת מיומנויות ביטחון הסייבר של אזרחיה. עם זאת, יחידה 8200 של צה"ל מתמקדת בלוחמת סייבר ופועלת כזרז בתחום ביטחון הסייבר ב"אומת ההיי־טק".

הבדל נוסף בין שתי המדינות הוא מערכת MedSOC הישראלית, המשתפת מידע על איומי סייבר ספציפיים בענף הבריאות. למרות שהמערכת עדיין נמצאת בשלבי פיתוח ראשונים, כל מוסדות שירותי הבריאות בישראל אמורים להיות מחוברים למערכת הפצת המידע בתוך חמש שנים.[71]

מסקנות

השינויים הטכנולוגיים בענף הבריאות והאיום המתמשך של מתקפות סייבר הממוקדות ברשתות ובמכשור רפואי בתחום שירותי הבריאות (שהולך ומתעצם בזכות הקישוריות המתפתחת), יוצרים מטרה מושכת למתקפות. אלו כוללות את "האינטרנט של הדברים הרפואיים", יישומים רפואיים, תוכנות, מערכות מידע והתקני אבטחה בכל מוסדות הבריאות. התגברות האיומים הללו על כל התשתיות הקריטיות גרמה למדינות רבות להתחיל לפתח אסטרטגיות ולגבש תקנות לחיזוק ביטחון הסייבר. האסטרטגיות הלאומיות והתקנות שגיבשו ישראל והולנד לביטחון סייבר הן מקיפות ונותנות מענה לשורה של איומי סייבר. עם זאת, שתי המדינות צריכות לבצע שיפורים מסוימים כדי לתת מענה לשינויים המתחוללים בתחום הסייבר בענף הבריאות.

משטר ניהול הסיכונים בתחום ביטחון הסייבר מאפשר לשתי המדינות לעדכן את יעדיהן האסטרטגיים ולהשיגם, תוך צמצום סיכונים. הן משטר ניהול הסיכונים והן המשרדים האחראים לכך בישראל ובהולנד מתמקדים בגישה של מטָה־מעלה, שבאה לידי ביטוי במפגשים בנושא ביטחון סייבר עם מנהלי IT ומנהלי בתי חולים. לעומת זאת, קיימת שונות ניכרת בין שתי המדינות בגישה שלהן כלפי אמצעי ביטחון הסייבר במכשור הרפואי; בעוד שישראל יצרה סביבה בטוחה לבדיקת המכשור הרפואי החדש טרם הכנסתו לשימוש, הולנד בחרה בדרך של הנחיות וייעוץ בלבד למפעילי שירותי הבריאות בכל מה שנוגע לבדיקת הציוד הרפואי לפני הכנסתו לשימוש.

---

70 "National Cyber Security Agenda, 'A Cyber Security Netherlands'", *Government of the Netherlands: Ministry of Justice and Security*, April 20, 2018.

71 ראיון עם אליאב נ„ 25 בנובמבר 2018.

שתי המדינות קבעו תקנות להגנה על נתונים בארגונים מפני פושעי סייבר, לרבות בתחום הבריאות, וכן על נתונים פרטיים של אזרחים. ישראל והולנד גם קבעו תקנות המחייבות ארגונים המטפלים במידע רגיש להעסיק מנהלי מידע (מנהלי אבטחת מידע ראשיים וקציני אבטחת מידע). חוק חשוב ורלוונטי נוסף בשתי המדינות הוא החוק ליידוע על פריצה לנתונים, המחייב את מנהלי המידע לדווח על אירועים הקשורים להגנת מידע. יש להניח שכמו הולנד, ישראל תחוקק בסופו של דבר גם חוק לביטחון סייבר, אשר ישפר את הטיפול באירועי סייבר.

בעלי עניין משפיעים מאוד על האסטרטגיה הלאומית לביטחון סייבר בכל מדינה, מאחר שלדרג האופרטיבי יש דעה שונה בנושא ביטחון סייבר מאשר לדרג המופקד על האסטרטגיה. איזון סביר בין סוגיות הנוגעות לביטחון סייבר ובין העבודה השוטפת יועיל לשיפור ביטחון הסייבר, ובכלל זה גם לעובדי מערכת הבריאות. ישראל והולנד מקיימות קשר קבוע עם בעלי העניין בענף שירותי הבריאות שלהן, במטרה לגבש אסטרטגיות סייבר אפקטיביות שיעודדו מחויבות פרו־אקטיבית ורב־תחומית מצידם. לצד הגדרת תחום התשתיות הקריטיות, גם מוסדות הבריאות צריכים להגדיר מהם הנכסים הקריטיים והלא קריטיים שלהם, כך שיוכלו ליישם אמצעי ביטחון סייבר מיוחדים על אותם נכסים שזקוקים לכך.

האסטרטגיות הלאומיות של ישראל והולנד בנושא ביטחון סייבר מתמקדות במיפוי נכסי ארגונים באמצעות תהליך של הערכת סיכונים ובדיקת מערכות קיימות להגנת סייבר. שתי המדינות גם מדגישות את חשיבות ביטחון הסייבר למניעת מתקפות ברשת.

ישראל והולנד מעמידות במרכז תשומת הלב של ענף שירותי הבריאות את הסודיות, השלמות והזמינות של המידע. ההבדל הגדול ביניהן בהתייחסותן לענף שירותי הבריאות הוא שממשלת ישראל לקחה על עצמה את האחריות לסייע לענף זה בנקודות התורפה של שרשרת האספקה, בעוד שהולנד בחרה למלא רק תפקיד אינפורמטיבי באבטחת שרשרת זו.

מודיעין סייבר ומודעות לביטחון סייבר הופכים להכרח בענף שירותי הבריאות. שירותי המודיעין של ישראל פועלים יחד עם משרד הבריאות וסורקים את "הרשת האפלה" לאיתור מתקפות סייבר חדשות. הצבא ושירותי המודיעין בהולנד הקימו את "הרשת הלאומית לתגובה למתקפות", במטרה לאתר ולהרתיע מתקפות סייבר באמצעות פתרונות ביטחון סייבר חדשים. יתרה מכך, ממשלת הולנד גיבשה תוכנית למודעות ביטחונית, העושה שימוש בפרסומות כדי ליידע על הסכנות הקיימות באינטרנט ולהגביר את החוסן האזרחי. בישראל אין כיום תוכנית דומה למודעות בנושא ביטחון סייבר, אך הידע בתחום הסייבר מתרחב באמצעות יחידות של צה"ל המתמקדות בלוחמת סייבר ומודיעין. מודיעין הסייבר בישראל מופץ גם באמצעות

מערכת MedSOC החדשה, המאפשרת למשרד הבריאות ולמערך הסייבר הלאומי להעלות אליה מידע על התקפות סייבר או על פגיעויות ברשת.

המלצות

להלן המלצות לשיפור ולהתנהלות בתחום האסטרטגיות הלאומיות לביטחון סייבר, שחלקן מסתמכות על החוזקות הנוכחיות של האסטרטגיות הקיימות בישראל ובהולנד.

ראשית, יעילותן של האסטרטגיות והתקנות בנושאי סייבר הקיימות בשתי המדינות תלויה ביכולת הממשלות להסתגל לעולם הסייבר המתפתח. אסטרטגיות ביטחון סייבר עתידיות יצטרכו, אפוא, להיצמד לבסיס הקיים של תקנות וחוקים, אך תוך עיצוב מחודש וגמיש של הסביבה הרגולטורית ומערכות המידע בארגונים בעלי תשתית קריטית. על הממשלות לעדכן את האסטרטגיות, המדיניות והתקנות שלהן על בסיס שנתי או דו־שנתי, כדי שיישארו רלוונטיות להתפתחויות החדשות בעולם הסייבר.[72]

שנית, בדיקה ופיתוח של אסטרטגיות ביטחון סייבר חדשות מצריכים תהליך מתמיד של הערכת סיכונים. על ישראל והולנד להמשיך ולהחזיק בגישתן לביטחון הסייבר, המגינה על ענף שירותי הבריאות מפני התקפות סייבר, שכן פושעי סייבר לעולם לא יפסיקו לנסות לפרוץ למערכות המידע של מוסדות המספקים שירותי בריאות. למרבה המזל, שתי המדינות נוהגות להעמיד למבחן את אסטרטגיות ביטחון הסייבר שלהן בתרגילים ארציים, ועושות זאת כדי לשפר ולחזק נוהלי אבטחה קיימים. מערך הסייבר הלאומי בישראל ומקבילו ההולנדי (NCSC) צריכים לקבל על עצמם אחריות רבה יותר לענף שירותי הבריאות באמצעות עידוד המוסדות ומנהלי אבטחת המידע שלהם לגבש תוכניות להמשכיות עיסקית ולתרגל מצבים שיכינו את העובדים למקרה של משבר סייבר.[73] בנוסף לכך, כדי להגן על בסיסי הנתונים הרפואיים הלאומיים מפני התקפות סייבר, על מערך הסייבר הלאומי של ישראל ו"מינהלת הבריאות והנוער" של הולנד לתת את הדעת למוסדות קטנים ופחות מאובטחים ולהגדיר עבורם גישה אבטחה נפרדת, מתוך הבנה שמוסדות כאלה נוטים פחות, או מסוגלים פחות, לבצע עדכוני מערכת או לרכוש מכשור רפואי חדש.

שלישית, על ממשלות ישראל והולנד לחקור אסטרטגיות ביטחון סייבר של בעלות ברית נוספות, כדי להבטיח יכולת טובה יותר להתייחס לאיומים המתעוררים בזירה הבין־לאומית. זאת, מתוך הנחה שככל שירבו הגורמים המעורבים בהתמודדות עם איומים כאלה, כך יפחת הנטל על כל אחד מהם. מה שחסר כיום הוא חלוקת נטל

72 ראיון עם יניב פ., 6 בינואר 2019.
73 ראיון עם אליאב נ., 25 בנובמבר 2018.

כזו בין ממשלות. בנוסף, קונצנזוס בין־לאומי סביב הגדרות, חוקים וחלופות בתחום ביטחון הסייבר יקל את האילוצים שבפניהם ניצבת הרגולציה במדינות שונות.

רביעית, יש לקדם מודעות רבה יותר לביטחון סייבר בחברה המקומית בכלל ובמוסדות שירותי הבריאות שלה בפרט. אחדות מההנחיות צריכות להתמקד בהגברת המודעות לביטחון סייבר אצל צוותי שירותי הבריאות, מכיוון שאלה מִטבעם אינם נוטים לעסוק בכך, אלא מתמקדים בבריאות המטופלים. על הארגונים ואנשי הצוות המספקים שירותי בריאות להכיר את הסכנות לביטחון הסייבר ואת שיטות המתקפה במרחב זה.

חמישית, למרות שישראל והולנד מחזיקות בגישה מתקדמת כלפי ביטחון הסייבר, יש לציין כי בשתי המדינות גם נותרו פערים לא מטופלים בתחום זה. יש לקוות שמחקרים עתידיים ומאמצים נוספים להבנת איומי הסייבר בתחום שירותי הבריאות ישפרו את החוסן החברתי בשתי המדינות. בנוסף לכך, שיתוף פעולה נרחב עם מספר רב יותר של מדינות ברחבי העולם יתרום גם הוא להפיכתו של מרחב הסייבר בשתי המדינות לטוב ולבטוח יותר.

סיכוני סייבר למערכות בינה מלאכותית: אתגרים טכנולוגיים ודרכי התמודדות

לירן ענתבי וגיל ברעם

מערכות אוטונומיות מבוססות בינה מלאכותית הולכות ותופסות מקום משמעותי בחיי היומיום ובמגוון תחומי חיים: תעשייה, רפואה, משקי בית וכמובן התחום הביטחוני. מערכות אלו, בהיותן ממוחשבות, חשופות לטעויות בקוד, שמצידן עלולות להוביל לקבלת החלטות שגויה ולביצוע פעולות לא רצויות. בנוסף לכך, הן פגיעות למתקפות סייבר שעלולות להוביל לפגיעה בפעילותן או אף להשבתתן. מאמר זה בוחן את הסיכונים המאיימים על מערכות אוטונומיות כחלק ממרוץ חימוש בין המעצמות, ודן בצעדים בתחום המדיניות שיאפשרו להתמודד עם סיכונים אלה ברמה הלאומית.

מילות מפתח: בינה מלאכותית, לוחמת סייבר, ביטחון לאומי, מרוץ חימוש

מבוא

"בינה מלאכותית היא העתיד, לא רק עבור רוסיה אלא עבור האנושות כולה [...] יש בה הזדמנויות אדירות, אך גם איומים שקשה לחזותם. מי שיהפוך למוביל בתחום זה יהיה לשליט העולם". כך אמר נשיא רוסיה, ולדימיר פוטין, בהרצאה שנשא בספטמבר 2017.[1] ואכן, נראה כי מערכות אוטונומיות מבוססות בינה מלאכותית

לירן ענתבי היא עמיתת מחקר במכון למחקרי ביטחון לאומי, מנהלת את המחקר בתחום הטכנולוגיות המתקדמות והביטחון הלאומי ב־INSS, מרצה באוניברסיטת בן־גוריון ויועצת בתחום הטכנולוגיות המתקדמות.

גיל ברעם היא מנהלת המחקר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון ועמיתת מחקר במרכז הסייבר הרב־תחומי ע"ש בלווטניק, אוניברסיטת תל אביב.

1 "Artificial intelligence is the future, not only for Russia, but for all humankind […] It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world": "'Whoever Leads in AI Will Rule the World': Putin to Russian Children on Knowledge Day", *RT World News,* 2017, https://www.rt.com/news/401731-ai-rule-world-putin.

הולכות ותופסות מקום משמעותי בחיי היומיום במגוון תחומי חיים: תעשייה, רפואה, משקי בית וכמובן בתחום הביטחוני. בהיותן מערכות ממוחשבות, הן חשופות לטעויות בקוד, שעלולות להוביל לקבלת החלטות שגויה ולביצוע פעולות לא רצויות. הן גם פגיעות למתקפות סייבר שעלולות להוביל לתוצאות לא רצויות, לפגיעה בפעילותן או אף להשבתתן. במקביל, מתרחב השימוש במערכות בעלות יכולות אוטונומיות, הדורשות אמנם רמה מסוימת של מעורבות אנושית בקבלת ההחלטה הסופית להפעלתן, אך תהליכי החישוב וההמלצה שלהן אוטונומיים, ולרוב אינם ניתנים להסבר.

מאמר זה בוחן את הסיכונים המאיימים על מערכות אוטונומיות ואת הדרכים להתמודד עימם ברמה הלאומית. חלקו הראשון נפתח בסקירת השימושים בבינה מלאכותית ובמערכות אוטונומיות בתחום הביטחוני, מתאר את מרוץ החימוש המתרחש בתחום זה ואת השפעתו על הזירה הבין־לאומית ודן בתמריצים לביצוע מתקפות סייבר על מערכות אלו. בחלק השני של המאמר מתוארות מתקפות סייבר אפשריות על מערכות מבוססות בינה מלאכותית – מתקפות ומניפולציות הייחודיות למערכות סייבר – וכן נסקרים שימושים שניתן לעשות בבינה מלאכותית בתחומי לוחמת הסייבר לצורכי הגנה והתקפה כאחת. לבסוף מציע המאמר צעדים בתחום המדיניות, שמטרתם היא לסייע בצמצום הסיכונים שעשויים להיות הרסניים ככל שהשימוש במערכות האוטונומיות מתרחב והתלות האנושית בהן גדֵלה.

בינה מלאכותית ומערכות אוטונומיות – התפתחות ושימושים מרכזיים

בינה מלאכותית היא ענף של חקר מדעי המחשב שקיים מאז שנות החמישים של המאה העשרים. אחת ההגדרות הפשוטות והמקובלות של בינה מלאכותית היא: "לגרום למכונה להתנהג בדרך שהייתה נחשבת לאינטליגנטית לו אדם התנהג כך".[2] בעשור האחרון, בין היתר עקב ההתקדמות בחקר מדעי המחשב, פיתוח חומרות ותוכנות מתקדמות בתחומי המחשוב והתקשורת ופריצת תחומים חדשים כמו מחשוב ענן ונתוני עתק, התאפשרה התקדמות משמעותית גם בתחום הבינה המלאכותית. במסגרת זו התפתחו תחומים כמו "למידת מכונה" ו"רשתות נוירונים עמוקות", שמאפשרים מגוון יישומים מתקדמים בתחומים שונים. בין השאר מדובר ביישומים בתחום פענוח התמונה, הפועלים בעולם הרפואה ומסייעים לנתח בדיקות מסוגים שונים; יישומים בתחום הקולי, המאפשרים פעולתם של "עוזרים חכמים", דוגמת "סירי" ו"אלקסה"; וכן אלגוריתמים רבים בתחום הניבוי, המציעים לקהל

2 Edward Geist and Andrew Lohn, "How Might Artificial Intelligence Affect the Risk of Nuclear War?", *RAND Corporation*, 2018, p. 9.

הרחב ברשת האינטרנט מוצרים או שירותים כמו אלה שהם רכשו קודם לכן או כאלה שהתעניינו בהם בעבר.

בדרפ"א (DARPA – Defense Advanced Research Projects Agency) שבמשרד ההגנה האמריקאי מתייחסים אל בינה מלאכותית כאל "יכולת מתוכנתת לעבד מידע".[3] למרות ההגדרה, חשוב להבהיר כי לא כל מערכת מחשוב עושה שימוש בבינה מלאכותית. אלגוריתמים של בינה מלאכותית מעוצבים לצורך קבלת החלטות ועושים זאת לרוב באמצעות שימוש בנתונים שמוזנים להם בזמן אמת. לא מדובר במכונות פסיביות שמסוגלות לתגובות מכניות או קבועות מראש בלבד, כפי שהורגלנו בעידן האוטומציה (למשל, דלתות אוטומטיות), אלא במכונות שבעזרת חיישנים, נתונים דיגיטליים ואפילו קלטים מרוחקים, מסוגלות לשלב מידע ממקורות שונים, לנתח אותו באופן מיידי ולפעול בהתאם לתובנות הנגזרות מן הנתונים. הדבר מאפשר תחכום ומהירות בקבלת הנתונים ברמה שלא הייתה קיימת קודם לכן.[4]

מרבית היישומים הנפוצים בתחום הבינה המלאכותית בימינו שייכים לתחום הקרוי "למידת מכונה". תחום זה כולל שימוש באלגוריתמים סטטיסטיים המחקים משימות אנושיות קוגניטיביות על ידי גזירת חוקים בנוגע אליהן באמצעות ניתוח כמויות גדולות של נתונים בנושא. למעשה, האלגוריתם "מתאמן" על מידע קיים, ותוך כדי תהליך "האימון" יוצר מודל סטטיסטי משלו, שיוכל לבצע בעתיד את אותה משימה על נתונים חדשים שבהם לא נתקל קודם לכן.[5]

השימוש בטכנולוגיה של בינה מלאכותית הולך וגובר, ומדינות, חברות וגורמים ביטחוניים רבים מסתמכים כיום על מערכות כאלו לצרכיהם השונים. בין השימושים האזרחיים בבינה מלאכותית ניתן למנות שירותים שונים, כגון אפליקציות ניווט, אלגוריתמים המציעים סחורות או שירותים מותאמים, אלגוריתמים בתחומי הבנקאות והסחר הפיננסי, מערכות בתחומי אחזקה, לוגיסטיקה ועוד. כאמור, מערכות מבוססות בינה מלאכותית נפוצות גם בתחום הביטחון, וכבר כיום קיימים תחומים ביטחוניים רבים בהם נעשה שימוש במערכות כאלו. ביניהם ניתן למנות:

- **מודיעין:** שימושים רבים מאוד בבינה מלאכותית קיימים בתחום המודיעין. כיום נפוץ השימוש באלגוריתמים מתחום למידת מכונה ותחומים נוספים לצורך ניתוח

3 John Launchbury, "A DARPA Perspective on Artificial Intelligence", *TechnicaCuriosa*, 2017, https://machinelearning.technicacuriosa.com/2017/03/19/a-darpa-perspective-on-artificial-intelligence./

4 Darrell M. West and John R. Allen, "How Artificial Intelligence Is Transforming the World", *Brookings*, 2018, https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world./

5 Kelley M. Sayler and Daniel S. Hoadley, "Artificial Intelligence and National Security", *Congressional Research Service*, 2019, p. 2.

תמונות וטקסטים. כמו כן, נעשה שימוש באלגוריתמים לתרגום שפות, לניתוח וידיאו ואודיו ועוד. בין הידועים בפרויקטים מתחום זה נמצא "פרויקט מייבֶן" ("Maven") שבוצע בשיתוף פעולה בין "גוגל" ובין משרד ההגנה האמריקאי, שבמסגרתו נעשה שימוש בבינה מלאכותית לצורך ניתוח של תצלומי מל"טים.[6] בנוסף לארצות הברית, גם בסין ובמדינות נוספות מתקיימת פעילות לייצור מערכות לסינון מיטבי של תוכן מודיעיני והיתוך מידע ממערכות שונות לצורך הפקת מודיעין, תוך שימוש ביכולות בינה מלאכותית.[7]

- **לוגיסטיקה:** כמו בתחום האזרחי, יישומי בינה מלאכותית קיימים גם בתחומי הלוגיסטיקה הצבאית השונים. צבא ארצות הברית עושה שימוש במערכות כאלו כבר משנות התשעים של המאה הקודמת, ואחת מהן אף סייעה בתכנון ואופטימיזציה של העברת כוחות בזמן מלחמת המפרץ הראשונה. הדבר הוביל לחיסכון שהחזיר את ההשקעה שנעשתה במשך שלושים שנה במחקר הבינה המלאכותית.[8] בין המערכות החדשניות יותר ניתן למנות כאלו המסייעות בתחום האחזקה של מערכות באופן שלא היה מתאפשר בעבר, כמו למשל מערכות שמדווחות מראש על בלאי עתידי בחלפים ומאפשרות להחליף אותם על בסיס שימוש פרטני ולא על בסיס מידע סטטיסטי כללי, כפי שהיה מקובל עד כה. שיטה זו מובילה לחיסכון משמעותי, כמו גם להגברת הבטיחות.[9]
- **פיקוד ושליטה:** במערכות פיקוד ושליטה עתיד להיעשות שימוש הולך וגובר בבינה מלאכותית, בין היתר כמערכות מייעצות שיפעלו כמערכות מסייעות החלטה, בכפוף לגורם האנושי ובשיתוף פעולה איתו.
- **כלי רכב אוטונומיים:** נהיגה אוטונומית מזוהה בעיקר עם "מכוניות ללא נהג", שאבות הטיפוס שלהן מתחילים לצוץ על הכבישים במקומות שונים ברחבי העולם. למעשה, מדובר באחד האתגרים המרכזיים של דרפ"א עוד מהעשור הקודם, שאפשר את קפיצת המדרגה בתחום זה.[10] בעוד שבתחום האזרחי

6 Samuel Gibbs, "Google's AI Is Being Used by US Military Drone Programme", *The Guardian*, May 7, 2018, https://www.theguardian.com/technology/2018/mar/07/google-ai-us-department-of-defense-military-drone-project-maven-tensorflow.
יש לציין כי הפרויקט הוביל להתנגדות בקרב עובדי "גוגל", לאור החשש שהידע שנוצר בו יסייע לא רק בניתוח חומרים מודיעיניים, אלא גם ביצירת מערכות נשק אוטונומיות שיוכלו לתקוף ללא מעורבות יד אדם.

7 להרחבה בנושא זה ראו: Stephen Chen, "Inside the AI Revolution that's Reshaping Chinese Society", *South China Morning Post*, June 29, 2017, https://www.scmp.com/news/china/society/article/2100427/chinas-ai-revolution-and-how-its-rivalling-us.

8 נורית כהן־אינגר וגל קמינקא, "והרי התחזית: צה"ל בדרך לצבא תבוני – מפת דרכים לאימוץ טכנולוגיות בינה מלאכותית בצה"ל", **בין הקטבים**, גיליון 18, 2018, עמ' 95.

9 Sayler and Hoadley, "Artificial Intelligence and National Security", p. 9.

10 DARPA, "The Grand Challenge for Autonomous Vehicles", 2019, https://www.darpa.mil/about-us/timeline/-grand-challenge-for-autonomous-vehicles.

השימוש הבולט הוא האוטונומיות הקרקעית, בתחום הביטחוני נעשה, כבר מספר עשורים, שימוש בכלים בלתי מאוישים באוויר, בים וביבשה, חלקם בעלי יכולות אוטונומיות שונות. לכלים אלה משמעות גדולה מאוד בשדה הקרב, והם יכולים להוות מכפיל כוח או להחליף גורם אנושי באזורי סכנה. יחד עם זאת, מרבית הכלים הללו, חרף יכולותיהם האוטונומיות, נסמכים במידה רבה על מעורבות והפעלה אנושיות.

- **מערכות אוטונומיות צבאיות:** מדובר באחד התחומים הבולטים המבוססים על בינה מלאכותית. מדינות רבות זיהו בעשורים האחרונים את הפוטנציאל הטמון בשימוש בכלים בלתי מאוישים לצורכי ביטחון, והן נוקטות צעדים שונים לרכש ולפיתוח מערכות כאלו באופן עצמאי. בין המדינות המובילות בתחום זה: ארצות הברית, ישראל, בריטניה וצרפת. בתוך המערכות האוטונומיות הצבאיות ניתן להתייחס לתת־קבוצה של מערכות נשק אוטונומיות. אלו מערכות המסוגלות לחפש, לזהות ולתקוף מטרות באופן עצמאי, ללא מעורבות אנושית.[11] מערכות אלו מהוות גורם "משַנה כללי־מִשחק", משום שהן ניתנות להפעלה כמעט ללא מעורבות אנושית, אך בה בעת מסוגלות לגרום לפגיעה קטלנית. תחום המערכות האוטונומיות הצבאיות מעורר ויכוח ציבורי נרחב, ובאו"ם אף מתקיימים דיונים בנוגע להגבלתו. למרות זאת, פיתוחו מואץ מאוד כיום, עד שיש מי שחושש שהעולם נמצא על סף מרוץ חימוש בתחום זה,[12] או אף בעיצומו. מדובר אמנם בתחום שנמצא בתחילת דרכו, אך מספר מדינות כבר רכשו ניסיון מבצעי בשימוש במערכות אוטונומיות מסוגים שונים. בין המערכות שצברו ניסיון ניתן למנות מערכות הגנה אווירית, דוגמת "פטריוט" האמריקאית או "כיפת ברזל" הישראלית. אלו הן מערכות בעלות אוטונומיות גבוהה מאוד, ואפילו יכולת לפעול באוטונומיות מלאה. יחד עם זאת, לאור החלטה עקרונית של המדינות המפעילות אותן, הן עדיין נסמכות על החלטת המפעיל האנושי הנמצא במעגל ההפעלה שלהן.[13] לצד מערכות ההגנה האווירית ניתן למנות את "החימוש המשוטט", דוגמת "הארופ" ("Harop"). מדובר במערכת אווירית בעלת יכולת טיסה, שהייה באוויר, איתור, מעקב ותקיפת מטרות ללא מעורבות

11 "Autonomous Weapon Systems – Q & A", *International Committee of the Red Cross*, November 12, 2014, https://www.icrc.org/en/document/autonomous-weapon-systems-challenge-human-control-over-use-force.

12 Billy Perrigo, "A Global Arms Race for Killer Robots Is Transforming the Battlefield", *TIME*, April 9, 2018, http://time.com/5230567/killer-robots.

13 "Losing Humanity: The Case Against Killer Robots", *Human Rights Watch*, November 2012, pp. 11-12, http://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf

יד אדם, בין השאר באמצעות התבייתות על אותות מכ"ם.[14] מחקרים עדכניים מצביעים על מגמה, לפיה כלים אוטונומיים לחלוטין עתידים להפוך תוך כשני עשורים לאפשריים מבחינה טכנולוגית. במצב כזה, קיימת סבירות גבוהה לכך שכלים כאלה יהפכו לגורם מרכזי יותר בפעולתם של צבאות מודרניים.[15]

- **לוחמת סייבר:** זהו אחד התחומים המובילים בשימוש בבינה מלאכותית. בתחום זה נמשך השימוש בבינה מלאכותית מ"הדור הראשון",[16] במקביל להתפתחות יכולות גם מדורות מתקדמים יותר. אלגוריתמים מסייעים למנוע תקיפות במסגרת לוחמת סייבר, או לאתר ולהתריע מפני מתקפות על מערכות ממוחשבות שונות. יחד עם זאת, יכולות של בינה מלאכותית עשויות לשמש בדרכים מגוונות גם את הצד התוקף.

מרוץ החימוש בתחום הבינה המלאכותית[17]

מדינות רבות זיהו בשנים האחרונות את הפוטנציאל הטמון בתחום הבינה המלאכותית לכלכלותיהן ולביטחונן הלאומי. **ארצות הברית** נחשבת למובילה בתחום זה ופועלת לגיבוש אסטרטגיה מקיפה בנושא. אסטרטגיית ההגנה הלאומית של ארצות הברית כוללת מחויבות של משרד ההגנה האמריקאי להשקיע ביישומים צבאיים בתחום האוטונומיות, הבינה המלאכותית ולמידת מכונה, לצד שימוש

---

14 Dan Gettinger and Arthur Holland Michel, "Loitering Munitions", *The Center for the Study of the Drone at Bard College*, 2017, http://dronecenter.bard.edu/files/2017/02/CSD-Loitering-Munitions.pdf

15 יואב זקס ולירן ענתבי (עורכים), **השימוש בכלים צבאיים בלתי מאוישים עד שנת 2033: המלצות למדיניות לאומית על בסיס חיזוי טכנולוגי – הערכת מומחים**, מזכר 145, המכון למחקרי ביטחון לאומי, דצמבר 2014, http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/memo145_7%20%20%D7%A1%D7%95%D7%A4%D7%99%20%D7%9C%D7%90%D7%AA%D7%A8%20.pdf ; Paul Scharre, "Robotics on the Battlefield Part I: Range, Persistence and Daring", *Center for a New American Security*, May 2014, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_RoboticsOnTheBattlefield_Scharre.pdf?mtime=20160906081925; Launchbury, "A DARPA Perspective on Artificial Intelligence".

16 John Launchbury, "A DARPA Perspective on Artificial Intelligence," *TechnicaCuriosa*, 2017, https://machinelea

17 נכון למועד כתיבת שורות אלו מתקיים מעין "מרוץ" בין המעצמות לפיתוח יכולות בינה מלאכותית מתקדמות. במקביל לכך יש הקוראים להפחית את השימוש במונח "מרוץ חימוש", שהוא בעל הקשר שלילי, בטענה כי יש לדבר על שילוב בין תחרות ובין שיתוף פעולה. הם גם קוראים לארצות הברית ולסין לפתוח בדיאלוג שיוביל לשיתוף פעולה בפיתוח בינה מלאכותית. להרחבה בנושא זה ראו: Tim Hwang and Alex Pascal, "Artificial Intelligence Isn't an Arms Race", *Foreign Policy*, December 11, 2019, https://foreignpolicy.com/2019/12/11/artificial-intelligence-ai-not-arms-race-china-united-states/.

בטכנולוגיות מסחריות פורצות דרך, וזאת במטרה לשמר את היתרון התחרותי הצבאי של ארצות הברית.[18]

בתחילת 2019 עדכן הבית הלבן את האסטרטגיה הלאומית למחקר ופיתוח של טכנולוגיות בינה מלאכותית, שפורסמה על ידי ממשל אובמה ב־2016. האסטרטגיה המעודכנת קוראת, בין היתר, לפתח שיטות אפקטיביות לשיתוף פעולה אדם–בינה מלאכותית ולהבטיח את השמירה על אבטחתן של מערכות בינה מלאכותית.[19] ארצות הברית משקיעה תקציבים גדולים בתחום זה ופועלת לשרטט אסטרטגיה רחבה לקידום ולהגנה על טכנולוגיית בינה מלאכותית ברמה הלאומית, תוך שיתוף פעולה בין הממשל, המגזר הפרטי, האקדמיה, הציבור ושותפויות בין־לאומיות.[20]

ביולי 2019 קרא "המרכז המשותף לבינה מלאכותית" של הפנטגון (Joint Artificial Intelligence Center – JAIC) לחברות להגיש רעיונות והצעות בטכנולוגיות של בינה מלאכותית לצורך הגנה בסייבר, שיכללו תיקון אוטומטי של חולשות אבטחה ברשתות צבאיות, איסוף מודיעין סייבר על פעילים ב"רשת האפלה" ועוד.[21] למרות מכלול מאמציה, ארצות הברית עדיין ניצבת בפני מספר אתגרים בתחום הבינה המלאכותית. בין הבולטים שבהם הַתחרות הגוברת עם סין, לאור השאיפה הסינית להפוך בתוך כעשור למובילת התחום.

סין מהווה, כאמור, מתחרה רצינית בתחום הבינה המלאכותית וכבר הוכיחה בעבר את יכולתה לקדם במהירות פרויקטים טכנולוגיים מתקדמים (לדוגמה, הפיכתה ליצרנית ויצואנית בולטת של מל"טים תוך עשור אחד בלבד). ההשקעה התקציבית הכוללת של סין במחקר ופיתוח של בינה מלאכותית אינה חשופה לציבור, אך לפי ההערכות היא מגיעה למיליארדי דולרים לכל הפחות. לפי חלק מההערכות, מדובר בהשקעות עתידיות בסך של 150 מיליארד דולר.[22] הדבר נובע, בין היתר, מאחד היתרונות הבולטים של סין בתחום זה, והוא היעדר כמעט מוחלט של גבולות או חסמים בין תחומים "אזרחיים" ל"ביטחוניים", בשל העובדה שבסין גם התחום האזרחי נתון לפיקוח הדוק של השלטון.

יתרון בולט נוסף של סין נובע מהעובדה שהיא אינה פועלת על פי ערכים מערביים, המעודדים דמוקרטיה, זכויות פרט ושמירה על הפרטיות, ולכן כבר שנים

18 James N. Mattis, "Summary of 2018 National Defense Strategy of The United States of America", *Department of Defense*, Washington, D.C., 2018, p. 5.

19 Aaron Boyd, "White House Updates National Artificial Intelligence Strategy", *Defense One*, June 22, 2019, http://bit.ly/2ZYY2U4.

20 "Artificial Intelligence for the American People", *The White House*, 2019, https://www.whitehouse.gov/ai/executive-order-ai.

21 "DoD's JAIC to Call for Private Sector Cyber Tech Pitches", *MeriTalk*, July 8, 2019, https://www.meritalk.com/articles/dods-jaic-to-call-for-private-sector-cyber-tech-pitches/.

22 Ibid.

רבות היא אוספת ומקודדת מידע על אזרחיה. תהליך זה הפך את סין למכרה עצום של נתוני עתק, ומוביל גורמים וחברות ברחבי העולם לעבוד יחד איתה כדי לקבל גישה אליהם. יש לציין כי הסינים אוספים מידע גם על אזרחים של מדינות אחרות באמצעות ביצוע תקיפות סייבר וגניבת מאגרי מידע עצומים, וזאת במקביל לניטור מידע ממערכות ויישומים מתוצרת סין המצויים בשימוש בקרב אזרחים במדינות רבות. כמו כן, החקיקה הסינית מאפשרת לגורמי הממשל הסיני להגיע לפסי הייצור של כלל היצרנים בסין ולהחדיר לתוכם "דלתות אחוריות" במידת הצורך. אותה חקיקה גם מחייבת את יצרני הטכנולוגיה הסיניים לתת לממשל הסיני את קוד המקור של הטכנולוגיה שלהם.[23]

יש הערכות, לפיהן סין תעקוף בעתיד את ארצות הברית בתחום הבינה המלאכותית ותהיה המדינה הדומיננטית בעולם בתחום זה. בנובמבר 2017 העריך אריק שמידט, אז יושב ראש חברת "גוגל", כי סין צפויה להשתוות כבר בשנת 2020 לארצות הברית ביכולות הבינה המלאכותית שלה, וכי בשנת 2025 היא אף צפויה לעקוף אותה בתחום זה.[24] הערכות עדכניות תומכות בהערכותיו של שמידט. נראה כי מספר המחקרים האקדמיים בנושא הבינה המלאכותית שמפורסמים על ידי חוקרים סינים ישתווה בשנת 2020 למספר המחקרים המפורסמים על ידי חוקרים אמריקאים.[25]

בנוסף לסין ולארצות הברית, גם **רוסיה** מנהלת תוכניות בתחום הבינה המלאכותית, ובשנת 2019 אף נוסחה בה אסטרטגיה לאומית לבינה מלאכותית.[26] יחד עם זאת, רוסיה מצויה בפיגור ביחס לארצות הברית ולסין: מלבד השקעה נמוכה בתחום זה יחסית למתחרותיה העיקריות, היא גם סובלת מבעיות שקשורות ל"אקוסיסטם" הטכנולוגי שלה.[27] על רקע זה יש הערכות לפיהן רוסיה תוכל להוביל רק בתחומים צרים וממוקדים של בינה מלאכותית, ולא את התחום כולו.[28]

---

23 המחברות מודות לד"ר הראל מנשרי, ראש תחום סייבר במכון הטכנולוגי חולון, על הערותיו המועילות בנושא זה.

24 Sam Shead, "Eric Schmidt on AI: 'Trust me, these Chinese People are Good'", *Business Insider*, November 1, 2017, https://www.businessinsider.com/eric-schmidt-on-artificial-intelligence-china-2017-11.

25 Tom Simontie, "China is Catching up to the US in AI Research – FAST", *Wired*, March 13, 2019, https://www.wired.com/story/china-catching-up-us-in-ai-research/.

26 Samuel Bendett, "Putin Orders Up a National AI Strategy", *Defense One*, 2019, https://www.defenseone.com/technology/2019/01/putin-orders-national-ai-strategy/154555/.

27 Ibid.

28 Andrew P. Hunter et al., "Artificial Intelligence and National Security: The Importance of an AI Ecosystem", *CSIS*, Washington, D.C., 2018, p. 48, https://www.csis.org/analysis/artificial-intelligence-and-national-security-importance-ai-ecosystem.

בין המדינות הרבות המתחרות בתחום הבינה המלאכותית ניתן למנות גם את **ישראל**, הנחשבת למובילה טכנולוגית עולמית, במיוחד בתחומי סייבר וכלי טיס בלתי מאוישים. כיום אין לישראל אסטרטגיה סדורה לנושא הבינה המלאכותית, אם כי ועדה מטעם ראש הממשלה פועלת בימים אלה לביצוע מחקר מקיף בתחום, שעל בסיס מסקנותיו והמלצותיו ינוסחו אסטרטגיה ומדיניות ועשוי לקום מטה לבינה מלאכותית.[29] יתרונה המשמעותי של ישראל הוא ה"אקוסיסטם" הייחודי שלה, הכולל קשרים בין הממשלה, האקדמיה, התעשייה והצבא, וכן היכולת להגיב במהירות לשינויים בזירה. לכך מתווסף היתרון של מעבר ידע משמעותי בין הצבא ובין התעשיה וחברות אזרחיות, הנובע מהמודל הייחודי של גיוס חובה ושירות מילואים. מודל זה יוצר אצל חלק מהעובדים הזדמנות לרכוש ידע ולהעביר ידע בין מערכת הביטחון ובין התעשייה, באופן מתמשך ומַפרה.[30]

בישראל פועלות חברות רבות העוסקות בתחום הבינה המלאכותית. בחלקן מהווה התחום את ליבת החברה ובחלקן הוא מהווה מכפיל כוח או טכנולוגיה מאפשרת. לצד זה, הוקמו בישראל מרכזי פיתוח של חברות בין־לאומיות גדולות, כמו "אמזון", "אינטל", "מייקרוסופט" ו"אנבידיה", השמים דגש על בינה מלאכותית.[31] כמו כן, קיימות בישראל חברות מובילות בתחום הבינה המלאכותית המפתחות לא רק תוכנה אלא גם חומרה.[32] בתחום הביטחוני מפתחת ישראל בינה מלאכותית במסגרת משרד הביטחון, מפא"ת ויחידות טכנולוגיות שונות בצבא, וכן בתעשיות הביטחוניות.

מרוץ החימוש הבין־לאומי בתחום הבינה המלאכותית, הפיכתן של מערכות אלו לשכיחות, וההסתמכות עליהן בתחומי חיים רבים, מחייבים דיון באיומים עליהן ובדרכים האפשריות לאתר, לזהות, למנוע או לסכל אותם.

מתקפות סייבר ומניפולציות על מערכות בינה מלאכותית

איום הסייבר, ההולך וגובר בשנים האחרונות, מהווה איום גם על מערכות בינה מלאכותית. במקביל הוא מעלה חשש מניצול טכנולוגיות בינה מלאכותית גם לצורך הוצאה לפועל של מתקפות סייבר בקנה מידה הרסני הרבה יותר מזה שמוכר

29 "ועדת המדע: דיון ראשון על מוכנות הממשלה לתחום הבינה המלאכותית", *כנסת ישראל*, 2018, https://m.knesset.gov.il/News/PressReleases/pages/press04.06.18ec.aspx.

30 דפנה גץ ואחרים, **בינה מלאכותית, מדעי הנתונים ורובוטיקה חכמה**, דו"ח ראשון, מוסד שמואל נאמן למחקר מדיניות לאומית, 2018.

31 Amir Mizroch, "In Israel, A Stand Out Year for Artificial Intelligence Technologies", *Forbes*, March 11, 2019, https://www.forbes.com/sites/startupnationcentral/2019/03/11/in-israel-a-stand-out-year-for-artificial-intelligence-technologies/#13acbc7530a8.

32 כדוגמאות ניתן להביא את החברות הישראליות "מלאנוקס" ו"הבאנה לאבס", שנמכרו לחברות בין־לאומיות במיליארדי דולרים. לקריאה נוספת בעניין זה ראו: https://www.themarker.com/technation/.premium-1.8285726.

לנו עד כה. הסיכון גדל עוד יותר כשמדובר בפגיעה במערכות ביטחוניות שאינן מנותקות לגמרי מהרשת, וכן לאור השימוש ההולך וגובר של צבאות בטכנולוגיית בינה מלאכותית.

טכנולוגיית הבינה המלאכותית נחשבת כיום לחלק בלתי נפרד מהאפשרויות לביצוע תקיפות סייבר. יחד עם זאת, בינה מלאכותית יכולה להיות כלי להתמודדות יעילה יותר עם תקיפות סייבר, למשל באמצעות שימוש בטכניקות למידה עמוקה (Deep Learning) שמסוגלות לעקוב אחר פעילות חשודה ולסווג וירוסים שונים. מנגד, מערכות הבינה המלאכותית רגישות למתקפות סייבר עליהן ועלולות להיות נתונות למניפולציות שונות. מערכות אוטונומיות ומערכות בינה מלאכותית הן מערכות מחשוב, ולכן הן חשופות, כמו מערכות אחרות, למתקפות סייבר מן הסוגים המוכרים לנו ממערכות מחשוב רגילות. יחד עם זאת, בגלל אופיין המיוחד, המערכות האוטונומיות ומערכות הבינה המלאכותית חשופות גם למתקפות ייחודיות, בין היתר מהסיבות הבאות:

- הרצון לאפשר את פעולתן האוטונומית, ללא מעורבות אדם, משיקולים של יעילות, דיוק ומהירות, עשוי להשאיר אותן חשופות למתקפות. עם זאת, אפשר להעריך כי גם מערכות אלו יתנו חיווי למפעילים על אנומליות או זיהוי תקיפה.
- חלק מן המערכות המבוססות על בינה מלאכותית פועלות כיום באופן שאיננו יודעים להסביר או לנתח בדיעבד. הדבר מכונה אתגר ה"הסבריות" (explainability) או אתגר "הקופסה השחורה". הדבר משאיר פתח למתקפות שיהיה קשה לזהותן לפחות בחלק מהמקרים, מכיוון שמדובר במתקפה ולא בתהליך שהמערכת ביצעה באופן תקין.
- תהליכי ה"אימון" של מערכות בינה מלאכותית, המתבצעים על כמויות גדולות מאוד של מידע, משאירים פתח להכנסת מידע ש"יזהם" את התהליך באופן מכוון ויוביל לתוצאות מוטות או בלתי רצויות.

מספר דוגמאות מהעת האחרונה ממחישות את האיום: באפריל 2019 אמר ראש אגף המבצעים ב"מרכז המשותף לבינה מלאכותית" במשרד ההגנה האמריקאי, קולונל סטוני טרנט (Trent), כי הבעיות בהערכת איומי הסייבר נגד טכנולוגיות של בינה מלאכותית נובעות מחוסר מודעות בקרב מקבלי ההחלטות וממחסור בכלים ובשיטות לבדיקת חסינות הסייבר של מערכות בינה מלאכותית. לדבריו, אחד מתפקידיו של המרכז הוא לעודד פיתוח של כלים כאלה, שפיתוחם אינו נחשב לכדאי בענף המסחרי האזרחי.[33]

33 Theresa Hitchens, "Rush to Military AI Raises Cyber Threats", *Breaking Defense*, April 25, 2019, https://breakingdefense.com/2019/04/rush-to-military-ai-raises-cyber-threats/.

לדברי מי שהיה ראש אגף המחקר ב"סוכנות לביטחון לאומי" (NSA), פרדריק צ'אנג (Chang), המרוץ לפיתוח טכנולוגיות צבאיות המבוססות על בינה מלאכותית יגדיל משמעותית את מרחב התקיפה, אולם ממשלות עדיין אינן מודעות למרבית חולשותיהן של המערכות הללו. צ'אנג הזהיר שתוקפים עלולים להטעות את מנגנון הזיהוי של המערכת באמצעות "תשומות נגד" (Adversarial Inputs), "להרעיל" את המידע המשמש ללימוד המערכת (Data Poisoning) ולהסתנן לתוכה במטרה להבין את מערכת ההפעלה שלה ולפגוע בפעילותה.[34]

בנוסף, השילוב בין אמצעי לוחמת סייבר ובין טכנולוגיית בינה מלאכותית עלול להוביל לפיתוח סוגים חדשים של נוזקות. לדוגמה, חוקרים בחברת IBM פיתחו נוזקה מבוססת בינה מלאכותית בשם DeepLocker, במטרה להבין כיצד ניתן לשלב מספר מודלים קיימים של בינה מלאכותית כדי ליצור סוג חדש ויעיל יותר של נוזקה שטרם נראה. הנוזקה החדשה מסווה את מטרתה עד שהיא מגיעה אל היעד, אותו היא מזהה באמצעים כגון זיהוי קול או זיהוי פנים. נוזקות מסוג זה נחשבות ליעילות במיוחד, שכן הן מסוגלות להדביק מיליוני מערכות מבלי להתגלות, וזאת בניגוד לתקיפות סייבר, שלעיתים עשויות להיות רחבות היקף ו"רועשות" ("spray and pray" approach).

מכיוון שמערכות אוטונומיות אמורות לפעול ללא מעורבות יד אדם, או במעורבות נמוכה מאוד שלו, מניפולציה או מתקפה יעילה עליהן עלולה לא להתגלות במשך זמן רב. הייחודיות של נוזקה משולבת בינה מלאכותית כמו זו שהוזכרה, לעומת נוזקות קיימות, נעוצה בכך שבשל תחכומן יידרשו מומחיות עמוקה וכלי פורנזיקה מתקדמים כדי לזהותן.

נוזקת DeepLocker שינתה את כללי המשחק בכך שהיא "מחביאה" את פעילותה מאחורי אפליקציות נפוצות, כמו אפליקציות לשיחות וידאו. זאת ועוד, השימוש שהיא עושה בבינה מלאכותית כמעט ואינו מאפשר לזהות אותה ולבצע הנדסה לאחור של הקוד שלה. DeepLocker תתחיל לפעול רק אם תזהה את המטרה שנבחרה, והיא תעשה זאת באמצעות שימוש במודל של "רשת נוירונים עמוקה" (Deep Neural Network). מודל זה תוכנן לפעול רק כאשר הוא יזהה קלט ספציפי, כלומר רק כאשר יזהה את הקורבן המיועד.[35]

דוגמה נוספת לשימוש עוין בטכנולוגיית בינה מלאכותית לצורך תקיפה סייבר הוצגה במחקר שפורסם בשנת 2017, במסגרתו הפעילו חוקרים כלי בינה מלאכותית

34 Ibid.

35 Marc P. Stoecklin, "DeepLocker: How AI Can Power a Stealthy New Breed of Malware", *SecurityIntelligence*, August 8, 2018, https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/.

כדי לזהות סיסמאות של משתמשי הרשת החברתית "לינקדאין". סקירה של 43 מיליון פרופילים של משתמשים אפשרה לחוקרים לזהות 27 אחוזים מהסיסמאות.[36]

חוקרים מעריכים כי מערכות הבינה המלאכותית יאפשרו לבני האדם לבצע מתקפות שלא ניתן היה לבצע לפני השימוש במערכות מסוג זה. בנוסף, תוקפים יוכלו לאתר מקורות חדשים למתקפות על מערכות בינה מלאכותית על ידי מציאת נקודות תורפה חדשות בהן. תרחיש נוסף הוא תקיפה של מערכות שאחראיות על מספר כלים אוטונומיים. תקיפה כזאת עלולה לגרום לשיבוש נרחב, שישפיע על יותר מאשר כלי אחד.[37]

אפשר להצביע על שלושה סוגים עיקריים של תקיפות על מערכות בינה מלאכותית: (1) הכנסת מידע שגוי למערכת, כך שתסיק מסקנות שגויות; (2) שיבושים זעירים בתמונות (או קלטים אחרים) שהמערכת מעבדת, באמצעות הכנסת פריטים גלויים או שיבוש בלתי נראה בפיקסלים של התמונה, כך שהיא תסווג את התוצרים באופן שגוי; (3) שיבוש בשיפוט מידע באמצעות חבלה פנימית באמצעי המיון של המערכת, וזאת במקום התמקדות במידע בודד שמוזן למערכת.[38]

להלן פירוט של כמה מסוגי המתקפות הייחודיות למערכות בינה מלאכותית:

- **מניפולציה במידע המוצג למערכות הבינה המלאכותית (Adversarial Attacks)**: זוהי טכניקה להטעיית מערכות בינה מלאכותית (machine learning classifier) באמצעות ניצול רגישותן למניפולציה במידע המוזן להן ומשמש לאימון המערכת. בדרך זו יכולים התוקפים לייצר קֶלֶט הנראה כבעל סיווג מטעה, וכן "הפרעות" למידע המוזן למערכת, כדי לגרום לסיווג שגוי. השינויים כמעט ואינם נראים בעין אנושית. אחד המחקרים מצא כי ניתן "לשַטוֹת" בקלות רבה ב"רשתות נוירונים עמוקות" באמצעות הכנסת קֶלֶט שגוי.[39]
- **"הרעלת מידע" (Data Poisoning)**: מדובר בטכניקה שבה התוקף מכניס נתונים שגויים ומשבש באופן שיטתי את המידע המוזן לצורך אימון המערכת. לשם כך,

36 Matthew Hutson, "Artificial Intelligence Just Made Guessing Your Password a Whole Lot Easier", *Science*, September 15, 2017, https://www.sciencemag.org/news/2017/09/artificial-intelligence-just-made-guessing-your-password-whole-lot-easier.

37 Allan Dafoe, "AI Governance: A Research Agenda", *Future of Humanity Institute*, University of Oxford, 2017, p. 5, https://doi.org/10.1176/ajp.134.8.aj1348938 ; Miles Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation", 2018, p. 20, https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217.

38 Jian hua Li, "Cyber Security Meets Artificial Intelligence: A Survey", *Frontiers of Information Technology and Electronic Engineering* 19, no. 12 (2018): 1462-1474, https://doi.org/10.1631/FITEE.1800573.

39 Mesut Ozdag, "Adversarial Attacks and Defenses against Deep Neural Networks: A Survey", *Procedia Computer Science*, 140 (2018): 152-161, https://doi.org/10.1016/j.procs.2018.10.315.

צריך שתהיה לתוקף גישה למידע המשמש לאימון המודל. שיבוש המידע עלול להיטיב עם התוקפים או להפלות קבוצות אחרות – למשל מודלים המחשבים פרמיות ביטוח או הענקת הלוואות.[40]

- **מתקפות להתחמקות מגילוי (Evasion attacks)**: אלו מתקפות שבהן מבצע התוקף מניפולציה על יכולת הסיווג של מודלים במטרה להתחמק מזיהוי. מתקפות כאלו נועדות לעקוף מודלים המשמשים כמסַנני ספאם, כמזַהֵי קודים זדוניים או כמנטרֵי תעבורת רשת ומגלֵי אנומליות.[41]
- **גניבה והעתקה של מודל ה־AI (Model Extraction)**: אלו הן מתקפות שבהן התוקף שולח דוגמאות של נתונים למודל המערכת ומנתח את הפֶלֶט במטרה לבנות מודל משל עצמו.[42]
- **מתקפות על תיוגי Watermarks**: Watermarks הוא מושג המתייחס למתקפות שבהן התוקף מוסיף פיקסלים מיוחדים לתמונה במטרה לגרום למודל להגיב באופן מסוים.[43] מתקפה אפקטיבית מסוג זה עשויה להיות בעייתית מאוד כאשר מדובר במערכות מודיעיניות או במערכות נשק.

מערכות המבוססות על למידת מכונה מחזיקות לעיתים במידע רגיש שיכול להיות יעד לתקיפות סייבר, כמו מערכות לזיהוי פנים, שהתוקפים יכולים להוציא מהן מידע על האנשים המזוהים במערכת. תקיפות כאלו יכולות להתבצע בשני שלבים שונים של בניית המערכת: בשלב אימון המערכת ובשלב הבחינה והסקת המסקנות מפעילותה. יחד עם זאת, קיימים אמצעי הגנה שונים בתחום זה, שאפשר להכניסם בשני השלבים הללו.[44]

---

40 Jacob Steinhardt, Pang Wei Koh and Percy Liang, "Certified Defenses for Data Poisoning Attacks", *Advances in Neural Information Processing Systems*, no. i (December 2017): 3518-3530 ; Patrick Hall, "Proposals for Model Vulnerability and Security", *O'Reilly Media*, 2019, https://www.oreilly.com/ideas/proposals-for-model-vulnerability-and-security.

41 Battista Biggio et al., "Evasion Attacks against Machine Learning at Test Time", *Lecture Notes in Computer Science*, Part 3 (2013): 387-402, https://doi.org/10.1007/978-3-642-40994-3_25 ; Erwin Quiring and Konrad Rieck, "Adversarial Machine Learning against Digital Watermarking", *European Signal Processing Conference* (September 2018): 519-523, https://doi.org/10.23919/EUSIPCO.2018.8553343.

42 Florian Tramèr et al., "Stealing Machine Learning Models via Prediction APIs", *Cornell University*, October 2016, http://arxiv.org/abs/1609.02943.

43 Romain Artru, Alexandre Gouaillard and Touraj Ebrahimi, "Digital Watermarking of video streams: Review of the State-Of-The-Art", *arXiv preprint arXiv:1908.02039*, August 2019.

44 Qiang Liu et al., "A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View", *IEEE Access* Vol. 6 (2018): 12103-12117, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8290925.

אפשר לבצע התקפות של "הרעלת מידע" בשלב האימון, שיכללו הכנסת מידע שגוי למערכת ושינוי תוויות המידע. הדרך להגן על המידע בשלב זה היא באמצעות פיתוח אמצעים שיסננו מידע שגוי הנכנס למערכת (data sanitization), שימוש בתרחישים כדי ללמוד על פעולותיו הצפויות של היריב (adversarial training), זיקוק אמצעי הגנה (defense distillation), שילוב שיטות (ensemble methods) וחיזוק הפרטיות באמצעים שונים (differential privacy).

בשלב הבחינה אפשר לבצע סוגים שונים של התקפות, ביניהם התקפות להתחמקות מגילוי (evasion) על ידי שימוש באמצעי תקיפה שמסוגל לחמוק מאמצעי הזיהוי של המערכת. שיטה נוספת לתקיפה היא התחזות (Impersonation), המאפשרת לגורמים עוינים להתחזות לגורמים לגיטימיים כדי להיכנס למערכת ולשבש את המידע. שיטה שלישית לתקיפה היא היפוך (inversion). שיטה זו מאפשרת לגנוב מידע רגיש מתוך המערכת. בתקיפות כאלו ניתן להגן על המערכת באמצעות שימוש ברעש כ"מסך עשן" להגנה על מידע, או שימוש רנדומלי באמצעי הגנה במהלך האימון (differential privacy).[45]

כפי שניתן לראות, קיים מגוון רחב של מתקפות אפשריות על מערכות אוטונומיות ומערכות בינה מלאכותית, שחלקן ייחודיות לסוג זה של מערכות ושונות ממתקפות על מערכות מחשוב "רגילות". יש צורך להבחין בין המתקפות הרלוונטיות למערכות ממוחשבות באופן כללי ובין מתקפות בעלות ייחודיות לתחום הבינה המלאכותית והמערכות האוטונומיות, כפי שביקשנו להבהיר במאמר זה.

הסיכון במתקפות על מערכות בינה מלאכותית עולה מאוד, משום שלעיתים קרובות אין אדם שיוכל לזהות את הבעייתיות שנוצרה תוך פרק זמן קצר או סביר, וזאת עקב מאפייני המערכת. לבעיה זו מצטרפת בעיה נוספת שהוזכרה לעיל – אתגר "הקופסה השחורה" או ה"הֶסבריוּת". אתגר זה מתייחס לעובדה שחרף התוצאות המוצלחות של פעולות שונות של מערכות בתחום למידת מכונה או למידה עמוקה, לא ניתן להסביר את הדרך שעשתה המערכת כדי להגיע לתוצאה.[46] היעדר השקיפות מקשה לבצע ביקורת על פעולת מערכות באופן כללי. כאשר מוסיפים לכך את כמויות המידע ואת הקצב שבו המערכות הללו מעבדות אותו, ניתן להבין מדוע גם פיקוח אנושי שיוצב עליהן עשוי להיות למראית עין בלבד. מומחים ואנשי צבא טוענים כי על בני אדם להיחשב אחראים (accountable) לפעולותיהן של מערכות הבינה המלאכותית, אולם זוהי טענה שמחייבת דיונים

45 Ibid.

46 Richard Gall, "Machine Learning Explainability vs Interpretability: Two Concepts That Could Help Restore Trust in AI", *KDnuggets*, 2018, https://www.kdnuggets.com/2018/12/machine-learning-explainability-interpretability-ai.html.

נוספים, מכיוון שבני אדם אינם יכולים לאתר ולזהות את כל הסיכונים והפגיעויות הקיימים במערכות אלו.[47]

כדי ליצור פיקוח אפקטיבי ויכולת התמודדות עם הבעיות, יש צורך בהשקעת מאמצים ותשומת לב לנושא זה כבר בשלב המחקר והפיתוח של המערכות, וזאת כדי לנסות ולגבש מנגנונים אפקטיביים לבקרה אנושית עליהן. מאמצים לפתור את אתגר ה"הֶסבריות" נעשים מזה זמן,[48] אולם עד שיושג פתרון טכנולוגי מספק בתחום זה, יש צורך במנגנונים אחרים להתמודדות עם היעדר השקיפות, כולל מתחומי הרגולציה או המשפט. הדבר חשוב בעיקר כאשר מדובר במערכות אסטרטגיות, או בכאלו שתוצאות פעולותיהן עשויות לפגוע בחיי אדם.

סיכום והמלצות

השימוש במערכות מתחום הבינה המלאכותית, ובכלל זה במערכות מבוססות למידת מכונה ולמידה עמוקה, הולך והופך לנפוץ יותר ויותר במגוון תחומי חיים, ובתוכם התחום הביטחוני. מערכות אלו פועלות בקצב מהיר ובאופנים שלעיתים קרובות מקשים על בקרה אנושית עליהן. קושי זה מצטרף לשאיפה לאפשר למערכות אלו לפעול באוטונומיות מלאה כדי לחסוך במעורבות אנושית, וזאת ממגוון סיבות. במצב זה חשוב להבין מהן המתקפות האפשריות על מערכות אלו ולפתח אמצעי שיבוש שעשויים לפעול עליהן. כמו כן, חשוב להגיע להבנה של המתקפות הייחודיות למערכות מסוג זה, כדי שניתן יהיה לפתח מנגנוני פיקוח והגנה אפקטיביים שיאפשרו את פעולתן התקינה של אותן מערכות ואת האמון בהן. כדי להשיג את כל אלה, ניתן לפעול במספר אפיקי מדיניות.

ישראל, שהיא מעצמה בתחום הסייבר ואחת המדינות המובילות בעולם בתחום הבינה המלאכותית,[49] היא בעלת פוטנציאל גדול להפוך לגורם מוביל בתחום מחקר הסייבר והגנת הסייבר גם בכל מה שקשור לבינה מלאכותית ולמערכות אוטונומיות. לאור זאת, להלן מספר המלצות למדיניות עבור ישראל (שעשויות להיות רלוונטיות גם עבור מדינות נוספות):

---

47 Connor McLemore and Charles Clark, "The Devil You Know: Trust in Military Applications of Artificial Intelligence", *War on the Rocks*, September 23, 2019, https://warontherocks.com/2019/09/the-devil-you-know-trust-in-military-applications-of-artificial-intelligence/.

48 Zelros AI, "A Brief History of Machine Learning Models Explainability", *Medium*, 2018, https://medium.com/@Zelros/a-brief-history-of-machine-learning-models-explainability-f1c3301be9dc.

49 אורי ברקוביץ, "השקעה של 2 מיליארד ש' בשנה בעיר חכמה, בחקלאות ובאקדמיה: כך מתכננת ישראל להפוך למעצמת בינה מלאכותית", **גלובס**, 18 בנובמבר 2019, https://www.globes.co.il/news/article.aspx?did=1001307714.

- יש להגדיר תקנים בתחום המערכות המבוססות על בינה מלאכותית. במסגרת זו יש להטמיע במערכות אלו אמצעים שיאפשרו לפקח עליהן, או לוודא שלא בוצעו בהן תקיפה או מניפולציה. התקנים שיוגדרו צריכים לחול לא רק על מערכות ביטחוניות, אלא גם על מערכות אזרחיות קריטיות (ורצוי שגם על מערכות שאינן קריטיות, אך מסייעות בשמירה על שגרה). כמו כן, יש צורך בתקצוב לאומי של הגנת מערכות בתחומים שבהם קיים כשל שוק ואין תמריץ מספיק שפותר את העניין.
- על הגורמים הרלוונטיים במערכת הביטחון להשקיע במחקר שיאפשר מיפוי ואיתור מתמשך של התחומים שבהם ייתכנו פגיעויות ומתקפות ייחודיות במערכות אוטונומיות. כמו כן, יש להשקיע בפיתוח של פתרונות ייעודיים בתחום זה.
- על הגופים הרלוונטיים במדינה להגדיר נהלים להשגחה על מִבצעי סייבר מבוססי בינה מלאכותית, כדי להימנע מהשלכות בלתי רצויות של מבצעים כאלה. הנהלים שיוגדרו צריכים להיות מגובים באמצעי אכיפה אפקטיביים.[50]
- רצוי לקיים תרגילים משותפים של בעלות ברית, בהם יִבחנו את יכולות ההגנה של הבינה המלאכותית. התרגילים יחשפו חולשות שיש לתקן ויעניקו למערכות את המידע שהן זקוקות לו כדי ללמוד ממנו.
- יש להרחיב את הדיון הבין־לאומי בנושא במטרה ליצור שיתופי פעולה בין מדינות בעלות עוצמה בתחום הבינה המלאכותית ובעלות אינטרסים משותפים (Like Minded Nations). זאת כדי לנסות ולהשפיע על הזירה הבין־לאומית כולה, לאור העובדה שקשה להשיג הישגים מהירים במוסדות בין־לאומיים כמו האו"ם. כן יש לגבש אמנות בין־לאומיות בתחום זה. חשיבותו של הנושא מתחדדת עוד יותר כאשר לוקחים בחשבון את השונות התרבותית הקיימת בין מדינות ואת השפעתה האפשרית הן על עיצוב הבינה המלאכותית במדינות שונות והן על הגדרת המושג "מוסרי" בקבלת החלטות בתחום זה.

יישום המלצות מדיניות אלו, ונוספות שניתן לגבש לאור הכרת הבעיה, עשוי לסייע במניעה של מתקפות בעלות פוטנציאל פגיעה. פוטנציאל זה הולך וגדל ככל שמערכות מבוססות בינה מלאכותית הופכות לנפוצות יותר ולאחראיות לתפקודים קריטיים שונים. טיפול בנושא מבעוד מועד עשוי לסייע במניעת תוצאות הרסניות ברמות הלאומית והבין־לאומית.

---

50 Mariarosaria Taddeo and Luciano Floridi, "Regulate Artificial Intelligence to Avert Cyber Arms Race", *Nature*, 556, no. 7701 (April 16, 2018): 296-298, https://doi.org/10.1038/d41586-018-04602-6.

קולוניזציה של הסייבר: החיבור המסוכן בין בינה מלאכותית למשטרים אוטוריטריים

מתיו קרוסטון

קידום ופיתוח של תשתיות בינה מלאכותית הם מהלכים רצויים ומבורכים בזכות הפוטנציאל שיש בהם לפתיחת הדלתות בפני עולם חדש ומופלא של יכולות סייבר חיוביות. אולם, לפוטנציאל זה יש גם צד אפל, ההולך ומתפתח בימים אלה. מדינות כמו סין משווקות באגרסיביות טכנולוגיות בינה מלאכותית מתקדמות למדינות בכל רחבי העולם, ובמיוחד לבעלות בריתה במזרח התיכון ובצפון אפריקה, באפריקה שמדרום לסהרה ובאמריקה הלטינית. לא מדובר רק ברצון של סין להיות שותפה פעילה בכלכלה העולמית או לסייע בפיתוח תשתיות הסייבר של מדינות מתפתחות; סין גם מפיצה את הטכנולוגיות שלה בתחומי הצנזורה, הדיסאינפורמציה ועיצוב דעת הקהל – טכנולוגיות שיודעות לספק הגנה למשטרים ולפגוע באקטיביזם הדמוקרטי של ההמונים. במקום לראות בכוח הסייבר הזדמנות לעידן חדש של פתיחות וחילופי מידע, סין רואה את כוחו האמיתי ביכולתו לשמש כלי לשמירה על הביטחון הלאומי ועל אינטרסים פוליטיים בזירה הפנימית. מעניינים במיוחד המחקרים הרבים שחוזים כי סין תדביק את ארצות הברית בתחום הבינה המלאכותית, ולאחר מכן אף תעקוף אותה כמדינה המובילה בעולם בתחום זה, דבר הצפוי לקרות עד שנת 2030. השאלה היא אם פירוש הדבר הוא שינוי הפרדיגמה של פוטנציאל הבינה המלאכותית - מסייבר משכין שלום לסייבר קולוניאליסטי.

מילות מפתח: ביטחון סייבר, סין, העברת טכנולוגיות, גיאו־פוליטיקה, בינה מלאכותית, פיקוח ומעקב

מתיו קרוסטון הוא עמית מחקר בתוכנית לביטחון סייבר במכון למחקרי ביטחון לאומי וסגן יו"ר של ModernDiplomacy.eu. הוא מחזיק בתארים מאוניברסיטת בראון (PhD), הקולג' האוניברסיטאי של לונדון (MA) ואוניברסיטת קולגייט (BA).

מבוא

קידום ופיתוח של תשתיות בינה מלאכותית הם מהלכים רצויים ומבורכים בזכות הפוטנציאל שיש בהם לפתיחת הדלתות בפני עולם חדש ומופלא של יכולות סייבר חיוביות. עם זאת, לפוטנציאל זה יש, ללא ספק, גם צד אפל, ההולך ומתרקם בימים אלה. מדינות כמו סין משווקות באגרסיביות טכנולוגיות בינה מלאכותית מתקדמות למדינות בכל רחבי העולם, ובמיוחד לבעלות בריתה באזור המזרח התיכון וצפון אפריקה, באפריקה שמדרום לסהרה ובאמריקה הלטינית. לא מדובר רק ברצון של סין להיות שותפה בכלכלה העולמית או לסייע בפיתוח תשתיות הסייבר של מדינות מתפתחות; מדינות כמו ארצות הברית חוששות כי להעברת הטכנולוגיות הסיניות יש גם היבט אסטרטגי: האם המדינות שיקבלו אותן יאמצו לא רק את השיפורים הטכנולוגיים, אלא גם את הגישה הסינית לשליטה על הזירה פנימית, העושה שימוש בטכנולוגיות של צנזורה, דיסאינפורמציה ועיצוב דעת הקהל כדי להגן על המשטר ולערער אקטיביזם דמוקרטי המגיע מקרב ההמונים? האם ייתכן שסין יוצרת למעשה עתיד של אוטוריטריות טכנולוגית כמודל מתחרה לדמוקרטיה?

במקום לראות בכוח הסייבר, על כל ההתפתחויות החיוביות והמגוונות שעברו עליו, פֶּתח לעידן חדש של פתיחות וחילופי מידע, סין נוטה למקסם את הכוח האסטרטגי־דיפלומטי הנסתר של הסייבר ככלי לשמירה על הביטחון הלאומי ועל האינטרסים הביטחוניים והפוליטיים שלה. מרשימה במיוחד (או אולי מטרידה) העובדה שרבים חוזים שסין צפויה להדביק את ארצות הברית בתחום הבינה המלאכותית, ואף להשיג אותה עד שנת 2030 ולהפוך למובילה העולמית בתחום זה. האם יש בכך משום סימן מעיד לשינוי הצפוי בפרדיגמה של פוטנציאל הבינה המלאכותית ושל הסייבר באופן כללי – מכוח בונה שלום לכוח קולוניאליסטי?

מאמר זה מבקש לבחון אפשרויות אלו על ידי העמקה בפרויקט המכונה "תוצרת סין 2025" ("Made in China 2025 – MIC"). הפרויקט הושק בשנת 2015 כפרויקט פיתוח כלכלי, שזכה להסכמה רחבה למדי והוצג כנועד לקדם את סין מיצרנית של מוצרים זולים ליצרנית של טכנולוגיה מתקדמת, אלא שעד מהרה הוא הפך לגורם של מחלוקת עולמית ברמות שונות, שביטוייה היו מתיחות דיפלומטית, ביקורת על מדיניות החוץ ושמועות על מלחמת סחר כלכלית. הסיבה לכך היא שסין הדגישה תמיד כי פרויקט "תוצרת סין" הוא בעיקר יוזמה שנועדה לצרכים פנימיים (לגרמניה היה פרויקט דומה שהסינים השתמשו בו כמודל לחיקוי), וכמעט לא התייחסה לכך שבכוונתה לייצא את הטכנולוגיות שלו. במקום זאת היא דיברה על אימוץ ושיפור הטכנולוגיות שתצליח לשים עליהן את ידה באמצעות השקעות, מיזוגים ורכישות, וכן על פיתוחים מקומיים.

המאמר מבקש להתמקד בעקרונותיו של פרויקט "תוצרת סין" באופן שונה מזה שהיה נהוג עד כה. במקום לבחון כיצד הוא הפך לסלע מחלוקת כלכלי בין

ארצות הברית לסין, יעסוק המאמר בפוטנציאל המינוף האסטרטגי והפוליטי של הפרויקט, מתוך הנחה שסין תצליח, בסופו של דבר, לחולל את השינוי שבו היא מעוניינת. אם סין לא תהיה תלויה בארצות הברית לצורך העברת טכנולוגיות, ובמקום זאת תהפוך ליצרנית הגדולה ביותר של טכנולוגיות חדשות, כיצד מצב זה יבוא לידי ביטוי בהתנהלותה מול שאר מדינות העולם, כאשר על הפרק יעמדו השקעות כלכליות והון פוליטי? במילים אחרות, אם פרויקט "תוצרת סין" יצליח, האם הוא יהווה גורם מדרבן נוסף לצמיחתה של סין כמשפיעה עולמית בתחום הטכנולוגיה, בהתאם לסטנדרטים ולנורמות של התנהגותה הפוליטית?

אין זה סוד שארצות הברית הצליחה במשך עשרות שנים לשמור על עליונות בהשפעתה הדיפלומטית, בין היתר בזכות היותה עמוד התווך של הכלכלה העולמית. בעידן של המאה ה־21, שבו פיתוח נקשר ליכולתה של מדינה להפוך את הכלכלה המקומית למתקדמת מבחינה טכנולוגית, השאלה היא אם פרויקט "תוצרת סין" יהפוך את סין למעצמה עולמית "חכמה" טכנולוגית, שתוכל להיות בעלת השפעה ניכרת בתחומי הדיפלומטיה, האסטרטגיה ומדיניות החוץ בדרכים שיהיו מנוגדות לאינטרסים ולערכים האמריקאיים? האם "תוצרת סין" יהיה התמריץ שיהפוך את המשטר הסיני למודל חיקוי למדינות אחרות, תוך התעלמות מהמודל האמריקאי אותו הנהיגה ארצות הברית במשך כמעט מאה שנה? סין אמנם מכחישה באופן רשמי שיש לה מטרה חשאית כזאת, ואף על פי כן יש לשאול את השאלה האם אין זו הדרך שבאמצעותה היא תוכל להגשים, סוף־סוף, את "מודל הפיתוח הסיני" – אותו מודל של קפיטליזם בעל "מאפיינים סיניים", שרבים טענו כי סין מנסה לייצא באופן סמוי לעולם המתפתח; מודל שפירושו, באופן כללי, שלילת הדמוקרטיה הליברלית, החלת מגבלות שמונעות ליברליזציה מלאה של השוק, וריסונים ניכרים המוטלים על חירויות האזרח במדינה.

השלכות אלו הן שעומדות במוקדו של מאמר זה. המאמר שואף להפנות את תשומת הלב לקשר האפשרי בין הצלחתו של פרויקט "תוצרת סין" ובין הצלחתה של סין לתפוס את ההובלה הגלובלית בתחום החדשנות הטכנולוגית – קשר שעד כה סבל מהתעלמות מסוכנת ושגויה. "מלחמת הסחר" המתוקשרת שיזם נשיא ארצות הברית טראמפ אמנם עוררה זרמים תת־קרקעיים של חששות מפני הפיכתה של סין למובילה עולמית בחדשנות טכנולוגית, אך הנטייה של אלה היא להתמקד בשוק הסיני המקומי ולא בהערכת מדיניות החוץ הסינית כלפי אזורים קריטיים ברחבי העולם.

המאמר אינו מתיימר להתמודד עם השאלות הפילוסופיות העמוקות שנובעות ממציאות חדשה זו, אך יש לו רלוונטיות לתזה העיקרית הנוגעת לעתידה של סין כמובילה טכנולוגית עולמית: אם סין אכן תוכיח כי חדשנות, מוטיבציה וגאונות טכנולוגית אינן תלויות בקיומן של חירות דמוקרטית וחירויות אזרח, כפי שחשבנו,

מדוע בעצם שמדינות אוטוריטריות ירצו בקשרים עם ארצות הברית לצורך רכישות טכנולוגיות עתידיות? ואולי חשוב מכך, מדוע שיקשיבו לדמוקרטיות ותיקות שאומרות להן כי קידמה כלכלית יכולה להתרחש רק בדמוקרטיה ובהיצמדות לעקרונות הדמוקרטיים?

"תוצרת סין 2025": מהו הפרויקט ומדוע הוא חשוב?

כשבוחנים לראשונה את החשיבה המקורית שמאחורי פרויקט "תוצרת סין 2025", קשה לכאורה למצוא פגם בתיאוריה הסינית. מבלי להסתבך יתר על המידה בנבכי הפרויקט, נציין רק כי כמה מהיעדים העיקריים שלו היו חיזוק משקלם של המרכיבים המקומיים ברכיבים ובמוצרים הטכנולוגיים הסיניים, וזאת לא רק כדי שסין תוכל לתת מענה לצורכי הטכנולוגיה הפנימיים שלה, אלא גם כדי שתהפוך לשחקנית מרכזית ולמתחרה מובילה בשוקי הטכנולוגיה העולמיים.[1] ספציפית, פרויקט "תוצרת סין" שם לו למטרה לשלוט על ארבעים אחוזים משוק החדשנות הטכנולוגית העולמי עד שנת 2020 ועל שבעים אחוזים ממנו עד שנת 2025, כאשר האידיאל הוא שעד שנת 2049 – יובל המאה לרפובליקה העממית של סין – תושג עליונות סינית גורפת ובת־קיימא בזירת הטכנולוגיה העולמית.

"התוכנית לפיתוח התעשייה 4.0" של גרמניה שימשה השראה לסין בניסיונה להצטרף, בעזרת הפרויקט שלה, לְמה שמכונה "המהפכה התעשייתית הרביעית". הכוונה היא להצליח לשלב היטב מחשוב ענן, נתוני עתק (ביג דאטה) וטכנולוגיות מתפתחות אחרות עם שרשראות אספקה גלובליות. מבחינתה של סין, התעשיות שיושפעו מכך הן רבות: לא רק טכנולוגיות המידע והבינה המלאכותית, שהן בבחינת הברור מאליו, אלא גם רובוטיקה מתקדמת, הנדסת אווירונאוטיקה וחלל, מדע החומרים וביו־רפואה, וזאת בנוסף להשלכות שיהיו לכך על פרויקט העתיד הגדול הנוסף שלה – "יוזמת החגורה והדרך" – ובכלל זה תשתיות מתקדמות והנדסה ימית.[2]

מכיוון שרבים מן היעדים האלה נראים הגיוניים לחלוטין עבור מעצמה החותרת לקיימות ולמינוף מרבי של כוחה, נשאלת השאלה מדוע פרויקט "תוצרת סין" כה שנוי במחלוקת בעיני מדינות אחרות, ובמיוחד בעיניה של ארצות הברית? אחרי הכל, ארצות הברית עצמה מקדמת מעת לעת, מזה חמישים שנה לפחות, קמפיין של "תוצרת אמריקה" ו"קנו תוצרת אמריקאית". המפתח להבנת המחלוקת הוא

1 Dezan Shira & Associates, "What is Made in China 2025 and Why Has it Made the World So Nervous?", *China Briefing,* December 28, 2018, https://www.china-briefing.com/news/made-in-china-2025-explained/.

2 James McBride and Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?", *Council on Foreign Relations*, May 13, 2019, https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

פוליטי הרבה יותר מאשר כלכלי: אם פרויקט "תוצרת סין" ישיג את יעדיו, לא יהיה מדובר אך ורק בחיזוקן של חברות סיניות מקומיות; החשש (בעיקר של ארצות הברית והאיחוד האירופי) נובע מכך שסין אינה שוק ליברלי שמשַחק "על פי הכללים" של סחר חופשי, ולכן חברות סיניות שיהפכו למובילות בעולם יזכו לגיבוי המדינה בצורת סובסידיות, הלוואות נוחות מבנקים הנמצאים בבעלות המדינה וגיבוי פוליטי רב בכל הקשור לתחרות בשוק הסיני המקומי.[3] חשש זה בא לידי ביטוי בצורה הברורה ביותר בהתנהלות הנשיא טראמפ ובמלחמת הסחר שיצר מול סין. טראמפ המחיש כיצד פרויקט "תוצרת סין" הפך לשיטת הסחטנות של ימינו: בתמורה להעברה "כפויה" זו של טכנולוגיות מחברות אמריקאיות לסין, תעניק סין לחברות אמריקאיות גישה רחבה יותר (אם כי עדיין מוגבלת ומרוסנת) לשוק המקומי שלה. מגרש המשחקים הלא מאוזן הופך, אפוא, למציאות: מכיוון שלסין יש שליטה ישירה (או חצי ישירה) על התעשיות המקומיות הגדולות שלה, חברות סיניות פטורות מהדאגות והסיכונים המאפיינים את השוק, ששחקנים חיצוניים אחרים נאלצים להתמודד איתם.

הנקודה החשובה יותר שמאמר זה מבקש להעלות היא שהביקורת המקורית על פרויקט "תוצרת סין" אמנם רלוונטית, אלא שהיא הסוגייה הפחות בעייתית. אם סין תצליח להבטיח לעצמה מעמד קבוע של עליונות גלובלית בזירת החדשנות הטכנולוגית, הבעיה הגדולה ביותר לא תהיה עד כמה חברות אמריקאיות יצליחו להתחרות בתוך סין עצמה, אלא עד כמה סין תשפיע פוליטית על מדינות אחרות בזירה העולמית.

מלחמת הסחר של טראמפ שואפת להחליש את היתרון המקומי של סין, ולפחות רטורית טוענת שארצות הברית מנסה לשכנע אותה לבצע רפורמות מבניות בכלכלתה, כדי שתהיה דומה יותר לכלכלה ליברלית מאשר למה שמכונה "קפיטליזם מדינתי". למרות זאת, ארצות הברית מחמיצה את ההשלכות האסטרטגיות העמוקות יותר ולטווח הארוך: אם סין תוכל להמיר את תשומת הלב שמופנית כיום כלפי הסוגייה של גישה לשוק המקומי שלה בעצמאות טכנולוגית בטווח הארוך ובעליונות גלובלית בכל מה שנוגע לחדשנות טכנולוגית בעתיד (על כל היתרונות האסטרטגיים הנלווים לכך), סביר להניח שהיא תסכים לכך ללא היסוס. עדיין לא ברור מדוע ארצות הברית נכשלה בהפניית תשומת הלב לנזק העצום שתוצאה כזו תסב לאסטרטגיה האמריקאית ברמה הגלובלית. הדגש שמושם כיום על הגישה לשוק הסיני המקומי פוגע לא רק במנהיגות הכלכלית העולמית של ארצות הברית, אלא גם באינטרסים הביטחוניים הממשיים שלה ברחבי העולם.

---

3 Dezan Shira & Associates, "What is Made in China 2025 and Why Has it Made the World So Nervous?".

סין עידנה כמה מההצהרות הגרנדיוזיות שלה בנוגע לפרויקט "תוצרת סין" בעקבות הביקורת החריפה של הנשיא טראמפ (לַרַבות הימנעות מלהזכיר פרויקט זה בישיבת הפתיחה של "הקונגרס הלאומי העממי" הסיני ב־2019, לראשונה מאז הושק הפרויקט ב־2015),[4] אך רק מעטים סבורים שמחווה זו מבטאת יותר מאשר מיתוג מחדש של הפרויקט במטרה למשוך אליו פחות תשומת לב, וזאת במקביל להמשך החתירה לקידום יעדיו המקוריים.[5] ואכן, חלק מהמחקרים אינם מסתפקים בתיאור הפשטני של פרויקט "תוצרת סין" כמאמץ לעבור מייצור צעצועים וחולצות טריקו לייצור טכנולוגיות מהשורה הראשונה, ורואים בו תוכנית סינית הנשענת על "יחס מפלה כלפי השקעות זרות, העברות כפויות של טכנולוגיות לסין, גניבת קניין רוחני וריגול קיברנטי".[6] פרויקט "תוצרת סין" מעתיק למעשה את הגישה הגרמנית כלפי "המהפכה התעשייתית הרביעית" הצפויה ומתמקד בשילוב של נתוני עתק, מחשוב ענן וטכנולוגיות מתפתחות רבות נוספות. אין זה מקרי שתחומים אלה משמשים את סין בימים אלה כדי לשכלל תוכניות בינה מלאכותית בעלות אופי פוליטי, כמו טכנולוגיות מעקב, פיקוח וניטור, זיהוי פנים, טכנולוגיות פריצה לצרכים פוליטיים והפצת קמפיינים של מידע כוזב.

הבעיה היא, כמובן, בעיית אמינות: סין אולי מתכוונת להגדיר את יוזמת "תוצרת סין" כשאיפה בלבד וכמהלך שאינו רשמי, אך המודל הכלכלי שלה דאג, מאז ומתמיד, לתת עדיפות לפיקוח המדינה על פני הצלחת השוק ולשליטה פוליטית על פני יזמות אינדיבידואלית. לכן, יש להניח שסין תמקסם את המנוף הפוליטי והאסטרטגי שייתן לה המעמד של מדינה מובילה טכנולוגית ברמה העולמית, והמנוף הפוליטי/אסטרטגי הזה יהיה, ללא ספק, מותאם לאינטרסים הסיניים ולמודל הסיני. אין מדובר ברצון להפוך את סין למשהו "דמוי אמריקה", אלא במנוע לקידום החזון הסיני של התפתחות כלכלית על חשבון גיוון פוליטי אמיתי ובגרות פוליטית במקומות שונים ברחבי העולם.

במונחים של משחק שחמט, מה שנראה כהרגעה מצד סין, אינו אלא הקרבת החַיל כדי למקם טוב יותר את המלכה. מהלך כזה תואם לחלוטין את מדיניות החוץ הסינית המסורתית, ובאופן שאולי משביע רצון אף יותר – משַחק בנטייתו של הנשיא הנוכחי של ארצות הברית לבקש "ניצחונות תקשורתיים" שיש להם מעט מאוד השפעה של ממש. אולם, גם אם הבית הלבן מפגין כרגע קוצר ראייה לגבי פוטנציאל האיום האמיתי של פרויקט "תוצרת סין", אין זה אומר שהתקשורת ומכוני המחקר עושים עבודה טובה יותר בניתוח ההשלכות האסטרטגיות של

4 McBride and Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?".

5 Dezan Shira & Associates, "What is Made in China 2025 and Why Has it Made the World So Nervous?".

6 McBride and Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?".

מדיניות החוץ הסינית. החשש הוא שהדבר יוצר מעגל סגור של משוב שלילי בארצות הברית, שרק יקבע עוד יותר את קוצר הראייה הנוכחי וישמור אותו גם לטווח הארוך.

הביקורת על פרויקט "תוצרת סין": האם הוא ממוקד או סושה מהיעד?

הוויכוח סביב פרויקט "תוצרת סין" מתרכז בשני מחנות ברורים, וההשתייכות למחנה האחד או השני היא שקובעת את העמדה כלפי הפרויקט. ניתן לתאר את עמדת שני הצדדים המתחרים באופן הבא:

- הצד האחד טוען כי פרויקט "תוצרת סין" שם לו למטרה להשתמש בסובסידיות ממשלתיות, לגייס מפעלים בבעלות המדינה ולעשות מאמצים להשיג קניין רוחני, וכל זאת כדי להדביק את היכולות הטכנולוגיות של התעשיות המערביות המתקדמות ואף להתעלות עליהן.
- דעתו של הצד השני היא שפרויקט "תוצרת סין" יכול להצליח רק בעזרת הסתמכות על מדיניות המַפלה השקעות זרות, מעודדת העברות טכנולוגיה בצורה כפויה עד כדי סחטנות של ממש, ותומכת בגניבת קניין רוחני, בגיבוי של ריגול קיברנטי.[7]

הדבר המשמעותי ביותר בנושא זה הוא האופן שבו שני המחנות עדיין ממוקדים בחשש מפני יעדיה של סין ומפני ההשפעה שתהיה להשגתם על יכולת התחרות של חברות אמריקאיות. במקרה הטוב, קיים גם חשש קל מפני השאיפה ארוכת הטווח של סין להחליף את ארצות הברית כמובילה הכלכלית באותן תעשיות הייי־טק שנמצאות על הכוונת, ובמקרה הקריטי יותר – בקביעת הסטנדרטים הבין־לאומיים. בזירה זאת נכנס לתמונה הסייבר, שיכול להוות דרך מתוחכמת ויעילה "להנדס" עליונות בצורה סמויה. מה שרבים מדי דוחקים לפי שעה לשוליים הם החששות של קהילת המודיעין האמריקאית, הרואה בפרויקט הסיני פוטנציאל למלחמה "רכה" יעילה מצידה של סין, שלמרות שהיא עשויה להיות בלתי חוקית מבחינה טכנית, היא נעשית בצורה שאינה בוטה מספיק כדי להצדיק פעולת תגמול צבאית. אלה הנמנים על מחנה החוששים שמים את הדגש על התמקדותה של סין בגיוס מדענים, בגניבה נועזת ומתמשכת של קניין רוחני כמדיניות רשמית ובהשקעות ישירות שיכולות להביא למיזוגים ולרכישות ענק של טכנולוגיות קריטיות ותשתיות אסטרטגיות (למשל, ב־2016 בלבד הסתכמו מאמצים סיניים אלה בסכום עתק של 45 מיליארד דולר).[8]

עצם העובדה שקהילת המודיעין האמריקאית מפרסמת התייחסות רשמית לתוכנית כלכלית, שסביר להניח שאין לה סיכוי רב להבשיל לפני שנת 2050,

7 Ibid.
8 Ibid.

ראויה לבחינה מעמיקה. למעשה, התרחיש המסוכן ביותר הוא שפרויקט "תוצרת סין" יהפוך ליוזמה האסטרטגית שבה ההיתוך בין הביטחון הלאומי ובין הכלכלה הפוליטית הבין־לאומית ייצור איום ברמה הגלובלית. לדוגמה, כשלוקחים בחשבון את המעורבות המתמשכת והאינטנסיבית של סין בעשור האחרון בהשקעות ברחבי אפריקה, ובהנחה שמעורבות דומה תיושם במסגרת פרויקט "תוצרת סין", אין זה מופרך לדמיין שליטה סינית עתידית בשוק הקובלט העולמי.[9] שליטה כזו תעניק לסין השפעה על מרבית מוצרי האלקטרוניקה העילית בעולם. יהיו לכך השלכות עצומות על ארצות הברית, בהינתן שוק הטכנולוגיות כפולות־השימוש (האזרחי והצבאי) שמתאפיין כיום בערפול. שוק זה היה נתון, מאז שצמח והתפתח, לשליטה ודומיננטיות אמריקאיות מוחלטות. העברת השליטה בו לידי סין תגרום להשלכות מפליגות על הביטחון והמודיעין הלאומיים של ארצות הברית, שקשה להמעיט בערכן ויהיה קשה עוד יותר לחזות אותן או לתת להן מענה.

ממד הזמן של הסכנה הכרוכה בפרויקט הסיני פועל, במידה מסוימת, נגד אזהרותיה של קהילת המודיעין האמריקאית. אמנם, אף אחד אינו מבטל על הסף אזהרות אלו, אולם הנטייה הרווחת היא לדחוק אותן לסוף רשימת העדיפויות. אין ספק שזרם הנתונים המתחרים והסותרים המגיעים מסין עצמה מעניק לשני המחנות הדומיננטיים בוויכוח על הפרויקט הסיני את התירוץ שהם זקוקים לו כדי להישאר ממוקדים ב"כאן ועכשיו". כתוצאה מכך, כשמתעורר החשש מפני הסכנה שיש בפרויקט "תוצרת סין" לביטחון הלאומי של ארצות הברית בטווח הארוך, נשמעת בלא מעט ממסדרונות הממשל "קריאת הקרב" לפיה הפרויקט אינו יותר מאשר "נמר של נייר".[10] אין ספק שחלק מהנתונים אכן מפתים לחשוב כך:

- סין עצמה התייחסה בפומבי לאפשרות שהיא עשויה "לעכב" מימוש חלק מהיעדים של פרויקט "תוצרת סין", ויש בסין מי ששואלים אם לא כדאי להחליף את הפרויקט בתוכניות אחרות.
- הוצאות המחקר והפיתוח של סין, החיוניות להצלחה של פרויקט "תוצרת סין", נותרו הרבה מתחת לרף של כלכלות מתקדמות כמו ארצות הברית ויפן. עובדה זו משמשת כאינדיקטור כללי למידת היעילות והתבונה שבה מדינה מוציאה את כספיה.
- רבים מהמנכ"לים הבכירים בתעשיית המכונות ברחבי העולם ציינו, כי למרות שסין עלתה לרמה השלישית או אולי אפילו השנייה מבין המדינות המובילות

9 Ibid.

10 Anjani Trivedi, "China's Made in 2025 Plan is a Paper Tiger", *Bloomberg,* December 15, 2018, https://www.bloomberg.com/opinion/articles/2018-12-16/china-s-made-in-2025-industrial-ambitions-are-a-paper-tiger.

בעולם, עדיין יש לפניה דרך ארוכה מאוד לפני שתוכל להגיע לרמה העליונה ולהתמודד עם אותן מדינות.

- אפילו יעדים ספציפיים בתעשייה, כמו כלי רכב המופעלים באנרגיה חדשה, ממחישים את הבינוניות ביכולותיה של סין. למרות המאמץ הממושך למצב את עצמה כ"טסלה העתידית", המציאות היא שסין לא הגיעה להצלחה מקומית בייצור מכוניות חשמליות, ובסופו של דבר אף פנתה למהנדסיה של חברת "טסלה" כדי שיסייעו לה בכך – מהלך שקרוב לוודאי מבטא מידה של צניעות.[11]

סיוע נוסף למחנה הספקנים כלפי פרויקט "תוצרת סין" ניתן למצוא בטיעונים הכלכליים הקלאסיים המטילים ספק ביכולתם של משטרים אוטוקרטיים להיות סתגלניים וחדשניים מספיק כדי להתמודד עם קשיים דמוגרפיים טבעיים. למרות שסין שואפת להפוך למובילה עולמית בייצור טכנולוגיות כבר במחצית השנייה של המאה ה־21, הדבר אמור להתרחש בדיוק כאשר יבשילו ההשלכות השליליות של מדיניות "הילד האחד" שהיא הנהיגה בעבר. מדיניות קיצונית זו צפויה להביא לכך שהאוכלוסייה הסינית בגיל העבודה תיחתך במאה ה־21 בחצי לעומת חמישים השנים הקודמות. נתון מרתיע אף יותר הוא שחלקה של האוכלוסייה הסינית מעל גיל שבעים ישַלש אז את עצמו. זו הסיבה שהמדיניות הנוקשה של "ילד אחד" רוככה בצורה שקטה אך נחושה.[12]

כלכלנים קלאסיים מלגלגים על הרעיון שפרויקט "תוצרת סין" הוא התוכנית שתעזור להתגבר על בעיות אלו, במיוחד לאור העובדה שהאסטרטגיה השאפתנית של הפרויקט לאמץ שיטה קפיטליסטית של שוק חופשי הולכת יד ביד עם מה שאותם כלכלנים רואים כשלטון אוטוקרטי מדכא, הנשען במקרים רבים על זיוף נתונים כלכליים כדרך לביסוס מעמדו הגלובלי. ספקנות זו מבוססת על העובדה שסין מכירה היטב את שיטת ההתערבות הממשלתית בכלכלה ואינה מוכרת כמי שמאפשרת יצירת צמיחה פנימית באמצעות חדשנות. מנקודת מבט זו, פרויקט "תוצרת סין" אינו אלא תרגיל ממשלתי ענק ומתוכנן בתיעוש מודרני עם מעטה טכנולוגי.[13] לפי אנשי מחנה זה, אם אכן הפרויקט אינו יותר מכך, האופי האוטוקרטי של המשטר הסיני לא רק שלא יקדם את הצלחת הפרויקט, אלא יפגע בה. סין אולי תוכל לספק מקורות מימון כמעט בלתי מוגבלים להשגת יעדיה, אך מימון אינו יוצר הון אנושי; והון אנושי הוא דבר שסין עדיין מפגרת בו מאוד, בעיקר

11. Ibid.
12. Keith Balmer, "Can China Really Become the Technology Kingpin? ", *Investment Week,* May 7, 2019, https://www.investmentweek.co.uk/investment-week/opinion/3075178/-china-main-player-technology.
13. Ibid.

מכיוון שמשטרים אוטוריטריים חוששים, מעצם טבעם ובצדק מבחינתם, מלעודד הון אנושי חדשני.

כדי לבסס הנחה זו ניתן לבחון את הבקשות לרישום פטנטים חדשים בסין. מכיוון שבסין מוגשות יותר בקשות לרישום פטנטים מאשר בכל מקום אחר בעולם, הרושם הכללי שהיא מנסה ליצור הוא שמדובר בעם תוסס, שאפתני ועתיר יכולת המצאה. אך דומה שהמציאות שונה למדי: הרוב המכריע של הפטנטים המוגשים לרישום בסין תקפים רק לסביבה המקומית ואין להם טווח והיקף בין־לאומיים.[14] משום כך, מחנה הספקנים מרגיש בטוח למדי לתייג את החדשנות הסינית ואת כל הפרויקטים העתידיים שלה (דוגמת "תוצרת סין") כלא יותר מאשר "זהב של שוטים". כשעושים שימוש בדילמה הכלכלית הידועה כ"הימלטות ממלכודת ההכנסה הבינונית", ניתן לקבוע כי אם פרויקט "תוצרת סין" יצליח בהשגת יעדו, סין תהיה המשטר האוטוריטרי המדכא הראשון בהיסטוריה שיוכל לרשום הצלחה כזו.[15]

ייתכן בהחלט שבסופו של דבר יתגלה מחנה הספקנים כצודק, ופרויקט "תוצרת סין" יסתכם ב"מהפכה" נוספת של משטר אוטוריטרי שאינה יותר מ"רוח וצלצולים". "הדגל האדום" הקטן, אך המשמעותי, שעדיין מתנופף הוא שסין מודעת לכך ואינה מפתחת תוכנית לטפל בבעיות הנוכחיות באמצעות פתרונות עכשוויים. דחיית הצורך לתקן בעיות עכשוויות באופן מיידי, פירושה שאפשר לתת עדיפות לפיתוח תוכניות ארוכות טווח. מרבית הביקורת על פרויקט "תוצרת סין" נשענת על המקום שבו סין נמצאת כיום ולא על המקום אליו היא שואפת להגיע. אם סין תאמץ את דרך החשיבה, המסגרות והכוונות הדרושות כדי להתפתח באיטיות ובהדרגה לעבר המטרות של פרויקט "תוצרת סין", סביר מאוד להניח שהמכשולים של העת הנוכחית הניצבים בפניה לא יהיו כה הרסניים כפי שהספקנים במערב מדַמים.

דוגמה מובהקת לכך היא העובדה שכל האזכורים הרשמיים לפרויקט "תוצרת סין" הושמטו ממושב הפתיחה של "הקונגרס העממי הלאומי" הסיני בשנת 2019. הספקנים מיהרו לקפוץ על עובדה זו כהוכחה ישירה לכך שהפרויקט הגיע לקצה גבול היכולת שלו וכבר כורע תחת כובד תחזיותיו לנוכח המכשולים הניצבים בפניו. עם זאת, ולמרות שראש ממשלת סין, לי קיצ'יאנג, לא הגה רשמית את השם "תוצרת סין", התוכן והמהות של נאום הפתיחה שלו עסקו במדויק במטרות וביעדים של הפרויקט.[16] זוהי טקטיקה מרומזת המאפיינת את מדיניות החוץ הסינית בכללותה.

14 Lulu Yilin Chen, "China Claims More Patents than Any Country – Most are Worthless", *Bloomberg News,* September 26, 2018, https://www.bloomberg.com/news/articles/2018-09-26/china-claims-more-patents-than-any-country-most-are-worthless.

15 Balmer, "Can China Really Become the Technology Kingpin?".

16 Issaku Harada, "Beijing Drops 'Made in China 2025' from Government Report", *Nikkei Asian Review,* March 6, 2019, https://asia.nikkei.com/Politics/China-People-

כאשר סין נתקלת בביקורת חריפה או מרגיזה שותפים אסטרטגיים כמו ארצות הברית, היא תאמר את מה שארצות הברית תרצה לשמוע, למרות שאין לה שום כוונה לסגת בה מיעדיה. לפיכך, השאלה אינה האם פרויקט "תוצרת סין" מאבד את תמיכת המפלגה הקומוניסטית הסינית, אלא האם המהלך האסטרטגי הפשטני הזה – לדבר ברכות המסווה נוקשות – ישכנע משקיפים אמריקאים במסדרונות השלטון בארצות הברית? אם כך יהיה, הדבר ינבע מהנטייה האמריקאית להישען על תחושת העליונות הקבועה של ארצות הברית בטכנולוגיות ובחדשנות.

האם פרויקט "תוצרת סין" יכול לשים קץ לעליונות האמריקאית?

כאמור, אין זה מפתיע שהמבט הספקני ביותר על היעדים הסופיים של סין מגיע מקהילות המודיעין והביטחון. קהילת הביטחון האמריקאית חשדנית במיוחד כלפי "פרויקטים לשיפור החברה", שבממדים הבין־לאומיים שלהם יכולים לאפשר לסין להפוך ל"מדינה דיגיטלית אוטוריטרית".[17] לכן, מרתק מצד אחד לראות קבוצות המודעות להשלכות הפוטנציאליות של היוזמות הכלכליות האסטרטגיות של סין על הביטחון הלאומי ומשמיעות קול נגדן, אולם מצד שני, כשמדובר בעצות מעשיות כיצד למנוע את הבעיה, דומה שהיכולת לְצפות את הנולד מתפוגגת. הפיכתה של סין למובילה העולמית החדשה בהעברת טכנולוגיות רגישות של בינה מלאכותית, במיוחד למדינות שאינן מקיימות יחסי ברית עם ארצות הברית, היא בעיה קריטית.

תחום אחד שמצביע הן על היכולות האסטרטגיות העתידיות של פרויקט "תוצרת סין" והן על ההתמקדות הכלכלית השגויה של ארצות הברית הוא הגרסה הסינית ל־GPS. מאז שנת 2017 בונה סין ומציבה באגרסיביות סדרת לווייני ניווט. לוח הזמנים של הפריסה היה כה נמרץ, עד שסין כבר יכולה להציע לשותפים המעוניינים בכך חלופה מתַפקדת למדי ליכולות ה־GPS של ארצות הברית. התלונות האמריקאיות התמקדו עד היום רק בתביעה לאסור על סין לעסוק בניסיונות להעביר אליה שותפים מסחריים חדשים ממערכת ה־GPS האמריקאית. אולם על ארצות הברית להיות מודאגת יותר מהאפשרות שמנוף כזה בידי סין ישמש אותה לצרכים אסטרטגיים: למשל, בתמורה לגישה לחלופה הסינית ל־GPS, סין עשויה לדרוש להקים שותפות בלעדית עם חברות סיניות לצורך האצת העברתן של

---

17 Nicholas Eftimiades, "China's Theft & Espionage: What Must be Done", *Breaking Defense*, April 19, 2019, https://breakingdefense.com/2019/04/chinas-theft-espionage-what-must-be-done/.

s-Congress/Beijing-drops-Made-in-China-2025-from-government-report.

טכנולוגיות בינה מלאכותית, תשתיות דיגיטליות וציוד.[18] כאשר המדינה שולטת באמצעי ההייטק, פוטנציאל הפיקוח והמעקב שלה הוא כמעט בלתי מוגבל.

דוגמה נוספת היא הקרב העתידי על העליונות בתחום ה־5G. אם פרויקט "תוצרת סין" יצליח לקדם את סין לעמדת המובילה לא רק בפיתוח, אלא גם בהעברת טכנולוגיית 5G לרחבי העולם, לאירוע כזה תהיה דינמיקה אסטרטגית אדירה. בניגוד לארצות הברית, יש בסין 650 מיליון משתמשי אינטרנט פעילים הצמאים למהירות של 5G, ויש לה גם פרויקט לשיפור הדדי של תשתיות כחלק מיוזמת "החגורה והדרך". פרויקט "החגורה והדרך" הוא יוזמה לחיבור בין דרכי היבשה והים, שכבר כיום מעוררת דאגה בקרב משקיפים מערביים במה שנוגע לטווח ההשפעה שהוא יניב לעוצמה הסינית – מָיָם סין הדרומי ועד מערב אירופה. אם פרויקט "תוצרת סין" יאפשר לסין לשלב עליונות בתחום 5G בפרויקט "החגורה והדרך", ייתכן שתהיה זו מכת האגרוף המכרעת שתסמן לא רק השגת עצמאות כלכלית סינית, אלא גם השפעה אסטרטגית של סין לרוחב סביבה שנמצאת כיום מחוץ לתחום ההשפעה האמריקאית. פירוש הדבר הוא מודל סיני של פיקוח פוליטי וחופש חלקי באינטרנט, אותו אפשר יהיה להמיר במהירות גישה גבוהה יותר ובפיקוח על היסטוריות דיגיטליות. הדבר מראה כי סין למדה היטב בשני העשורים האחרונים את מה שבעבר היה נחלתה הבלעדית של ארצות הברית: "היתוך אזרחי–צבאי".[19]

אף מדינה לא התקרבה עד היום ליכולת להעתיק הצלחה אמריקאית זו. אולם ההתקדמות ההדרגתית של הכלכלה הסינית בארבעת העשורים האחרונים הניבה יכולת ייחודית לצאת ביוזמות כמו יוזמת "החגורה והדרך" ופרויקט "תוצרת סין", הכוללות בתוכן היבטים ניכרים של היתוך אזרחי–צבאי ושימוש כפול. סין מראה בכך כיצד הצלחה כלכלית יכולה להוביל פוטנציאלית להתפשטותה של עוצמה צבאית/ביטחונית. לרוע המזל, נראה כי המערב מתעקש להמשיך לעסוק בניסיון לעצור את רכבת ההצלחה הכלכלית, למרות שזו כבר עזבה את התחנה. ההתמקדות באסטרטגיות עכשוויות של גישה כלכלית עלולה, בסופו של דבר, להביא לתוצאות הפוכות ולהמעיט בחשיבותן של תוכניות בעלות פוטנציאל צבאי־אסטרטגי ארוך טווח, דוגמת פרויקט "תוצרת סין".

---

18 Alex Capri, "How A Growing U.S-China Rivalry Is Reshaping The Global Tech Landscape", *Forbes,* December 9, 2018, https://www.forbes.com/sites/alexcapri/2018/12/09/how-a-growing-u-s-china-rivalry-is-reshaping-the-global-tech-landscape/#3275b134398e.

19 Ibid.

הניתוח האמריקאי מתבסס על השקפת עולם הרואה במערכת היחסים בין סין לארצות הברית נושא הנמצא בראש סדר העדיפויות.[20] אך מה יקרה אם, במקום זאת, המטרה הסופית של סין תהיה מעמדה של סין בדרום אסיה, במזרח התיכון, באמריקה הלטינית ובאפריקה? לא קשה לחשוב שלפחות חלק מההצלחה הסינית בפיתוח תוכניות כמו "תוצרת סין" נובע מהיהירות האמריקאית קצרת הרואי, המתייחסת לסין רק כאל מדינה "מעתיקה" שאינה מסוגלת להתמודד עם החדשנות האמריקאית, ומתעלמת ממכלול האיומים שהיא מציבה, דבר שהוא חלק בלתי נפרד מהמצב כשמדובר בביטחון לאומי ובמודיעין. התוצאה היא אגף קריטי שנותר חשוף ופגיע: חדשנות טכנולוגית שנשענת על מנופי השפעה, אך מנותקת לחלוטין מדאגה לעקרונות דמוקרטיים, לזכויות אדם ולחירויות אזרח במדינות שאינן ידידותיות במיוחד לארצות הברית. מצב זה מהווה סכנה מסוג חדש לאינטרסים אסטרטגיים אמריקאיים.[21]

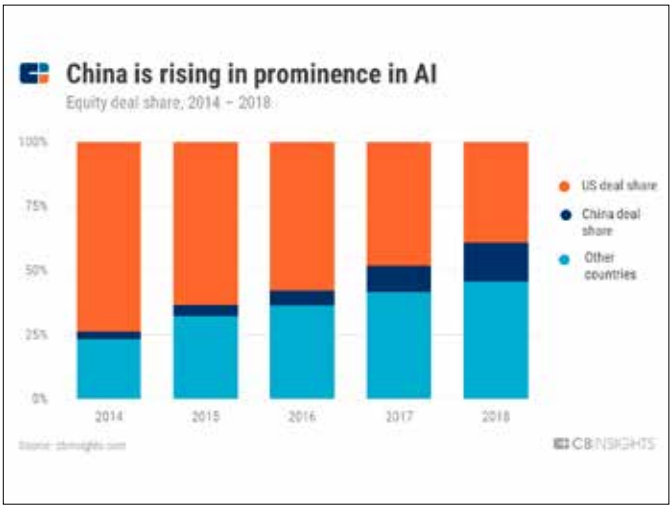
לאחר שנתפסה לא מוכנה ולא ממוקדת ביעדים לטווח ארוך, על ארצות הברית לחתור לפעילויות כמו "התגוננות" ("shielding") או "ריסון" ("stifling"), כדי למנוע את המשך הרכישות ובניית היתרונות על ידי סין.[22] כאמור, מאמצים אלה אינם רק בגדר "מעט מדי, מאוחר מדי", אלא גם זוכים לדגש חזק מדי, שכן הם עדיין נוטים לחשוב על ארצות הברית כעל המוקד העיקרי של האסטרטגיות ארוכות הטווח של סין. כל עוד זה המצב, ארצות הברית לא רק תתקשה להפוך את כיוונה של המגמה הנוכחית, הנוטה להעניק יתרון טכנולוגי לסין בסייבר; היא גם תישאר עיוורת לתהליכים ארוכי הטווח שיביאו לאיבוד העליונות האסטרטגית האמריקאית באזורים קריטיים בעולם לטובת הפרגמטיזם הדיפלומטי של סין. לאחר שארצות הברית השיגה עליונות בבינה מלאכותית, היא חוותה בחמש השנים האחרונות צניחה בנתח העולמי שלה בתחום זה.

---

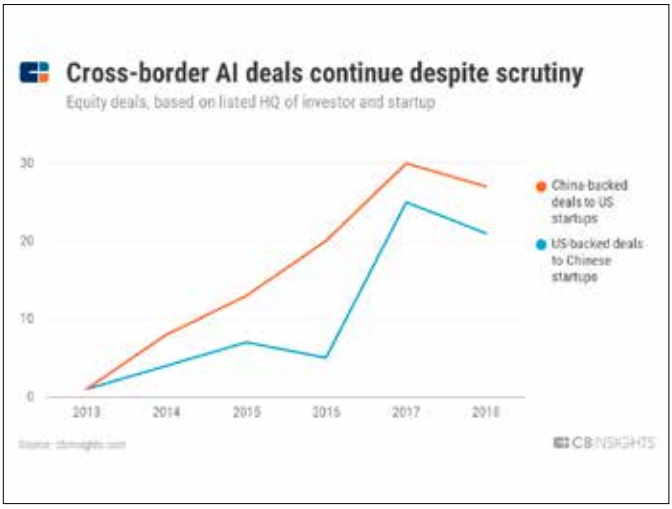
20 C.H. Tung, "America and China Need Each Other", *The Diplomat,* February 8, 2018, https://thediplomat.com/2018/02/america-and-china-need-each-other/.

21 Robert D. Atkinson and Caleb Foote, "Is China Catching Up to the United States in Innovation?", *Information Technology & Innovation Foundation,* April 2019, http://www2.itif.org/2019-china-catching-up-innovation.pdf.

22 Anthea Roberts, Henrique Choer Moraes, Victor Ferguson, "The US-China Trade War Is a Competition for Technological Leadership", *Lawfare,* May 21, 2019, https://www.lawfareblog.com/us-china-trade-war-competition-technological-leadership.

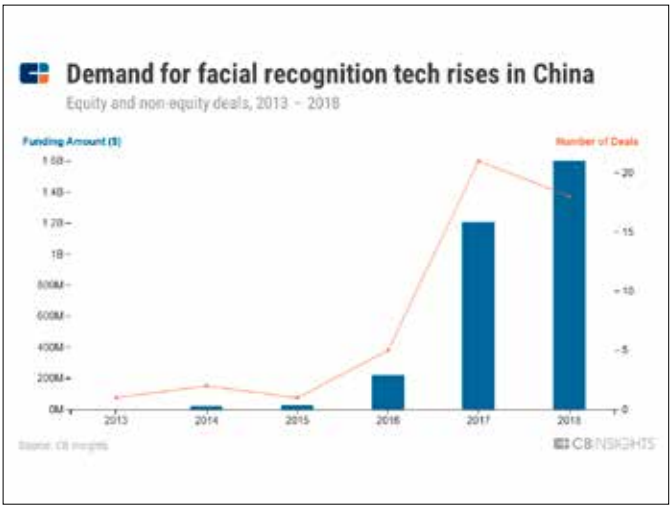


פרויקט "תוצרת סין" תוכנן מלכתחילה להיות מודל כלכלי של פיתוח סיני "מבחוץ־פנימה", וגם מודל של השקעות/מעורבות "מבפנים־החוצה" לטיפוח העוצמה הסינית.



אם יש עדיין מי שמטיל ספק בכך שההיקף האסטרטגי של הפרויקט הוא הרבה מעֵבר לפיתוח כלכלי, כל שעליו לעשות הוא להסתכל כיצד סין פעלה בחמש השנים האחרונות בטכנולוגיה לזיהוי פָּנים.[23]

23 Staff, "China is Starting to Edge Out the US in AI Investment", *CBInsights,* February 12, 2019, https://www.cbinsights.com/research/china-artificial-intelligence-investment-startups-tech/.



הפיתוח הכלכלי של סין אמור היה להתקדם כבר מראשיתו באופן שישמור על המדינה הסינית ללא פגע וכפי שהיא.[24] כתוצאה מכך, נכון יהיה להסתכל תמיד על פרויקטים כמו "תוצרת סין" כפרויקטים בעלי שימוש כפול, ולא ככאלה שעוסקים אך ורק בקיימות כלכלית. זווית זו נחקרה בצורה מרשימה במסגרת "הדרום הגלובלי", שעשה את הקישורים החשובים בין סין ובין הבינה המלאכותית, הפרויקט "תוצרת סין", הסייבר וההשפעה האסטרטגית. למרבה הצער, עד היום לא זכה חלק גדול ממחקר זה לתשומת לב מספקת:

> סין מוציאה סכומי עתק על מחקרים הקשורים לטכנולוגיות בינה מלאכותית, שכן הסייבר נמצא בצומת של כמה מסדרי העדיפויות הלאומיים והמדיניים שלה. שאיפות הסייבר הבין־לאומיות של סין קשורות קשר הדוק לשימוש הקיים והמתפתח שהיא עושה בטכנולוגיות בינה מלאכותית לצורך מעקב ושליטה חברתית במדינה. הדבר ניכר בתשתיות המעקב והפיקוח הפולשניות שלה, המבוססות על בינה מלאכותית, שמיושמות במדינת שינג'יאנג, וכן ב"חומת האש הגדולה" ("Great Firewall"). למרות שחברות אמריקאיות היו הראשונות להשיג יתרון בבינה מלאכותית (כפי שניתן למדוד, למשל, לפי היישומים של למידת מכונה ולפי מספר רישומי הפטנט בתחום הבינה המלאכותית), סין הולכת וסוגרת את הפער מול ארצות הברית. לפי קצב ההתקדמות הטכנולוגית הנוכחי שלה, הצפי הוא שעד שנת 2025 תעלה סין על ארצות הברית בתחום זה, ובשנת 2030 כבר תשלוט בתעשיית הבינה המלאכותית. יהיו לכך השלכות

24 Esther Pan, "The Promise and Pitfalls of China's 'Peaceful Rise'", *Council on Foreign Relations*, April 14, 2006, https://www.cfr.org/backgrounder/promise-and-pitfalls-chinas-peaceful-rise.

ניכרות על הַסדר העולמי הכלכלי, הפוליטי, הביטחוני והתרבותי ובתחום זכויות האדם.[25]

מעניין לראות כיצד יעדיה של סין בתחום הבינה מלאכותית והיתרונות האסטרטגיים שהיא מבקשת להשיג בתחום ההשפעה החיצונית, שלכאורה מנותקים זה מזה, תואמים בצורה מושלמת את לוחות הזמנים של פרויקט "תוצרת סין". מבחינתה של סין, אין טעם להפריד בין פיתוח כלכלי ובין ביטחון לאומי והשפעה גלובלית; אלה שלושה צדדים של "המשולש הסיני". זוהי גם הסיבה לכך שחיפושים בספרות אחר חברות הזנק לבינה מלאכותית וחברות לזיהוי פנים יניבו מספרים דומים, שכן שתיהן עוסקות בטכנולוגיות מתקדמות של פיקוח ומעקב.[26] השאלה היא עד כמה תהיה ההשפעה הסינית מגוונת מבחינה טכנולוגית ונרחבת מבחינה אסטרטגית, כאשר פרויקט "תוצרת סין" יגיע לבשלות.

האם סין היא המעצמה הרב־קושבית המשפיעה הראשונה?

חשוב לזכור כי סין הציגה את פרויקט "תוצרת סין" כשכבר הייתה פעילה בהעברת טכנולוגיות לרחבי העולם. מעמדה כיצרנית מוצרים זולים לכאורה לא פגע באטרקטיביות שלה כשותפת סחר בעיני מדינות רבות, שלא פעם מצאו את עצמן מוגבלות ואפילו נזנחות על ידי המעצמות הכלכליות המערביות הוותיקות. אחד התחומים המרכזיים שסין השיגה בו מעמד של מנהיגה הוא העברת טכנולוגיות של פיקוח ומעקב. מבחינות רבות, היה זה צעד מתבקש לאור ההצלחה הכלכלית בזירה הפנימית: המערכת הפוליטית בסין מפעילה יד קשה כדי להבטיח שליטה רבה יותר על הפעילות הציבורית ועל דעת הקהל. אין זה מפליא, אפוא, שמדינות אחרות ברחבי תבל, המודאגות באותה מידה מקולות אופוזיציוניים ומאקטיביזם ברמת השטח, עשויות לגלות עניין בלימוד ממי שנחשבת למנהיגה עולמית בתחום זה, ובסופו של דבר להצטייד בטכנולוגיות שלה? סקר מהיר על עיסקאות פיננסיות שנחתמו במהלך חמש השנים האחרונות מראה כי סין שיווקה והעבירה באגרסיביות את טכנולוגיות הפיקוח והמעקב שלה למדינות כמו אקוודור, זימבבואה, פקיסטן, אוזבקיסטן, קניה ואיחוד האמירויות הערביות, וכי שכפולים של הטכנולוגיה הרשמית (גם הם מתוצרת סין ובשיווקה) נמכרו למדינות כמו ונצואלה, בוליביה ואנגולה.[27]

---

25 Arthur Gwagwa, "AI, Foreign Policy and National Governance Impact: Focus on China", *ModernDiplomacy.eu*, May 10, 2019, https://moderndiplomacy.eu/2019/05/10/ai-foreign-policy-and-national-governance-impact-focuson-china/.

26 "China is Starting to Edge Out the US in AI Investment".

27 Paul Mozur, Jonah M. Kessel and Melissa Chan, "Made in China Exported to the World: The Surveillance State", *The New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

מותחי הביקורת על סין חוששים שפעילות כזו שלה אינה רק עוד מילוי של נישה בתוך הקפיטליזם של השוק החופשי הגלובלי. לדבריהם, לא מדובר ביישום ראוי של טכנולוגיות מעקב שנועדו לסייע ליוזמות חיוניות כמו מאבק בטרור וברדיקליות, או בפעילות פלילית בתוך המדינה. הדאגה מתבססת על החשש שסין מייצרת בפועל אוטוריטריות עתידית מבוססת טכנולוגיות, אותן היא מעבירה מתוך כוונה להגביל את יכולות הביטוי וההתפתחות החיוניות של תנועות דמוקרטיות הנמצאות בשלבי התעוררות. אין ספק כי תשתיות מסיביות ויוזמות פיתוח גלובליות כמו "תוצרת סין" ו"החגורה והדרך" רק יגדילו וירחיבו את ההזדמנויות להעברת טכנולוגיות כאלו.

ההבדל בין האופן שבו סין מתייחסת למעורבות גלובלית ובין האופן שעושות זאת מדינות כמו ארצות הברית הוא משמעותי. מזה זמן רב סין מתעקשת על כך שהיא מעוניינת רק בעיסקאות כלכליות פרודוקטיביות ורווחיות. חברת Huawei, ענקית הטכנולוגיה הסינית שנמצאת תכופות במוקד החששות הבין־לאומיים הללו, תמצתה שלא במתכוון את פילוסופיית יחסי החוץ הסינית במשפט אחד: "Huawei מספקת טכנולוגיה התומכת בתוכניות של ערים חכמות וערים בטוחות בכל העולם. בכל אחד מהמקרים, Huawei אינה מעורבת בקביעת המדיניות הציבורית ובשימוש שייעשה בטכנולוגיה זו".[28] לא יהיה זה מוגזם להחליף את המילה "Huawei" במילים "הרפובליקה העממית של סין".[29] זאת ועוד, קל למדי להמיר את הטכנולוגיה כפולת השימוש, שכאמור נפוצה בשוק הגלובלי של ימינו ונמכרת למטרות מסחריות, ולהפוך אותה ליעילה למטרות רבות אחרות, לרבות מטרות צבאיות ומודיעיניות. כשזוכרים את שני הפרמטרים הללו, ההצהרה של Huawei היא הודאה בפועל בפני קונים פוטנציאליים שהם יקבלו את **כל** השימושים הפוטנציאליים של הטכנולוגיה המועברת. כל מה שסין רוצה הוא לשמור על יכולת הכחשה סבירה בהמשך הדרך, היה והטכנולוגיה תתגלגל בסופו של דבר לשימושים שאינם מסחריים.

סין התמודדה בעבר עם ביקורת מסוימת על כך שמהלך הפתיחה המסיבי הראשון שלה בכניסתה אל זירת הכלכלה הגלובלית היה התמקדות במדינות בעלות משאבי טבע, וזאת כדי להזין את צורכי האנרגיה שלה שאינם יודעים שובע. כך, למשל, מדינות רבות באפריקה החלו, באמצע העשור האחרון, לתהות אם רכישת משאבי הטבע שלהן על ידי סין אכן הביאה להתפתחות כלכלית חיובית ל"חצר

28 Ibid.

29 Keith Johnson, Elias Groll, "The Improbable Rise of Huawei", *Foreign Policy*, April 3, 2019, https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/.

האחורית" של אפריקה.[30] עם זאת, היוזמות החדשות של סין, דוגמת פרויקט "תוצרת סין", הן בעלות פוטנציאל ברור לסלק ביקורת כזאת לפני שתהפוך לרצינית מדי. הפרויקט יודע "למכור" העברת טכנולוגיות לא רק לצורכי פיתוח כלכלי של היום, אלא גם ליכולת שלטונית של המחר.[31] מבחינתם של מבקרים אמריקאים, מסר כזה פירושו משילות עתידית בדרך שבה רואה אותה סין: שימוש בטכנולוגיית בינה מלאכותית כדי לשלוט על ההמונים, להגביל את אלה המאתגרים את השלטון ולשבש אקטיביזם שמקורו מקרב ההמונים. ומה שאולי גרוע עוד יותר הוא האופן שבו סין סוגרת עיסקאות של העברות כאלו, המחזקות את מעמדה כמשפיעה גלובלית: היא מציעה הלוואות למדינות שבעבר מעולם לא היו מסוגלות להרשות לעצמן טכנולוגיה כזו. זאת ועוד, אופי המערכת הפוליטית הפנימית בסין הוא כזה, שהשוק הגלובלי כמעט ואינו יכול לעקוב אחרי מידת השקיפות של העברות מסוג זה ואת מידת הנכונות הסינית לקבל את האחריות עליהן.[32]

סיבה נוספת לדאגה היא העובדה הפשוטה שסין התעלתה על ארצות הברית מבחינה אסטרטגית ובתבונה שבה נהגה בכמה סוגיות דיפלומטיות, חוקיות ומסחריות שנגעו להעברת טכנולוגיה של בינה מלאכותית. התוצאה היא שארצות הברית מוצאת את עצמה בעמדה המביכה של מי שמביעה מחאה נגד אסטרטגיית החדשנות הסינית, אך נאלצת להודות שבסופו של דבר סין מצליחה להשיג את יעדיה מבלי לעבור על אף חוק אחד. למרות האשמות על ריגול כלכלי וגניבת IP, סין ניצלה למעשה את העקרונות והחוקים של השוק החופשי האמריקאי כדי להגדיל את המנופים שבידיה. לדוגמה, מרכיב מרכזי בחדשנות ובכושר ההמצאה האמריקאיים הוא היכולת למשוך השקעות זרות ותמיכה חיצונית מגורמים פרטיים.[33] כלל פשוט זה עולה בקנה אחד עם האסטרטגיה הסינית: שפיכת מאות מיליונים, אם לא מיליארדים, של דולרים על חברות הזנק אמריקאיות, אך לא כדי לעודד חדשנות אמריקאית, אלא פשוט כדי לקבל גישה לטכנולוגיה כבר בשלב מוקדם. בדרך זו יכולה סין לממש את מה שהתמחתה בו מזה עשרות שנים – לבצע הנדסה לאחור ולייצר מקבילה סינית שניתן לשווק אותה למדינות העולם השני והשלישי, שממילא אינן על הכוונת של מדינות מתועשות ושל טכנולוגיות מובילות. למעשה,

30 Eleanor Albert, "China in Africa", *Council on Foreign Relations,* July 12, 2017, https://www.cfr.org/backgrounder/china-africa.

31 Mozur, Kessel and Chan, "Made in China Exported to the World: The Surveillance State".

32 Ibid.

33 Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of US Innovation", *Defense Innovation Unit Experimental*, January 2018, https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.

הנתונים מראים כי העברת הטכנולוגיות מארצות הברית לסין (הצעד הראשון באסטרטגיה ארוכת הטווח של סין להשגת מעמד של משפיעה גלובלית בעתיד) כמעט ולא נשענה על ריגול או על גניבת סייבר; האסטרטגיות הסיניות העיקריות היו השקעות חוץ ישירות, השקעות הון סיכון, מיזמים משותפים, הסכמי רישוי וגיוס כישרונות – כולן בהתאם לחוק האמריקאי.[34]

בנוסף לנאמר לעיל, סין, ולא ארצות הברית, היא שהתחייבה לאסטרטגיה ארוכת טווח הוליסטית הממוקדת בכל הטכנולוגיות המתפתחות המרכזיות שעשויות להפוך לכוח המניע השולט בשוק הכלכלי העולמי העתידי. ארצות הברית פשוט בחרה שלא להקדיש לכך את הזמן, המאמץ והכסף, כפי שעשתה סין. גרוע מכך, ארצות הברית הפגינה אדישות מתוך מחשבה שהנדסה לאחור היא קרובת משפחה רחוקה ולא מוצלחת של החדשנות, אשר לעולם לא תשכיל להפוך לגאונות טכנית מקורית אמיתית. נראה כי מדובר היה בטעות חמורה בהערכה, בהתחשב באפשרות שסין עשויה להגיע עד שנת 2050 ל־150 אחוזים מגודלה של כלכלת ארצות הברית. קוצר ראייה אמריקאי זה הוא כמעט בלתי נסלח.[35]

כל הדברים האלה מעלים חשד לגבי העיסוק התקשורתי הרב בימים אלה בגניבת קניין רוחני ובריגול כלכלי על ידי סין. אין פירוש הדבר שצריך לאפשר לסין לפעול בגלוי באופן בלתי חוקי, אלא שהניסיון לייחס את ההתקדמות הטכנולוגית שלה אך ורק להצלחתה ב"גניבה והעתקה" מארצות הברית, יהיה הסחת דעת לא מדויקת. אמונה בכך אולי משפרת את הרגשתם של התאגידים האמריקאיים, אך היא מחמיצה את החדשנות האסטרטגית שבזכותה התקדמה סין במהירות רבה כל כך. היא גם מעידה על אי־הפקת לקחים מההיסטוריה: ישנן הוכחות רבות לכך שגם דרום קוריאה וגם יפן השתמשו בחיקוי כאסטרטגיה של חדשנות, וכיום הן שחקניות יציבות ומשמעותיות בשוק הכלכלי העולמי.[36] סין אינה בעלת ברית של ארצות הברית, כפי שדרום קוריאה ויפן הן כיום, אך הלקחים שהיא למדה מהן ראויים לציון.

כדי שלא יהיה מי שיטען שהתוכניות של סין אינן יותר מאשר ניסיון להדביק את הקצב של ארצות הברית, או ינסה לנתח את העמדה הסינית רק דרך עיניים אמריקאיות, יש לומר שכל היוזמות הסיניות הללו עוררו את תשומת הלב גם של

34 Sean O'Connor, "How Chinese Companies Facilitate Technology Transfer from the United States", *US-China Economic and Security Review Commission*, May 6, 2019, https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf.

35 Brown and Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of US Innovation".

36 Atkinson and Foote, "Is China Catching Up to the United States in Innovation?".

מערב אירופה ואף וגרמו שם לדאגה גדולה יותר. רוב האנליסטים הביטחוניים של האיחוד האירופי סבורים כי לוח הזמנים שקבעה סין כדי להגיע לרמתן של היכולות הטכנולוגיות האירופיות, ואף לעקוף אותן, הוא הרבה יותר קצר מלוחות הזמנים האמריקאיים. לרוע מזלו של האיחוד האירופי, האסטרטגיות הסיניות, שהיו כה יעילות ביכולתן "לתפוס את האמריקאים כשהם אינם מוכנים", מסוגלות לעשות זאת בדרך אגרסיבית עוד יותר כשמדובר באירופה. האיחוד האירופי מודה שסין פשוט נכנסה מהר יותר ממדינות אירופה להשקעות בטכנולוגיות כפולות־שימוש, שיאפשרו שילוב אזרחי–צבאי בעתיד. היא עשתה זאת בעיקר באמצעות שיטת ההשקעה ה"כלל ממשלתית" ("whole-of-government") ורגולציה מגוננת, וכן באמצעות קבלת גישה אל גופי החדשנות הטכנולוגית הטובים ביותר של האיחוד האירופי כבר בשלב מוקדם.[37]

באופן אירוני, חלק מהביקורת באירופה עוסקת פחות בגניבות ובריגול הסיניים שמטורידים את ארצות הברית, ויותר ביתרונות הלא הוגנים שיש למערכת אוטוריטרית כמו זו של סין על פני דמוקרטיות ותיקות. מכיוון שחדשנות כלכלית בדמוקרטיות נוטה לרוב להיות תהליך עצמאי של "מטָה–מעלה", היא יוצרת חפיפה קטנה הרבה יותר בין שלושת הגורמים המזינים ככלל את החדשנות – תעשייה, ממשלה ואקדמיה. לעומת זאת, סין מיישמת מודל אוטוריטרי של "מעלה–מָטה" להשגת חדשנות כלכלית, ובכך היא יוצרת באופן טבעי נקודת מפגש רחבה ועמוקה הרבה יותר של שלושה היבטים אלה (חִשבו בהקשר זה על תרשים Venn הכולל שלושה מעגלים שלובים של תעשייה, ממשלה ואקדמיה).[38]

מה שצריך לעניין ולהטריד את ארצות הברית היא העובדה שהתגלו כמה סדקים בעמדה המשותפת של האיחוד האירופי בכל מה שנוגע למאבק ביוזמות הסיניות או לחילופין להצטרפות אליהן. גרמניה, יותר מכל מדינה אירופית אחרת, החליטה כי הפיתוח הטכנולוגי הכלכלי העתידי שלה יושג ביתר יעילות אם תפעל בדרך של שותפות אמינה עם סין. סין, מצידה, יצרה תווים חדשים במנדרינית, במיוחד כדי לבטא את המונחים "ייצור חכם" ו"תעשייה 4.0", שבאים לידי ביטוי אך ורק במשא ומתן הסיני–גרמני. יוזמות כאלו אינן נחלתה של סין בלבד: גם גרמניה הקימה סוכנות לשיתוף פעולה בין־לאומי (GIZ) כדי "ליצור תנאי מסגרת טובים יותר לחברות גרמניות וסיניות בפרויקטים של 'תעשייה 4.0' ו'תוצרת סין

37 Meia Nouwens and Helena Legarda, "Emerging Technology Dominance: What China's Pursuit of Advanced Dual-Use Technologies Means for the Future of Europe's Economy and Defence Innovation", *China Security Project – The International Institute of Strategic Studies*, December 2018, https://www.merics.org/sites/default/files/2018-12/181218_Emerging_technology_dominance_MERICS_IISS.pdf.

38 Ibid.

2025"."[39] השאלה שיש לשאול בהקשר זה היא: אם אין חזית מערבית מאוחדת אפילו כשמדובר במענה לפרויקטים כמו "תוצרת סין", מה הסיכוי שתתעורר התנגדות לכך מצד מדינות שאינן בעלות ברית של ארצות הברית ואשר לא פעם אפילו נאלצו לספוג הטפות מצידה?

סיכום

מתברר כי הגישה הסינית של שימוש בצמיחה כלכלית כמנוף גיאו־פוליטי כבר הפכה למודל: יפן, טייוואן, הונג קונג, סינגפור, ואפילו דרום קוריאה והפיליפינים, כולן קשורות בעיסקאות עם הרפובליקה העממית של סין, אלא שמדובר בעיסקאות שהן בגדר "רחוב חד־סטרי": סין ממקסמת את המנופים שבידיה, ובעשור האחרון אף הפעילה לחץ מתון על שכנותיה האזוריות כאשר אלו קידמו יוזמות שלא עלו בקנה אחד עם היעדים הסיניים לטווח ארוך.[40]

אפילו נוכח מציאות זו, הנטייה המערבית היא להחליף מסקנות אובייקטיביות וקרות בדברים הקרובים יותר למשאלת לב דיפלומטית. הרעיון שמדינות מזרח אסיה יוכלו להציע למדינות מרוחקות יותר לקחים על הדרך לנהל מגעים כלכליים עם סין מבלי להיות מושא לניצול פוליטי, אינו מעיד על הבנת המציאות. העובדה שסין לא השתלטה על שכנותיה, או לא כבשה אותן, אינה עדות לכוחן האסטרטגי של מדינות אלו או על יכולתן לרסן אותה, אלא לכך שסין אינה אובססיבית לכוח בדרך המיליטריסטית המסורתית החביבה כל כך על ארצות הברית. המודל המועדף על סין הוא המודל הגרמני שתואר לעיל. במקום לראות בסין איום גיאו־אסטרטגי אותו יש לרסן, גרמניה הטילה את מלוא כובד משקלה על יצירת ברית כלכלית איתה שתביא תועלת לשני הצדדים, תוך שהיא מעלימה עין מחששות אסטרטגיים/מדיניים. ההשלכות שיהיו לאסטרטגיה זו, המיושמת לאורך המאה ה־21, עשויות לשנות באופן משמעותי את הַסדר העולמי הנוכחי, שמושתת על הובלה אמריקאית ונותן משקל שווה לעוצמה כלכלית וללחץ גיאו־דיפלומטי.

בסופו של דבר, ארצות הברית צריכה להיות מודאגת מהאפשרות שיום אחד היא תתעורר ותבין שמנהיגותה העולמית הוחלפה בזו של מדינות רבות אחרות, שלמעשה אימצו את מודל מדיניות החוץ של חברת Huawei. כאמור, Huawei אינו רק קונצרן סיני מצליח ומשגשג השוכן ופועל במדינה בעלת שלטון אוטוריטרי שמתנגד לרעיון של אימוץ הערכים הדמוקרטיים האמריקאיים; Huawei משגשג דווקא משום שהוא מצליח לתפקד בתוך הכללים והתהליכים המגבילים של המשטר

39. Ibid.
40. Ibid.

הסיני.[41] מבחינתה של ארצות הברית, Huawei פועל מכוח "עיסקה עם השטן": הצלחת החברה מותנית בכניעה לערכים הסיניים של עוצמה והירכיה; אם לא תסכים לכך, היא לא תורשה להתקיים. אלא שזהו היגיון אמריקאי שאינו משקף באמת את מצב העניינים בסין: "עיסקה עם השטן" מרמזת לכאורה על החלטה שהתקבלה באי־רצון ומתוך ויתור. לעומת זאת, ל־Huawei לא הייתה שום דילמה: מטרת החברה הייתה להפוך לשחקן מרכזי בכלכלה העולמית, וכך להגדיל את השפעתה ואת כוחה של המדינה הסינית. אין לחברת Huawei מטרה להפיל או להחליף את המשטר הסיני; זוהי כבר משאלת לב אמריקאית.

סביר להניח כי מדינות ברחבי דרום אסיה, אפריקה ואמריקה הלטינית יתלהבו ממודל מדיניות החוץ של Huawei. מצב כזה יכול להביא בפועל ליצירת מערכת של קולוניזציית סייבר סינית, אך כזו שבמקביל תחזק את הצמיחה והשגשוג של אותן מדינות. לכן, המחאה שלהן על "קולוניזציה" כזו תהיה מינורית. מבחינתה של ארצות הברית, יהיה זה בלתי נסבל לחזות בשורה של מדינות שיאמצו רעיונות כמו: דרישה מאזרחים, מחברות ומארגונים לסייע לגופי הביון הממלכתיים; הימנעות מלהעמיד לרשות אותם אזרחים, חברות וארגונים מנגנון משפטי שיאפשר להם לסרב לפניות מצד שירותי המודיעין או גופי הביטחון; ניצול גורמים אזרחיים לצורך איסוף מודיעין (כפי שעושה סין).[42] אם רעיונות אלה יתקזזו עם התקדמות טכנולוגית מהירה והתפתחות והתקדמות כלכלית, סביר להניח כי יהיו מדינות שיקפצו על ההזדמנות ואף יתחילו להביע מורת רוח כלפי הנטייה האמריקאית לקשור בין שותפות כלכלית וסיוע בפיתוח ובין חירויות דמוקרטיות ואזרחיות.

ארצות הברית אינה רואה את עצמה כמי שמציעה "עיסקאות עם השטן" למדינות באפריקה, באמריקה הלטינית, במזרח התיכון ובדרום אסיה. אף על פי כן, לעיתים קרובות היא נתפסת במקומות אלה כמי שעושה בדיוק כך.[43] הרבה יותר קל לה לראות את עצמה כמו "הקאובוי הטוב עם הכובע הלבן", ואת כל מי שלא נמצא בצד שלה כ"נבל בכובע השחור". בעידן שלאחר המלחמה הקרה, כאשר ארצות הברית הייתה המעצמה היחידה בעולם, היה לה קל יותר להשיג את מבוקשה. אולם במאה ה־21, כאשר היא ניצבת בפני פרויקטים כמו "תוצרת סין" ואינטרסים סיניים אסטרטגיים ארוכי טווח המציגים מודל מעורבות מסוג אחר לחלוטין, כבר אין לה הביטחון שתוכל לשמור על מעמדה כמובילה העולמית הבלעדית. ההתמקדות של סין בחיבור ה"הווה" הכלכלי עם "עתיד" גיאו־אסטרטגי ובתפיסה שאינה מפרידה

41 Priscilla Moriuchi, "The New Cyber Insecurity: Geopolitical and Supply Chain Risks From the Huawei Monoculture", *Recorded Future*, June 10, 2019, https://www.recordedfuture.com/huawei-technology-risks/.

42 Ibid.

43 Stephanie Savell, "The American Empire's Long Reach", *The Nation*, February 19, 2019, https://www.thenation.com/article/america-empire-war-terror-counterterrorism/.

בין טכנולוגיות כפולות־שימוש המועברות למדינות שאינן בעלות ברית של ארצות הברית, היא אסטרטגיה מבריקה, גם אם מקיאווליסטית לחלוטין.[44] הדגשים האמריקאיים הנוכחיים "מחמיצים את הרכבת" של פוטנציאל זה. אם הדבר יימשך, ניתן יהיה לומר שהאשם האמיתי ביצירת רשת בינה מלאכותית גלובלית בעלת מאפיינים של קולוניזציה סינית, קרי סייבר אוטוריטרי הנתמך בטכנולוגיה מתקדמת, הוא ההיבריס האסטרטגי של הקהילות המסחריות, הביטחוניות והדיפלומטיות בארצות הברית.

44 Moriuchi, "The New Cyber Insecurity: Geopolitical and Supply Chain Risks from the Huawei Monoculture".

סייבר, מודיעין וביטחון
קול קורא להגשת מאמרים לכתב העת

כתב העת **סייבר, מודיעין וביטחון** הינו כתב עת **שפיט** היוצא לאור שלוש פעמים בשנה בעברית ובאנגלית. עורך כתב העת הינו פרופ' גבי סיבוני, העומד בראש תוכנית צבא ואסטרטגיה ותוכנית ביטחון בסייבר במכון למחקרי ביטחון לאומי.
פנייה זו הינה קול קורא להגשת מאמרים ומחקרים שיפורסמו במסגרת כתב העת, על פי שיקולי המערכת.

ייבחנו מאמרים הנוגעים לתחומים הבאים:

- מדיניות גלובלית ואסטרטגיה בסייבר
- רגולציה במרחב הקיברנטי
- אבטחת החוסן הלאומי בסייבר
- לוחמת סייבר והגנה על תשתיות חיוניות
- בניין הכוח הקיברנטי על מרכיביו: המשאב האנושי, אמצעי לחימה, תורה, ארגון, הכשרה ופיקוד
- היבטים אתיים, מוסריים ומשפטיים במרחב הקיברנטי
- טכנולוגיה במרחב הקיברנטי
- הרתעה במרחב הקיברנטי
- ניתוח איומים וסיכונים במרחב הקיברנטי
- ניתוח תקריות ומשמעויות במרחב הקיברנטי
- חשיבה צבאית ואסטרטגית, הפעלת הכוח הצבאי במרחב הסייבר ומבצעי תודעה
- מודיעין, שיתוף מידע ושותפות ציבורית־פרטית (PPP)
- שיטות מחקר, פעולה והליכים (TTPs)

ניתן לעיין במאמרים בתחומים קרובים שנכתבו בגיליונות כתב העת **צבא ואסטרטגיה**, באתר האינטרנט של המכון: http://www.inss.org.il

ייבחנו מאמרים בהיקף של עד 5,000 מילים בעברית (עד 6,000 מילים באנגלית) כולל הערות שוליים ומראי מקום. המאמרים יכללו תקציר בהיקף של 100–120 מילים ורשימת מילות מפתח בהיקף של עד עשר מילים.

להגשת מאמרים ולפרטים נוספים ניתן לפנות לח"מ.

בברכה

גל ספיר galps@inss.org.il | **גל פרל פינקל** galp@inss.org.il
מתאמי כתב העת **סייבר, מודיעין וביטחון**

המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
אוניברסיטת תל אביב
TEL AVIV UNIVERSITY

המכון למחקרי ביטחון לאומי – תוכנית ביטחון סייבר
רח' חיים לבנון 40, ת"ד 39950, רמת אביב, תל אביב 61398 | טל': 03-6400400 | פקס: 03-7447588