# טורקיה – האתגרים למדיניות המאבק באיומי סייבר

אופיר איתן

טורקיה היא אחת המדינות המפותחות ביותר במזרח התיכון מבחינה טכנולוגית, כלכלית ומוסדית, ויחד עם זאת היא אחת המדינות המאוימות ביותר בעולם בממד הסייבר. הממשל הטורקי פועל בשנים האחרונות כדי לגשר על הפערים הקיימים באמצעי ההתגוננות מפני איומי הסייבר, אך המאמצים שהוא עושה בתחום זה טרם הניבו את הפירות הרצויים.
מאמר זה מנתח את תמונת המצב של ההיערכות הלאומית הטורקית להגנה בסייבר ומצביע על מספר אתגרים מובנים הניצבים בפני היערכות זו, שמקורם במדיניות טורקית ארוכת שנים. הממשל הטורקי ייאלץ למצוא פתרונות לאתגרים אלה כדי שיוכל לעמוד ביעדי תוכניות הביטחון הלאומי שלו להגנה בסייבר.

**מילות מפתח**: סייבר, טורקיה, מדיניות, ביטחון לאומי, כלכלה פוליטית

## מבוא

איומי הסייבר משפיעים בשנים האחרונות באופן הולך וגובר על חיינו, ובתוך כך גם על מדיניותן של ממשלות רבות. על רקע זה החלו מדינות רבות לנקוט צעדים שמטרתם לגבש אסטרטגיה לאומית במרחב הסייבר ולהקים תשתיות הגנה נגד תקיפות ברשת. מאז שנשמעו באמצעי התקשורת השמות Stuxnet, Flame ו־Shamoon ופורסם דבר התקפות מניעת שירות (DDOS) נגד המגזר הפיננסי בארצות הברית, נראה כי גם המזרח התיכון הפך להיות גורם פעיל בזירת המלחמה התוססת בסייבר. זהות התוקפים במרחב הסייבר הינה סוגיה מעורפלת, ועם זאת שורבבו בה בשנים האחרונות שמותיהן של ארצות הברית, ישראל, איראן ומדינות נוספות במפרץ הפרסי.

אופיר איתן הוא מנהל אבטחת מידע והגנת סייבר מוסמך וקצין מודיעין סייבר בדרגת רס"ן (מיל') באגף המודיעין. בעל תואר ראשון ושני בהיסטוריה של המזרח התיכון מאוניברסיטת תל אביב.

טורקיה הינה אחת המדינות המפותחות ביותר במזרח התיכון, מעצמה אזורית וחברה מרכזית בנאט"ו. למרות זאת, קיים פער ניכר ביכולותיהם של מוסדותיה להתמודד עם התקפות סייבר. לראיה, רק בשנת 2016 הוקם מרכז לאומי לתיאום ולשיתוף פעולה להתגוננות בפני מתקפות סייבר ורק בחודש יולי 2017 הוצגה בפני הקבינט הטורקי טיוטת חוק לחיזוק ההגנה על מרחב הסייבר בגופים הציבוריים, תוך שילוב מומחי אבטחה מדיסציפלינות שונות, לרבות האקרים מסוג "כובע לבן" (White Hat Hackers), כלומר אנשי מקצוע שתפקידם לשפר את רמת האבטחה של רשתות ואמצעי מחשוב באמצעות ניסיונות תקיפה מבוקרים וסקרי מערכות. מטרת המהלך הייתה להרחיב את סמכויותיו של המרכז הלאומי להתערבות נגד התקפות סייבר (NICC), שהינו מחלקה הכפופה למועצת טכנולוגיית המידע והתקשורת (Bilgi Teknolojileri ve İletişim Kurumu – BTK) ונושא באחריות לטיפול בתקיפות סייבר ברחבי המדינה והכלתן, וכן להפצת ידע ולסיוע בהגנה על כלל הגופים הציבוריים.[1]

טורקיה טרם מיסדה מעטפת הגנה לאומית בסייבר המאגדת את מוסדות המשטר, גופי הביטחון, התשתיות הלאומיות וגופים אזרחיים. זאת, הגם שהיא גיבשה זה מכבר מתווה אסטרטגי לאומי בעניין זה – National Cyber Security Strategy and Action Plan 2016–2019.[2] המתווה הטורקי דומה לתהליכים דומים שהבשילו במדינות אחרות בעולם המערבי, תוך שהוא מתייחס למציאות הפרטנית של טורקיה, הנדרשת להתמודד עם איומי סייבר מגוונים ורציפים על תשתיות המדינה.

נראה כי מעֵבר לחסמים הביורוקרטיים, קיימים בטורקיה אתגרים מובְנים הבולמים את הצעדים הדרושים לצמיחתה של תשתית מקומית איכותית בתחום הסייבר. ענף האינטרנט ותקשורת הנתונים, הנכלל בין ענפי התעשייה עתירת הידע, הוא בעל מאפיינים ייחודיים ושונים משאר ענפי התעשייה במשק. כפועל יוצא מכך, תחום הלחימה בסייבר, קרי עולם התקיפות וההגנות הווירטואליות על רשתות ומערכות מחשוב, מחייב הפנייה מיוחדת של משאבים, בראש ובראשונה לפיתוח ההון האנושי.

על רקע הבנות יסוד אלו, ברצוני לטעון כי מדיניותה הריכוזית של טורקיה לאורך השנים היא שהובילה לאתגרים היסודיים הניצבים בפניה כיום, בבואה להתמודד עם איומי הסייבר על תשתיותיה הלאומיות. ניתן לחלק אתגרים אלה

1 Seyma Nazli Gurbuz, "Turkey Adopts Cybersecurity Strategy, Fights Cyberterrorism", *Daily Sabah*, August 10, 2017, https://www.dailysabah.com/war-on-terror/2017/08/11/turkey-adopts-cybersecurity-strategy-fights-cyberterrorism.

2 Merve Seren, "Turkey Steps Up Counter-Cyber Attack Efforts", *The New Turkey*, January 24, 2017, https://thenewturkey.org/turkey-steps-up-counter-cyber-attack-efforts/.

לשני רבדים שהם בעלי השפעה רבה על מסוגלותה של טורקיה לפתח עוצמה בסייבר: אתגר המדיניות והביורוקרטיה ואתגר התרבות הארגונית.

הניתוח שיוצג בעמודים הבאים יפתח בתיאור קצר של תמונת המצב של המדיניות הלאומית הטורקית בתחום הגנת הסייבר. לאחר מכן ינותחו שני הרבדים שהוזכרו לעיל, המכילים את כלל האתגרים המובנים הניצבים בפני מקבלי ההחלטות הטורקים בדרך לפיתוח עוצמה בסייבר. המאמר יעשה שימוש במספר הנחות יסוד מן הגישה הכלכלית הקפיטליסטית לצורך ניתוח תיאורטי של התפתחות האתגרים הניצבים בפני המדיניות הטורקית.

## המדיניות הלאומית הטורקית להגנה בסייבר

מחקרים מן השנים האחרונות מציגים נתונים שצריכים להדיר שינה מעיניהם של מקבלי ההחלטות בצמרת הביטחונית הטורקית. כך, למשל, כבר בשנת 2012 פורסם כי טורקיה נמנית על עשר המדינות המותקפות ביותר בעולם בתחום הסייבר.[3] חברות אבטחת מידע ותקשורת מהמובילות בעולם, כמו Trend Micro, Fortinet ו־Akamai, פרסמו בשנים 2016־2017 כי טורקיה עומדת בראש רשימת המדינות המותקפות בסייבר באירופה ובעולם.[4]

ניתוח מפת איומי הסייבר מצביע על שלושה שחקנים מרכזיים המאיימים על רשתות האינטרנט הממשלתיות והמסחריות של טורקיה: גורמי הכוח הכורדים, האופוזיציה למשטר (FETO) ותשתיות הפשע המאורגן (Cyber crime, על פי המונח המקובל כיום). כדוגמה לאיום הסייבר הכורדי ניתן להביא מתקפה שזכתה להדים נרחבים בתקשורת, כאשר ארגון ה־PKK תקף את אתר משרד האוצר הטורקי עד שהביא לנפילתו, תוך השחתת תוכן האתר בתכני תעמולה התואמים את סדר היום של ארגון המחתרת הכורדי.[5] באירוע זה היה ברור מה היה השיקול שעמד מאחורי התקיפה "הרועשת", אף ששאלת זהותו של התוקף בעולם הסייבר נשארת בדרך כלל עלומה. בהקשר זה ניתן למנות רשימה ארוכה של תקיפות מפורסמות אחרות שכוונו נגד אתרי ממשל טורקיים, כמו אלה של משרד האוצר,[6] המשטרה

3 Aydin Albayark, "Turkey among Top 10 Countries Subjected to Cyber Attacks", *Sunday's Zaman*, July 1, 2012, https://www.todayszaman.com/news-285120-turkey-among-top-10-countries-subjected-to-cyber-attacks.html.

4 Seren, "Turkey Steps Up Counter-Cyber Attack Efforts".

5 Umit Kurt, "Cyber Security: A Road Map for Turkey", in *Strategy Research Project* (Pennsylvania: U.S. Army College, 2012), pp. 8-9; Umit Enginsoy, "Turkey Centralizes Efforts for National Cyber Security", *Hurriyet Daily*, November 21, 2011, https://www.hurriyetdailynews.com/turkey-centralizes-efforts-for-national-cyber-security.aspx?pageID=238&nID=7307&NewsCatID=344.

6 Kurt, "Cyber Security: A Road Map for Turkey".

הלאומית וחברת התעופה Turkish Airlines.[7] סביר ליחס תקיפות אלו ודומות להן לגורמי הכוח הכורדים וכן לגופי פשיעה בסייבר.

ככול שגובר השימוש של המוסדות והחברות בטורקיה ברשתות המחשוב והתקשורת, כך גדל האיום על תפקודם התקין. ההערכה היא כי מתוך כשמונים מיליון תושבים בטורקיה – המדינה העשרים בעולם מבחינת גודל האוכלוסייה[8] – קרוב ל־43 מיליון משתמשים ברשת האינטרנט. בכך הם תופסים את המקום ה־19 בעולם בשימוש באמצעי תקשורת זה.[9] מכאן עולה שטורקיה ניצבת בשורה הראשונה בעולם, לצד המדינות המפותחות ביותר במשפחת האומות, ביחס בין מספר התושבים ובין היקף השימוש באינטרנט. לעומת זאת, טורקיה מפגרת מאחור במה שנוגע למאמץ הלאומי להגנה על רשתות מפני תקיפות סייבר, בהשוואה לצעדים שיוזמות המדינות המפותחות.

באוקטובר 2010 פרסם הצבא הטורקי את "הספר האדום", המאפשר חלון הצצה, אחת למספר שנים, לנבכי אסטרטגיית הביטחון הלאומי הטורקית. מתוכן הספר ניתן להסיק כי הסייבר נתפס, בראייתה של טורקיה, כאיום בלתי קונבנציונלי. בהמשך לכך, המועצה הטורקית לביטחון לאומי אשררה בשנת 2011 אסטרטגיה לאומית חדשה, הכוללת לראשונה גם את היבט האיומים בסייבר.[10] כאמור, לאחרונה אף פורסמה תוכנית לאומית לאסטרטגיית הגנה בסייבר לשנים 2016־2019.[11] אסטרטגיה זו מגדירה שני יעדים מרכזיים: הראשון, הכרה טורקית בכך שהגנה בסייבר הינה מרכיב אינטגרלי של הביטחון הלאומי; השני, עמידת טורקיה בכשירות הנדרשת בכול הקשור לצעדים המינהלתיים והטכנולוגיים הדרושים כדי להשיג ביטחון מוחלט לכלל נכסיה בממד הסייבר.

מוסדות הממשל הטורקי מקיימים פונקציות הגנה בסייבר שהן פרי יוזמות מקומיות. למעשה, אין כל רשות אחודה או גוף עליון מתאם בטורקיה לנושא ההגנה בסייבר, והפעילות בתחום זה מסתמכת על מוצרים מיובאים. בין הגופים הקיימים ניתן למנות את ה־CERT הלאומי[12] הטורקי (TR-CERT) הפועל תחת רשות המידע והתקשורת, וכן את ה־Cyber Fusion Center (CFC) הראשון של

7 Albayark, "Turkey among Top 10 Countries Subjected to Cyber Attacks".

8 הנתון נכון לשנת 2009 ולכן, בסבירות גבוהה, היקף המשתמשים כיום רחב יותר. על כל פנים, אין בכך כדי לשנות מהותית את התמונה.

9 Central Intelligence Agency, *The World Factbook: Turkey*, January 7, 2013, https://www.cia.gov/library/publications/the-world-factbook/geos/tu.html.

10 J. A. Lewis and K. Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization* (Washington: CSIS, 2011), p. 20.

11 Seren, "Turkey Steps Up Counter-Cyber Attack Efforts".

12 CERT – Computer/Cyber Emergency Response Team – תפיסה שגובשה לראשונה על ידי אוניברסיטת קרנגי־מלון ומתייחסת לצורך בהקמת מרכזים לאומיים, מוסדיים או מגזריים שתפקידם הוא לסייע לקהלי יעד להיערך מול איומי סייבר ולהתמודד איתם.

משרד ההגנה הטורקי.[13] לעומת זאת, צבא טורקיה וארגון הביון הלאומי (MIT) נשענים על פתרונות טכנולוגיים מקומיים להגנה בסייבר, אותם מפתחת ומספקת "החברה הממשלתית לתוכנה ומערכות" (Havelsan).

בעקבות עבודת מטה שנערכה בשנים 2010־2011, גיבשה טורקיה תוכנית להקמת "מפקדת סייבר" במטה הכללי של הצבא הטורקי, שייעודה הוא להדוף מתקפות רשת נגד המדינה. המטות המשולבים של צבא טורקיה הכריזו על הקמת מפקדה זו בשנת 2013.[14] על פי הפרסומים בתקשורת, וכן מעדותו של קצין בכיר בצבא הטורקי השופך אור על הנעשה מאחורי הקלעים של המפקדה החדשה, גוף זה בנוי על פי המודל של מקבילו האמריקאי ותפקידו הוא לנטר את כל רשת האינטרנט הציבורית בטורקיה במטרה לספק מעטפת הגנתית למוסדות המדינתיים.[15] "מפקדת הסייבר" הטורקית אמורה לפעול בשיתוף פעולה עם משרד ההגנה הטורקי, המועצה הלאומית למחקרי מדע וטכנולוגיה (TÜBİTAK) והאוניברסיטה הטכנולוגית של המזרח התיכון (METU). המפקדה, שבראשה עומד קצין בדרגת גנרל, נשענת על תקציב ייעודי, הינה עצמאית מבחינת המבנה הארגוני וכוללת יחידה מיוחדת להגנה בסייבר.[16] על פי הצהרת שר התקשורת והתחבורה הטורקי, תוכנית ההגנה בסייבר של טורקיה יושמה בפועל בשנת 2013.[17]

המודעות בטורקיה לצורך בהגנה במרחב הסייבר ולפוטנציאל האיומים בממד זה אמנם גוברת בשנים האחרונות, כפי שניתן ללמוד מהתוכניות המדיניות ומהיוזמות המקומיות השונות, אולם מבחינה מעשית, טורקיה נמצאת בפער משמעותי בהיערכותה הלאומית להגנה בסייבר בהשוואה למדינות מערביות אחרות. צ'טין קיה קוץ', פרופסור לקריפטוגרפיה מאוניברסיטת קליפורניה, היטיב לתאר את מצבה בתחום ההגנה בסייבר: "מכיוון שטורקיה טרם השלימה את השינוי הקיברנטי בתשתיותיה [...] במקרה של תקיפת התשתיות בעתיד, דוגמת מערכות הרכבת התחתית או החשמל, אין בנמצא תהליכים מקדימים כדי להתמודד עם איום זה".[18]

---

13. Seren, "Turkey Steps Up Counter-Cyber Attack Efforts".
14. Burak Ege Bekdil, "Cyber Defense 'Indispensible Part' of Turkey's National Security: Senior Official", *Atlantic Council, Defense News*, December 13, 2013, http://www.atlanticcouncil.org/blogs/natosource/cyber-defense-indispensible-part-of-turkey-s-national-security-senior-official.
15. Kurt, "Cyber Security: A Road Map for Turkey", p. 14; Enginsoy, "Turkey Centralizes Efforts for National Cyber Security".
16. Lewis and Timlin, *Cybersecurity and Cyberwarfare.*
17. "Turkey's Cyber Defense Plan to be Ready in 2013", *Hurriyet Daily*, March 2, 2012, https://www.hurriyetdailynews.com/turkeys-cyber-defense-plan-to-be-ready-in-2013.aspx?pageID=238&nid=15054.
18. Gurbuz, "Turkey Adopts Cybersecurity Strategy, Fights Cyberterrorism".

תמונת המצב באה ללמדנו כי קידום מנגנוני ההגנה של טורקיה בסייבר מחייב לא רק זירוז התהליכים הביורוקרטיים, אלא גם התבססות על שתי אבני יסוד מההיצע הלאומי הטורקי – כוח אדם מקומי מיומן ותשתית מקומית של מחקר ופיתוח. עם זאת, כפי שכבר צוין בראשית המאמר, טורקיה נאלצת להתמודד עם אתגרים רבים נוספים, שמקורם במדיניות הריכוזית שהנהיגו ממשלותיה מאז היווסדה – אתגרים היוצרים חסמים ובלמים המעכבים את ההתבססות על שתי אבני היסוד הללו.

## האתגרים הניצבים בפני טורקיה בדרך לפיתוח עוצמה במרחב הסייבר

הגישה הקפיטליסטית לכלכלה הפוליטית גורסת כי מדיניות ריכוזית מהווה את אחד מכשלי השוק המעכבים התפתחות יצרנית וטכנולוגית וצמיחתה של יזמות פרטית. הפילוסוף והכלכלן אדם סמית' טען כי חלוקת העבודה בין כלל גורמי השוק מביאה להתמקצעות, חוסכת זמן במעבר בין שלבי הייצור השונים ומניעה אנשים לשכלל תהליכי ייצור. בנוסף לכך, הגישה הקפיטליסטית אינה חולקת על כך שלמדינה יש תפקיד חשוב בפיתוח המשק ובייצובו גם בעידן השוק החופשי של ימינו. במסגרת זו, המדינה משפיעה דרך רגולציה של שוק העבודה, החינוך, הכשרות מקצועיות ועוד, תוך נקיטת מדיניות כלכלית וצעדי חקיקה ואכיפה במסגרת המתח שבין ביזור השוק לריכוזו.[19]

בכלכלת שוק ליברלית פירמות פותרות כשלי שוק באמצעות יחסי הגומלין בין השוק החופשי, חוזים (הסדרים) והיררכיה (יחסים בין הפירמות). במילים אחרות, על פי הגישה הליברלית הקלאסית, כשלי שוק נפתרים על ידי הדינמיקה של "היד הנעלמה" של כוחות השוק. לעומת זאת, בכלכלת שוק מתואמת, המאפיינת את הכלכלה הטורקית, הפירמות מסתמכות פחות על תחרות ויותר על רשתות עסקיות ויחסי גומלין אסטרטגיים ("חוזה לא מושלם"). למעשה, גם תחת תכתיבי השוק החופשי נשמרת ריכוזיות במשק – בידיהן של המדינה ושל קבוצות כוח בודדות.[20]

### אתגר המדיניות והביורוקרטיה

עד שלהי שנות התשעים של המאה העשרים, ממשלות טורקיה לא נקטו מדיניות מוכוונת לדרבון וקידום יזמות פרטית בכלל, ובענף התעשיות עתירות הידע בפרט. הדבר היה פועל יוצא של מדיניות ארוכת שנים הנעוצה עוד בימי המעבר

19 Peter A. Hall, David Soskice, "Varieties of Capitalism", *The Political Economy Reader: Markets as Institutions*, eds. N. Barma and S.K. Vogel (Indiana: Routledge, 2007), pp. 292-303, 307-312.

20 שם.

מהאימפריה העות'מאנית לרפובליקה הטורקית המודרנית. הגם שהרפובליקה הטורקית ירשה מסורת בת למעלה ממאה שנים של אימוץ טכנולוגיה מערבית, ירושה זו כללה גם מדינה עניה שכלכלתה נשענת על יבולים חקלאיים ונעדרת תשתית ממוסדת כלשהי של מגזר פרטי.[21]

הממשלה הטורקית הראשונה חתרה אמנם למדיניות של פיתוח כלכלי וחברתי, אך משמעות הדבר בראייתה הייתה הקמת תעשייה כבדה ממוקדת ייצור. לשם כך, וכחלק מהמדיניות הריכוזית בכלל, הקימה ממשלת טורקיה חברות ממשלתיות בבעלותה ובניהולה, תוך אימוץ תוכניות חומש פרי המודל הסובייטי. מלבד המדיניות הריכוזית, שבלמה כל אפשרות ליזמות פרטית, ממשלות טורקיה לדורותיהן אימצו מדיניות פיתוח שאינה מקדמת דרישה לפיתוח מקומי. בתוך כך, טורקיה ביססה את הקמת התשתיות שלה על ייבוא מבחוץ מן המסד ועד הטפחות. הממשל הטורקי חתם על הסכמים עם תאגידים זרים כדי שאלה יתכננו, יקימו ויתפעלו מיזמים רחבי היקף, שבסופו של התהליך יועברו לידיים טורקיות. תהליך זה מתקיים למעשה עד ימינו. מדיניות זו הובילה לתלות בלעדית בטכנולוגיה חיצונית ולהיעדר צורך ביזמות מקומית.[22]

המתווה של הקמת חברות ותאגידים ממשלתיים הועתק במרוצת הזמן על ידי הממשל הטורקי גם למגזר הפרטי, כשהיעדים המדיניים ואופן הביצוע נשארו זהים. לכן, עד שלהי שנות התשעים של המאה העשרים התמקד העידוד הממשלתי של המגזר הפרטי בתעשיות כבדות, שתכליתן הייתה לייצר כמה שיותר מקומות עבודה. מדיניות זו הייתה בעלת השלכות נוספות, שמתוכן שתיים קשורות לענייננו: הראשונה, הזנחת ענפי התעשיות עתירות הידע, להן נדרש על פי רוב כוח אדם מיומן, משכיל ואיכותי, לצד הפחתה במספר המשרות בענפים אלה בהשוואה לענפים אחרים; השנייה, עליית שכבה של אוליגרכים, הלוא הם ראשי ובעלי התאגידים הגדולים. המדובר בקונגלומרט של משפחות המתוות את הביקוש בשוק הטורקי על פי צרכיהן, כאשר ברוב המקרים קיימת חפיפה כמעט מלאה בין האינטרסים שלהן ובין האינטרסים של המדינה. תאגידים אלה אינם זקוקים לרוב למהנדסים ולאנשי היי־טק, ובכך הם מחשקים את הקיבעון הטכנולוגי, הנחשלות בקרב האוכלוסייה ומיקודה בתעשיות "צווארון כחול".[23]

גם לאחר פתיחת השוק הטורקי, בשלהי שנות התשעים של המאה העשרים, ניצבו יזמים מקומיים בפני מסכת תלאות של ביורוקרטיה, שהקשתה ואפילו בלמה

---

21 Arnold Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms? Or, Why is Turkey so Dependent on Technologic Innovations Created Outside its Borders?", *SSRN*, May 26, 2006, pp. 1-4, https://ssrn.com/abstract=904780.

22 שם, שם.

23 שם, עמ' 1־4, 9.

כל ניצן של יזמות מקומית. מדובר באתגר משמעותי לענפי התעשייה עתירת הידע בכלל ולענף הסייבר והאינטרנט בפרט. היזם הטורקי, המבקש להקים חברת הזנק, נתקל עוד מראשית דרכו במצב שבו כמעט ואינו יכול לגייס כספים מלבד הון אישי או משפחתי. רוב האשראי הפוטנציאלי ליוזמות מסוג זה מצוי בידי הבנקים, אולם אלה נוקטים מדיניות זהירה נוכח המשברים התכופים שפקדו את שוק ההון הטורקי בשלושים השנים האחרונות.[24] הנתונים הסטטיסטיים מראים כי מתן האשראי הבנקאי לעסקים הקטנים והבינוניים בטורקיה עומד על שלושה־ארבעה אחוזים בלבד מכלל האשראי הניתן למגזר הפרטי.[25] יש בכך אירוניה מסוימת, מפאת העובדה שהתאגידים הקטנים והבינוניים מהווים כ־99 אחוזים מענף התעשייה בטורקיה, אך נותנים תעסוקה לכ־66 אחוזים מסך העובדים בענף ומספקים כ־34 אחוזים מהערך המוסף היצרני בו.[26]

גם כאשר הבנקים בטורקיה מחליטים לתת אשראי ליזמות עסקית, רבים מהם לא מסוגלים לגבש תוכנית מימון ראויה ולמצוא את המקורות הכספיים הרלוונטיים למימונה. גם מקורות מימון חלופיים, כגון קרנות הון־סיכון, משקיעים עצמיים ("איינג'לים" – Angels) וגיוס הון ממניות, אינם מפותחים דיים בטורקיה בהשוואה לנדרש במדינות מערביות. יתרה מכך, מי שמספק את מרבית ההלוואות לפירמות היזמיות בשוק הטורקי הוא הבנק הלאומי הטורקי, Halk Bank (המצוי תחת הליכי הפרטה).[27] זאת, בשונה ממקורות המימון של יזמים במדינות מערביות, המגיעים מקשת רחבה של אפיקי מימון וסיוע, בהם הממשלה עצמה, השקעות חוץ, פירמות לעידוד צמיחה, ארגונים חוץ ממשלתיים (NGO's), ארגוני סחר בין־לאומיים וכיוצא באלה.[28] כאמור, מנופי צמיחה כלכליים מסוג זה אינם מפותחים דיים בטורקיה. מצב זה מעמיד אתגרים וחסמים רבים בפני ענף התעשיות עתירות הידע במדינה, ובתוכן תעשיית הסייבר.[29]

כשמדובר בתהליכי הביורוקרטיה הניצבים בפני היזם הטורקי, ראוי להביא את דברי הפרופסורית לניהול מאוניברסיטת סבנג'י באיסטנבול, דילק צ'טינדמר, המתארים אתגר מהותי זה: "טורקיה היא המדינה ה־13 הכי ביורוקרטית בעולם. מומחים טוענים כי יזם זקוק ל־172 חתימות ממגוון מוסדות ממשלתיים כדי לקבל

24 שם, עמ' 8־9.
25 שם, שם.
26 "Small and Medium-Sized Enterprises in Turkey: Issues and Policies", *OECD Report* (Paris: OECD Publications, 2004), pp. 29-33.
27 שם.
28 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 8-9.
29 "Small and Medium-Sized Enterprises in Turkey".

אישור להשקיע [...] בטורקיה, יזם מבזבז לא פחות מעשרים אחוזים מזמנו בנושאים ביורוקרטיים, כאשר באיחוד האירופי הדבר עומד על שמונה אחוזים בלבד".[30]

היבט קריטי נוסף בעידן השוק החופשי הוא היעדר הנגישות של חברות הזנק טורקיות למידע. על פי עקרונות הכלכלה הניאו ליברלית, קידום צמיחה במשק מחייב פתיחות מרבית של ערוצי המידע והידע. ממחקר שערך ארגון OECD בשנת 2004 על פלח העסקים הקטנים והבינוניים, עולה כי בשוק הטורקי קיים חוסר בסוכני ידע ובערוצי תקשורת לשיתוף מידע. בתוך כך, ארגון OECD המליץ לממשל הטורקי להימנע מעימותים בין גופי החקיקה ומערכות האכיפה על רקע ניגוד אינטרסים, וזאת כדי לאפשר שקיפות לטובת העסקים הקטנים והבינוניים.

בשנת 2001, עם התנעת התוכנית הלאומית למימוש אמנת האיחוד האירופי, התחייבה טורקיה להנהיג רפורמות יסודיות במערכות הרגולציה המקומיות, על פי אמות המידה הבין־לאומיות המקובלות. תהליך זה, יחד עם צעדים נוספים שממשלת טורקיה מנסה לקדם, אמורים לשפר, בין היתר, את תהליכי הביורוקרטיה ואת מערכות הרגולציה במדינה.[31]

## אתגר התרבות הארגונית

עולם הסייבר מתייחד בהון האנושי שלו, המבדיל את מוקדי הידע והמומחים בענף זה משאר התעשיות עתירות הידע. בין היתר, דרושים מספר מאפיינים או תכונות מקצועיות כתנאי להתפתחותם, לקידומם ולהגעתם לרמה מקצועית נאותה של מהנדסי תוכנה, מומחי רשתות תקשורת ואבטחת מידע, וכן של פצחנים (Hackers). אין מדובר במדדים מדעיים, אלא בסביבה ממסדית וארגונית היוצרת אקלים המאפשר צמיחתם של פיתוחים ופתרונות טכנולוגיים חדשניים. קשה לנתק בין מרכיב חיוני זה של עולם הסייבר ובין מדיניות ממסדית ריכוזית המאפיינת את טורקיה, שכן לפחות על פי הגישות הליברליות לכלכלה פוליטית, מדיניות ריכוזית יוצרת חסמים להתפתחות של פירמות ויחידים גם בענפי האינטרנט ותקשורת הנתונים המבקשים לפרוץ דרך ולחדש בתחומם.

כדי לבחון את אתגרי התרבות הארגונית העומדים בפני יצירת שכבת הון אנושי בענף הסייבר הטורקי, יש להתמקד בשני מאפייני יסוד של טורקיה: יחסי צבא־מדינה ותרבות המחקר והפיתוח. כל זאת, תוך התבססות על הנחת היסוד, לפיה הריכוזיות בממסד הטורקי חוסמת תהליכים מבניים (כשלי שוק – Market Failure) הנחוצים לצמיחת תעשיות הסייבר במדינה.[32]

30. Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 8-9.
31. "Small and Medium-Sized Enterprises in Turkey".
32. Hall and Soskice, "Varieties of Capitalism".

מקובל על רבים שהתעשיות הביטחוניות הן כור מחצב וזרז לפיתוחים טכנולוגיים בענפי תעשייה רבים, ובמיוחד בענף התעשיות עתירות הידע. בהתחשב בהנחת יסוד זו, הגיוני להסיק כי טורקיה, בה הצבא מהווה עמוד תווך מרכזי של המשטר והחברה, צריכה למצב את עצמה כחלוצה גם בממד הסייבר, או לכול הפחות להיות בעלת "סל כלים" איכותי בתחום זה. אולם, תמונת המצב מורכבת יותר, ולכן המציאות בממד הסייבר הטורקי שונה בתכלית. פרופסור ארנולד רייזמן טוען כי טורקיה לא הצליחה לתעל את ניסיונה הצבאי ואת תעשיותיה הביטחוניות לפיתוחים טכנולוגיים משמעותיים בשוק האזרחי, דבר שכאמור הינו הכרחי לצמיחה בממד הסייבר. כדי להוכיח את טענתו, ערך רייזמן השוואה תיאורטית בין שלוש מדינות שיש ביניהן קווים משיקים לדיוננו: טורקיה, ישראל והודו. שלוש מדינות אלו עומדות מאז הקמתן באופן רצוף בפני איומים ביטחוניים משמעותיים על ריבונותן, ושלושתן התנסו בקליטה והטמעה של אמצעי לחימה איכותיים המאופיינים בטכנולוגיה ברמה גבוהה.[33]

התעשיות הביטחוניות של טורקיה מייצאות כיום תוצרי פיתוח עצמאיים הדורשים התמקצעות טכנית גבוהה בתחומי האוויר, הים, הלוחמה האלקטרונית ומערכות השליטה והבקרה.[34] אולם, יחסי הגומלין בין התעשיות הביטחוניות הטורקיות ובין הפירמות הפרטיות בטורקיה (יחידים וארגונים) בממד הסייבר לא הביאו לפיתוח "סל כלים" איכותי דיו. זאת, מכיוון שתעשיות הסייבר הממשלתיות, בדומה לכול תעשייה טכנולוגית אחרת בטורקיה, אינן מפותחות די צורכן. ממצאיו של רייזמן מראים כי ישראל הצליחה לתעל את הפיתוחים הצבאיים שלה גם לטובת הפירמות הכלכליות במדינה וגם להפצת טכנולוגיות וידע בשוק האזרחי. לעומת זאת, טורקיה כמעט ואינה נהנית מתהליך דומה. בדומה למדינות מתפתחות, טורקיה למדה כיצד לייצר אמצעי לחימה קלים ותחמושת, אך את הנשק המתוחכם יותר המצוי בארסנל הצבאי שלה היא רכשה באופן קבוע מבחוץ (בין היתר מישראל).[35]

פרופסור רייזמן מציג תיאוריה להבנת מציאות זו. הוא משווה בין המארג הצבאי־חברתי של ישראל לזה של טורקיה, תוך הדגשת ייחודיותה של ישראל כ־"Startup Nation", וזאת למרות שגם שבטורקיה, כמו בישראל, נהוג שירות חובה צבאי. מרבית תהליכי המו"פ הפנים ארגוניים של צה"ל מתבססים על אוכלוסיית המשרתים בצבא, אך הייחודיות הישראלית היא בכך שתכתיבי הביקוש הארגוניים מביאים את שכבת הפיקוד הצבאית לאפשר מרחב יצירתיות ופעולה רחב, והתרבות הארגונית מעודדת את צמיחתם של רעיונות ויוזמות "מלמטה למעלה". כאשר

---

33 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 10-15.

34 Ibrahim Sunnetci, "High-Tech in Turkey – Special Report", *Military Technology*, Vol. 35, No. 3 (2011): 107-110.

35 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 10-15.

מצרפים לתרבות ארגונית זו את העובדה שצה"ל הוא שמאתר וממיין את המועמדים מתוך מרבית האוכלוסייה המגיעה לגיל 18 וששיעור המתגייסים לצבא הוא גבוה, מתגבשים יחסי גומלין מפרים בין הצבא ובין החברה האזרחית.

ואכן, אזרחים רבים בישראל יוצאים לאחר שירותם הצבאי לשוק האזרחי עם מטען ידע איכותי וניסיון תעסוקתי. במצב זה נפתחות בפניהם דלתות רבות במטרה לתעל את יצרנותם לטובת חברות אזרחיות, שבראש חלק מהן עומדים בוגרי המערכת הביטחונית. לעומת זאת, בטורקיה אין מסורת כזאת וגם לא תהליך דומה של הפריה הדדית בין המערכת הצבאית ובין השוק האזרחי. כך, גם כאשר הממסד הביטחוני הטורקי מאתר גורם איכותי במערכת, רוב הסיכויים הם שהוא יעשה בו שימוש רק אם אותו גורם יבחר להישאר בתוך מסגרת התעשיות הביטחוניות שבבעלות המדינה, ואלו פועלות על פי רוב תחת אילוצים ותכתיבים ארגוניים וביורוקרטיים המעכבים צמיחה.[36]

חרף הנאמר לעיל ניתן לטעון, ובצדק רב, כי אין הכרח בקיומם של יחסי צבא־חברה הדוקים כדי ליצור שכבת הון אנושי איכותית לענף הסייבר. הגם שמדובר בציר המצמיח פיתוח, מדינות שונות ידעו להגיע בעבר ובהווה להישגים גם ללא הצורך למצוא פתרון לאיומים ביטחוניים. אלא שבמקרה הטורקי, המחקר והפיתוח טעונים שיפור ניכר גם בשוק האזרחי. ההשקעות של הממסד הטורקי, כמו גם של הפירמות הפרטיות, במחקר אקדמי או מסחרי הינן דלות ביותר. לכך יש לצרף את העובדה כי משכורותיהם של החוקרים באקדמיה בטורקיה אינן גבוהות, דבר הפותח פתח לרמת איכות אקדמית נמוכה. מדובר בתרבות ארגונית מוסדית שאינה מהווה קרקע פוריה לפיתוחים, לשיתוף רעיונות, ליצירת מידע וידע וכדומה, שהם אבני יסוד להתקדמות וצמיחה בתעשיית הסייבר.[37]

הן הממסד הטורקי והן בעלי ההון בטורקיה לא עשו ככלל די לאורך השנים כדי לטפח מחקר, פיתוח ויזמות טכנולוגית. חשוב להדגיש כי האוליגרכים הטורקים אמנם דואגים להזרים הון חזרה לציבור ולשוק הטורקי, אך רוב התרומות וקרנות ההשקעה מנותבות להקמת בתי ספר, אוניברסיטאות ומוזיאונים. אין בנמצא בטורקיה מנגנון ממוסד להעצמת מחקרים אקדמיים על ידי השוק הפרטי, לא כל שכן לעידוד יזמות טכנולוגית באשר היא. לשם המחשה, הפארק הטכנולוגי הראשון בטורקיה נוסד בשנת 1985 על ידי האוניברסיטה הטכנולוגית באיסטנבול ולשכת המסחר העירונית. מוסד דומה הוקם באנקרה רק בשנת 1991, על ידי האוניברסיטה הטכנולוגית של המזרח התיכון (METU). לעומת זאת, פרופסור רייזמן מצביע

36 Hall of Soskice "Varieties of Capitalism"; Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 5-8.

37 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 5-8, 10-12.

על כך שמכון ויצמן – מוסד שהוקם בישראל בין השאר במטרה לייצא ממצאים אקדמיים לשוק המסחרי – החל לפעול כבר בשנות החמישים של המאה העשרים.[38]

מצאתי לנכון לסכם דיון זה בציטוט של פרופסור רייזמן: "הגם שטורקיה שינתה את מדיניותה משנת 1923 והתניעה רפורמות נרחבות, היא לא שינתה את [אופי] אנשיה, השקועים במסורתיות. היסטורית, המשכילים הטורקים בתקופת האימפריה העות'מאנית היו מנהלים וביורוקרטים, אך לא היו בעלי 'ראש עסקי',[39] ובמיוחד לא בעלי אוריינטציה טכנית".[40]

## סיכום

עיון במקורות שונים מראה כי הדיון האקדמי בסוגיית הסייבר בטורקיה, לפחות בשפה האנגלית, טרם הגיע לבשלות. הגם שניתן למצוא ברשת האינטרנט לא מעט דיווחים חדשותיים ותקשורתיים על תקיפות סייבר שחוותה טורקיה, ניכר כי הדיון בכך מסתכם על פי רוב במאמרי דעה שנכתבים על ידי גורמים שונים. על כן, בבואי לבחון את עיקרי התהליכים שטורקיה חווה בתחום הסייבר, בחרתי להתמקד באתגרים הניצבים בפניה, ובעיקר בבעיית הליבה, שבראייתי היא החוסר בהון אנושי איכותי מהיצע מקומי. לשם כך, בחרתי להשעין את ניתוח תמונת המצב בעיקר על ממצאיו ומסקנותיו של פרופסור ארנולד רייזמן, לצד שימוש במקור נוסף – ממצאי דוח ארגון OECD משנת 2004, שהתמקד במחקר הכלכלה הטורקית ובמתן הצעות לפיתוחה. הגם שהדיון האקדמי והניתוח שפרסתי בעמודים אלה אינם שלמים, הם מצביעים על הצורך להעמיק בהבנת יסודותיה של התרבות הטורקית כדי לפענח את הבסיס לאתגרים העומדים בפני פיתוח תעשיית הסייבר המקומית.

ההבחנה שהצעתי בין ההשפעה של המדיניות הטורקית הריכוזית על האתגר המדיני־ביורוקרטי מצד אחד ועל אתגר התרבות הארגונית מצד שני, הינה הבחנה מלאכותית בלבד לצורך הבהרת הטיעון הלוגי. למעשה, מדובר ביחסי גומלין סימביוטיים בין תרבותה של החברה הטורקית ובין מדיניותן של ממשלותיה. תמונת המצב החברתית־כלכלית הנוכחית במדינה מראה שאחוז גדול מהאוכלוסייה הטורקית מתגורר במרחב הכפרי ומשמר חברה מסורתית, אסלאמית ופטריארכלית, דבר המשפיע על מדיניותן ותפקודן של הממשלות הטורקיות.

דבריה של הפרופסורית דילק צ'טינדמר מיטיבים להעביר את המסר: "[...] האופק התעסוקתי בראי בוגרי האוניברסיטאות [הטורקיות] כולל תעסוקה בחברות

38 שם, עמ' 12, 15.

39 רייזמן משתמש במונח "Business-minded". בכך הוא מכוון להערכתי לחשיבה עסקית ויזמות בשוק החופשי.

40 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 8-9.

גדולות, שכן הקמת פירמה פרטית נחשבת לסיכון גדול. על כן, אין בנמצא מסורת של יזמות פרטית".[41] משפט זה מבטא היטב את המסקנה המרכזית העולה מהמאמר, לפיה כדי לטפח הון אנושי איכותי בקהילת הסייבר הטורקית יש צורך בסביבה הבשלה לכך, קרי תשתית המעודדת יוזמה וחדשנות. אולם נראה כי טורקיה אינה "חממה" המעודדת יזמות פרטית, אשר על פי הנוסחה המקובלת הינה תנאי הכרחי להעצמת אנשי היי־טק ומהנדסים פורצי דרך. יתר על כן, כאשר טורקיה נדרשת לפתרונות טכנולוגיים ייחודיים, סביר להניח שתבחר בייבוא ידע חיצוני, וכול אחד משחקני המשולש מדינה־אוליגרכים־חברה יעדיף לנתב את ההון האנושי לחברות הגדולות והיצרניות, בעוד שהמקום למקוריות וליזמות, ההכרחיות בעולם הסייבר, יישאר מוגבל.

41 שם, עמ' 14.