במה טכנולוגית

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

המעוז הדיגיטלי: "המולדת הקיברנטית" של טורקיה והמעבר לריבונות סייבר

הנרי סגמן[1] | 2 ביוני, 2026

תקציר

המושג הטורקי "המולדת הקיברנטית" (Siber Vatan), אשר נוסח לראשונה מבחינה לשונית ודוקטרינרית בראשית שנות ה-20 של המאה ה-21 וזכה לאימוץ מפורש על ידי הנשיא ארדואן, הוא שיאה של שלישייה אסטרטגית (Triad) שתחילתה ב"מולדת הכחולה" (Mavi Vatan) ו"מולדת השמיים" (Gök Vatan). הדוקטרינה מבטאת תפיסה של המרחב הקיברנטי כטריטוריה לאומית. בעוד שבעולם המערבי מקובל לראות במרחב הסייבר ישות מבוזרת הכוללת רבדים לוגיים וערטילאיים של קוד ומידע, ההמשגה הטורקית יוצרת "טריטוריאליזציה" מכוונת של המרחב; היא מדגישה דווקא את האקוסיסטם הפיזי והארגוני המורכב מתשתיות מוחשיות כגון שרתים, חוות נתונים וסיבים אופטיים הממוקמים בגבולות המדינה. מנגד, המושג ריבונות (Egemenlik) מיושם כאן במובנו הקלאסי – הסמכות הבלעדית של המדינה לחוקק, לאכוף ולמנוע התערבות חיצונית. החיבור ביניהם יוצר את דוקטרינת Siber Egemenlik (ריבונות קיברנטית), המעתיקה את לוגיקת הגנת הגבולות המסורתית אל נכסי המחשוב הלאומיים, אשר מתורגמת לצעדים מעשיים כגון לוקליזציית נתונים ואוטרקיה טכנולוגית. המדיניות הלאומית ותוכנית הפעולה לאבטחת סייבר (2024-2028), הקמת מנהלת הסייבר (ינואר 2025) וחקיקת חוק מס' 7545 (מארס 2025) מהווים שלב חשוב במיסוד דוקטרינת "המולדת הקיברנטית".

מאמר זה בוחן את האירועים שמצביעים על כך שטורקיה מקדמת תהליך הדרגתי של "הינתקות ריבונית" (Sovereign Decoupling) – ממצב של תלות בטכנולוגיה מערבית ובמסגרת ברית נאט"ו לעבר בניית יכולת סייבר עצמאית ולמעצמת סייבר אזורית עצמאית, המסוגלת לבודד את המרחב הדיגיטלי שלה מהשפעה זרה ובו בזמן להקרין עוצמה דיגיטלית אסימטרית אל מעבר לגבולותיה. להשלכות על הביטחון האזורי – בפרט עבור ישראל, יוון, קפריסין ויכולת הפעולה המשותפת (Interoperability) של נאט"ו – נודעת משמעות רבה, המחייבת בחינה אסטרטגית קפדנית.

חלק ראשון: התשתית הדוקטרינרית

תפיסת הביטחון הלאומי המשתנה של טורקיה במרחב הדיגיטלי מהווה את שיאו של רצף דוקטרינרי קוהרנטי, המרחיב את מושג ה"מולדת" (Vatan) מיסודותיו הטריטוריאליים המסורתיים למרחבים חדשים של שליטה ריבונית. המשכיות זו ממסגרת את 'המדיניות הלאומית ותוכנית הפעולה לאבטחת סייבר (2024-2028)' לא כחדשנות מדינית מבודדת, אלא כהרחבה הלוגית הנוכחית של שלשת ה"מולדת": "המולדת הכחולה" (Mavi Vatan), "מולדת השמיים" (Gök Vatan) ו"המולדת הקיברנטית" (Siber Vatan). כל מרכיב בשלישייה זו מייצג תביעת ריבונות חד-צדדית (Unilateral) על מרחב נפרד אך קשור הדדית –ימי, אווירי ודיגיטלי. הגדרות מורחבות אלו של מולדת אינן מבוססות על קונצנזוס או על משפט בינלאומי מקובל, אלא מהוות מהלכים מדינתיים חד-צדדיים שנועדו להקרין עוצמה ולערער על הגדרות הריבונות

---

[1] הנרי סגמן הוא סטודנט לתואר שני במחלקה למדע המדינה באוניברסיטת בר-אילן ומתמחה במכון למחקרי ביטחון לאומי

הקלאסיות. במסגרת זו, פריצות למרחב הדיגיטלי מוגדרות מחדש באופן דוקטרינרי כאיומים על השלמות הלאומית, בדומה להפרות טריטוריאליות מסורתיות.

מקורו של הרצף הדוקטרינרי בחידושים לשוניים ואסטרטגיים הקשורים באסרטיביות האזורית של טורקיה, בייחוד בתגובה לסכסוכים ימיים ואוויריים בים האגאי ובמזרח הים התיכון. כפי שנותח במחקרים בלשניים, ביטויים אלו צמחו על רקע משברים מול יוון, והם משקפים שינוי חברתי ומוסדי לכיוון הגנה אקטיבית על מרחבים לאומיים מורחבים. דוקטרינת "המולדת הכחולה", שנוסחה לראשונה על ידי אדמירל (בדימוס) ג'ם גורדניז ב-2006, תופסת את המים הטריטוריאליים, את המדף היבשתי ואת האזורים הכלכליים הבלעדיים של טורקיה בשלושת הימים (השחור, האגאי והתיכון) כחלק בלתי נפרד מטריטוריית המולדת.

באופן אנלוגי, "מולדת השמיים" מרחיבה את הריבונות כלפי מעלה, אל המרחב האווירי שמעל המרחבים היבשתיים והימיים. היא משלבת עליונות אווירית המחוזקת על ידי טכנולוגיות כטב"ם מקומיות כמעטפת הגנה מעל "המולדת הכחולה".

"המולדת הקיברנטית" משלימה את השלישייה על ידי העתקת לוגיקת המולדת אל מרחב הסייבר. כפי שהצהיר הנשיא רג'פ טאיפ ארדואן, הריבונות הדיגיטלית מרחיבה את "הגנת המולדת" (Vatan Savunması) כך שתכלול רשתות, נתונים ותשתיות: "נרחיב את הגנת המולדת שלנו כך שתכלול את המולדת הקיברנטית בעולם הדיגיטלי, בדיוק כפי שאנו עושים עם המולדת הכחולה במרחב הימי". מסגור זה רואה במרחב הקיברנטי לא נחלת הכלל גלובלית חסרת גבולות אלא מרחב ריבוני שבו חומרה, תוכנה או זרמי נתונים זרים מהווים פוטנציאל לכיבוש או חדירה – הד לדימוי הסוס הטרויאני, המשמש לתיאור תלות בטכנולוגיות שאינן מקומיות.

אסטרטגיית 2024-2028 ממסדת מעבר זה מהגנה על רשתות לריבונות קיברנטית אקטיבית. המסמך הרשמי, שפורסם בצו נשיאותי בספטמבר 2024, מדגיש שישה יעדים אסטרטגיים: חוסן קיברנטי; הגנת סייבר אקטיבית; אבטחת סייבר מוכוונת אדם; שימוש בטוח בטכנולוגיה; מאבק באיומים מבוסס טכנולוגיה לאומית/מקומית; ושיתוף פעולה בינלאומי לקידום מעמדה הגלובלי של טורקיה. מסגור זה מזכיר במאפיינים מסוימים את מודל "הריבונות הדיגיטלית" הסיני, השם דגש על רתימת המשק הפרטי והאזרחי לטובת יעדים לאומיים, וידוא שליטה ממשלתית הדוקה על מרכזי הנתונים ומינוף הדיגיטציה כמקור עוצמה בזירה הבינלאומית. ייחודו של מסמך זה, המבדיל אותו ממתווי מדיניות פנימיים שגרתיים במערב, טמון בטרנספורמציה המבצעית שלו: הוא אינו מסתפק בהגדרת יעדים תאורטיים אלא מכפיף את כלל המגזרים האזרחיים והקריטיים במדינה לחובת רכש של טכנולוגיה מקומית-לאומית, וממסד את סייבר המדינה תחת שליטה נשיאותית ישירה וריכוזית כעניין ביטחוני קיומי.

ההתפתחויות העיקריות כוללות את הקמת מנהלת הסייבר (Siber Güvenlik Başkanlığı) בהוראת צו נשיאותי מס' 177 ב-8 בינואר 2025 כרשות מרכזית בעלת אוטונומיה פיננסית, האמונה על רגולציה ואכיפה. בעקבותיה נחקק חוק אבטחת הסייבר מס' 7545 (מארס 2025), המטיל חובות מחמירות על מפעילי תשתיות קריטיות ומשית סנקציות חריפות על הפרות – צעד המדגיש כי נכסים דיגיטליים הם טריטוריה ריבונית המחייבת אמצעים מניעתיים.

נכון לשנת 2026, שינויים מוסדיים אלו, בשילוב המיקוד של האסטרטגיה בהרתעה ובטכנולוגיות לאומיות, מציבים את "המולדת הקיברנטית" כאבן הראשה של הגנת המולדת הרב-ממדית של טורקיה. להתפתחות זו השלכות נרחבות על היציבות האזורית, על יכולת הפעולה המשותפת עם נאט"ו (NATO) ועל התחרות בין המעצמות במרחב הקיברנטי.

חלק שני: האבולוציה ההיסטורית של עמדת הסייבר הטורקית (תשתיות בתקופה שלפני 2024)

בהקשר המחקרי והאסטרטגי הנוכחי, המונח סייבר (Cyber) או המרחב הקיברנטי אינו מצטמצם לטווח הווירטואלי של רשת האינטרנט בלבד. הוא מתייחס לאקוסיסטם שלם המשלב תשתיות פיזיות (שרתים, חוות נתונים וסיבים אופטיים), נכסים דיגיטליים, מערכות מידע ומחשוב וקוד תוכנה – כל אלה מאפשרים הפעלה, זרימה, אחסון והצפנה של נתונים לאומיים.

המעבר הטורקי לריבונות קיברנטית אקטיבית במסגרת "המולדת הקיברנטית" לא צמח בחלל ריק, אלא נבנה על בסיס שני עשורים של התפתחויות מוסדיות, משפטיות ואסטרטגיות בתחום אבטחת הסייבר. מסלול היסטורי זה משקף תמורה הדרגתית – מבניית מודעות ראשונית ותגובה אקטיבית עד אירועים לתיאום לאומי מובנה, אינטגרציה צבאית ודגש על יכולות מקומיות – אשר הכשירו את הקרקע הדוקטרינרית לרצף ה"מולדת" הרב-ממדי שתואר בחלק הקודם.

שורשי מדיניות הסייבר הטורקית נעוצים בשלהי שנות ה-90. בשנת 1997 הקים המכון הלאומי למחקר אלקטרוניקה וקריפטולוגיה (UEKAE) של מועצת המחקר המדעי והטכנולוגי של טורקיה (TÜBİTAK) את היחידה לאבטחת מערכות מידע (BSG), שהתמקדה בפיתוח תקני אבטחה לתשתיות קריטיות. זהו הציון המוסדי הראשון לאיומי סייבר כעניין לאומי. באמצע העשור הראשון של שנות ה-2000 התעצמה המודעות בדרג המדינתי: חוק החתימה האלקטרונית מ-2004 (חוק מס' 5070) הניח את התשתית המשפטית לעסקאות דיגיטליות מאובטחות, בעוד שהקמת נשיאות תקשורת הטלקומוניקציה (TİB) ב-2006 הציגה פיקוח מרכזי על תוכני אינטרנט ופעילות מזיקה. ב-2008 החלה הרשות לטכנולוגיות מידע ותקשורת (BTK) בעבודת תשתית להקמת מבנים הדומים לצוות תגובה לאירועי מחשב (CERT) לאומי.

אבן דרך מכרעת נרשמה בשנים 2010-2011, כאשר איומי הסייבר שולבו במפורש במסמכי הביטחון הלאומי. טורקיה חתמה על אמנת מועצת אירופה בדבר פשעי סייבר (אמנת בודפשט) בשלהי 2010, ומסמך מדיניות הביטחון הלאומי מאותה שנה כלל את אבטחת הסייבר כעדיפות עליונה. תרגיל הסייבר הלאומי הראשון נערך ב-2011, במקביל למסגור איומי הסייבר על ידי המועצה לביטחון לאומי (MGK) בתוך פרמטרים רחבים יותר של ביטחון לאומי. עד 2012 הקים מכון TÜBİTAK BİLGEM מכון עצמאי לאבטחת סייבר לחיזוק המחקר, הפיתוח והייעוץ המדינתי.

בשנים 2013-2016 התמסדה המסגרת המקיפה הראשונה של טורקיה. בינואר 2013 פורסמה 'האסטרטגיה הלאומית הראשונה לאבטחת סייבר ותוכנית הפעולה ל-2013-2014' תחת הנהגת ה-BTK. מסמך זה מיסד ישויות מרכזיות: המרכז הלאומי לתגובה לאירועי מחשב (USOM) הוקם בתוך ה-BTK לתיאום התגובה במגזר הציבורי, בתשתיות קריטיות ובמגזר הפרטי. במקביל, הקמת צוותי תגובה לאירועי סייבר (SOME) הפכה לחובה במוסדות ציבוריים ובגופים פרטיים חיוניים. צבא טורקיה (TSK) מיסד את פיקוד הגנת הסייבר שלו ב-2013, ובכך שילב יכולות סייבר בדוקטרינה הצבאית. זהו איתות ברור לכך שאיומי הסייבר אינם מוגבלים עוד לתחום האזרחי, אלא נתפסים כמרכיב בלוחמה היברידית. תהליך מרכזי זה הבשיל בסוף 2014, כאשר הפרלמנט הטורקי אשרר רשמית את אמנת בודפשט (בחוק מס' 6533), והיא נכנסה לתוקף מלא במדינה ב-2015.

אסטרטגיות הסייבר בשנים 2016-2023 העמיקו את ההתמקדות בהגנה על תשתיות קריטיות, פיתוח טכנולוגיות סייבר לאומיות, שיפור המודיעין על איומים והשקעה בפתרונות מקומיים לטכנולוגיות מפציעות כמו 5G והאינטרנט של הדברים (IoT).

נתיב אבולוציוני זה – ממודעות מבוזרת (1997-2012) דרך מיסוד (2013-2016) ובניית יכולות (2016-2023) – יצר את התנאים המוקדמים לשינוי הפרדיגמה הגלום במסגרת 2024-2028. השלישייה הדוקטרינרית של ה"מולדת" סיפקה את הגשר האינטלקטואלי: כשם ש"המולדת הכחולה" ו"מולדת השמיים" הרחיבו את תביעות הריבונות למרחב הימי והאווירי, "המולדת הקיברנטית" ממסגרת מחדש את מרחב הסייבר כטריטוריה ריבונית הדורשת עמידה אקטיבית מול השפעות "כיבוש" זרות.

האסטרטגיה הלאומית ותוכנית הפעולה לאבטחת סייבר 2024-2028, שפורסמה בצו נשיאותי ב-7 בספטמבר 2024, מהווה את שיאו של התהליך ומגדירה, כאמור, שישה יעדים אסטרטגיים: חוסן קיברנטי; הגנה אקטיבית והרתעה; אבטחת סייבר ממוקדת אדם (המתבטאת בגיוס חברתי רחב ובניית מערך מתנדבים לאומי); שימוש בטוח בטכנולוגיה; מאבק באיומים באמצעות טכנולוגיות מקומיות; וחיזוק המותג הבינלאומי של טורקיה בסייבר.

מבחינה מוסדית, יישום האסטרטגיה הואץ עם הקמת מנהלת הסייבר בינואר 2025 (צו נשיאותי מס' 177), גוף בעל אוטונומיה פיננסית תחת לשכת הנשיא. מהלך זה חוזק באמצעות חוק אבטחת הסייבר מס' 7545 (מארס 2025), המטיל חובות על מפעילים קריטיים, מחייב דיווח על אירועים ומקים את 'מועצת אבטחת הסייבר' לתיאום מדיניות ברמה הגבוהה ביותר. מהלך זה מדגיש את נכונותה של אנקרה לשלם מחיר טכנולוגי אפשרי, שכן הסתמכות בלעדית על פיתוחים מקומיים נוטה לעיתים לייצר מוצרים מתקדמים פחות מאלו של השוק הגלובלי, ובלבד שתהיה לה עצמאות מבצעית ואי-תלות במדינות זרות.

במבט כולל, התפתחויות אלו ממסדות את המעבר מהגנת רשת תגובתית להגנה ריבונית אקטיבית במרחב הדיגיטלי, תוך ראיית תלות טכנולוגית זרה כנקודת תורפה פוטנציאלית ותעדוף חלופות מקומיות לשמירה על אוטונומיה תשתיתית ולוקליזציה של נתונים (Data Localization). תשתית היסטורית זו מדגישה כי העמדה האקטיבית הנוכחית של טורקיה היא נקודת הקצה של הבשלת מדיניות עקבית, המיושרת כעת באופן מלא עם דוקטרינת ה"מולדת" לריבונות רב-ממדית מקיפה.

חלק שלישי: ריכוזיות מוסדית (המהפך הביצועי)

הארכיטקטורה המוסדית העומדת בבסיס "המולדת הקיברנטית" מייצגת מעבר מפיקוח מיניסטריאלי (של משרדי הממשלה) לשליטה נשיאותית ישירה במרחב הסייבר. ריכוזיות זו משקפת מגמות רחבות יותר של התחזקות הרשות המבצעת בטורקיה מאז משאל העם החוקתי ב-2017, וממסגרת מחדש את המשילות הדיגיטלית כצורך ביטחוני קיומי ולא כעניין טכני או תשתיתי גרידא. המעבר מעלה את איומי הסייבר לרמה של פגיעה בשלמות הטריטוריאלית, מיישר קו בין מרחב הסייבר לשלישיית ה"מולדת" ומצדיק התערבות מדינתית מוגברת.

מבחינה היסטורית, תיאום אבטחת הסייבר היה באחריות משרד התחבורה והתשתיות (לשעבר משרד התחבורה, הספנות והתקשורת), אשר פיקח על פיתוחן ויישומן של אסטרטגיות הסייבר הלאומיות לאורך השנים. גופים כמו הרשות לטכנולוגיות מידע ותקשורת (BTK) והמרכז הלאומי לתגובה לאירועי מחשב (USOM) פעלו בתוך המערכת המיניסטריאלית הזו, תוך התמקדות בתגובה לאירועים, תיאום וסטנדרטים טכניים.

מבנה זה עבר ארגון מחדש יסודי בראשית שנת 2025. ב-8 בינואר הוקמה מנהלת הסייבר הלאומית של טורקיה (Siber Güvenlik Başkanlığı)[2] – גוף בעל אוטונומיה פיננסית ומנהלית הכפוף ישירות לנשיאות הרפובליקה של טורקיה. מהלך זה ניתק את משילות הסייבר מהמשרדים המגזריים והציב אותה תחת סמכותה המיידית של הרשות המבצעת. המנדט של המנהלת כולל רגולציה, ניתוח סיכונים, קביעת סטנדרטים, הסמכה, ביקורת, תיאום אירועים באמצעות צוותי תגובה (SOME)[3] ושיתוף פעולה בינלאומי – סמכויות המאפשרות אכיפה פרואקטיבית של עקרונות הריבונות במגזר הציבורי והפרטי כאחד.

תהליך ריכוז הסמכויות ומיסוד המרחב הדיגיטלי כצורך ביטחוני קיומי הגיעו לשיאם בחוק אבטחת הסייבר הלאומי,[4] שפורסם ב-19 במארס 2025. חקיקה זו מעניקה תוקף משפטי ומבצעי מקיף לדוקטרינת המולדת הקיברנטית באמצעות מערכת חובות מוגדרת ומנגנוני אכיפה וכפייה נרחבים. החוק מחיל חובות דיווח, רגולציה ואבטחה מחמירות על מוסדות ציבור, ארגונים מקצועיים וישויות משפטיות או פרטיות הפועלות במרחב הקיברנטי הטורקי.

ההוראות העיקריות כוללות:

הגנה על תשתיות קריטיות: מפעילים במגזרים כגון אנרגיה, פיננסים, טלקומוניקציה, בריאות ותחבורה – שיוגדרו על ידי מועצת אבטחת הסייבר – חייבים ליישם אמצעי אבטחה מאושרים על ידי הנשיאות, לדווח על פרצות ואירועים באופן מיידי ולרכוש מוצרי ושירותי סייבר אך ורק ממומחים או חברות שהוסמכו על ידי הנשיאות. עקרון ליבה בחוק קובע כי "במאמצים להבטחת אבטחת סייבר, תינתן עדיפות ראשונה למוצרים מקומיים ולאומיים".

סמכויות ביקורת ואכיפה: לנשיאות מוקנית הסמכות לבצע או להורות על בדיקות באתר, לגשת למידע, למסמכים, לתוכנה, לנתונים ולחומרה, וכן להטיל סנקציות חמורות על אי-ציות. מחדלים בשיתוף פעולה או בהגנה עלולים להוביל למאסר (שנה עד חמש שנים, בהתאם לעבירה), לקנסות שיפוטיים או לקנסות מנהליים של עד חמישה אחוזים ממחזור המכירות ברוטו של ישויות מסחריות.

שליטה על ישויות סייבר כמו מיזוגים, פיצולים, העברת מניות או שינויי שליטה בחברות אבטחת סייבר מחייבים אישור נשיאותי מראש. גם יצוא של מוצרי סייבר מחייב אישור, מה שמחזק את השליטה הלאומית על נכסים דיגיטליים אסטרטגיים.

---

[2] הצו הנשיאותי מס' 177, שפורסם ברשומות הרשמיות של הרפובליקה הטורקית (Resmi Gazete) ב-8 בינואר 2025, הגדיר את הקמת המנהלת כחלק מרה-ארגון של ביטחון המולדת. הצו מעניק לראש המנהלת סמכויות כמו של שר, ומחליף את המבנה המבוזר הקודם שהיה תחת משרד התחבורה והתשתיות.

[3] המונח SOME מייצג את *Siber Olaylara Müdahale Ekipleri* (צוותי תגובה לאירועי סייבר). אלו הן יחידות תקינה ואכיפה הפועלות ברמה הלאומית (USOM)וברמה המגזרית/ארגונית, ותפקידן להוות קו הגנה ראשון ותיאום מיידי מול מנהלת הסייבר בעת מתקפת סייבר על תשתיות קריטיות.

[4] חוק אבטחת הסייבר מס' 7545 אושר באספה הלאומית הגדולה של טורקיה (TBMM) ופורסם ברשומות ב-19 במארס 2025. החוק מסדיר את סמכויות האכיפה, הקנסות והסנקציות המנהליות שיכולה מנהלת הסייבר להטיל על גופים ציבוריים ופרטיים שאינם עומדים בתקני אבטחת המידע הלאומיים, ומהווה את התשתית המשפטית להגדרת הריבונות הדיגיטלית של המדינה.

מועצת אבטחת הסייבר: המועצה, המורכבת מבכירים בממשל, מיישבת סכסוכים בין-מוסדיים, מפקחת על מפת הדרכים הטכנולוגית של תחום הסייבר ומגדירה תשתיות קריטיות, תוך הבטחת תאימות מלאה למדיניות הרשות המבצעת.

שינוי מוסדי זה – מהפיקוח המיניסטריאלית לזה הנשיאותי מסמן את המהפך בניהול הסייבר בטורקיה: המרחב הדיגיטלי אינו מוסדר עוד כתשתית אזרחית בלבד אלא מוגדר מחדש כטריטוריה ריבונית חיונית. ייחודו של שינוי תפיסתי זה טמון בהבנה הממסדית כי מרחב הסייבר אינו רק זירת הגנה פסיבית אלא גם ממד לחימה מבצעי המשפיע ישירות על שדה הקרב הקינטי. כפי שמציין דוח 'האקדמיה הלאומית למודיעין' של טורקיה (Milli İstihbarat Akademisi) ממאי 2026, כלי לוחמת סייבר הפכו לגורמים המשיגים תוצאות אופרטיביות ישירות; תקיפת רשתות פיקוד ושליטה, מערכות חיישנים (ISR) ותשתיות עיבוד נתונים נתפסת כבעלת פוטנציאל לשתק את הכשירות המבצעית של היריב גם ללא אפקט קינטי.

תובנה צבאית זו היא שמניעה את אנקרה לזנוח את גישת הגנת הסייבר הדפנסיבית המסורתית לטובת תפיסה פרואקטיבית, הכוללת יכולות שיבוש, סיכול ומתקפת נגד כחלק בלתי נפרד מכוח הלחימה הלאומי. בעקבות זאת, שימוש בחומרה או בתוכנה זרה במגזרים קריטיים נתפס כסיכון אסטרטגי פוטנציאלי לחדירה חיצונית, מה שמחייב פיתוח חלופות מקומיות ולוקליזציה של נתונים (אחסון מידע בגבולות המדינה). מינויו של אומית אונאל (Ümit Önal), מנכ"ל טורק טלקום לשעבר, לראש המנהלת באוקטובר 2025, מדגיש עוד יותר את השילוב בין השליטה המדינתית למומחיות מהמגזר הפרטי ביישום דוקטרינה זו.

נכון לאמצע 2026, רפורמות אלו עיגנו את הריבונות הקיברנטית הפרואקטיבית, כאשר המנהלת אוכפת ביקורות, הסמכות ומנדטים המתעדפים טכנולוגיות לאומיות. בכך היא מיישרת את העוצמה המוסדית עם הרצף הדוקטרינרי של "המולדת הכחולה" ו"מולדת השמיים"). ריכוזיות זו מגבירה את החוסן מול איומים היברידיים, אך מעוררת שאלות בנושאי פיקוח, פרטיות ויכולת פעולה משותפת עם בעלות ברית כגון נאט"ו.

חלק רביעי: המגן המקומי (שרשרת האספקה כנשק)

חתירתה של טורקיה למימוש דוקטרינת המולדת הקיברנטית חורגת מעבר למסגור דוקטרינרי וריכוזיות מוסדית; היא מהווה אסטרטגיה מכוונת של אוטרקיה (עצמאות כלכלית) טכנולוגית במרחב הדיגיטלי. "מגן מקומי" זה שואף להקים אקוסיסטם של אבטחת סייבר ב"לולאה סגורה" (Closed-loop), כזה המבודד תשתיות קריטיות, רשתות צבאיות וזרימת נתונים לאומית מתלות חיצונית, שעלולה לשמש וקטור להתערבות זרה, דלתות אחוריות (Backdoors) או "מתגי השבתה" (Kill-switches).

באמצעות מתן עדיפות לטכנולוגיות "מקומיות ולאומיות" (Yerli ve Milli) שואפת טורקיה לחמש את שרשרת האספקה שלה, להפוך נקודות תורפה פוטנציאליות לעוצמה ריבונית וליישר קו בין מרחב הסייבר לבין התביעות האקטיביות של "המולדת הכחולה" ו"מולדת השמיים". ניסיון בידוד זה מתעצב ישירות מול מפת העוצמה העולמית והאזורית בתחום, כאשר אנקרה שואפת לצמצם את חשיפתה הן לשליטה התשתיתית והטכנולוגית של ארצות הברית) בתחומי הענן.

הדחף לעצמאות טכנולוגית מוחלטת מעוגן באסטרטגיית הסייבר הלאומית (2024-2028), המציינת במפורש את ה"מאבק באיומי סייבר באמצעות טכנולוגיות מקומיות ולאומיות" כאחד משש יעדיה האסטרטגיים. יעד זה מדגיש את צמצום התלות הזרה באמצעות חדשנות מקומית ואימוץ פתרונות לאומיים בכלל המערכת, תוך הדהוד הצורך הביטחוני לראות בחומרה ובתוכנות זרות במגזרים אסטרטגיים איומים סמויים על הריבונות.

ענקיות תעשיית הביטחון הטורקיות ממלאות תפקיד מרכזי במימוש חזון "הלולאה הסגורה". החברות ASELSAN, HAVELSAN ו-STM מובילות את המאמצים לבניית סביבות מחשוב ריבוניות ומאובטחות, כולל תשתיות ענן ברמה צבאית. גופים אלו מפתחים פלטפורמות משולבות התומכות ברשתות מוצפנות ומבודדות לצורכי פיקוד ושליטה, מודיעין ועיבוד נתונים. גישה זו משקפת את פילוסופיית ה"מערכת של מערכות", הניכרת בפרויקט 'כיפת הפלדה' (Celik Kubbe) הטורקי. זוהי רשת הגנה אווירית מקומית רב-שכבתית המשלבת מכ"מים, טילים ומערכות לוחמה אלקטרונית (כמו KORAL ו-VURAL) מתוצרת עצמית. פרויקט זה, שנפרס בהדרגה בשנים 2025-2026, ממחיש כיצד טורקיה מבודדת את עצמה מסיכוני שרשרת האספקה המערבית באמצעות השגת שליטה מקומית מלאה על ארכיטקטורות הגנה. בסוף 2025 נבחנה יכולתה של מערכת הלוחמה האלקטרונית המשודרגת KORAL-II לשבש אותות GPS ו-LTE, ובכך למנוע מהיריב ניווט ותקשורת אמינים. זהו ביטוי פיזי של המולדת הקיברנטית (Siber Vatan) באמצעות שליטה ב"אוויר הדיגיטלי" במרחבים

שבמחלוקת. חוזי העתק בהיקף 6.5 מיליארד דולר שנחתמו בנובמבר 2025 עם החברות המובילות מחזקים מחויבות זו למקורות אספקה מקומיים.

אבן ראשה נוספת של המגן המקומי ואחד המרכיבים העמומים שבו היא הקמתה ושיפורה של תשתית רשות הסמכה לאומית (National Certificate Authority), בעיקר באמצעות המרכז הציבורי להסמכה (Kamu SM), המופעל על ידי TÜBİTAK BİLGEM. רשות זו מנפיקה תעודות אלקטרוניות מאושרות עבור דומיינים ממשלתיים וצבאיים (.gov.tr, .mil.tr). באמצעות השליטה ברשות הסמכה עליונה (Root Certificate Authority - Root CA) משלה, המדינה יכולה לחייב אמצעי אמון בתקשורת פנים-מדינתית על בסיס תעודות מקומיות, תוך עקיפת רשויות הסמכה זרות (כגון גוגל או Let's Encrypt). בראשית 2026 הציגה מנהלת הסייבר את יוזמת 'מגן הנתונים הלאומי', המחייבת אחסון "נתוני אזרחים קריטיים" בשרתים הממוקמים בטורקיה והצפנתם באמצעות אלגוריתמים מקומיים, ובכך השלימה את שכבת הריבונות האחרונה בחומת הנתונים של "המולדת הקיברנטית".

יכולת זו מאפשרת "שקיפות סלקטיבית": זרמי נתונים מוצפנים מקומיים נותרים אטומים בפני גופי מודיעין זרים (כולל בריתות ה-Five Eyes), בעוד שהם ניתנים לניטור מלא על ידי הרשויות הטורקיות באמצעות מפתחות בניהול המדינה. משקיפים בינלאומיים, בהם ה-EFF, ציינו כי שליטה ממשלתית ברשויות הסמכה מאפשרת פוטנציאל לבחינת תעבורה מוצפנת (SSL Inspection), מה שמחזק את גישת "הגן הסגור" של טורקיה בתוך האינטרנט הגלובלי ומאיץ את ההינתקות הריבונית מהסטנדרטים החיצוניים.

אמצעים אלו – עננים מקומיים, שילוב הגנה שכבתי כמו 'כיפת הפלדה' ושליטה ברשות הסמכה לאומית – יוצרים מעוז דיגיטלי עמיד הנשען על עצמו. בשנים 2026-2028, אקוסיסטם זה בלולאה סגורה מציב את טורקיה בעמדת הרתעה מול איומים היברידיים ומקרין עוצמת סייבר אזורית, וזאת במחיר של אתגרי יכולת פעולה משותפת (Interoperability) עם בעלות ברית בנאט"ו, הנשענות על סטנדרטים מערביים. המעבר הופך את שרשרת האספקה לנשק, הממיר תלות טכנולוגית לנקודת תורפה עבור היריב תוך ביצור "המולדת הקיברנטית".

חלק חמישי: מהגנה ל"נוכחות קדמית" (שילוב יכולות התקפיות)

הבשלתה של דוקטרינת המולדת הקיברנטית במסגרת אסטרטגיית הסייבר הלאומית 2024-2028 מסמנת תמורה מבנית עמוקה: מעבר מעמדות מגננתיות בעיקרן לגישה משולבת הכוללת מרכיבים של מבצעי סייבר התקפיים (OCO)[5] והרתעה אקטיבית. בעוד שהשיח הרשמי שומר על התמקדות בהגנה, בחוסן ובמניעה, השפה האסטרטגית והסינרגיות המבצעיות חושפות יכולת מתהווה לפעולות סייבר מוכוונות קדימה – מיצוב מרחב הסייבר כזירה לשיבוש מקדים (Pre-emptive) ולא רק לתגובה. שינוי זה עולה בקנה אחד עם רצף ה"מולדת" הרחב: כשם ש"המולדת הכחולה" ו"מולדת השמיים" תובעות ריבונות מורחבת באמצעות נוכחות אסרטיבית (כגון פטרולים ימיים וגיחות כטב"מים), "המולדת הקיברנטית" חוזה "נוכחות קדמית". מטרה זו נועדה להרתעת יריבים על ידי הצגת היכולת לגבות מחיר במרחב הקיברנטי עוד לפני התממשותם המלאה של האיומים.

אסטרטגיית הסייבר הלאומית (2024-2028) מגדירה במפורש את ה"הגנה הקיברנטית האקטיבית וההרתעה" (Proaktif Siber Savunma ve Caydırıcılık) כאחד משלושת יעדי הליבה שלה. נדבך זה מדגיש פיתוח מנגנונים ל"זיהוי ומניעה של איומי סייבר מראש", תוך חיזוק ההרתעה באמצעות שיפור המודיעין על איומים ותיאום התגובה. פרשנויות רשמיות מציגות זאת כהתפתחות הגנתית, אולם הדגש על "הרתעה" (Caydırıcılık) ומניעה אקטיבית מרמז על סל כלים רחב יותר, הכולל איום אמין בפעולות תגמול או פעולות מקדימות נגד שחקני איום מזוהים. בהקשרים של סכסוך היברידי, שבהם מבצעי סייבר מטשטשים את הגבולות בין שלום למלחמה, שפה זו תומכת ביכולות המאפשרות שילוב התקפי, והדבר מאפשר לטורקיה לגבות מחיר אסימטרי מיריבים מבלי להסלים בהכרח לסף הקינטי.

---

[5] המונח OCO מייצג *Offensive Cyber Operations*(מבצעי סייבר התקפיים). בהקשר הדוקטרינרי הטורקי מדובר בשילוב יכולות שיבוש, חדירה ולוחמה אלקטרונית (EW - Electronic Warfare) המיועדות לנטרול איומים בשטח האויב לפני הגעתם לרשתות הלאומיות, כחלק מתפיסת "הנוכחות הקדמית" הדיגיטלית של המדינה.

מבחינה אמפירית, שילוב זה בא לידי ביטוי בבירור בסנכרון שבין לוחמה אלקטרונית קיברנטית (CEW) לבין פלטפורמות קינטיות, ובפרט מערכות בלתי מאוישות מקומיות. האקוסיסטם הביטחוני של טורקיה, בהובלת גופים כגון ASELSAN (מערכות ל"א ומכ"ם) ו-Baykar (כטב"מי תקיפה מדגמי TB3 ו-Kızılelma), קידם מבצעים רב-ממדיים שבהם חדירות סייבר משלימות תקיפות פיזיות או מקדימות אותן. כך למשל, יכולות CEW מאפשרות דיכוי אלקטרוני של הגנה אווירית (SEAD/DEAD), כולל שיבוש מכ"ם או הטעיה (Spoofing), שיכולים להיות מתוזמנים ל"עיוורון" חיישני היריב שניות לפני פגיעת טיל המשוגר מכטב"ם. מטוס הקרב הבלתי מאויש Kızılelma, שהוכיח בניסויים בסוף 2025 יכולות קרב אוויר-אוויר מעבר לטווח הראייה (BVR) באמצעות טילי Gökdoğan ומכ"ם MURAD AESA, ממחיש את המיזוג הזה: הפרופיל החמקני שלו, האוטונומיה מבוססת ה-AI והשילוב עם חליפות לוחמה אלקטרונית מאפשרים שיבושים מבוססי סייבר מתואמים (למשל, פגיעה בקישורי פיקוד ושליטה) כדי ליצור חלונות הזדמנות לאפקט קינטי.

השתתפותה של טורקיה בתרגילי ה-CCDCOE של נאט"ו ממחישה אף היא את הממד ההתקפי. בתרגיל Crossed Swords 2025 (טאלין, נובמבר 2025) הוכשרו המשתתפים, כולל יחידות סייבר צבאיות מטורקיה, במבצעי סייבר התקפיים בספקטרום מלא בתוך תרחישי משבר וסכסוך סימולטיביים. התרגיל שם דגש על אימוץ מנטליות של זמן מלחמה, שילוב רב-ממדי (סייבר עם כוחות מיוחדים) ותכנון מבצעי לפעולות התקפיות לשיבוש רשתות יריב. מעורבות זו עולה בקנה אחד עם בניית הרתעה אמינה ו"נוכחות קדמית" במרחב הקיברנטי, המשלימה כלים מקומיים כמו מערכות ה-KORAL.

סינרגיה זו בין לוחמה אלקטרונית ליכולות קינטיות מתרחבת למושגים מבצעיים נוספים. בתרחישים אזוריים, כגון מתיחות בים האגאי או במזרח הים התיכון, מבצעי סייבר יכולים לשמש לפגיעה מקדימה ברשתות היריב (למשל, שיבוש שידורי מכ"ם או תקשורת מודיעינית) כדי להקל על נחילי כטב"מים (כמו ה-TB3 הפועלים מספינת ה-TCG Anadolu). יעדי האסטרטגיה בהגנה אקטיבית כוללים חיזוק שיתוף מודיעין איומי סייבר והעלאת כשירותם של צוותי ה-SOME – מרכיבים התומכים בייחוס (Attribution) וברכישת מטרות לשימוש התקפי פוטנציאלי.

נוכחות קדמית זו במרחב הקיברנטי אומנם מגבירה את האוטונומיה האסטרטגית של טורקיה, אך טומנת בחובה סיכונים: פוטנציאל לחישוב מוטעה במבצעי "אזור אפור", סכנת הסלמה בסכסוכים רב-ממדיים ומתחים מול יכולת הפעולה המשותפת עם נאט"ו (שבה נורמות הסייבר ההתקפי נותרות מוגבלות). באמצעות מיסוד ההרתעה האקטיבית בתוך "המולדת הקיברנטית", טורקיה ממצבת את עצמה כשחקנית אזורית המסוגלת לכפייה רב-ממדית, תוך שילוב שיבוש דיגיטלי עם דיוק קינטי להגנה על ריבונותה המורחבת.

ראוי להדגיש כי חוסר הסבירות (או החריגה מהנורמה המערבית המקובלת) בפעולות שתוארו לעיל אינו נעוץ בעצם החתירה לחוסן טכנולוגי או בפיתוח יכולות צבאיות, שהן מטרות לגיטימיות שרוב המדינות המתקדמות חולקות. החריגה טמונה דווקא באופי הכופה והחד-צדדי של יישומן. בעוד שמדינות מערביות מעודדות שימוש בטכנולוגיה מקומית מטעמי ביטחון, אנקרה מחילה רגולציה המשנה את כללי השוק הפרטי: היא כופה רכש לאומי מוחלט כמעט על כלל המגזרים האזרחיים, ומגדירה חומרה ותוכנה זרה כאיום קיומי על הריבונות. יתרה מכך, היא פועלת להשגת שליטה בטווח הדיגיטלי דרך רשות הסמכה עליונה לאומית, בעלת פוטנציאל גישה לתעבורה מוצפנת (SSL Inspection) של אזרחי טורקיה.

חלק שישי: אקוסיסטם של שלוחים (מרחב ההכחשה המדינתית)

דוקטרינת המולדת הקיברנטית של טורקיה פועלת באזור האפור של הסכסוך ההיברידי, שבו קבוצות האקטיביזם (Hacktivism) לאומניות מבצעות פעולות סייבר משבשות, אשר לעיתים קרובות עולות בקנה אחד עם עמדות מדיניות החוץ של טורקיה בעת משברים דיפלומטיים. קבוצות כגון Ayyıldız Tim (צוות כוכב וסהר) ו-Akıncılar (הפושטים) סימנו כמטרות יריבים אזוריים - לדוגמה: ישראל על רקע המתיחות בעזה (הדלפות נתונים לכאורה והטרדות), יוון בסכסוכים בים האגאי (השחתת אתרים ומתקפות DDoS) או שחקנים אחרים הנתפסים כעוינים. הקבוצות משתמשות בטקטיקות ברמת תחכום נמוכה עד בינונית הכוללות השחתת אתרים, הדלפת מידע, מתקפות מניעת שירות (DDoS), פישינג והפצת תעמולה. פעולות אלו מתרחשות לעיתים קרובות במקביל לרטוריקה טורקית רשמית או להחרפת מתחים בילטרליים, ובכך יוצרות אימפקט פסיכולוגי, תהודה תקשורתית ולחץ אסימטרי ללא ייחוס (Attribution) מדינתי ישיר.

אף שאין ראיות ציבוריות חותכות המאשרות הכוונה או שליטה מדינתית ישירה בקבוצות אלו, התזמון שלהן, המטרות והמסרים (המתאפיינים לרוב במסגור לאומני-טורקי או אסלאמיסטי) משקפים תכופות את עמדותיה של אנקרה בנושאי

ריבונות, משקעי עבר היסטוריים או סכסוכים אזוריים. הלימה זו מאפשרת מרחב של הכחשה סבירה (Plausible Deniability): המבצעים יכולים לגבות מחיר מהיריבים בתרחישים באזור האפור, בעוד אנקרה שומרת על מרחק רשמי ומתנערת מפעולות של "שחקנים לא-מדינתיים". המיתוג העצמאי של הקבוצות והיעדר קשרים כספיים או פיקודיים הניתנים לזיהוי מגבירים את יכולת ההכחשה הזו.

אסטרטגיית הסייבר הלאומית (2024-2028) מדגישה את "אבטחת הסייבר הממוקדת אדם" (insan odaklı siber güvenlik), תוך התמקדות במודעות חברתית, חינוך, הכשרה והתנדבות לחיזוק החוסן הלאומי ודיווח על איומים. היבט זה של גיוס אזרחי, הממוסגר כהשתתפות קהילתית הגנתית, עשוי לתמוך בעקיפין באקוסיסטם רחב יותר שבו יחידים בעלי זיקה אידיאולוגית תורמים לאקטיביזם דיגיטלי. עם זאת, לשון האסטרטגיה נותרת הגנתית ואינה תומכת במפורש בפעולות התקפיות או בשימוש בשלוחים (Proxies).

אקוסיסטם מקביל זה של האקטיביזם לאומי מגביר את הגמישות האסטרטגית של טורקיה באזור האפור במהלכיה במזרח הים התיכון, בים האגאי ובמזרח התיכון. במהלך משברים, כגון סכסוכים על תיחום גבולות ימיים עם יוון או מתיחות סביב משאבי אנרגיה, פעולות כאלו יכולות לשחוק את מורל היריב, לחולל כותרות בינלאומיות ולאותת על נחישות מבלי להפעיל את סעיף 5 של אמנת נאט"ו או לחצות את סף התגובה הבילטרלית.

עם זאת, פעילויות אלו טומנות בחובה סיכונים משמעותיים: ייחוס שגוי עלול לעורר הסלמה בלתי מכוונת, לחשוף נקודות תורפה פנימיות אם הקבוצות ייפרצו, או לשחוק את האמון מול בעלות ברית בנאט"ו. נכון לשנת 2026, החפיפה הנראית לעין בין גלי פריצות של אקטיביסטים לבין האינטרסים הטורקיים הרשמיים מדגישה את ההסתגלות למציאות ההיברידית – הקרנת השפעה דיגיטלית בעלות נמוכה במרחבים שבמחלוקת תוך שמירה על ריבונות רשמית.

אקוסיסטם זה של שלוחים מייצג את "חיל החלוץ" של "המולדת הקיברנטית" הניתן להכחשה, שמאפשר לטורקיה לנהל קמפיינים דיגיטליים מתמשכים וזולים במרחבים שבמחלוקת.

חלק שביעי: סיכום – ההינתקות הריבונית (The Sovereign Decoupling)

'המדיניות הלאומית ותוכנית הפעולה לאבטחת סייבר (2024-2028)', שמוסדה באמצעות מנהלת הסייבר וחוזקה על ידי חוק אבטחת הסייבר הלאומי,[6] מייצגת נקודת מפנה מכרעת בעמדה הדיגיטלית של טורקיה. היא מגבשת את המעבר מצרכנית של טכנולוגיות מידע מערביות, המיושרת בעיקר עם נאט"ו, למעצמת סייבר עצמאית השואפת להשגת אוטונומיה אסטרטגית אזורית. דוקטרינת המולדת הקיברנטית, ששורשיה ברצף הדוקטרינרי של שלשת ה"מולדת" (Vatan) – בהתאם לניתוח הלשוני והמושגי של Erdal Aydın – ממסגרת מחדש את מרחב הסייבר לא כמרחב גלובלי משותף אלא כטריטוריה ריבונית המחייבת עמידה אקטיבית, שליטה מקומית ובניית יכולות הגנה עצמאיות.

אבולוציה זו באה לידי ביטוי לאורך כל פרקי המאמר: החל מהבשלה היסטורית וריכוזיות מוסדית תחת סמכות נשיאותית ישירה, דרך הקמת מגן טכנולוגי מקומי באמצעות גופים כגון ASELSAN ו-HAVELSAN ותשתיות הסמכה לאומיות, ועד מעבר מחוסן הגנתי לנוכחות קדמית משולבת הכוללת הרתעה אקטיבית וסנכרון בין יכולות לוחמה אלקטרונית (CEW) לאמצעים קינטיים, והקרנת עוצמה באזור האפור באמצעות שלוחים בעלי יכולת הכחשה. שילוב הרכיבים הללו מאפשר לטורקיה לנתק השפעה זרה בתוך גבולותיה הדיגיטליים באמצעות מנדטים ללוקליזציה של נתונים, תעדוף רכש מקומי ושליטה ברשויות הסמכה, ובו בזמן להקרין "עוצמה דיגיטלית" מעבר להם באמצעות הרתעה התקפית ואקוסיסטם של האקטיביזם.

אף שטורקיה נותרה חברה בנאט"ו, המחויבת להגנה קולקטיבית ומשתתפת בתרגילי הברית, מסגרת "המולדת הקיברנטית" מעניקה לה מרחב תמרון חד-צדדי משמעותי. הדגש של האסטרטגיה על טכנולוגיות לאומיות (2024-2028)

---

[6] חוק אבטחת הסייבר מס' 7545, מארס 2025

מתעדף אוטונומיה ריבונית על פני יכולת פעולה משותפת (Interoperability) מלאה עם סטנדרטים מערביים, בפרט במגזרים קריטיים שבהם תלות זרה מוגדרת מחדש כנקודת תורפה.

הינתקות ריבונית זו, שאינה קרע פורמלי אלא צמצום סיכונים אסטרטגי (Strategic de-risking), משקפת מגמות רחבות יותר במדיניות החוץ הטורקית לעבר איזון רב-וקטורי. מהלך זה מאפשר לאנקרה לקדם אינטרסים לאומיים באופן עצמאי גם כאשר הם חורגים מהקונצנזוס של הברית. ראוי לציין כי הרחקת טורקיה מתוכנית ה-F-35 ב-2019 ביטלה את תלותה בתשתית הדיגיטלית הלוגיסטית האמריקאית (ALIS), ובכך האיצה את המעבר לאקוסיסטם עצמאי עבור מטוסי ה-KAAN וה-Kızılelma – מה שמשחרר את ארכיטקטורות הסייבר מתלות חיצונית ומאפשר שרשרת פיקוד דיגיטלית ריבונית.

להתפתחויות אלו השלכות מעמיקות על הביטחון האזורי והטרנס-אטלנטי. מחד גיסא, יכולת סייבר טורקית אוטונומית עשויה לשפר את ההרתעה כלפי איומים משותפים (למשל, שחקנים היברידיים במזרח הים התיכון או בים השחור). מאידך גיסא, היא טומנת בחובה סיכון לחיכוך בנושאי תאימות, סכסוכי ייחוס בפעולות שלוחים ומתיחות גוברת מול בעלות ברית החוששות מחד-צדדיות. ככל שאי-הוודאות הגיאופוליטית נמשכת – החל מהדינמיקה המשתנה בנאט"ו ועד לתחרות המעצמות בסייבר – "המולדת הקיברנטית" ממצבת את טורקיה כשחקנית היברידית: בעלת ברית אך כזו שנסמכת יותר ויותר על עצמה, הגנתית אך אסרטיבית ויוזמת.

מסגרת 2024-2028 מעגנת חזון של ריבונות דיגיטלית שבו טורקיה שולטת בגורלה הקיברנטי, מבצרת את המולדת במובן המורחב ומקרינה השפעה בתנאים שלה. שאיפה זו להינתקות מחסות טכנולוגית חיצונית, תוך שימור החברות בברית נאט"ו, מדגישה את שאיפתה של אנקרה להגיח כמעצמת סייבר אזורית המסוגלת הן לבידוד והן להקרנת עוצמה בעידן של תחרות רב-ממדית.

במעוז דיגיטלי זה טורקיה מצהירה כי הריבונות משתרעת ללא חיץ מהיבשה, הים והשמיים אל תוך הרשתות המגדירות את העוצמה המודרנית, ומבטיחה כי "המולדת הקיברנטית" תישאר חסינה ומוגנת באופן עצמאי.

דוקטרינת המולדת הקיברנטית והשלכותיה על ישראל

דוקטרינת המולדת הקיברנטית (Siber Vatan) של טורקיה משלימה את תפיסת ה"מולדת" הטורקית העכשווית, לצד ה"מולדת הכחולה" (Mavi Vatan) ו"מולדת השמיים" (Gök Vatan). הדוקטרינה ממסגרת מחדש את מרחב הסייבר כטריטוריה טורקית ריבונית ומרחיבה את ההגנה הלאומית מהממדים הפיזיים אל עבר רשתות דיגיטליות, זרמי נתונים ותשתיות. הדוקטרינה, המעוגנת בתפיסת ריבונות פרואקטיבית ומתופעלת באמצעות 'המדיניות הלאומית ותוכנית הפעולה לאבטחת סייבר (2024-2028)', מסמנת מעבר מהגנת רשת תגובתית לשליטה אסרטיבית.

מעבר זה כולל תעדוף של טכנולוגיות מקומיות, ריכוז סמכויות תחת הנשיאות באמצעות מנהלת הסייבר (שהוקמה בינואר 2025) וחקיקה, הקמת אקוסיסטם בלולאה סגורה (כגון עננים צבאיים ורשות הסמכה לאומית), שילוב יכולות התקפיות במבצעים רב-ממדיים (סייבר ולוחמה אלקטרונית) ומינוף שלוחים מקרב ההאקטיביסטים לפעולות באזור האפור. התפתחות זו מציבה את טורקיה כמעצמת סייבר השואפת לעצמאות אסטרטגית, המבצעת הינתקות (Decoupling) מהסתמכות טכנולוגית מלאה על המערב ונאט"ו, תוך שימור חברותה בברית. הדבר מאפשר לה בידוד מהשפעה זרה (באמצעות לוקליזציה של נתונים ורכש מקומי מחייב), לצד הקרנת עוצמה דיגיטלית (הרתעה אקטיבית ושיבוש מתואם).

דוקטרינה זו מעצימה את הסיכונים האסטרטגיים לישראל על רקע ההידרדרות ביחסים הבילטרליים, שהוחרפה עקב המלחמה בעזה, התמיכה הטורקית בחמאס והרטוריקה של ארדואן, הממסגרת את ישראל כאיום אזורי. להלן ההשלכות העיקריות:

החרפת איומי סייבר ופעילות שלוחים: קבוצות האקטיביזם מזוהות עם המדינה (state-aligned) (כגון Ayyıldız Tim, Akıncılar או התארגנויות פרו-טורקיות דומות) הגבירו את פעילותן נגד מטרות ישראליות בעיתות מתיחות. אירועים בולטים בשנת 2025 כוללים הדלפת נתונים צבאיים לכאורה ומתקפת הטרדה נגד שר הביטחון ישראל כץ, שכללה שיחות וידאו מטרידות וחשיפת מספרו האישי (ספטמבר 2025). פעולות אלו עולות בקנה אחד עם מרכיבי הגיוס האזרחי של דוקטרינת המולדת הקיברנטית, המספקת יכולת הכחשה תוך הפעלת לחץ אסימטרי.

הסלמה באזור האפור סביב טורקיה ושכנותיה: ההרתעה האקטיבית של טורקיה ושילוב יכולות הל"א (למשל, "עיוורון" מכ"מים לפני תקיפת כטב"מים) עלולים לאתגר בעקיפין את חופש הפעולה הישראלי במרחבים משותפים (מזרח הים

התיכון, סוריה). האסרטיביות הטורקית המופעלת באמצעות שלוחים בסוריה או תביעות ימיות נעזרת בכלי סייבר ועלולה לשבש תשתיות אנרגיה, מערכות מודיעין (ISR) או תקשורת ישראלית באזורים שבמחלוקת.

יריבות אסטרטגית והרחבת סל הכלים של טורקיה: הערכות ישראליות רואות בטורקיה איום אסטרטגי גובר (למשל, דוח ועדת נגל משנת 2025), מה שמחייב היערכות לעימות רב-ממדי. בתוך כך גובר העניין המחקרי והמודיעיני בעליית מדרגה של איום הסייבר הטורקית. תקרית הטרדת שר הביטחון כץ מספטמבר 2025 הדגישה את הפגיעות הקיימת ברשתות משניות של ספקי שירות ממשלתיים. איום זה משתלב בסל הכלים המורחב של אנקרה, אשר עלה מדרגה והפך לישיר ואגרסיבי יותר: ארדואן מנסה למסגר את פעולותיה הצבאיות של ישראל באזור לא רק כמאבק מקומי אלא גם כחלק משאיפות התפשטות ישראליות, המאיימות במישרין על יציבות הרפובליקה הטורקית ועל ריבונותה. במקביל, פרויקט 'כיפת הפלדה' ורשות ההסמכה העליונה מצמצמים את האפקטיביות הפוטנציאלית של יכולות סייבר התקפיות מול אנקרה, ומאיצים מרוצי חימוש אזוריים.

דינמיקת בריתות והרתעה: חברותה של טורקיה בנאט"ו, לצד פיתוח יכולות סייבר עצמאיות, יוצרת אומנם אתגרים ליכולת הפעולה המשותפת שלה עם המערב, אך הדואליות הזו – העובדה שהיא גם חלק מברית גלובלית וגם חותרת לאוטונומיה דיגיטלית – מגבירה את כוח המיקוח של אנקרה מול ישראל. סיכוני ההסלמה נותרים גבוהים בתרחישי אזור אפור, אם כי הרתעה הדדית (הנשענת על עוצמת הסייבר הישראלית מול רשת השלוחים הטורקית) עשויה למנוע גלישה לעימות גלוי. ואולם דואליות זו יוצרת מורכבות אסטרטגית נוספת עבור ירושלים: החברות הפורמלית של טורקיה בנאט"ו והצורך המערבי בשימור הלכידות של הברית מונעים פגיעה קולקטיבית באנקרה או הטלת סנקציות כבדות משקל עליה מצד בעלות הברית. בשל כך, חסות זו של נאט"ו מצמצמת את מרחב התמרון הדיפלומטי והבינלאומי של ישראל ומאלצת אותה להתמודד עם איומי הסייבר והשלוחים הטורקיים באופן עצמאי, עם קושי לגייס מנופי לחץ מערביים אפקטיביים נגד אנקרה.

דוקטרינת המולדת הקיברנטית מרחיבה את סל הכלים של טורקיה נגד ישראל ותורמת למאזן כוחות נפיץ במזרח הים התיכון ובמזרח התיכון, שבו ריבונות דיגיטלית מצטלבת עם יריבויות קינטיות ופעילות שלוחים. מהלכיו והצהרותיו של הממשל הטורקי מבהירים כי אנקרה מכירה היטב בעליונותה הטכנולוגית והמבצעית של ישראל. הכרה זו באה לידי ביטוי מפורש בדבריו של שר החוץ הטורקי, הקאן פידאן (Hakan Fidan) אשר התייחס למאזן הכוחות האזורי מול ישראל והדגיש:

> מודיעין סייבר, מודיעין אותות [סיגינט], מודיעין אלקטרוני, מודיעין מניעתי, זיהוי נתיבים אוויריים, מודיעין חזותי, מערכות מבוססות חלל [...] – ראשית, אם לא עשית את שיעורי הבית שלך ולא פיתחת את היכולות הללו, אינך צריך אפילו להיכנס לעימות מילולי עם ישראל או עם אמריקה. זהו קו מחשבה חיוני. מעצמה חייבת להיות במצב ללא רבב בתחומים הללו אם היא באמת מכינה את עצמה למאבק כזה [...] מעבר לכך, מערכות הגנה אווירית, מערכות מכ"ם, מערכות שיבוש [...] – מדינה צריכה להיות אפקטיבית מאוד בתחומים הללו כדי שתוכל להגן על המרחב האווירי שלה'

לסיכום, בהתאם לתפיסה זו דוקטרינת המולדת הקיברנטית היא מאמץ טורקי מובהק לצמצם פער אסטרטגי מול המעצמות הטכנולוגיות וגם מול ישראל, בדומה למהלכיה בתחומי ההגנה האווירית והלוחמה האלקטרונית. כדי להתמודד עם אתגר מתפתח זה, על ישראל להימנע משאננות דוקטרינרית; אין מדובר במסמך תאורטי בלבד אלא במהלכים עם שיניים תקציביות ומבצעיות, כפי שמעידים חוזי העתק עם התעשיות הביטחוניות הטורקיות בהיקף של מיליארדי דולרים, והקמת מנהלת הסייבר בעלת האוטונומיה הפיננסית.

כדי לשמר את יתרונה האיכותי, על מערכת הביטחון הישראלית לפעול במספר צירים: ראשית, הקמת זירת מודיעין סייבר ייעודית – פתיחת דסק מחקרי ומבצעי ממוקד באמ"ן ובמערך הסייבר הלאומי, אשר יעקוב באופן רציף אחר שיפור היכולות של אקוסיסטם הסייבר הטורקי והתפתחות הכלים המקומיים שלו; שנית, היערכות לתרחישי ייחוס קונקרטיים, כמו מתקפות משולבות (Cyber-EW) מצד אנקרה, לצד מבצעי השפעה ותודעה טורקיים מתוחכמים המכוונים לזירה הבינלאומית (באנגלית ובערבית) לשחיקת הלגיטימיות הישראלית; שלישית, מעקב אחר פעילות שלוחים באזור האפור, כגון קבוצות ההאקטיביזם הלאומניות כדוגמת (Akıncılar), המשמשות כזרוע התקפית הניתנת להכחשה, כפי שבא לידי ביטוי בתקריות תקיפה והטרדה נגד בכירים ישראלים; לבסוף, מעקב הדוק אחר הדינמיקה בנאט"ו וניצול הפער המתרחב בין השאיפה הטורקית לאוטרקיה טכנולוגית לבין דרישות יכולת הפעולה המשותפת (Interoperability) של הברית.