

הערכה אסטרטגית ימית רבתי לישראל 2022/23

עורך ראשי: פרופ' שאול חורב
עורך: ד"ר זיו רובינוביץ



שער 6: ניהול משברים וטכנולוגיה במרחב הימי

שלושת המאמרים עוסקים בהיבטים שונים של איומים והזדמנויות במרחב הימי ואיך לנהל אותם. מאמר אחד דן בצורך להקים מסגרות עבודה ממשלתיות שיכילו את הגופים השונים שעוסקים במרחב הימי של ישראל כדי לשתף במידע ולייעל זמן תגובה ושימוש ביכולות שכל גוף מחזיק בהן. המאמר מציג כמה דגמים של מסגרות הקיימות במדינות אחרות וניתן ללמוד מהניסיון שלהם כדי להקים מסגרות כאלו בישראל כדי לשפר מוכנות לאירועי חירום במרחב הימי ולהתמודדות טובה ויעילה יותר איתם. מאמר אחר סוקר את איום התקפות הסייבר על פלטפורמות ימיות וכיצד ניתן וצריך להיערך לקראתן. הוא מציג את היקף האיום והנזק החמור שמתקפת סייבר על פלטפורמות ימיות יכולה לגרום ומציע פתרונות שאומנם עולים ממון רב אבל הם נדרשים לצורך הגנת סייבר יעילה וראוי לאכוף את יישומם ולא להותיר את הפתרונות בגדר המלצות בלבד. המאמר השלישי דן בהזדמנויות הכלכליות, האזוריות והאסטרטגיות לישראל בעידן הנוכחי בספנות. היא יכולה לפתח לדוגמה כלי שיט בלתי מאוישים וספנות אוטונומית. לישראל יש יתרון טכנולוגי בתחומים רבים שניתן לנצל אותו לפיתוח כלכלי של המדינה בכלל ואזור חיפה והצפון בפרט ולהעצים את העוצמה הרכה של ישראל בתחומים אלו. כלכלה כחולה יכולה לעודד שיתופי פעולה אזוריים. ברמה האסטרטגית, יש לישראל הזדמנות להתפכח מ"העיוורון הימי" שלה וליצור תנאים שיגבירו את השפעתה בזירה הבין-לאומית.

מסגרות עבודה ממשלתיות לביטחון ימי

אלנור דיין

ב־17 בפברואר 2021 התעוררה מדינת ישראל לתחילתו של אסון אקולוגי רחב היקף. משעות הבוקר המוקדמות נפלטו לחופי ישראל אלפי טונות של זפת באירוע שכונה "זפת הסערה"¹. ההערכה הראשונית הייתה שמדובר בפליטת שמנים מכלי שיט ששט מול חופי ישראל, אך המקור נשאר לא ידוע, ולכן גם לא היה ממי לתבוע החזר על הוצאות הניקיון והנזק שנגרם למערכת החופית־אקולוגית. עקב כך הנחתה השרה להגנת הסביבה דאז, גילה גמליאל, לפנות לקרן למניעת זיהום הים כדי להשתמש בתקציב המאושר למימון מבצעי ניקוי בחירום.² מאות צוותים ומתנדבים ירדו לחופים כבר מהיום השני לאירוע כדי לצמצם ככל האפשר את הפגיעה לאורך רצועת חוף של 160 ק"מ. כמה מהמתנדבים אושפזו עקב שאיפת אדי זפת, אך זה לא היה המחדל היחיד באירוע.³ השרה גמליאל טענה כי מאז 2008 הזניחה הממשלה חקיקה לאישור תוכנית מוכנות לאירוע זיהום בים (תלמ"ת) עם תקציב של 15 מיליון שקל להקמת מערך מודיעין להתראה על זיהום. כמו כן תוכנית שהייתה מחייבת רשויות מקומיות להיערך מראש עם ציוד ייחודי לניקוי זיהום בעודו בים ותקנים נוספים לתפקידים ברשויות בגופים הנותנים מענה לזיהום ימי. תזכיר חוק פורסם ונסגר להערות עוד במאי 2021, אך לא הונח על שולחן הכנסת מאז.⁴ יתר על כן, בחקירה התברר שב־11 בפברואר (שישה ימים לפני הגעת הזפת לחופים) גופים בין־לאומיים כבר גילו כתם נפט של מאות טונות שנשפכו במרחק של 50 ק"מ בלבד מחופי אשדוד.⁵ הכתם התגלה על ידי לווין של סוכנות האיחוד האירופי. ישראל אומנם לא חברה באיחוד, אך יכולה הייתה לרכוש את שירות הלוויין או לפתח את היכולת לצלם בעצמה.⁶ בתחקיר חדשות 13 עלה כי אחת המכליות (מתוך 10) החשודות בשפיכת הדלקים עם היתכנות גבוהה להיותה קשורה לאירוע הייתה מעורבת בדליפה דומה ב־2008 מול חופי דנמרק.⁷ כל זאת ממחיש את המידע והמשאבים שבעזרתם היה ניתן לנהל את האירוע טוב יותר.

¹ שני אשכנזי, "[מהצפון ועד ראשל"צ: כמויות גדולות של זפת נפלטות אל חופי ישראל](#)", גלובס, 17 בפברואר 2021.

² שני אשכנזי, "[אסון אקולוגי שחור: זפת נפלטת לחופי ישראל, מבצע הניקיון החל](#)", גלובס, 18 בפברואר 2021.

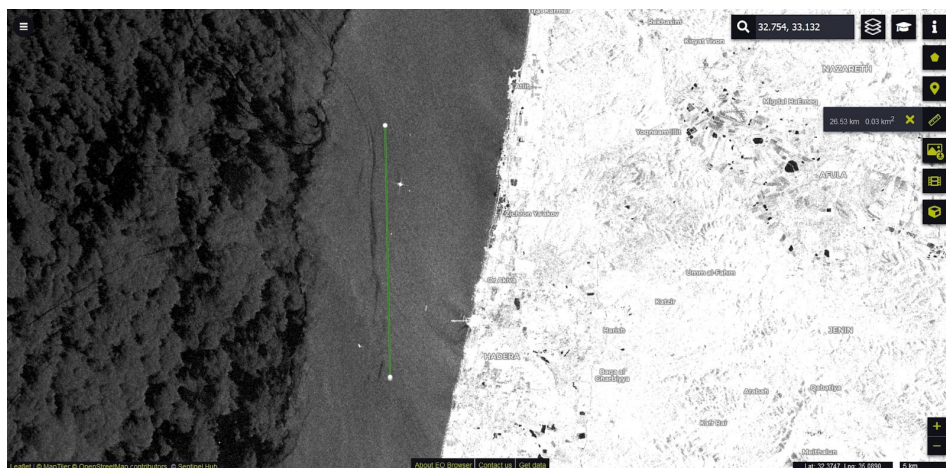
³ כרמל ליברמן, "[זיהום הזפת בחופי ישראל: יש מספר מאושפזים, מצב חירום אקולוגי](#)", N12, 20 בפברואר 2021.

⁴ אילנה קוריאלי, "[דו"ח של הכנסת: ישראל לא ערוכה לזיהום בים](#)", Ynet, 28 בפברואר 2022.

⁵ יובל בגנו ומשה כהן, "[האסון האקולוגי בחופים: אחרי הנזקים, כעת נחשפים גם המחזלים הרבים](#)", מעריב, 21 בפברואר 2021.

⁶ ענת רואה, "[אסון הזפת בחופים: ישראל הייתה יכולה למנוע חלק מהנזק](#)", כלכליסט, 21 בפברואר 2021.

⁷ יואב זהבי וחן ביאר, "[אחת הספינות החשודות בזיהום הייתה מעורבת בדליפת נפט גדולה לפני 13 שנה](#)", כאן 11, 22 בפברואר 2022.



איור 1: צילום לוויין של שפך הזפת באורך 26.4 ק"מ ומרחק של בערך 10 ק"מ ממחדרה⁸

אחת הבעיות עם השגת ביטחון במרחב הימי היא מורכבות האיומים במרחב. הדבר נובע מהמגוון הגדול של מצבים שמתרחשים במרחב הימי שהיכולת לצפות אותם מראש דורשת איסוף וניתוח של כמות עצומה של מידע, ותגובה יעילה מצריכה שיתוף פעולה בין מספר גדול של גופים וארגונים. המאמר דן בעיקרו במסגרת עבודה ממשלתית לביטחון ימי, גישה שנועדה להתמודד עם איומים וסכנות במרחב הימי, ובתוך כך יעול התגובה והתיאום בין כל הגופים הרלוונטיים שמתבטאת בפועל כמרכז עצמאי או בניהול משרד ממשלתי לידע ותיאום פעולות במרחב הימי. ראשית אציג הסבר תאורטי למסגרת עבודה ממשלתית ולביטחון הימי, לאחריו אציג דוגמאות לכך מהעולם, ולבסוף אבחן את חשיבות המסגרת במקרה הישראלי, ובשם אילו עקרונות ולקחים ממקרי הבוחן שהוצגו על מקבלי החלטות לתכנן את המסגרת.

מסגרת עבודה ממשלתית לביטחון ימי – רקע תאורטי

אין הגדרה מוסכמת לביטחון ימי (Maritime Security). ניתן לפרש ביטחון ימי כהיעדר של איומים במרחב הימי, בהם טרור ימי, היעדר אסונות ותאונות, סחר לא חוקי ופגיעה סביבתית. ניתן גם להגדיר ביטחון ימי כשאיפה למצב אידאלי מסוים של שקט ויציבות של המרחב הימי (stable order of the sea), או להגדיר אותו כאוסף פעולות כגון הגנה על כלי שיט, נמלים והסביבה הימית.⁹ דבר אחד ברור, שהשגת ביטחון ימי והתמודדות עם איום או אירוע במרחב הימי דורשים השתתפות ושיתוף פעולה של גופים ממשלתיים, פרטיים ובין-לאומיים רבים, ידע בנושאים רחבים, ויכולת תגובה מהירה לאירועים מורכבים. במציאות מורכבת שבה שחקנים רבים צריכים להשתתף במטרה להביא לתוצאה הרצויה נדרש גוף שינצח על המאמץ

⁸ מקור האיור: Sue Surkes, "[Satellite images of oil slicks off coast show recent spill far from a one-off](#)", *The Times of Israel*, February 28, 2021

⁹ Christian Bueger, "What Is Maritime Security?", *Maritime Policy*, 53, no. 1 (2015): 161–164.

המשותף.¹⁰ ההתמודדות עם איומים על הביטחון הימי צריכה להכיל ארבעה שלבים: זיהוי האירוע בזמן אמת, מעקב והתראה אחר התפתחות האירוע והערכה מקדימה של תמונת המצב עקב איסוף מידע, הפעלת כוחות ומשאבים כמתן תגובה מהירה ככל האפשר והערכת נזקים ובניית תוכנית שיקום.¹¹ כל אחד מהשלבים מצריך יכולת של איסוף ואימות מידע, יכולת תיאום בין גופים רבים, הבנה של הנסיבות המשפטיות והמדיניות של האירוע והסוגיה, יכולת תכנון והוצאה לפועל של תגובה ראשונית, ויכולת הפקת לקחים והטמעתם בארגונים הרלוונטיים. מסגרת עבודה ממשלתית לביטחון הימי נועדה להשיג כל זאת.

טבעם המורכב של איומים ביטחוניים במרחב הימי מעלה כמה בעיות ייחודיות. אומנם ראש מדינה או ועדה פרלמנטרית יכולים לכוון ולתאם תגובה לאיומים, כזו המייצגת את האינטרסים של המדינה, אך לא הגיוני לצפות מהם להיות מעורבים מיידית בכל סוגיה ומקרה ביטחוני, כגון מה לעשות במקרה של עצורים ומטען עצור, איסוף ראיות, זכות לעלות על ספינה בים והצהרות תקשורתיות. הבעיה נובעת ממהירות העברת המידע שמשנה מדיניות. כמות המידע והצורך להעבירו במהירות, יחד עם מורכבות האירועים במרחב הימי גורמים לכך שמגיבים ראשונים לאירוע לעיתים לא יכולים או לא יודעים לשתף מידע מהשטח בזמן אמת עם כל הגורמים האחראיים להגיב לאירוע. לפיכך, כיום נדרש גוף שזה אחד מתפקידיו. בעיה זאת גדלה בעקבות מספרם הגדל והולך של תחומי ידע והתמקצעות הנדרשים כדי להגיב לאיומים, כגון דליפת דלקים וחומרים מסוימים, פירטיות, פגיעה בתשתיות אנרגיה, סחה, דיג והגירה לא חוקיים באופן שווה. ללא נוהל לתיאום מאמץ תגובתי, חסימת מידע וחוסר יעילות עלולים לגרום לקבלת החלטות ללא תמונת המצב המלאה, והסיכוי לחזור על טעויות מן העבר גדל.¹² ככתוב:

אין שום ארגון יחיד שיכול לממש ביטחון ימי או להתמודד עם איומים עליו ללא תמיכה של גופים ובעלי עניין אחרים, כגון הקהילה או התעשייה. היכולת שלנו להבין, לפעול יחד עם שותפים, וגם למנוע ולהגיב לאיומים ימיים בנויה על הבסיס של גישת מסגרת עבודה ממשלתית המביאה לניצול מרבי ומאוחד של כל מגוון היכולות הלאומיות.¹³

A Whole-of-Government Approach – WGA; or: A Comprehensive Multi-Agency Approach) נועדה להביא גופים וארגונים בממשלה למאמץ משותף כדי לנצל במלואם את המשאבים הקיימים בתגובה מתואמת ומשותפת לכל הארגונים.

¹⁰ Duane M. Smith and Thomas C. Fitzhugh, *International Perspectives on Maritime Security* (Washington D.C.: Department of Transportation, 1996), 1–4; Brett Doyle, "Lessons on Collaboration from recent conflicts: The Whole of Nation and Whole of Government Approaches in Action", *Inter-Agency Journal*, 10, no. 1 (2019): 105–122.

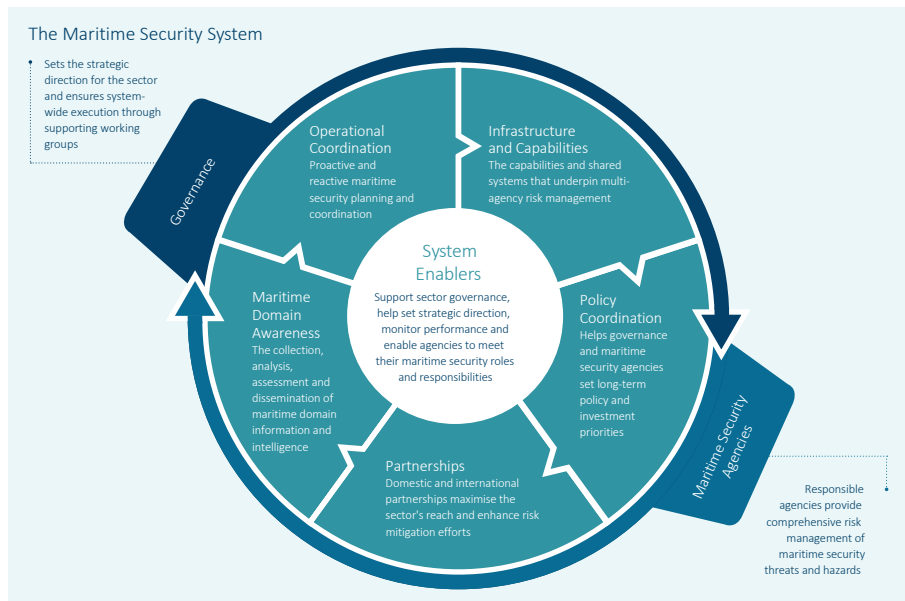
¹¹ עידו בן משה ואהוד גונן, "זיהום מי הים – איך נמנע את האסון הבא", הסדרה הגאוסטרטגית 2021, (אוניברסיטת חיפה, 2022), 61–67.

¹² Brian Wilson, "The complex nature of today's maritime issues: why whole-of-government frameworks matter", In Joachim Krause and Sebastian Bruns (eds.), *Routledge Handbook of Naval Strategy and Security* (New York: Routledge, 2016), 153–156.

¹³ Ministry of Transport, "[Maritime Security Strategy](#)", New Zealand Ministry of Transport, December 2020.

הגישה נבנית על ידי חזון של תיאום ושיתוף פעולה מתוך הבנה שבלעדיהם כל גוף (ארגון) יתמקד באינטרסים והמטרות שלו. האינטגרציה של יכולות ומידע בין ארגונים תביא להרחבה של אופציות פעולה, יעילות והורדת תלות בגופים מסוימים (כמו חיל הים).¹⁴ הגישה מכוונת לשפר יעילות על ידי שיתוף מידע, משאבים ויכולות של כל ארגון. יתרה מכך, WGA מובילה להבנה מערכתית של מורכבות האיומים הדורשים מענה, ולכן מביאה מומחים מתחומים שונים כדי לתת מענה לאיומים. השימוש המרוכז במשאבים ומידע נועד בין השאר להוזיל עלויות ולהגביר יעילות.¹⁵ מסגרת עבודה ממשלתית (Whole of Government Framework – WOGF) משלבת גופים בתוך הממשלה, והיא נותנת מענה למספר אתגרים, בהם השגת יכולות פעולה ימיות, מינוף משאבי הגופים וארגונים, קיום דיונים, תיאום מאמץ וקבלת החלטות בין אגפים במשרדים השונים בממשלה ומחוצה לה, והקמה מראש וקיום פרוצדורות לאיסוף ואימות מידע. הליך ניהול משברים קיים מאפשר לארגונים ביטחוניים ואזרחיים ממשלתיים ולא־ממשלתיים להתכונן ולענות על חוסר ודאות עוד לפני תחילת אירוע, ולאחר האירוע לתעד לקחים ולהטמיעם בהליכים ארגוניים.¹⁶

The success of the multi-agency approach relies on effective maritime security system enablers.



איור 2: מסגרת עבודה ממשלתית בביטחון הימי (ראיית ניוזילנד)
(מקור: Maritime Security Strategy 2002)

Terry A. Fellows Jr. & Jason L. Percy, *A whole of government approach for national security* ¹⁴
. (MBA professional report, Naval Postgraduate School, Calhoun, 2009), 4, 17–19

Andrea Baumann, *Whole of Government: Integration and Demarcation* (Center for ¹⁵
.Security Studies, ETH Zurich, 2013), 1–4

.Wilson, "The complex nature of today's maritime issues" 2016 ¹⁶

מסגרות עבודה ממשלתיות לביטחון הימי בעולם

סוגיית ההתמודדות עם מורכבות האיומים על הביטחון הימי היא חדשה יחסית, ומתפתחת בשנים האחרונות יחד עם העידן הדיגיטלי וגידול בכמות המידע שניתן לאסוף. מתחילת המאה ה-21 ישנן ברחבי העולם מספר מדינות שהקימו מסגרת עבודה ממשלתית לביטחון הימי, וכפי שיתברר, שתי הסיבות המרכזיות להימצאותן במדינות אלה הן גודל שטח המרחב הימי וחשיבותו היחסית של המרחב הימי למדינה. חשוב לציין שתפקידן בכל מדינה שונה לפי האיומים, האילוצים ומאפיינים שונים של כל מרחב. קודם אציג את סינגפור כדוגמה למדינה קטנה המתפקדת באופן הדומה מאוד למדינת אי כמו ישראל (בכך שנמליה הימיים והאוויריים הם שיערה המרכזי לעולם, במיוחד בכל הקשור לכלכלת הסחר הנכנס ויוצא ממנה), ועם יכולות כלכליות לא שונות מאוד. אתמקד ביכולות איסוף המידע שהמרכז מבצע במרחב מורכב כמו מיצר סינגפור. לאחר מכן אציג את בריטניה כדוגמה למדינה שבה למרחב הימי יש חשיבות רבה במשך שנים רבות, אך הקימה את המרכז לתיאום לביטחון הימי רק ב-2020, ועל כן אבחן את מיקומה הארגוני של המסגרת כגוף מתוקצב ומאויש באופן משותף על ידי כמה גופים ממשלתיים. לבסוף, אציג את ניו־זילנד ואוסטרליה במבט השוואתי, ואבחן את סוגיית הסמכות של המסגרת כגוף מתאם מצד אחד, אל מול גוף מבצע של ביטחון ימי, מצד שני.

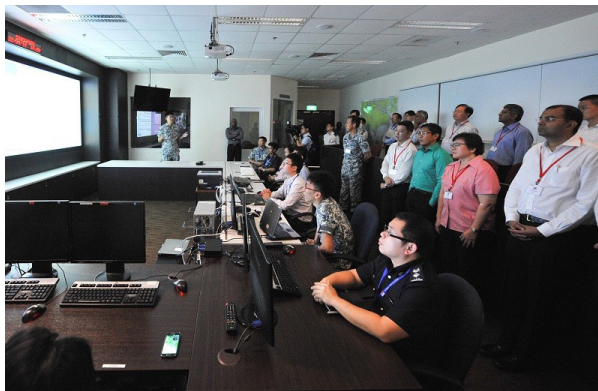
סינגפור

במרכזה של מסגרת העבודה הממשלתית לביטחון ימי בסינגפור (National Maritime Security System Crisis) עומד מרכז סינגפור למשברים ימיים (Singapore Maritime Crisis Centre – SMCC) שהוקם ב-2011 ועורך תיאום בניהול הקבוצה לניהול משברים (Management Group) שמוביל מפקד הצי, ונמצאת תחת מנכ"ל משרד ההגנה והפנים בקבוצה לניהול משברים בעורף (Homefront Crisis Executive Group). ה-SMCC מחזק את יכולת הפעולה ההדדית בין הגופים השונים על ידי בניית תמונת מצב והערכת איומים, תכנון תגובה למשברים, ניהול ובקרה על מבצעים בזמן אמת, פיתוח יכולות וכלים להתמודדות עם משברים וקיום אימונים לגופים השונים. המרכז מורכב משלושה עמודי תווך: הראשון מורכב מנציגים מהגופים השונים האחראים למרחב הימי, בהם חיל הים הסינגפורי, רשות הנמלים והים של סינגפור (Maritime and Port Authority of Singapore), רשות ההגירה וביקורת גבולות (Immigration and Checkpoints Authority), משמר החופים של המשטרה (Police Coast Guard) והמכס. המרכז השיג יכולת מבצעית מלאה ב-2013 ומאז בנה תיאום עם גופי מודיעין, צוותי חשיבה וחברות ממגזר הספנות.¹⁷

המרכיב השני הוא הקבוצה לבניית מודעות ימית לאומית (National Maritime Sense-making Group – NMSG) המשתמשת במערכות בינה מלאכותית וניתוח נתונים הנאספים ממקורות רבים כדי לבנות פרופילים לכל כלי השיט העוברים בסביבת המרחב הימי של סינגפור, ומזהה

¹⁷ Ministry of Defence, "[Fact Sheet: Singapore Maritime Crisis Centre \(SMCC\) and Launch of SMCC Next-Generation Maritime Sense-making System](#)", MINDEF Singapore, November 12, 2021.

איומים פוטנציאליים, חריגות או התנהגות חשודה (Big-data analytics). המערכת מחוברת בקביעות למאגרי מידע של ארגוני מודיעין וחברות וגופים ממגזר הספנות. את ההערכות הללו היא משתפת עם גורמי ביטחון רלוונטיים שמבצעים פעולות לאימות המידע ובדיקת כלי השיט.¹⁸ המרכיב השלישי הוא הקבוצה הלאומית למבצעים ימיים National Maritime Operations Group – NMOG, המבצע אימונים, בונה פרוטוקולים לתרחישים אפשריים ועורך בקרה ולמידת לקחים במטרה לשפר את יכולות התיאום והביצוע בזמן משבר והתמודדות עם איום. בזמן כזה או בתרגילים כהכנה לאירועים כאלו יתאם המרכז עם כוח משימה לביטחון ימי (Maritime Security Task Force) של צי סינגפור ונציגים מגופים רלוונטיים לאירוע דרכי מניעה ותגובה לאיומים בשטח.¹⁹



איור 3: ועדת חוץ וביטחון של סינגפור מבקרת במרכז סינגפור למשברים ימיים (SMCC). (מקור: *MINDEF Singapore 2014*)²⁰

בין האיומים שהמרכז זיהה ומנע ניתן לציין את זיהויו ב-2014 של איש צוות שהיה רשום ברשימות של שתי ספינות שהיו מיועדות להיכנס לסינגפור באותו יום, וברקע היו איומי פיגוע על ידי זרוע של דאע"ש בסרי לנקה, וכך שיתף ה-NMSG את המידע ומנע את כניסתו.²¹ ב-2015 זיהתה מערכת הבינה המלאכותית תומך דאע"ש פוטנציאלי על סיפון מכלית שנועדה להיכנס לנמל סינגפור, ועל אותו אדם נאסר לרדת מהספינה. ב-2016 זיהה המרכז ספינה עם פעילות חשודה, משמר החופים המשטרתי עלה על הספינה ומצא עליה סחורה מוברחת. עקב כך גם

¹⁸ Ibid; Nicholas Lim & Chong De Xian, "Maritime Sense-Making and The Role of Big Data Analytics for Enhancing Maritime Security", *PONTER Journal* (September 2020).

¹⁹ Ministry of Defence, "[Fact Sheet: Safeguarding Singapore's Maritime Security](#)", *MINDEF Singapore*, June 30, 2017.

²⁰ News Releases, "[Government Parliamentary Committees Visit Singapore Maritime Crisis Centre](#)", *MINDEF Singapore*, April 22, 2014.

²¹ Joseph Franco & Romain Quivoij, "[Terrorist Threats from the Maritime Domain: Singapore's Response](#)", RSIS, No. 197, October 10, 2014.

נעצר אחד מאנשי הצוות.²² ההיבט המרכזי שניתן ללמוד ממקרה הבוחן הסינגפורי הוא יכולת איסוף המידע האיכותית שהמסגרת מבצעת. נמל סינגפור הוא השני העמוס ביותר בעולם, ומיצר סינגפור הוא המעבר הימי העמוס בעולם. ב-1,067 קמ"ר המים הכלכליים של סינגפור משייטים בכל עת בממוצע כ-1,000 כלי שיט, ובכל שתיים עד שלוש דקות נכנס ויוצא כלי שיט. היכולת לבנות תמונה רחבה של המתרחש במרחב הימי בכל עת ולהגיב בזמן לאיומים הוא עמוד תווך מרכזי בגישת מסגרות עבודה ממשלתיות לביטחון ימי.²³

בריטניה

חשיבות הביטחון במרחב הימי, אם למטרת סחר בין-לאומי, צמיחה כלכלית או חוק וסדר בין-לאומיים בימים הוא לא דבר חדש לממלכה המאוחדת. האסטרטגיה הלאומית לביטחון ימי (National Strategy for Maritime Security – NSMS) מ-2014 מכירה בכך שאג'נדת הביטחון הימי מתמודדת עם סוגיות אחרות חוץ מאשר עם עליונות ימית צבאית, והיא מתווה לראשונה את חשיבות גישת מסגרת העבודה הממשלתית בבריטניה. כחלק מאותו מאמץ הוקם המרכז המשותף לביטחון ימי (The Joint Maritime Security Centre – JMSC) ב-2020 כחיבור בין שני הגופים: Joint Maritime ו-National Maritime Information Centre. Operations Coordination Centre – JMOCC, והוא הגוף הבין-ארגוני המייצג את מסגרת העבודה הממשלתית לביטחון הימי בבריטניה, והאחראי על שימור ההבנה של המרחב הימי ומתן תגובה לאיומי ביטחון, חוק וסדר ושמירה על הסביבה הימית.²⁴

משימתו העיקרית היא חיזוק המוכנות לאיומים במרחב הימי, ותיאום ותגובה ממשלתית רחבים לאותם איומים. את המרכז מוביל צוות עם נציגים מהצי המלכותי, משרד ההגנה, Border Force ו-MMO (Marine Management Organization), ומעליו בהיררכיה עומד הדירקטוריון. נוסף לנציגי משרדים אלו, JMSC מתאם בין ארגונים ממשלתיים נוספים, בהם משרד התחבורה, משרד החוץ, משרד הפנים, המכס הבריטי, משמר החופים הבריטי, סוכנות הפשע הלאומית (National Crime Agency), משטרת בריטניה והדירקטוריון הימי הסקוטי (Maritime Scotland). JMSC נותן מספר שירותים לארגונים וממשלת בריטניה: איסוף וניתוח מידע במטרה ליצור תמונת מצב של המתרחש במרחב הימי כמרכז ידע לביטחון ולמרחב הימי; תכנון וניהול תגובות במרחב הימי על ידי תיאום בין ארגונים, נכסיהם ויכולותיהם. בדומה למודל של מסגרת העבודה הממשלתית בסינגפור, המרכז הבריטי מורכב משלושה מרכיבים: הראשון הוא הצוות המנהל שהוצג קודם לכן, השני הוא המרכז הלאומי למידע ימי (NMIC)

²² Ministry of Defence, "Fact Sheet", 2017.

²³ Nicholas Lim and Chong De Xian, "Maritime Sense-Making and The Role of Big Data Analytics for Enhancing Maritime Security", *Pointer, Journal of the SAF*, (September 2020): 1–10.

²⁴ Scott Edwards, "[The United Kingdom's Conceptualization of Maritime Security](#)", *Asia Maritime Transparency Agency*, March 4, 2022; Cristian Bueger, Timothy Edmunds & Scott Edwards, "[Innovation and New Strategic Choices](#)", *The RUSI Journal*, 166, no. 4 (2021): 66–75.

שהוקם עוד ב-2017 ומטרתו לספק לארגונים הנותנים מענה לביטחון הימי ניתוח מידע, מודיעין וניהול יכולות כדי למקסם יכולות מבצעיות, השלישי הוא מרכז המבצעים של המרכז הבריטי (JMOC). באמצעים מתקדמים וצוות מאוחד של נציגים מארגונים ממשלתיים הוא מפקח מסביב לשעון על המרחב הימי של בריטניה, מזהה איומים ותקריות בים ומתאם תגובה ימית ואווירית.²⁵

נוסף ליכולת איסוף המידע והמגוון הרחב של יכולות ומשאבים שהמרכז הבריטי מחזיק ומפעיל, ההיבט הייחודי שלו הוא חוסר השייכות למשרד או גוף ממשלתי יחיד. המרכז מאויש ומתוקצב באופן משותף על ידי גופים מרכזיים השותפים להשגת מטרותיו במרחב הימי, בהם הצי המלכותי, ה־MMO ומשרד ההגנה. מאפיין זה מאפשר לכל הארגונים שהמרכז מתאם ביניהם לעבוד בתנאים שווים במטרה להגביר את רצונם להשתתף בתגובה מאוחדת בתיאום המרכז.²⁶ כדוגמה לכך, הצי המלכותי רכש עבור המרכז (JMOC) מדי שנה שירותי איסוף מודיעין מבוססי לוויין של חברת Airbus, המספקים למרכז הבנה מרחבית של המתרחש במרחב הימי הבריטי, ומאפשרים תגובה מהירה לאיומים אפשריים.²⁷ אומנם חוסר שייכות למשרד מסוים נשמע ארגונית חסר סדר, אך רעיון מעניין למחשבה הוא שהמרכז הבריטי, שהוקם מאוחר יחסית ביחס למרכזים אחרים ולמד את לקחייהם בהקמתו, בחר להקים את המסגרת באופן הזה ולא תחת משרד אחד.



איור 4: שגריר תאילנד בבריטניה מבקר במרכז המשותף לביטחון הימי (JMOC) (מקור: ²⁸Royal Thai Embassy, London 2021)

²⁵ HM's Government, "[Joint Maritime Security Centre](#)" (Accessed August 6, 2022).

²⁶ Scott Edwards, "[Safe Seas Visits UK's Joint Maritime Security Centre](#)", *Safe Seas*, October 12, 2021.

²⁷ Press release, "[Airbus to provide satellite-based maritime surveillance services for the UK Royal Navy](#)", *Airbus*, June 28, 2021.

²⁸ "[Thai Ambassador visited the Joint Maritime Security Centre and National Maritime Information Centre in Portsmouth](#)", *Royal Thai Embassy, London*, September 8, 2021.

ניו־זילנד מול אוסטרליה

סקירה של ממשלת ניו־זילנד מתחילת 2001 במטרה לבחון אילו משאבים נדרשים כדי לסייר (צבאית ואזרחית) במרחב הימי שסביבה מצאה שעשרה גופים ממשלתיים סיירו אותו עצמאית לצורכיהם בלבד, מה שמנע את האפשרות להבין כמה יעיל איסוף המידע הכללי מנקודת מבט לאומית. אותה סקירה המליצה על הקמת מרכז תיאום ימי שינהל חלוקת עבודה בין כל המשאבים במדינה שנועדו למטרה זאת, ויזהה פערים חוקתיים שמונעים סיור ואיסוף מידע ימי יעיל. הוא מורכב מצוות משולב של אנשי מטה הכוחות המזויינים ואזרחים מגופים ממשלתיים, וממוקם כגוף עצמאי בשטח צבאי. – The National Maritime Co-ordination Centre – NMCC הוקם ב-2002, וכיום מתקצב על ידי משרד המכס (Ministry of Customs).²⁹ נוסף לניהול יעיל של כלי סיוור, NMCC אוסף נתונים למטרותיו כגון נתוני Automatic Identification System, Long-Range Identification and Tracking, Vessel Monitoring Systems, נתוני מכס ונתונים גיאוגרפיים מספקי שירות אזרחיים וגופים ממשלתיים לצד הנתונים שנאספים על ידי הצבא.³⁰ המרכז משתמש בפלטפורמה לזיהוי והתרעה על אנומליות ימיות (Maritime Anomaly Indication and Alerting tool) כדי לנתח את הנתונים שנאספו מאלפי כלי שיט בו זמנית, ולהתריע על התנהגות חשודה.³¹ המרכז מעביר את המידע לחיל הים והוא הגוף המבצע בים.

שינויים רבים פקדו את אוסטרליה מבחינת ביטחון ימי בתקופה שלאחר 11 בספטמבר 2001. המרכזי ביניהם הוא הקמת פיקוד הגנת הגבולות ב-2005 (Border Protection Command). ב-2015 שונה שמו לפיקוד הגבולות הימיים (Maritime Border Command – MBC) כאשר הוכפף תחת גוף אכיפת חוק של משרד הפנים האוסטרלי (Australian Border Force).³² MBC כמסגרת עבודה ממשלתית לביטחון הימי באוסטרליה נועד לזהות, להרתיע ולהגיב לאיומים ימיים לא צבאיים, ולמנוע פעילות לא חוקית במרחב הימי על ידי שימוש בכלי שיט וכלי טיס למבצעים ימיים אזרחיים.³³ המרכז נועד להתמודד עם פעילות לא חוקית, ניצול לא חוקי של משאבי טבע, זיהום ימי, סחר לא חוקי, הגירה לא חוקית, טרור ימי, פירטיות ודליפת

²⁹ Office of the Auditor-General, "[Effectiveness of arrangements for Co-ordinating civilian maritime patrols](#)", *Controller and Auditor-General*, April 12, 2010.

³⁰ Chris Rahman, "Maritime Domain Awareness in Australia and New Zealand", in Natalie Klein, Joanna Mossop & Donald R. Rothwell (eds.), *Maritime Security: International Law and Policy Perspectives from Australia and New Zealand* (New York: Routledge 2009), 202–223.

³¹ The Defence Technology Agency – DTA "[Maritime Domain Awareness](#)", (Accessed September 12, 2022).

³² Donald Rothwell and Cameron Moore, "Australia's Traditional Maritime Security Concerns and Post-9/11 Perspectives", in Natalie Klein, Joanna Mossop & Donald R. Rothwell (eds.); *Maritime Security: International Law and Policy Perspectives from Australia and New Zealand* (New York: Routledge 2009), 37–53.

³³ Australian Border Force, "[Maritime Border Command](#)", (Accessed September 12, 2022).

דלקים. נוסף לתפקיד תיאום הכלים והצוותים של ABF וניהול מבצעים בשיתוף פעולה עם חיל הים האוסטרלי, המרכז אוסף מידע על המרחב הימי על ידי שימוש ב־Australian Maritime Identification System³⁴.

ההבדל המרכזי בין אוסטרליה לניו־זילנד (ושאר הדוגמאות שהובאו במאמר) הוא ברמת העצמאות וביכולת של המסגרות לפעול עצמאית במרחב הימי. במקרה האוסטרלי יש למרכז כלי שיט וטיס וצוותי תגובה מהצבא וחיל הים האוסטרלי, שמקצים אליו באופן קבוע, בעוד במקרה של ניו־זילנד המרכז תלוי בגופים אחרים (בעיקר בחיל הים) כדי לפעול על סמך המידע שנאסף. כלומר, בעוד המרכז האוסטרלי מבצע פיקוד בביטחון ימי (Command Activity) המשרד בניו־זילנד מבצע תיאום (Coordination Activity)³⁵.



איור 5: כלי שיט מוקצה ל-MBC. (מקור shipshub.com)

מסגרת עבודה ממשלתית לביטחון הימי בישראל

אירוע "זפת הסערה" הדגיש את חסרונו של מאמץ ממשלתי מתואם ומאוחד לאיסוף מידע ומתן תגובה לאירועים במרחב הימי, אך הסוגייה עדיין לא מקבלת מקום בסדר העדיפויות, ולא מובנת אצל מקבלי ההחלטות. המצב הוא שלמרות חשיבותו של המרחב הימי לכלכלת המדינה וביטחונה, בישראל אין גוף המתאם ומגיב לאירועים במרחב הימי. חיל הים מצויד ומוכן להגנה על ביטחון המדינה, אך אינו בעל סמכות להתמודד עם אירועים שאינם ביטחוניים, בין אם אסונות, תאונות, זיהום, או הברחה, סחר ודיג לא חוקיים. בעוד נושא ביטחון מתקני האנרגיה והמרחב מאיומים חיצוניים זוכה לתשומת לב, שאר האיומים על ביטחון המרחב הימי ועל הסביבה הימית נדחקו הצידה. כיום מתחלקת האחריות להיבטים השונים בין תשעה ארגונים ממשלתיים, וביניהם אזורי מחלוקת פוטנציאליים רבים כל אימת שמדובר בשאלה 'מי אחראי' כאשר מתרחש אירוע או תקרית במרחב הימי. חוסר היכולת להבין מי צריך להגיב לאירוע, לקבל

Department of Immigration and Border Protection, "[Maritime Border Command](#)",³⁴ (Accessed September 12, 2022).

Michael Blades, "[Focusing New Zealand's approach to maritime domain security](#)"³⁵ (Unpublished thesis, Massey University, New Zealand), 2014.

את המידע הדרוש כדי להעריך את התגובה הראויה, וחוסר היכולת לתאם פעולות בין ארגונים תורמים לאי-הבנת התמונה הרחבה במרחב הימי הישראלי, ועקב כך לניצול לא יעיל של נכסים מדינתיים במרחב הימי.³⁶

בהנחה שמקבלי החלטות רואים במסגרת עבודה ממשלתית עניין חיוני למדינת ישראל, כחלק ממאמץ גדול יותר לעיצוב האסטרטגיה הימית הלאומית של המדינה,³⁷ אפשר להציע שני לקחים ממקרי הבוחן שהוצגו במאמר זה. הלקח הראשון דן בחשיבות בניית מערך איסוף ממוגון מקורות מידע. אלו יכולים להיות מאגרי ידע (Databases), מכוני מחקר וגופים אקדמיים, מקורות פתוחים לקהל הרחב, כגון מאגרי מידע באינטרנט ומתקשורת ושיתופי פעולה עם ארגונים בממשלה, ארגונים בין-לאומיים ונותני שירות כמו שירותי צילום וניתוח צילומי לוויין (כפי שהוצג במקרה של בריטניה). נוסף לכך, פלטפורמה ליכולת ניתוח, ניהול ואימות מידע, תוך היעזרות במערכות בינה מלאכותית כדי לבנות תמונת מצב מאוסף מידע רב שנדרש לפענחו. נושא זה נדון בהערכה אסטרטגית ימית רבתי לישראל 2021/22, שהוצג בה כי טכנולוגיות לניטור המתרחש במרחב הימי קיימות, ונדרש להפעילן כדי למקסם את ביטחונם של אזרחי מדינת ישראל והמרחב הימי.³⁸ זאת ועוד, נדרשת יצירת מנגנון תיאום בעזרת נציגים של כל הארגונים האחראים למרחב הימי לתיאום תגובה בזמן אירוע, ותכנון דרכי פעולה לתרחישים אפשריים מבעוד מועד. בין הגופים שיצופה מהם להשתתף במאמץ התיאום ניתן למנות את חיל הים, משטרת ישראל, משרד הביטחון, המשרד להגנת הסביבה, רשות הטבע והגנים, משרד האנרגיה, משרד התחבורה, משרד המשפטים, נמלי ישראל וחברות ספנות, החברה להגנת הטבע, רשויות מקומיות לאורך החוף ואחרים, על פי מטרות המסגרת שיוגדרו ומגבלות אחרות.

הלקח השני דן בסמכות. ראינו מקרי בוחן שבהם למסגרת מוקצים משאבים, כלים וכוח אדם, כך שהוא יכול לפעול עצמאית במטרה להגיב לאיומים ואירועים במרחב הימי (אוסטרליה), ומסגרות המבצעות רק איסוף ושיתוף מידע ותיאום משאבים של גופים אחרים. הבחירה הראשונה תיתן למסגרת סמכות ויכולת לתרום לביטחון הימי, בעוד השנייה לא תשנה סדרי אחריות בין גופים קיימים, אלא רק תייעל את עבודתם ותתאם ביניהם. נושא זה מתקשר גם לשאלת העצמאות ההיררכית והתקציבית של המסגרת מכל ארגון שאיתו קיים תיאום. על מקבלי ההחלטות להחליט אם על המסגרת להיות בניהולו של גוף ממשלתי מסוים, וכך גם לתקצב על ידי משרד מסוים, או שעליה לפעול באופן עצמאי ולהיות מתוקצבת באופן משותף על ידי כלל הגופים וארגונים המשתתפים במאמץ התיאום שלו. האפשרות הראשונה תקשור

³⁶ Sue Surkes, "[Experts: Israel has 'no strategy' for managing 'lifeline' Mediterranean Sea](#)", *The Time of Israel*, November 25, 2021; Shaul Chorev, "[Israel must increase its maritime awareness in light of recent oil spill](#)", *The Jerusalem Post*, March 1, 2021

³⁷ לקריאה נוספת: עודד גור לביא, מודל ומתודולוגיה לקביעת אסטרטגיה ימית רבתי למדינת ישראל, המרכז לחקר מדיניות ואסטרטגיה ימית, אפריל 2017.

³⁸ סמיון פולינוב ושאל חורב, "מודל למערכת ניטור ימי אקדמית ישראלית", בתוך שאול חורב וזיו רובינביץ (עורכים), *הערכה אסטרטגית ימית רבתי לישראל 2021/22* (חיפה: המרכז לחקר מדיניות ואסטרטגיה ימית, אוניברסיטת חיפה, 2022), עמ' 275–287.

את פעילות המרכז למשרד מסוים, אך תביא יציבות למאמצי, בעוד השנייה תחלק את עלויות המסגרת בין גופים מרכזיים בפעילותו, ותיצור מרחב שבו כלל הגופים יעבדו באופן שוויוני, כפי שפועל המרכז הבריטי.

מה יכול להיות מקומה של מסגרת כזו במערכת הממשלתית ומה יהיו מרכיביה הפיזיים? ראשית, מסגרת העבודה הממשלתית תבוא לידי ביטוי במרכז לתיאום ביטחון ימי שצריך להיות מובחן על ידי אסטרטגיה ימית והקבינט בו זמנית, ופעולותיו יכולות להיות מבוקרות על ידי אחת הוועדות של הכנסת. במבט פנימה, מסגרת (ומרכז התיאום) מצריכה צוות ניהול שמורכב מראש מרכז, נציגים/ים מגופים מרכזיים מאוד לפעילות המרכז (כגון חיל הים), וראשי הקבוצות המבצעות את שאר פעילות המרכז. ממקרי הבוחן אנו למדים שקבוצה אחת תיידרש לאסוף ולנתח מידע על המרחב הימי. צוות איסוף מידע יעביר את הנתונים לצוות ניתוח מידע שעם תוכנות ומערכות לניהול נתונים יוכל לבנות את תמונת המצב במרחב הימי. נוסף אליהם, צוות פיתוח יידרש לעסוק בפיתוח מתמיד של כלים לניתוח ואימות מידע כיוון שגם כמות המידע שמצריכה התייחסות גדלה באופן קבוע. הקבוצה השנייה תצטרך לתאם ולנהל מבצעים ותגובה לאירועים, ולכן תיידרש לכלול נציגים מכל הגופים הרלוונטיים למתן תגובה לאיומים ותקריות במרחב הימי. הקבוצה יחד עם צוות הניהול יכינו אפשרויות תגובה לתרחישים אפשריים לפני אירוע, ינהלו את התיאום במהלך תרגילים, ויתנו הערכה אחריהם. נוסף לשתי הקבוצות יהיה גם צוות המרכז, אם מבחינה מנהלית, מבצעית או אחרת.



איור 6: הצעה למבנה ארגוני של מסגרת עבודה ממשלתית לביטחון הימי

לסיכום, המאמר הציג את גישת מסגרת העבודה הממשלתית בהקשרה לביטחון ימי ודוגמאות למדינות שמטמיעות גישה זאת כחלק מהאסטרטגיה הימית שלהן. כמו כן בחנו את שאלת חשיבות המסגרת למקרה הישראלי. אכן, המרחב הימי משמעותי יותר לרוב המדינות בעלות מסגרת לביטחון הימי כיום לעומת ישראל. עדיין, חשוב לציין שמסגרת עבודה ממשלתית נועדה

לייעל את ביטחונה הימי של אותה מדינה ללא תלות בסוג איום מסוים, שהרי ניתן להקים מסגרת על ידי התמקדות בפירטיות וטרור או בדליפת דלקים, זיהום ימי, בטיחות אנרגטית וסביבתית והתכונות לאסונות טבע, ומדינת ישראל אינה יכולה להיות חסינה לכל אחת מהם. העידן הדיגיטלי־מודרני מביא איתו אתגרים חדשים – התמודדות עם כמות מידע עצומה והצורך באיסוף וניתוח מהיר של מידע, התמודדות עם אתגרים מסובכים שדורשים התערבות ממספר רב של גופים, והתמודדות עם תלות גדלה במרחב הימי. עקב כך נדרשות גם דרכי התמודדות חדשות נגד אותם איומים. מסגרת העבודה הממשלתית נועדה להתמודד עם שינויים ואיומים אלו, ולכן גם הדרישה למסגרת כזו והטמעתה הולכת וגדלה בקרב יותר מדינות, בהן קנדה, ארצות הברית, הודו, יפן, פיליפינים, שוודיה, קייפ ורדה, בריטניה, אוסטרליה, סינגפור וניו זילנד.³⁹

איום הסייבר על פלטפורמות ימיות ותובנות מהתמודדות עם מגפת הקורונה

איתי סלע

הקדמה

תהליך הגמילה מאנרגייה רוסית שעובר על אירופה בעקבות המלחמה בין רוסיה לאוקראינה ותגליות הגז האחרונות מול חופי ישראל העלו את הפלטפורמות הימיות המתבססות בפעילותן על מערכות מחשוב תפעוליות על סדר היום הציבורי בארץ ובעולם, ומסמנות אותן כמטרה איכותית לתקיפות סייבר עם השלכות רחבות בהיבטים אסטרטגיים, ביטחוניים, כלכליים, סביבתיים ומדינתיים.

מאז התפרצות מגפת הקורונה התרחבה המגמה של השימוש בנשק הסייבר לתקיפה של מערכות מחשוב תפעוליות, לדוגמה: חברת מייקרוסופט דיווחה על יותר מ-200 תקיפות סייבר, ויותר מ-40% מהן כוונו לרשתות תפעוליות ולתשתיות קריטיות.¹ גם דוח של הבולשת הפדרלית האמריקנית (FBI) המסכם את שנת 2021, מצביע על כ-649 תקיפות כופר שפגעו בארגונים העוסקים בתשתיות קריטיות בארצות הברית;² על גילוי התוכנה הזדונית Incontroller/ Pipedream שיועדה לפגוע במערכות תפעוליות ובעלת יכולת תקיפה נדירה ומסוכנת במיוחד (ההערכה היא שהתוכנה פותחה בחסות מדינתית);³ על תקיפה באמצעות תוכנת הכופר "Ekans" שהתמקדה במערכות תפעוליות;⁴ על מתקפת סייבר נגד רשתות תקשורת לווייניות מסחריות (SATCOM Network);⁵ על תקיפת סייבר רחבה שפגעה במערכות תפעוליות במסופי נפט במערב אירופה (הולנד, בלגיה וגרמניה);⁶ על תקיפת חברת קידוח המפעילה אסדות קידוח ימיות;⁷ ועל תקיפה של יצרן מערכות תפעוליות ימיות.⁸

¹ Ravie Lakshmanan, [Microsoft Documents Over 200 Cyberattacks by Russia Against Ukraine](#), *The hacker news*, April 29, 2022.

² Federal Bureau of Investigation, [Internet crime report 2021](#), FBI IC3, 2022.

³ Nathan Brubaker, Keith Lunden, Ken Proska, Muhammad Umair, Daniel Kapellmann Zafra, Corey Hildebrandt, Rob Caldwell, [Incontroller: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems](#), *Mandiant*, April 13, 2022; [Pipedream: Chernovite's Emerging Malware Targeting Industrial Control Systems](#), *Dragos*, Free whitepaper, April 2022.

⁴ Scott Ferguson, [New Ransomware Targets Industrial Controls: Report](#), *Info risk today*, February 5, 2020.

⁵ Antony J. Blinken, [Attribution of Russia's Malicious Cyber Activity Against Ukraine](#), *U.S. Department of State*, May 10, 2022.

⁶ The Editorial Team, [Cyber-attacks hit European oil terminals](#), *Safety4Sea*, February 4, 2022.

⁷ KCA Deutag Alpha Limited, [Annual Report and Financial Statements for the year ended 31 December 2021](#), May 12, 2022.

⁸ Sam Chambers, [Voyager Worldwide hit by cyber attack](#), *Splash247*, December 9, 2022.

מאמר זה מנתח את איומי הסייבר על פלטפורמות ימיות אזרחיות מתוך התייחסות לייחודיות ולפגיעות מערכות המחשוב התפעוליות (Operation Technology – OT) הנמצאות על גבי פלטפורמות ימיות, בהיבטי סייבר. ייעשה ניסיון להשיב על השאלות המתבקשות: האם איום זה הוא משמעותי? ואם כן, האם ניתן להשליך מדרכי ההתמודדות עם מגפת הקורונה על תפיסות ההגנה בהתמודדות מול איום הסייבר הימי?

רקע

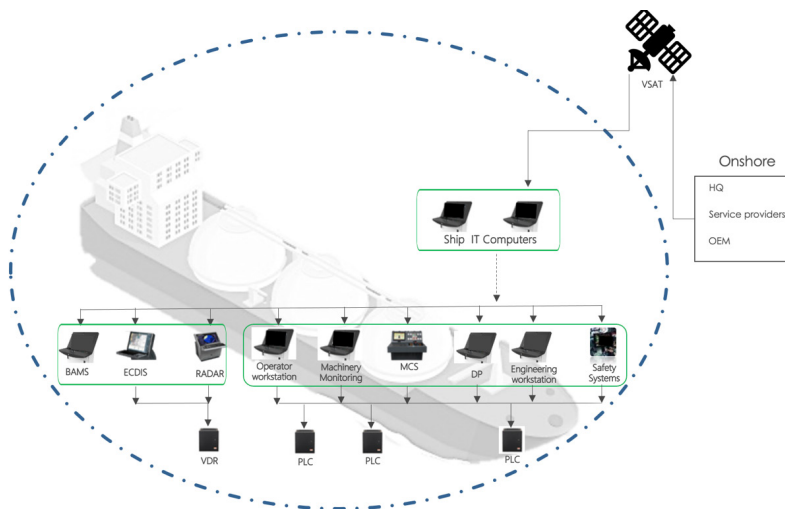
במהלך ארבעת העשורים האחרונים חלה התקדמות ניכרת בטכנולוגיות הנמצאות בשימוש על גבי פלטפורמות ימיות (כלי שיט מסחריים, אוניות נוסעים, אסדות קידוח, הפקה וכדומה) – מפלטפורמות שנבנו בתחילת שנות ה-80, והתבססו על טכנולוגיה פשוטה יחסית, דרך פלטפורמות שנבנו בתחילת המאה ה-21 שבהן רואים שימוש גובר בטכנולוגיות מבוססות מחשוב ועד כניסתן לשימוש של הפלטפורמות שנבנו בעשור האחרון, המתבססות כמעט באופן מוחלט על טכנולוגיות מחשוב מתקדמות, הן מבחינת טכנולוגית המידע (Information Technology), והן מבחינת הטכנולוגיה התפעולית (Operation Technology).

טכנולוגיית ה-IT מסייעת בניהול והעברת מידע בין הפלטפורמות הימיות למטה החברה, ספקים שונים, נמלי הים והרשויות המגוונות שאיתן נמצאות הפלטפורמות הימיות בקשר רציף. טכנולוגיה זו משתמשת ברשתות תקשורת לווייניות, סלולריות ואלחוטיות במטרה להעביר את המידע בין הפלטפורמה הימית לגורמים השונים בחוף ובים. מחשבי רשתות המידע נמצאים בדרך כלל בגשר הפיקוד, משרדים, המדורים השונים ובמגורים שעל גבי הפלטפורמה – מערכות ורשתות אלו מופרדות בהגדרה מהמערכות ומהרשתות התפעוליות.

טכנולוגיית ה-OT משמשת כממשק המחבר בין האדם למכונה, ובכך מסייעת בביצוע הפעולות הקריטיות. על גבי פלטפורמה ימית יש בממוצע כ-70 מערכות תפעוליות. מערכות אלו מסופקות ומתוחזקות על ידי מגוון יצרנים, פועלות על סוגים שונים של מערכות הפעלה (Win XP/7/10, Linux), מריצות אפליקציות מגוונות, דורשות רמת אמינות וזמינות גבוהה, ונדרשות לפעול ברציפות 24/7, במשך מרבית ימות השנה. מערכות אלו מופעלות על ידי אנשי צוות ימיים הנדרשים להפעיל את הפלטפורמה במשמרות מסביב לשעון למשך תקופות ארוכות (מספר שבועות עד מספר חודשים ברציפות), ופעמים רבות ללא הכשרה מתאימה בתחום הגנת הסייבר.

איום 1 מציג סוגים שונים של מערכות תפעוליות המותקנות על גבי פלטפורמות ימיות כדוגמת: מערכת ניווט ECDIS (Electronic Chart Display and Information System) המחליפה את תרשימי הניווט מנייר, ותפקידה לייעל את הניווט ולצמצם תאונות על ידי ריכוז והצגת מידע גאוגרפי המבוסס על תרשימי ניווט דיגיטליים ושילובו עם שכבות מידע נוספות (עצמים שהתגלו על ידי מכ"מ, מיקום GPS, נתוני AIS, עומקים ועוד); מערכת (Radio Detection And Ranging) RADAR; מערכת (Ranging Bridge Alert Management) BAMS או בעברית מכ"מ (מגלה כיוון ומרחק) המאפשרת בניית תמונת מכשולי ניווט בעזרת גלי רדיו אלקטרומגנטיים; מערכת ריכוז התראות (System) הממוקמת בגשר כלי השיט ומטרתה לסייע לקצין המשמרת לנהל את ההתראות

המתקבלות מהמערכות השונות; מערכת בקרת מכונות (Machinery Control System) MCS המשמשת לשליטה, בקרה וניטור מערכות המכונה דוגמת מנועים, משאבות, מערכות יציבות, מערכות ייעודיות דוגמת: מערכות בקרת לחץ (Managed Pressure Drilling) MPD; מערכת ניתוק חירום (Blowout Preventer) BOP; מערכת (Voyage Data Recorder) VDR המשמשת כקופסה השחורה הימית המחוברת לרוב מערכות הניווט, המכונה והבטיחות שעל גבי כלי השיט; מערכת לשמירת מיקום (Dynamic Positioning) DP, מיזוג אוויר, מעליות, וסנסורים שונים כדוגמת (Global Positioning System) GPS ו-(Automatic Identification System) AIS) המזינים את המערכות התפעוליות השונות. התקשורת בין המערכות השונות על גבי הפלטפורמה מתבססת על תקן תקשורת בשם (NMEA 0183/2000 National Marine Electronics Association) הנמצא בשימוש בתעשייה הימית, ומגדיר תקינה לאותות חשמליים, פרוטוקולים, זמן העברת נתונים ותבניות ספציפיות.⁹



איור 1: פריסת מערכות מחשוב תפעוליות מרכזיות בבלי שיט מסחרי

ייחודיות מערכות המחשוב התפעוליות בהיבטי סייבר

במשך השנים האחרונות נצפתה עלייה ניכרת בשימוש בנשק הסייבר כנגד פלטפורמות ותשתיות ימיות.¹⁰ הופעתו של נשק הסייבר, שהוגדר על ידי ריד ומקברני כתוכנה זדונית המשמשת להשגת מטרות צבאיות או מודיעיניות כחלק מתקיפת סייבר,¹¹ הפכה את מערכות

⁹ National Marine Electronics Association, [NMEA 2000, standard for serial-data networking of marine electronic devices](#), Version 2, December 2014; Eric S. Raymond, [.NMEA Revealed](#), Retrieved December 2022

¹⁰ F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, & M. Michaloliakos, [Cybersecurity Challenges in the Maritime Sector](#). *Network*, 2, no. 1 (2022): 123–138

¹¹ Thomas Rid & Peter McBurney, [Cyber-Weapons](#), *The RUSI Journal*, 157, no. 1 (2012): 6–13

המחשוב התפעוליות על גבי פלטפורמות ימיות לחשופות ופגיעות ביותר בעקבות מספר גורמים המייחדים אותן ואת סביבתן.

הגורם הראשון הוא שמערכות המחשוב התפעוליות מתבססות על מערכות הפעלה מיושנות, אשר אינן נתמכות על ידי יצרן מערכות ההפעלה מבחינת עדכוני אבטחה ועדכוני תוכנה. אחת מהסיבות המרכזיות לכך היא הפער המובהק במחזור החיים של גוף הפלטפורמה הימית הנע בין 20–30 שנה, למחזור החיים של המערכות התפעוליות השונות הנע בין 5–10 שנים, בעקבות ולמחזור החיים של מערכות ההפעלה במחשבים התפעוליים הנע בין 5–10 שנים. בעקבות פער זה נוצר מצב שבמרבית הפלטפורמות הימיות הפעילות כיום, הרוב המכריע של מערכות המחשוב התפעוליות מתבססות על מערכות הפעלה מיושנות שפותחו בעידן שבו לא הייתה מפותחת המודעות לאיום הסייבר, ולכן באופן מובנה יש בהן פרוצדורות אבטחה רבות. נוסף לכך, מערכות אלו אינן נתמכות על ידי יצרן מערכות ההפעלה, לדוגמה מערכות ההפעלה "Windows XP" של חברת Microsoft, שהתמיכה הטכנית ועדכוני האבטחה של Microsoft בהן הסתיימו באפריל 2014¹² ומערכות ההפעלה "Windows 7" שהתמיכה הטכנית ועדכוני האבטחה שלהן הסתיימו בינואר 2020.¹³ לאחרונה התחילו יצרני המערכות התפעוליות לשווק מערכות חדשות המבוססות על מערכות הפעלה "Windows 10" הנחשבת לעדכנית, ושעדיין נתמכת על ידי חברת Microsoft בהיבטים טכניים ובהיבטי אבטחה, אולם כבר כיום מפרסמת Microsoft שהיא תתמוך בתוכנה זו רק עד אוקטובר 2025.¹⁴

הגורם השני הוא משמעויות השדרוג (עלות וזמן "עמידה"). אף על פי שיצרני המערכות התפעוליות (בממוצע כעשרה יצרנים שונים על גבי פלטפורמה ימית אחת) מעדיפים ודוחפים את בעלי הפלטפורמה לערוך שדרוג גרסה כל 4–6 שנים, בעלי הפלטפורמה יעשו כל שביכולתם להימנע מהשדרוג הנדרש, וינסו לתחזק ולשמר את המערכות הקיימות. זאת מכיוון שמבחינת בעל הפלטפורמה שדרוג בסדר גודל כזה יכול להסתכם בעלויות ישירות של מאות אלפי דולרים (בכלי שיט מסחרי) ולהגיע עד עשרות מיליוני דולרים (בפלטפורמת אנרגייה ימית) לשדרוג המערכות עצמן, נוסף למשמעויות והעלויות הכרוכות בהעמדת הפלטפורמה (עצירת פעילות) למטרת השדרוג הנדרש. לנוכח מגמות השוק כיום, שלפיהן מרבית הפלטפורמות הימיות פועלות בשיטה הנקראת "פלטפורמה חמה" שמשמעותה עבודה רציפה למעט הפסקות קצרות הנדרשות לצורך מעבר מחוזה אחד למשנהו, המגמה הרווחת בתעשייה היא לערוך חוזים קצרים בלבד. כך כל עצירה וניסיון להטמיע שדרוג מערכות כלשהו, המחייב עצירת פעילות לתקופה של בין חודשיים עד שנה, ישפיעו ישירות ומשמעותית על רווחיות הפלטפורמה הימית.

הגורם השלישי הוא הפער בהפרדת רשתות התקשורת המנהלתיות והתפעוליות. ניתן לחלק את רשתות התקשורת הפרוסות על גבי פלטפורמה ימית לשניים: רשתות מנהלתיות המחברות בין מערכות המידע השונות ורשתות תפעוליות, המחברות בין מערכות המחשוב התפעוליות

¹² Eve Blakemore, [Support for Windows XP ends in April 2014](#), Microsoft, April 30, 2013

¹³ [Windows 7 support ended on January 14, 2020](#), Microsoft, 2020

¹⁴ [Windows 10 Home and Pro](#), Microsoft, 2021

השונות. התפיסה הרווחת כיום בתעשיית הימית מתייחסת למערכות ולרשתות התפעוליות כמבודדות ומנותקות מהרשת המנהלתית ומהאינטרנט, ולכן רשתות אלו נתפסות כחשופות פחות לאיומי הסייבר השונים. וזאת למרות שבפועל נוהלי העבודה המקובלים בתעשייה הימית חושפים את הרשתות והמערכות התפעוליות לרשתות המנהלתיות, ויוצרים מצב הנקרא "רשת שטוחה", המאפשר לקוד זדוני הנכנס לרשת אחת להתפשט בקלות יחסית לרשתות אחרות ולמערכות תפעוליות קריטיות רבות על גבי הפלטפורמה.

הגורם הרביעי הוא נתיבי התקיפה שמשמשים בהם התוקפים כדי לחזור ולפגוע במערכות מחשוב תפעוליות בפלטפורמה ימית. הנתיב הראשון, כפי שניתן לראות באיור 2, הוא נתיב התקיפה החיצוני (External Attack Vector), המשתמש ברשת המידע של הפלטפורמה (המתבססת על תווך תקשורת לווייני, סלולרי ואלחוטי) ובנותני השירותים הרבים (מטה החברה, החברה החוכרת את הפלטפורמה, גורמים רגולטוריים בין-לאומיים ומדינתיים, גורמים טכניים, אחזקה והספקה) כדלת כניסה למערכות התפעוליות שעל גבי הפלטפורמה הימית. לאחר שהקוד הזדוני הצליח להיכנס למערכת אחת על גבי הפלטפורמה, הקוד הזדוני ינצל את הפערים בהפרדת הרשתות, ויתפשט בקלות יחסית בין הרשתות והמערכות התפעוליות השונות. דוגמה לתקיפה שהשתמשה בנתיב תקיפה זה דווחה בפברואר 2017 לאחר שזוהתה פגיעה במערכת תפעולית של אוניית מכולות ששטה מקפריסין לג'יבוטי. לפי התיאור, קובץ התקיפה נכנס מרשת המידע של כלי השיט לרשת התפעולית, והשתלט על מערכת הניווט של כלי השיט למשך כעשר שעות, ובתוך כך פגע בבטיחות השיט וביכולתו של הצוות לתפעל את המערכות. לפי הדיווח, כוונתם של התוקפים הייתה להשיג שליטה מלאה במערכות הניווט, ולהפנות את כלי השיט לאזור שבו יוכלו להשתלט עליו פיזית, ורק לאחר סיוע ממטה החברה הצליח הצוות להחזיר לעצמו את השליטה במערכת הניווט.¹⁵

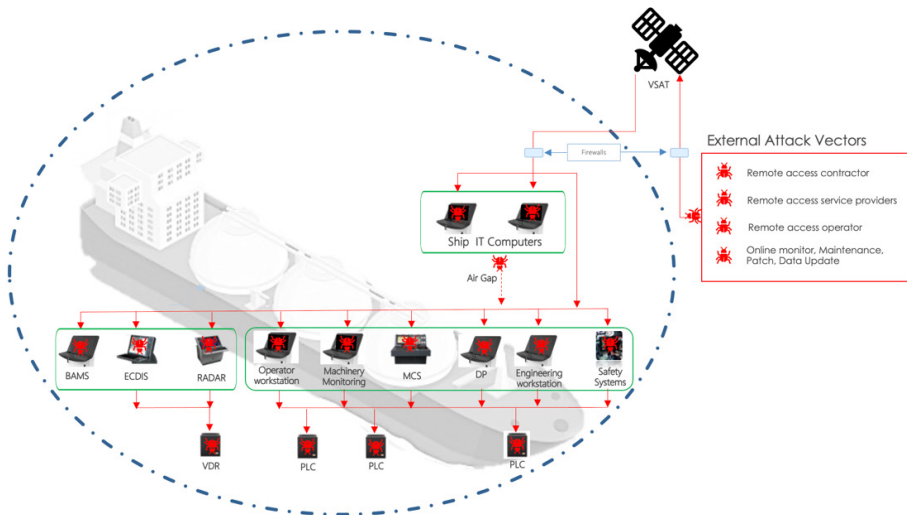
הנתיב השני, כפי שניתן לראות באיור 3, הוא נתיב התקיפה הפנימי (Internal Attack Vector) המשתמש בגורמים עם הרשאות גישה למערכות התפעוליות לצורך פעילות שגרתית (אנשי הצוות וטכנאים של היצרנים העובדים על הפלטפורמה) וללא ידיעתם, להחדרת הקוד הזדוני ממחשב מנהלתי למערכת תפעולית. דוגמאות לתקיפות שעשו שימוש בנתיב תקיפה זה הן: (א) בשנת 2013 דווח על תקיפת סייבר אשר הצליחה להחדיר קוד זדוני למחשב טכנאי חוף, שבמסגרת אחזקה שוטפת על גבי פלטפורמת אנרגייה ימית, וללא ידיעתו של הטכנאי העביר את הקוד הזדוני ממחשב הטכנאי למערכות תפעוליות באסדה – אירוע שהוביל להשבתת האסדה לאחר שהתברר שמערכות הניווט, ההנעה, שמירת המיקום ומערכות הקידוח נפגעו באופן ניכר.¹⁶ (ב) בשנת 2018 דווח על תוכנה זדונית רדומה שהתגלתה במערכות כלי שיט לאחר כ־875 יום. מניתוח האירוע נמצא כי ספק השירות החדיר, ללא ידיעתו, את התוכנה הזדונית למערכת כלי השיט באמצעות כונן זיכרון נייד (USB) בעת עדכון תוכנה.¹⁷ (ג) באותה

¹⁵ IMO, [International Maritime Organization maritime knowledge centre "sharing maritime knowledge"](#), Current Awareness Bulletin, XXIX(11), November 2017

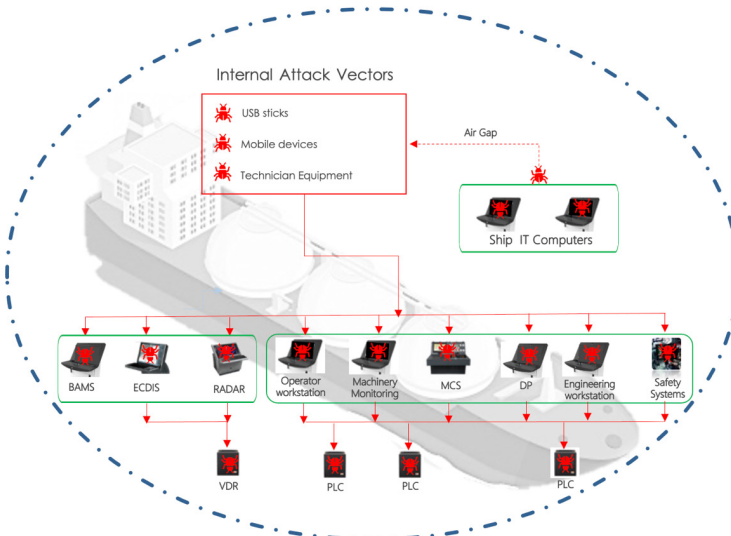
¹⁶ Zain Shauk, "[Malware on Oil Rig Computers Raises Security Fears](#)", *Houston Chronicle Energy*, February 23, 2013

¹⁷ [The guidelines on cyber security onboard ships](#), Version 4 (2021)

השנה דווח על תקלה טכנית בשתי מערכות ECDIS על גבי אוניית משא חדשה, שבהמשך התגלו כנגועות בתוכנה זדונית אשר גרמה לעיכוב הפלגת האונייה, ונזק של מאות אלפי דולרים.¹⁸



איור 2: נתיבי תקיפה חיצוניים בכלי שיט, ותיאור התפשטות הקוד הזדוני ממערכות המידע למערכות התפעוליות השונות

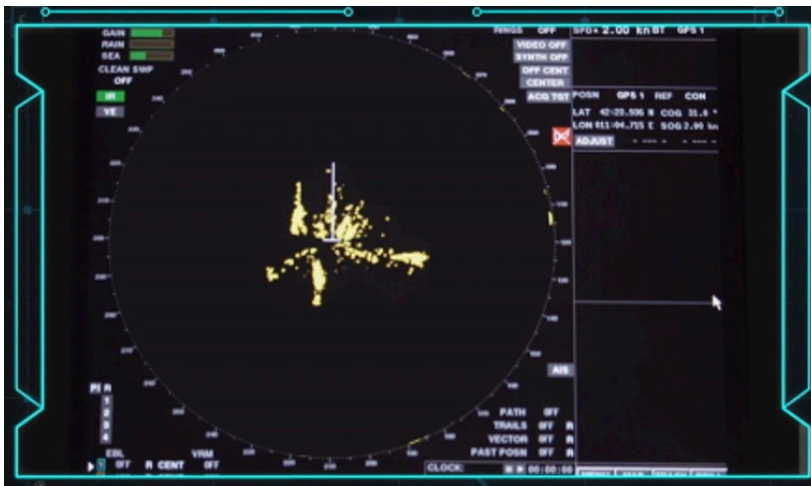


איור 3: נתיבי תקיפה פנימיים בכלי שיט והתפשטות הקוד הזדוני לכלל מערכות המחשוב התפעוליות

האם איום הסייבר על פלטפורמות ימיות הוא משמעותי?

במטרה להתמודד עם שאלה זו ונוסף לאיסוף נתונים של תקיפות סייבר שפורסמו, נבחנו ונתחו ממצאים מרכזיים של מספר סימולציות של תקיפת סייבר: הסימולציה הראשונה בחנה היתכנות ומשמעות של פגיעת סייבר במערכות מחשוב תפעוליות קריטיות על גבי כלי שיט כדוגמת: מכ"מ (RADAR), מערכת ניווט אלקטרונית (ECDIS), מערכת בקרת מכונה (MCS).¹⁹ הסימולציה השנייה בחנה את ההיתכנות והמשמעות של פגיעת סייבר במערכת שמירת מיקום דינמית (DP) בסביבה המדמה אסדת קידוח.²⁰

כחלק מבחינת ההיתכנות של תקיפת סייבר על מערכת מכ"מ בפלטפורמה ימית הוחדר קוד זדוני למערכת המכ"מ (מערכת מחשוב תפעולית) המשמשת כעזר ניווט שמטרתו לאתר ולהתריע על מכשולי ניווט ובכך למנוע התנגשות. מערכת המכ"מ משדרת גלי רדיו אלקטרומגנטיים ומציגה את האותות החוזרים ממכשולי הניווט על גבי צג המכ"מ כנקודה בהירה. הקוד הזדוני שהוחדר למערכת המכ"מ הצליח ליצור מניפולציה, כך שבתמונת המכ"מ שהוצגה לקצין הניווט בגשר, כפי שניתן לראות באיור 4, לא הופיעו (הועלמו) מכשולי הניווט בסביבת הפלטפורמה הימית, ולא הוצגו התראות המאפשרות למפעיל המערכת להבין שמשוה אינו כשורה.²¹



איור 4: תמונת המכ"מ שהוצגה לקצין הניווט בגשר

¹⁹ [Northern California area maritime security committee, cyber security Newsletter](#), Edition 2018-07, July 2018

²⁰ Paola Rossi, Itai Sela, Adam Rizika, Diogenes Angelidis, Mark Duck, and Ron Morrison, [Cyberdefence of Offshore Deepwater Drilling Rigs](#). *Offshore Technology Conference*, Virtual and Houston, Texas, August 2021

²¹ [Tests Show Ease of Hacking ECDIS, Radar and Machinery](#), *The Maritime Executive*, December 21, 2017

וזאת למרות שבפועל ישנם מכשולי ניווט רבים בסביבת הפלטפורמה הימית, כולל כאלו הנמצאים בהמשך נתיב ההפלגה אשר הועלמו על ידי הקוד הזדוני, כפי שניתן לראות באיור 5, בתמונת המכ"מ האמיתית (ללא המניפולציה של התקיפה) (מסומנים בעיגולים אדומים).²²



איור 5: תמונת המכ"מ האמיתית שהועלמה מקצין הניווט באמצעות מניפולציה

סימולציה זו הדגימה שתקיפת סייבר מסוגלת לייצר מניפולציה על הנתונים המוצגים לקצין הניווט, ויכולה להוביל לבניית תמונת מכשולי ניווט שגויה שתוביל להתנגשות, פגיעה בחיי אדם, נזק סביבתי ופגיעה ברכוש.

איור 6 מציג הדגמה של תקיפת מניפולציה על מערכת ניווט (ECDIS) של כלי שיט, שבעזרתו בונה הקצין בגשר את תמונת העולם ומתכנן את נתיב ההפלגה.²³ בתקיפה זו רואים בחלונית השמאלית של האיור את צג המערכת שבה מופיע מיקום כלי השיט למול מכשולי הניווט והעומק כתקינים, וזאת למרות שבפועל, כפי שניתן לראות בחלונית הימנית של האיור, מיקום כלי השיט שונה, וקרוב מאוד למכשולי ניווט. כמו כן, ניתן לראות שעומק המים רדוד ומסוכן. תקיפה זו מכוונת להציג מידע שקרי למפעיל המערכת התפעולית, כך שההחלטות שיקבל בעניין תכנון ההפלגה ובטיחות השיט יהיו שגויות, ויובילו לסטייה מהמסלול המתוכנן ואף לתאונה.

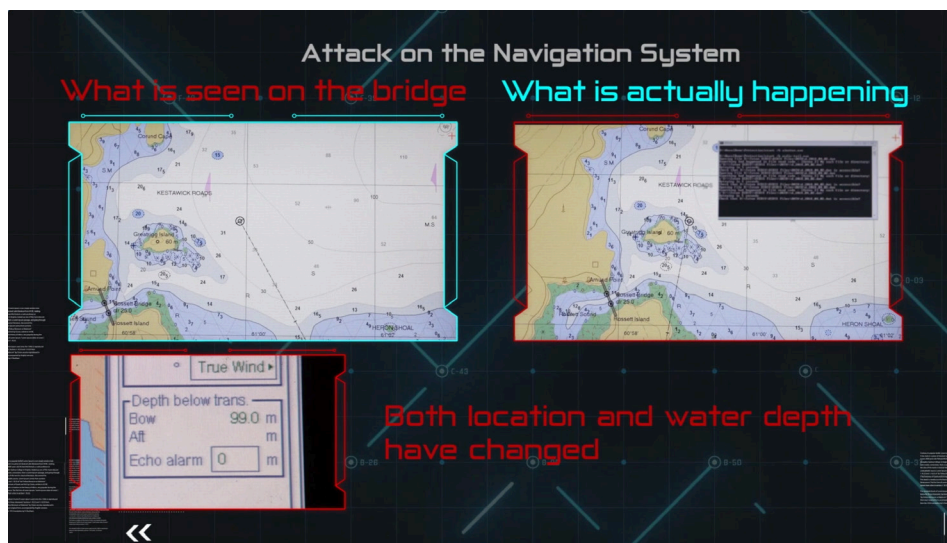
איור 7 מציג הדגמה של תקיפת מניפולציה על מערכת בקרת מכונה (MCS) השולטת על מנועי כלי השיט, מערכות היציבות, האיזון ומערכות נוספות שמאפשרות לקצין המכונה להפעיל ולבקר את פעולת מערכות כלי השיט.²⁴ בתקיפה זו ניתן לראות בחלונית השמאלית של האיור את מסך בקרת המכונה המציג משאבה אחת פועלת, למרות שבפועל, כפי שניתן לראות

²² Ibid.

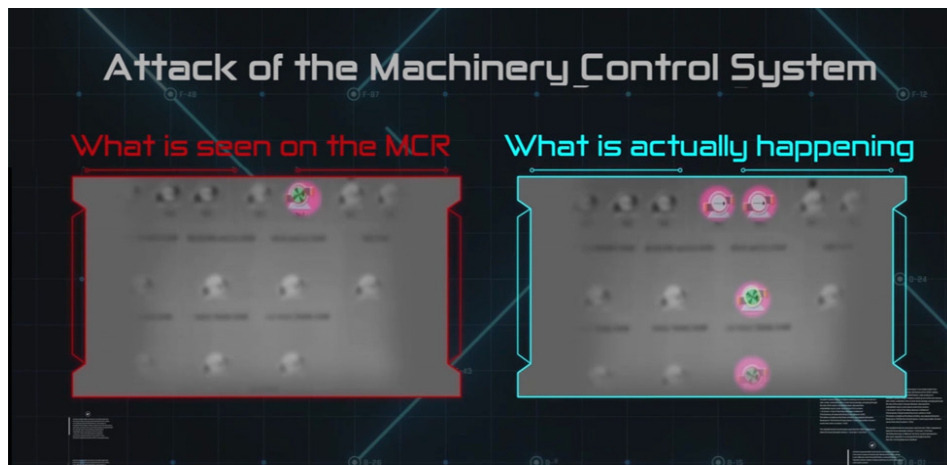
²³ [Ethical hackers demonstrate weaknesses in shipboard systems](#), *Digital Ship*, January 2, 2018.

²⁴ [The Challenge](#), *NavalDome Website*, Retrieved December 2022

בחלונות הימנית, אותה משאבה כלל אינה פועלת, ואילו מספר משאבות אחרות המוצגות ככבויות כן פועלות ללא ידיעתו של קצין המכונה. תקיפה זו מכוונת למנוע ולשבש פעולות קריטיות, ולהציג מידע שקרי למפעיל המערכת, ובכך להוביל לפגיעה בכושר השיט, לפליטת נוזלים/גזים לא רצויה ולא מבוקרת, לשליטה על מערכות ההנעה וההיגוי של כלי השיט שיכולים להוביל לפגיעה כלכלית, סביבתית ובחיי אדם.



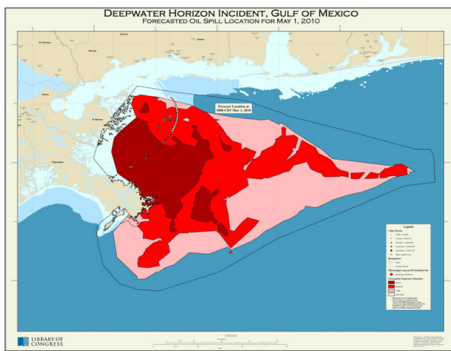
איור 6: תקיפת מניפולציה על מערכת ניווט (ECDIS)



איור 7: תקיפת מניפולציה על מערכת בקרת מכונה (MCS)

סימולציית תקיפת סייבר על מערכת שמירת מיקום דינמית בסביבה המדמה אסדת קידוח

כחלק מבחינת ההיתכנות של תקיפת סייבר על מערכת שמירת מיקום דינמית (DP) (מערכת מחשוב תפעולית), הודגם שימוש בציר תקיפה פנימי (Internal Attack Vector) שבו מחשב שהיה בשימוש טכנאי היצרן הודבק, ללא ידיעתו, בקוד זדוני. הקוד הזדוני השתלט על מערכות שמירת המיקום והתפשט למערכות קריטיות נוספות הקשורות לבטיחות האסדה והקידוח.²⁵ סימולציה זו הוכיחה את היכולת של קוד זדוני לעבור דרך מנגנוני אבטחת הסייבר הנמצאים כיום בשימוש על גבי אסדות קידוח, לשלוט שליטה מלאה על מערכות תפעוליות קריטיות על גבי אסדת קידוח,²⁶ ולשחזר באמצעות תקיפת סייבר כשלים דומים לאלו שהובילו לאירוע דליפת הנפט "Deepwater Horizon" שהתרחש בשנת 2010 במפרץ מקסיקו, שבו נהרגו 11 אנשי צוות, נגרם נזק כלכלי בעלות של יותר מ-140 מיליארד דולר ונזק סביבתי אדיר, כפי שניתן לראות באיור 27.8.



איור 8: אירוע דליפת הנפט "Deepwater Horizon" שהתרחש בשנת 2010 במפרץ מקסיקו

מניתוח תקיפות הסייבר והסימולציות על מערכות תפעוליות הפועלות על גבי פלטפורמות ימיות שונות ניתן להסיק, שאיום הסייבר על פלטפורמות ימיות הוא משמעותי, ויש לו פוטנציאל נזק אסטרטגי רחב עם השלכות סביבתיות, כלכליות, מדיניות ולחיי אדם.

²⁵ Rossi et al., Cyberdefence of Offshore Deepwater, 2021.

²⁶ Mahesh Sonawane, Ryan Koska, Mike Campbell [Riser failure study IDs well control weak links](#), *Drilling Contractor News*, March 15, 2012.

²⁷ National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, [Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling](#). Report to the President, January 2011.

אופן ההתמודדות עם האיום ניתן להשליך מדרכי ההתמודדות עם מגפת הקורונה על תפיסות הגנת סייבר?

לאחר שהוגדר איום הסייבר על פלטפורמות ימיות כמשמעותי, נעשה ניסיון לבחון את השאלה: האם ניתן להשליך מדרכי ההתמודדות עם מגפת הקורונה על תפיסות ההגנה בהתמודדות מול איום הסייבר הימי? במטרה להשיב על שאלה זו נבחנו תפיסות הגנה שונות, והיכולת לבחון אותן למול אופן ההתמודדות עם מגפת הקורונה.

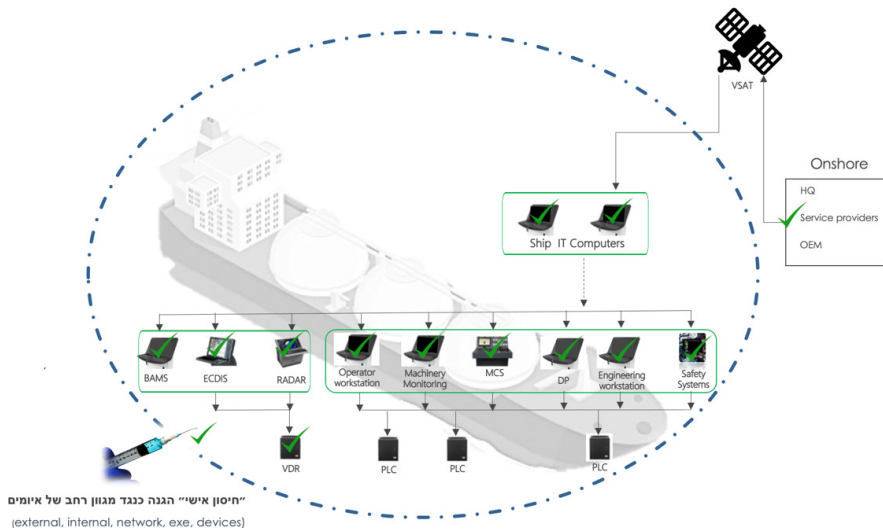
ניתן להצביע על שלוש תפיסות הגנה מרכזיות הנמצאות כיום בשימוש על גבי פלטפורמות ימיות אזרחיות במטרה להגן כנגד איום הסייבר על מערכות מחשוב תפעוליות: התפיסה הראשונה והמקובלת ביותר רואה בגורם האנושי אחראי מרכזי לשמירה על הפלטפורמה מפני איום הסייבר, ולכן מתמקדת בחינוך והדרכה של אנשי הצוות והטכנאים להיגיינת סייבר, וזאת בדומה לתפיסת ההתמודדות עם מגפת הקורונה, שבשלב הראשון התמקדה בחינוך והדרכה של האוכלוסייה (הקפדה על עטיית מסכות, ריחוק חברתי ונטילת ידיים) ובהמשך התבררה כתפיסה המתקשה להתמודד מול איומים מורכבים כדוגמת איומי סייבר ומגפות. התפיסה השנייה מתבססת על הניסיון ליצור הפרדת רשתות פיזית, לצמצם כניסה והתפשטות התקיפה, בדומה לתפיסת הסגרים בקורונה, והטמעת פתרונות ניטור טכנולוגיים שתפקידם לזהות ולהתריע על התנהגויות חריגות או לא מורשות בעקבות כניסת קוד זדוני, בדומה לניטור הטלפונים הסלולריים, הצבת מחסומים בכבישים, ובדיקות במעברי הגבול. כפי שהיה בהתמודדות עם מגפת הקורונה ומול איום הסייבר הימי, מתברר שהתראה וניטור נותנים מענה הגנתי חלקי אך ורק לנתיב התקיפה החיצוני. לעומת זאת, כאשר אנחנו בוחנים את רמת ההגנה של תפיסה זו בהתבסס על תקני הגנת סייבר בין-לאומיים למערכות תפעוליות,²⁸ ניתן לראות שתפיסה זו מספקת הגנה ברמה בסיסית (SL-1) בלבד, כמפורט בטבלה 1 להלן בהתאם לתקן שפורסם בשנת 2018 על ידי חברת הסיווג DNV-GI, ומכיל את תקן ISA/IEC 62443 (של הנציבות הבין-לאומית האלקטרו-טכנית) המשמש כתקן בטיחות סייבר במערכות אוטומציה ובקרה בתעשיית הנפט והגז על טכנולוגיות מחשוב המוטמעות בתעשייה הימית.

טבלה 1: הגדרת רמות הגנה למול יכולות ההגנה ואופי האיום

רמת הגנה (Security Levels)	יכולות הגנה למול אופי האיום
SL-1	הגנה כנגד תקיפות סייבר אקראיות או עם יכולות בסיסיות
SL-2	הגנה כנגד תקיפות סייבר מכוונות באמצעים פשוטים, משאבים ומוטיבציה נמוכים ויכולות בסיסיות
SL-3	הגנה כנגד תקיפות סייבר מכוונות באמצעים מתוחכמים, משאבים ומוטיבציה בינוניים, היכרות טובה של המערכות ויכולות טכניות מתאימות
SL-4	הגנה כנגד תקיפות סייבר מכוונות באמצעים מתוחכמים, משאבים ומוטיבציה גבוהים, היכרות טובה של המערכות, יכולות טכניות מתאימות ומוטיבציה גבוהה.

²⁸ [International Electrotechnical Commission \(ISA/IEC\) 62443, Security for industrial automation and control systems, Part 4-1: Secure product development lifecycle requirements \(2018\)](#); [DNVGL-CP-0231 Cyber security capabilities of systems and components, \(2018\)](#)

התפיסה השלישית מתבססת על תוכנות הגנה אקטיביות המותקנות על כל אחת ממערכות המחשוב התפעוליות ומשמשות כ-"חיסון אישי"²⁹, אותה ניתן לכנות גם בשם "הגנה מהפנים החוצה" (Inside-Out). כפי שניתן לראות באיור 9, תפיסה זו מתמקדת בהטמעת תוכנת הגנה מניעתית ואקטיבית בכל אחת ממערכות המחשוב התפעוליות הפזורות על גבי הפלטפורמה הימית, ובכך מספקת מענה הגנתי לשני נתיבי התקיפה גם יחד (החיצוני והפנימי), ומספקת את רמת ההגנה הגבוהה ביותר כנגד תקיפות מדינתיות (SL-4). תפיסה זו אינה מצריכה שדרוג מערכות, עדכונים שוטפים, הכשרה וידע מקדים בסייבר, היא מתאימה להגנה על מערכות ישנות וחדשות, מנותקות או מחוברות, ומאפשרת ליצרני המערכות (OEM's) התקנה עצמאית ובזמנים קצרים (מערב בין חוזים). בהקבלה למגפת הקורונה, משפותח והוטמע החיסון האישי לקורונה, שגם אותו ניתן לכנות "הגנה מהפנים החוצה", נצפתה ירידה דרמטית במספר החולים, ההדבקה ומסוכנות המגפה, מה שאיפשר לאנשי המקצוע ולמנהיגים לקבוע שזו הדרך המתאימה ביותר להתמודדות עם המגפה.



איור 9: תפיסת ההגנה "מהפנים החוצה" על פלטפורמה ימית

סיכום והמלצות

הממצאים העיקריים במאמר זה מצביעים על כך שבעשור האחרון נהיו פלטפורמות ימיות אזרחיות תלויות יותר ויותר במערכות מחשוב תפעוליות, המבוססות, ברובן, על מערכות הפעלה מיושנות ללא עדכוני אבטחה, עם יכולות ניטור מוגבלות, ובדרך כלל ללא הגנת סייבר. פערים טכנולוגיים אלו הופכים את המערכות התפעוליות לנקודת תורפה בהיבטי סייבר, עם רמת הגנה בסיסית (SL-1) שאינה מותאמת להתמודדות עם האיום הגובר הן בהיקפים והן בתחום. אלה יוצרים חשש אמיתי לפגיעה בפלטפורמות ימיות הפועלות, מפליגות ועוגנות

בנמלים ובשטחים הימיים הישראליים (טריטוריאליים והכלכליים), מה שעלול להוביל להשלכות ניכרות בהיבטים אסטרטגיים, ביטחוניים, כלכליים, סביבתיים ומדינתיים.

מומלץ למקבלי ההחלטות השונים ולנציגי התעשייה הימית בישראל (רגולטורים, בעלי כלי שיט מסחריים, חברות שילוח ימיות, חברות אנרגייה ונמלי ים) לבחון מחדש את רמת איום הסייבר הנשקפת לכל אחד מהמרכיבים השונים של התעשייה הימית למול רמת הגנת הסייבר הקיימת על גבי הפלטפורמות הפועלות בשטח הימי של ישראל. כמו כן, מומלץ למקבלי ההחלטות בישראל לאמץ את תקינת הסייבר ISA/IEC 62443 המאפשרת לכמת את האיום ולהגדיר את רמת ההגנה הנדרשת (Security Levels – 1,2,3,4), לחדד בהתאם את הגדרות האסדרה, ולהפוך אותה למחייבת, להדק את הביקורות בהקשרי הגנת סייבר על בעלי הפלטפורמות הימיות (חברות הספנות וחברות האנרגייה) הפועלות בנמלי ישראל ובתחומי המים (הטריטוריאליים והכלכליים) של ישראל. כמו כן לבנות תוכנית עבודה שתאפשר הערכות מדינתית להתמודדות עם אירוע המתחיל בתקיפת סייבר על פלטפורמה ימית הפועלת בתחומי ישראל ומסתיים בנזקים והשלכות רחבות היקף בהיבטי חיי אדם, סביבה, כלכלה וביטחון.

שינויים טכנולוגיים משבשים בתחום הספנות והנמלים כהזדמנות לישראל¹

אהוד גונן

תחומי הספנות וחלקים מענף הלוגיסטיקה הימית הקשורים אליה הם חלק ממגזר 'הכלכלה הכחולה'², קרי פעילות כלכלית הקשורה לים.³ פיתוח טכנולוגיות ימיות תואר על ידי OECD כאחד מהגורמים המרכזיים בפיתוח כלכלה כחולה. בדוח מפורט שפורסם בשנת 2016 והצופה את התפתחות הכלכלה הכחולה עד שנת 2030 מציין הארגון שורה של טכנולוגיות כגון חיישנים, לוויינים, מערכות אוטונומיות וביג-דטא המאוגדים לכדי מכלולים חדשים המשנים את פני הכלכלה הכחולה, ובאופן ספציפי את תחום הספנות, הניווט, התחבורה הימית ו'האונייה החכמה'.⁴

יש לציין כי תחום הספנות והנמלים הוא תחום שמרני יחסית הפועל לפי אסדרה (רגולציה) עולמית, וכולל השקעות הון גדולות. זאת אחת הסיבות לכך שהתחום חווה מהפכה דיגיטלית מאוחרת יחסית, וכניסת טכנולוגיות משבשות (Disruptive Technologies) רק בעשור האחרון. הגופים העולמיים המאסדרים את תחום הספנות ובעיקר ארגון הספנות העולמי International Maritime Organization – IMO פועלים בשנים האחרונות לבניית מסגרת רגולטורית לכניסת טכנולוגיות חדשות ובהן טכנולוגיות אוטונומיות לתחום, אולם נושא טכנולוגיות מתקדמות לספנות עדיין לא התקבע לפי תקנים בין-לאומיים ברורים, וטרם ברורה בו הובלה טכנולוגית של חברה זו או אחרת. לפיכך, השינויים הטכנולוגיים המובהקים שחלים בתחום הספנות בשנים האחרונות הם הזדמנות ברמה הלאומית עבור ישראל.

מאמר זה עוסק בהשלכות עבור ישראל של ההתפתחויות הטכנולוגיות בתחום הספנות המסחרית והלוגיסטיקה הימית. התפתחויות אלו מגלמות בתוכן הזדמנויות עבור ישראל

¹ מאמר זה מבוסס על עבודת מחקר בנושא 'בדיקת היתכנות לאזור ניסוי לכלי שיט אוטונומיים במימי ישראל והרחבתו העתידית לאזור שבין ישראל וקפריסין' שהוכנה עבור המועצה לכלכלה וחברה במשרד ראש הממשלה.

² האיחוד האירופי מחלק את מגזר הכלכלה הכחולה לשישה ענפים: (א) תעבורה ימית וספנות, (ב) מזון, הזנה, בריאות ושירותי מערכת, (ג) אנרגיה וחומרי גלם מהים וקרקעית הים, (ד) פנאי, קיט, נופש ומגורים, (ה) הגנה על חופים ומצוקים, (ו) ניטור, שימור ובקרה. ראו: [United for Mediterranean](#).

³ לסקירה מקיפה על תחום הכלכלה הכחולה בישראל: אהוד גונן, [סקירת הכלכלה הכחולה בישראל – מצב קיים והזדמנויות](#), המרכז למחקרי מדיניות ואסטרטגיה ימית, אוניברסיטת חיפה 2022.

⁴ "The ocean Economy in 2030", OECD, 2016, (pp. 119–126, 128–130): "These include Automated Identification System (AIS), Electronic Chart Display and Information System (ECDIS), Integrated Bridge Systems/Integrated Navigation Systems (IBS/INS), automatic radar plotting aids (ARPA), radio navigation, long-range identification, and tracking (LRIT) systems, Vessel Traffic Service (VTS) and the Global Maritime Distress Safety System (GMDSS). Moreover, ships now carry global satellite navigation systems (GNSS) and will soon all have reliable ECDIS"

בשלושה מישורים: **הזדמנות כלכלית**: טכנולוגיות ספנות אוטונומיות כמנוע צמיחה ותעסוקה הן לאומי והן לאזור חיפה והצפון, **הזדמנות אזורית**: כלכלה כחולה כמצע לשיתוף פעולה אזורי במזרח הים התיכון וצפון הים האדום, **הזדמנות אסטרטגית**: טכנולוגיה ימית ככלי להתפכחות מהעיוורון הימי שבו שרויה ישראל, ככלי להגדלת העוצמה הרכה הישראלית המהווה מנוף להשפעה ישראלית אפשרית במערכת הבין-לאומית. נוסף לכך, טכנולוגיות ספנות ובעיקר 'ספנות אוטונומית' כזו הקשורה לסחר הבין-לאומי מאפשרת איסוף מידע והשפעה על שחקנים מעבר לתחום הספציפי של הספנות.

הזדמנות בתחום הכלכלי

ברמה הלאומית, ישראל ידועה בעולם בזכות האקוסיסטם המקומי בתחומי החדשנות הטכנולוגית עד כדי מיתוג המדינה כ"אומת הסטארט-אפ".⁵ עוד בשנות ה-90 הייתה ישראל מובילה עולמית בתחום כלי הטיס הבלתי מאוישים (כתב"מ). בעוד רבים מאיתנו גאים בעובדה זו, הרי שלא לעולם חוסן, ויש להמשיך בפיתוח האקוסיסטם לתחומים חדשים. השנים הקרובות הן חלון הזדמנויות עבור התעשייה הישראלית לתפוס נתח שוק משמעותי בתעשיית הספנות העולמית מעבר למשקלה היחסי של ישראל בכלכלה העולמית או בסחר העולמי, וזאת כפי שתפסה בשוקי הכתב"מים, תעשיית החלל וכלי הרכב האוטונומיים היבשתיים.

בתחום התחבורה אפשר לציין שתי יוזמות לאומיות מקבילות המתקיימות בשנים האחרונות בישראל, ומקדמות את טכנולוגיית העילית בתחומי הכלים הבלתי מאוישים באוויר וביבשה. בתחום התעופה, רשות התעופה האזרחית במשרד התחבורה בישראל (רת"א) מאשרת לכלי טיס בלתי מאוישים לטוס במרחבי תעופה אזרחיים. בזאת ישראל היא המדינה הראשונה בעולם המאשרת פעילות כזו. כטב"ם, הרמס סטארליינר מתוצרת אלביט, הנחשב למתקדם מסוגו בעולם, קיבל רישוי תעופה אזרחי המשלים את עמידתו בתנאי התקינה הבין-לאומיים (נאט"ו) לשילוב כטב"מים במרחבי תעופה אזרחיים. יש לציין כי אישור המהלך על ידי רשות התעופה האזרחית פותח אפשרויות לכלליות רחבות בפני יצרנית הכטב"ם (חברת אלביט) שכבר זכתה בחוזים לספק את כטב"ם הרמס סטארליינר למשרד ההגנה של שווייץ ולמשרד התחבורה של קנדה, והיא מספקת את כטב"ם הרמס ליותר מעשר מדינות נוספות.⁶

נוסף לכך, בינואר 2021 הושק בישראל 'מיזם הרחפנים' על ידי רשות החדשנות. במשך הניסוי מבוצעות הטסות רחפנים מעל אזורי מגורים בתל-אביב-יפו, רמת שרון, הרצליה וחדרה,⁷ ותופעל בה בעת הטסה בברזיל בניהול של אותה מערכת הניהול בישראל. החברות המשתתפות צפויות לבצע יחד כ-300 הטסות ביום מעל שטחים פתוחים, בין היתר לביצוע משימות מסוגים שונים במסלולי תעופה שאותם הקצתה מערכת השליטה המשותפת.⁸ מדובר במיזם משותף

⁵ דן סינור ושאלו זינגר, מדינת הסטארט-אפ, מנוע הצמיחה הכלכלי של ישראל (תל אביב: הוצאת מטר, 2009).

⁶ "מהפכה בתעופה העולמית", משרד התחבורה, 13 בפברואר 2022.

⁷ "מיזם הרחפנים הלאומי החל בפילוט מעל העיר חדרה", TechTime, 30 ביוני 2021.

⁸ "השלב השלישי של מיזם הרחפנים הלאומי יוצא לדרך", רשות החדשנות, 12 באוקטובר 2021.

לחברות מסחריות רבות יחד עם רשות החדשנות, רשות התעופה האזרחית (רת"א) במשרד התחבורה, חברת נתיבי איילון והרשויות העירוניות הרלוונטיות. כמו כן מוקם בירוחם שדה הרחפנים הראשון בארץ.⁹ פעילות משולבת זו של רשויות ממשלתיות, מסחור טכנולוגיות צבאיות, חברות ממשלתיות וחברות פרטיות לפי מעטפת רגולטורית מתאימה מזניקה את התחום קדימה ברמה העולמית.

תחום נוסף הוא הרכבים האוטונומיים. גם כאן ישראל היא מובילה עולמית במערכות מסוימות, מעמד שאליו הגענו הודות לתרבות יזמית, השקעות צבאיות ותוכניות ממשלתיות ורגולטוריות מתאימות. בשנת 2017 הוכרזה תוכנית לאומית לתחבורה חכמה.¹⁰ הסעיף הראשון בתוכנית הוא "קידום הקמת מרכז ניסויים לרכב אוטונומי ותומך תחבורה חכמה". עם השנים צמחו בישראל מאות חברות בתחום התחבורה החכמה, מהן מובילות עולמיות בתחומן כגון חברת "מובילאיי".

מנהלת תחבורה חכמה במשרד התחבורה בשיתוף משרד התחבורה והגורמים הרלוונטיים בממשלה, עושה מאמצים כדי ליזום, לסייע ולקדם מהלכים שיקדמו את נושא עליית הרכב האוטונומי לכביש.¹¹ משרד התחבורה מצוין כי בין הפעולות שנעשו ניתן למנות את העברת 'חוק לניסויים ברכב האוטונומי בישראל' בקריאה שנייה ושלישית בכנסת, והכנת חקיקת משנה בנושא (החוק נכנס לתוקפו באפריל 2022).¹²

בהקשר לחדשנות ולפיתוח מציינת המועצה לכלכלה במשרד ראש הממשלה כי:

מינוף החדשנות הטכנולוגית בישראל: בעוד שעד כה לא הייתה ישראל שחקן בתעשיית הרכב המסורתית, היא מסתמנת כשחקן מרכזי בתחום התחבורה החכמה, שבה יש לישראל יתרון יחסי. המעבר משלבי הפיתוח לשלבי ההטמעה של התחבורה החכמה מייצר הזדמנות משמעותית נוספת עבור ישראל, שיכולה להפוך למוקד גם של אתרי בטא.¹³

מובילות טכנולוגית ישראלית זו בתחומי התעופה והרכב האוטונומיים וכן בתחום החלל (שלא פורט) הושגו למרות שבישראל אין ייצור מובהק של פלטפורמות יבשתיות או אוויריות.

בעשור האחרון ישנן אינדיקציות על שינוי מהותי באופן פעילות תחום הספנות והנמלים, וניתן לזהות מספר תחומי תפעול שבהם מתרחש שינוי מהותי. הראשון הוא אוטומציה של תהליכים

⁹ קינן כהן, "הביקוש לניסויים המריא, ושדה הרחפנים הראשון בישראל יוקם בירוחם", חדשות וואלה, 8 באפריל 2021; נורית זומר, "שדה ניסויים ייחודי לרחפנים יוקם בקרוב ליד ירוחם", YNET, 20 בדצמבר 2020.

¹⁰ "תכנית לאומית לתחבורה חכמה", החלטת ממשלה מס' 2316 מיום 22 בינואר 2017 (הממשלה ה-34 בראשות בנימין נתניהו).

¹¹ "רכב אוטונומי", משרד התחבורה, 5 באפריל 2021.

¹² "הכנסת החלה לדון בהצעת החוק שתאפשר לראשונה בישראל לבצע ניסויים בכלי רכב אוטונומיים ללא נהג", משרד התחבורה, 8 בדצמבר 2021.

¹³ רוני בר, "ישראל נערכת למהפכת התחבורה החכמה: כלי רכב אוטונומיים, חשמליים, ההשלכות המשקיות של מחוברים ושינויים", המועצה לכלכלה, משרד ראש הממשלה, אפריל 2019.

וספנות אוטונומיות. מגמה נוספת הקשורה לאוטומציה היא התפתחות סייבר לתחום הימי, והשלישית היא ביג־דטא לתחום. בכל התחומים הללו יש בישראל גופי ידע מובהקים ויכולות פיתוח. יש מקום להרחבת הפעילות בתחומי טכנולוגיות חלל, אוויר ויבשה גם לתחום הים.

אוטומציה של תהליכים וספנות אוטונומיות: קושי בגיוס כוח אדם לספנות ורצון להפחתת עלויות תפעול האוניות דוחפים את התעשייה להקטנת הצוותים על ידי הצגת טכנולוגיה מתקדמת בתחומי הניווט וההפעלה של האוניות. מדובר על הפעלה מרחוק של אוניות ממרכזי בקרה מהחוף או ספנות אוטונומיות לחלוטין בקווים קבועים כגון קווי מעברות, אספקת אסדות קבועות בלב ים וכדומה.

הגנות סייבר: הופעתו של נשק הסייבר ומעורבות גוברת של שחקנים מדינתיים ולא־מדינתיים בתקיפות סייבר על תשתיות קריטיות כגון נמלים, הן מבחינת טכנולוגיית מידע, והן מבחינת טכנולוגיה תפעולית, ובתוך כך שימוש בגורמים פרטיים ובטכנולוגיות מתקדמות במטרה להשיג ערך אסטרטגי – כל אלה הופכים את הזירה הימית לפגיעה ביותר. בעשור האחרון נהייתה התעשייה הימית האזרחית (ענפי הספנות, כלי שיט, אוניות נוסעים, מספנות, נמלים, מסופים ותשתיות גז ואנרגיה) תלויה מאוד במערכות מחשוב ובקרה המתבססות על טכנולוגיות תפעוליות. מערכות אלו מבוססות ברובן על מערכות הפעלה מיושנות, ללא עדכוני אבטחה, הן בעלות יכולות ניטור מוגבלות (אם בכלל) ולרובן אין כלל הגנת סייבר.¹⁴

ביג־דטא לתחום הימי: בתחום הימי פועלות מערכות רבות כגון אוניות, מנופים, מטענים ועוד המייצרים כמויות גדולות מאוד של נתונים. מדובר למעשה על האינטרנט של הדברים, Internet of Things (IoT). "הדברים" הם החל באונייה ומנוף וכלה במכולה בודדת. נתונים אלו ניתנים לעיבוד וניתוח בכלים של ביג־דטא ובינה מלאכותית (AI). התובנות מתהליכים אלו משפרות ומיעילות את זרימת המוצרים בשרשרת הערך הלוגיסטית.

יש לציין כי יזמים ישראלים מגלים בשנים האחרונות את התחום הימי והפוטנציאל הגלום בו כ'תחום ורטיקלי' לפיתוחים טכנולוגיים, וכבר קיים בסיס איתן למדי לפיתוח תעשייה זו, אולם יש צורך בפעילות ממשלתית משלימה לצורך פיתוח התחום. בין הפעילויות המסחריות בתחום הטכנולוגיות הימיות שכבר קיימות בישראל יש לציין:

פעילות הון סיכון: קרן TheDock¹⁵ הכריזה בשנת 2022 על סבב גיוסים שני בהיקף 30 מיליון דולר. קרן Arieli Capital עוסקת בין השאר בתחומי הטכנולוגיות הימיות. החברה מפעילה את מרכז החדשנות באילת (כולל פעילות בתחום חקלאות ימית בנגב) וכן הכריזה על שיתוף פעולה עם חברת China Merchants לניהול מרכז חדשנות לטכנולוגיה ימית שיוקם בסין.¹⁶

¹⁴ לדיון בנושא ראו איתי סלע, "הערכת עלות אבטחת נמלי הים בישראל בפני איומים במרחב הקיברנטי", בתוך שאול חורב וזיו רובינוביץ (עורכים), *הערכה אסטרטגית ימית רבתי לישראל 2021/22* (חיפה: המרכז לחקר מדיניות ואסטרטגיה ימית, אוניברסיטת חיפה, 2022), עמ' 288–297.

¹⁵ אתר חברת TheDock: thedockinnovation.com

¹⁶ גונן, סקירת הכלכלה הכחולה בישראל, 2022.

בטא-סייט **בנמל חיפה**: הנמל פועל להקמת מיזמים בתחום החדשנות הטכנולוגית לעולם הספנות, הנמלים והלוגיסטיקה. עם זאת יש לציין כי עקב תהליכי ההפרטה של הנמל (הכרזה על זוכה בהפרטת נמל חיפה ניתנה באוגוסט 2022 אולם הקונסורציום הישראלי-הודי שזכה במכרז טרם התחיל בניהול בפועל של הנמל¹⁷) נבלמה פעילות החדשנות הטכנולוגית.¹⁸

חממה טכנולוגית **בנמל אשדוד**: נמל אשדוד הקים חממת חדשנות לתחום הלוגיסטיקה, הספנות והנמלים ולאחרונה הצטרף האקסלרטור Global 500, המתמחה בניהול חממות טכנולוגיות לפעילות הנמל.¹⁹

מרכז לאומי לכלכלה כחולה: ביולי 2022 הושק על ידי עיריית חיפה, המרכז הלאומי לכלכלה כחולה. המרכז נמצא בניהול התאגיד העירוני HiCenter העוסק בפיתוח יזמות בעיה.²⁰

ייצור כלי שיט: בתחום תעשיית כלי השיט, בישראל חברת מספנות אחת לבניית אוניות. 'מספנות ישראל' מייצרת כלי שיט בינוניים בסדרי גודל של עד כ-70 מטר, כגון שלדג או ספינות טילים (סטי"ל) בעיקר למטרות צבאיות ואכיפת חוק (משמר חופים וכדומה). מדובר במספנות בעלות מוניטין בין-לאומיים בנישת פעילותם. כמו כן כלי שיט צבאיים בלתי מאוישים יוצרו/ מיוצרים על ידי רפאל (ספינת הפרוטקטור), אלביט (סיגול), ותע"א (קטינה).

בסוף 2021 חתמה התעשייה האווירית עם חברת EDGE מאיחוד האמירויות על הסכם שיתוף פעולה לייצור משותף של כלי שיט אוטונומיים למגוון יישומים צבאיים ומסחריים.²¹ בתחום התת-ימי פיתחה אלתא (חברת בת של התעשייה האווירית) כלי שיט צולל בלתי מאויש עם יכולות להחלפת סנסורים ומשימות בהתאם לצורך המבצע.²²

חברות פרטיות: בתחום האזרחי ניתן לציין מספר חברות גדולות יחסית כגון חברת 'טוטם' העוסקת במערכות ניווט והיא חברה מובילה בתחום מערכות הניווט הימיות ומערכות תומכות החלטה, וכן חברת 'אורקה'. באתר פורום הטכנולוגיות הישראליות רשומות כמה עשרות חברות בישראל בתחום הימי, אולם מדובר ברשימה חלקית בלבד של החברות הפועלות בישראל.²³ חברת 'צים' היא כמובן חברת ספנות ישראלית גדולה, אולם עסקי הליבה של החברה הן הובלה

¹⁷ "גדות זכתה במכרז להפרטת נמל חיפה - תמורת 4.1 מיליארד שקל", כלכליסט, 14 ביולי 2022.

¹⁸ "נמל חיפה פרסם מכרז להקמת מיזם חדשנות טכנולוגית בתחום הספנות", port2port, 24 בינואר 2019.

¹⁹ "חדשנות בנמל אשדוד", נמל אשדוד, אוחר בנובמבר 2022.

²⁰ אתר המרכז הלאומי לכלכלה כחולה. blueconomy-il.com

²¹ Press Releases "EDGE Announces Strategic Deal with IAI to Develop Advanced Unmanned Surface Vessels", IAI, November 18, 2021

²² רועי נגלה, "האתגרים בהפעלת כלי שיט אוטונומיים בעידן הגלובליזציה – המקרה של אוניות סוחר אוטונומיות", בתוך שאל חורב ואהוד גונן (עורכים), הערכה אסטרטגית ימית רבתי לישראל 2019/20 (חיפה: המרכז לחקר מדיניות ואסטרטגיה ימית, אוניברסיטת חיפה, 2020), עמ' 266–279.

²³ אתר פורום הטכנולוגיות הימיות בישראל. israelmaritime.org

ימית ומשולבת ולא פיתוחים טכנולוגיים. עם זאת, בהינתן המעטפת המתאימה היותה של 'צים' חברה ישראלית מאפשרת אולי התקנות ניסיוניות של טכנולוגיות חדשניות.

נוסף להיותו של תחום הטכנולוגיות הימיות מנוע צמיחה לאומי פוטנציאלי, הוא יכול לשמש גם מנוע צמיחה מובהק ספציפי לאזור מפרץ חיפה והגליל המערבי. מאז 2015 מתקיים בממשלה תהליך קביעת מדיניות פיתוח חברתי וכלכלי אל מול צפון המדינה והעיר חיפה. בתהליך זה התקבלה בשנת 2017 החלטת ממשלה מס' 2262 בנושא 'פיתוח כלכלי של מחוז הצפון וצעדים משלימים לעיר חיפה',²⁴ שכללה התייחסות לנושא הנמל ותשתיותיו. בשנים 2020–2021 בהתאם להחלטת ממשלה על 'פיתוח וקידום מפרץ חיפה',²⁵ כונסה במסגרת המועצה הלאומית לכלכלה ועדת מנכ"לים ממשרדי הממשלה הרלוונטיים לנושא, והיא קיימה הליך ארוך ומקיף שהתמקד בעיקר בתעשיות הפטרוכימיות במפרץ חיפה, אך הקיף את כל היבטי הכלכלה והתעסוקה באזור. ועדת המנכ"לים קבעה:

על פי ניתוח שנעשה במסגרת עבודת הוועדה נמצא כי היתרונות היחסיים של אזור המפרץ כוללים: תעשייה עתירת ידע, נמלים ולוגיסטיקה, תעשיות ייצור "ירוקות" לאנרגיה וכימיה ותיירות נופש ופנאי. על בסיס ניתוח זה קיים פוטנציאל רב לתעסוקה במפרץ חיפה, ומימוש מתווה "מפרץ החדשנות".²⁶

אחת ההמלצות של ועדת המנכ"לים הייתה פיתוח אזורי תעשייה עתירי ידע במרחב חיפה לצורך הסטת המוקד התעשייתי של חיפה מתחומי התעשייה הפטרוכימית לתחום תעשיות עתירות ידע. מגמה זו עולה בקנה אחד עם מדיניות עיריית חיפה עצמה לפיתוח העיר כמרכז תעשיות עתירות ידע. מדיניות העיר חיפה היא כי מנועי צמיחה לעיר הם תיירות, ים, חקלאות ימית, סביבה, קיימות וביטחון.

טכנולוגיות מתקדמות בתחום הספנות והנמלים יכולות לתרום לפיתוח כלכלי במשק הישראלי וצמיחה לכדי מגזר שבו יפעלו מאות חברות שיעסיקו אלפי עובדים בשכר גבוה, וייצרו מעגלי תעסוקה והעברת טכנולוגיה רחבים, וזאת כפי שמתרחש בתחומי החלל וכלי הטיס והרכב הבלתי מאוישים. יש צורך בבניית תשתית כלכלית הכוללת תוכניות פיתוח ייעודיות לתחום, וזאת מעבר לפעילות חברות הטכנולוגיה וקרנות הון הסיכון הפרטיות שכבר פועלות בתחום זה, וכן פיתוח תשתית רגולטורית מתאימה כגון מתקני ואזורי ניסוי.

²⁴ "פיתוח כלכלי של מחוז הצפון וצעדים משלימים לעיר חיפה", החלטת ממשלה מס' 2262 מיום 8 בינואר 2017.

²⁵ "פיתוח וקידום מפרץ חיפה", החלטת ממשלה מס' 472 מיום 25 באוקטובר 2020.

²⁶ "המלצות ועדת המנכ"לים לפיתוח וקידום מפרץ חיפה", המועצה לכלכלה וחברה, משרד ראש הממשלה, 7 ביוני 2021.

צעד ראשון בכיוון היה עם החלטת משרד החדשנות והמדע על תחום הים כאחד מחמשת תחומי העדיפות הלאומית. יש להמשיך ולגבות החלטה זו בתקציב ופעילות רגולטורית מתאימים, והדבר אכן נמצא בתהליכי עבודה.²⁷

הזדמנויות בתחום שיתוף הפעולה האזורי

שיתופי פעולה כלכליים חוצי גבולות הם אחד הכלים לבניית יציבות אזורית-ביטחונית, וזאת מעבר לתועלת הכלכלית הישירה הגלומה בהם. הפוטנציאל הכלכלי הגלום בפרויקט המשותף עבור כל צד מניע את הרצון ההדדי לשימור המיזמים חוצי הגבולות על אף תהפוכות ואירועים חיצוניים. נוסף לכך, נוצרים ערוצים של יחסים ישירים בין פרטים וארגונים משני צידי הגבול, שבתורם תורמים גם הם ליציבות הכללית. בהקשר הישראלי ניתן לציין את פרויקט QIZ בין ישראל וירדן ובין ישראל ומצרים²⁸ וכן שיתופי פעולה בעבר בין ישראל ומצרים בתחום החקלאות. בשנים האחרונות שיתופי פעולה בתחומי הגז כגון הסכם בין ישראל ומצרים²⁹ ומיסוד ברית אזורית במזרח הים התיכון (ראו להלן).

שיתופי פעולה טכנולוגיים עם קפריסין ומצרים בתחום טכנולוגיית ספנות ונמלים הם ייחודיים, וזאת לאור המאפיינים הימיים של מדינות אלו (ראו להלן). ניתן לתכנן אזורי ניסוי בין-לאומיים משותפים לטכנולוגיות ספנות ולוגיסטיקה, מתקני הדגמה ובדיקת היתכנות (בטא-סייט), שיתוף פעולה בין-לאומי ככלי להשגת מימון מגופים בין-לאומיים (כגון הבנק העולמי או קרנות אירופיות) לתמיכה בפרויקטים משותפים ועוד.

קפריסין

שיתופי פעולה אזרחיים בין ישראל וקפריסין בעיקר בתחומים הקרובים לנושא הימי הם בעלי פוטנציאל גבוה להצלחה. בהיות קפריסין אי היא תלויה בים בכל היבט של קיומה. באי שבו כמיליון תושבים תעשיית ספנות פורחת, מובילה ברמה עולמית וגדולה בסדרי גודל מזו הישראלית. הצי הקפריסאי בהנפת דגל לאום כלל (נכון לשנת 2020) 1,056 אוניות במעמס כולל של 35 מיליון טונות. נוסף לכך, אוניות רבות הן בדגלי נוחות או בשותפות עם שחקנים יוניים (יוון היא מדינת ספנות מהחשובות בעולם).³⁰ כמו כן קפריסין תומכת בתחום היזמות והחדשנות ומנסה לקדם תחומים אלו. לדוגמה, קיומו של תפקיד מדען ראשי ואחראי על מחקר ויזמות.³¹

²⁷ המועצה הלאומית למחקר ופיתוח אזרחי, "בין קונברג'נס, פודטק, אנרגיות מתחדשות, חלל ובלו-טק: אלו הם תחומי העדיפות הלאומיים של מדינת ישראל", משרד החדשנות המדע והטכנולוגיה. 4 בספטמבר 2022.

²⁸ אזורי Qualify Industrial Zone – QIZ הם אזורי תעשייה בירדן ובמצרים שבהם פעלו מפעלים בבעלות ישראלית או בעלות משותפת אשר נהנו מייצוא ללא מכס של סחורה (בעיקר טקסטיל) לארצות הברית בחסות הסכם הסחר החופשי של ישראל עם ארצות הברית.

²⁹ דני זקן, "עכשיו זה רשמי: ישראל, האיחוד האירופי ומצרים חתמו על הסכם יצוא גז", גלובס, 15 ביוני 2022.

³⁰ "Maritime Profile: Cyprus", UNCDATSTART, 2021.

³¹ אתר המדען הראשי בקפריסין למחקר וחדשנות. chiefscientist.gov.cy

בין קפריסין וישראל יש בשנים האחרונות התחממות של היחסים הדיפלומטיים, ובעיקר בהיבטים של אנרגייה ופעילות ימית. המנוע להתחממות היחסים הוא אינטרסים משותפים בנושאי אנרגייה כגון גז וחשמל מצד אחד, וקיומו של יריב משותף – טורקיה, מהצד השני. קפריסין חברה באיחוד האירופי משנת 2004. לישראל וקפריסין גבול ימי משותף במים הכלכליים ולמעשה באופן זה לישראל גבול ימי משותף עם האיחוד האירופי. שתי המדינות הסכימו על תיחום הגבול הימי ביניהן בהסכם בין המדינות שנחתם בדצמבר 2010.³² בשנת 2021 הגיעו המדינות להסכמות מסוימות בנוגע למאגר אפרודיטה-ישי המשותף לשתי המדינות.³³ כמו כן חתמו ישראל וקפריסין על הסכם לחיבור רשת החשמל בין המדינות בכבל תת-ימי שעתיד להיות הארוך מסוגו בעולם.³⁴

מצרים

לנוכח ההיסטוריה הכוללת חמש מלחמות עם מצרים (קוממיות 1948, סיני 1956, ששת הימים 1967, ההתשה 1967–1970, יום הכיפורים 1973), הסכם שלום שנחתם ב־1979 והשפעתה של מצרים על הנעשה ברצועת עזה, הרי שיציבות היחסים עם מצרים היא יעד אסטרטגי ראשון במעלה עבור ישראל.

מצרים היא מדינת מפתח בתחום הספנות העולמית וזאת בגלל תעלת סואץ העוברת בשטחה. בתעלה מועברים כ־10% מהסחר העולמי. התעלה שהורחבה בשנים האחרונות בפרויקט לאומי מצרי מופעלת על ידי רשות ממשלתית המפעילה מאות כלי שיט שונים ומעסיקה אלפי עובדים. נמל פורט-סעיד במוצא הצפוני של התעלה הוא אחד מנמלי השיטעון הגדולים באזור.

הגבול הימי עם מצרים לא נקבע באופן רשמי, וקיימת גם בעיה של הגדרת תחום ימי לרצועת עזה הנמצאת בין המדינות. עם זאת בטווחים רחוקים יותר במים הכלכליים ישראל ומצרים חולקות גבול ימי משותף; בין המדינות יש צנרת גז תת-ימית; שיתופי פעולה כלכליים בתחום הכלכלה הכחולה, אנרגייה וטכנולוגיות ספנות בין ישראל ומצרים רלוונטיים גם בים סוף, שם נמצאת מצרים בתנופת פיתוח כלכלית וימית רחבה.

ממשלת ישראל החליטה בדבר "תוכנית לקידום ולהרחבת הקשרים הכלכליים בין מדינת ישראל והרפובליקה הערבית של מצרים".³⁵ ההחלטה כוללת אלמנטים של פיתוח משותף של כלכלה כחולה כגון בתחומי החקלאות הימית (הן בים התיכון והן בים האדום), אנרגייה מהים וכן תיירות ימית. יש לשקול הרחבת התוכנית גם לתחומי טכנולוגית ספנות ולוגיסטיקה.

³² אבי בראלי, "ישראל וקפריסין הסכימו על גבול המים הכלכליים", דה מרקר, 19 בדצמבר 2010.

³³ "השר שטייניץ ומקבילתו מקפריסין – נטאשה פילידס הגיעו להסכמה על פתרון למחלוקת במאגר אפרודיטה-ישי", משרד האנרגיה, 9 במארס 2021.

³⁴ "ישראל מתחברת לרשת החשמל האירופית: השר שטייניץ חתם על מזכר הבנות להנחת כבל החשמל התת-ימי הארוך בעולם", משרד האנרגיה, 9 במארס 2021.

³⁵ "תוכנית לקידום ולהרחבת הקשרים הכלכליים בין מדינת ישראל והרפובליקה הערבית של מצרים", החלטת ממשלה מס' 1522, ממשלת ישראל, 29 במאי 2022.

פורום הגז של מזרח אגן הים התיכון

בין מדינות מזרח הים התיכון קיים פורום שיתוף פעולה כלכלי על בסיס ימי, והוא 'פורום הגז של מזרח אגן הים התיכון'. פורום זה החל כ'ברית ההלנית' בין ישראל קפריסין ויוון שאליו הוזמנה גם מצרים. בהמשך הורחבה המסגרת לכדי פורום ממוסד בשם 'פורום הגז של מזרח אגן הים התיכון' שבו חברות איטליה, יוון, ישראל, ירדן, מצרים, צרפת, קפריסין והרשות הפלסטינית. ארצות הברית והאיחוד האירופי חברים בפורום במעמד משקיפים. במקור הוקם הפורום לצורך התייעצויות בנושא הקמת מיזם של צינור גז תת-ימי שירכז את ייצוא הגז מאזור המים הכלכליים של ישראל, קפריסין ומצרים ויגיע עד לשוקי אירופה דרך איטליה.³⁶

נוסף לכך קיים פורום 3+1 הכולל את ישראל, קפריסין ויוון וכן את ארצות הברית. במסגרתו עולה תחום הכלכלה הכחולה כתחום רלוונטי וחשוב בקשר בין חברות הפורום.³⁷

הזדמנויות ברמה האסטרטגית-לאומית

פיתוח טכנולוגיות ימיות יסייע ברמה האסטרטגית לחידוש ידע ימי חיוני ההולך ונעלם מישראל, יגדיל את העוצמה הרכה (soft power) הישראלית, ויספק מנופי השפעה דיפלומטיים לישראל בזירה הבין-לאומית.

בישראל שישה נמלים מסחריים (נמלי חיפה, המפרץ, אשדוד, הדרום, מספנות ישראל ואילת) ושלושה נמלי אנרגיה (חדרה, אשקלון, אילת). אורך הרציפים המצטבר בנמלים אלו הוא יותר מ-13.5 ק"מ ופועלות בהם טכנולוגיות מתקדמות (מרביתן המוחלט אינן ישראליות) כגון מנופי גשר חצי אוטומטיים, מתקנים אוטומטיים לצובר (גרעינים ומלט) ועוד. מפעילות הנמלים הן חברות ממשלתיות ישראליות לצד חברות בין-לאומיות מובילות כגון SIPG מסין, TIL משווייץ ו-Adani מהודו.³⁸

מנגד הספנות הישראלית נמצאת בשפל. צי האוניות שבבעלות ובשליטה ישראלית עומד על 35 אוניות בלבד (בשנת 2021), מתוכן רק 7 אוניות מניפות דגל ישראל. הגיל הממוצע של אוניות צי הסוחר עומד על 13.3 שנים. בצי הסוחר שבבעלות ושליטה ישראלית מועסקים בסך הכול 129 ימאים ישראלים, כולם קצינים בלבד ללא דירוגים (מלח כשיר).³⁹ מספרים אלו נמוכים באופן מובהק 'ימי הזוהר' של הספנות העברית בשנות ה-60 וה-70 עת הפליגו עשרות רבות של אוניות בדגל ישראל, ואלפי ימאים ישראלים.

³⁶ "קפריסין, יוון, ישראל ואיטליה חתמו היום בניקוסיה על מזכר הבנות להקמת צינור הגז מישראל לאיטליה", משרד האנרגיה, 15 בדצמבר 2017,

³⁷ שגריר ישראל בקפריסין, אורן אבוליק, בשיחת זום, יוני 2022.

³⁸ קבוצת Adani מהודו זכתה באוגוסט 2022 במרכז להפעלת נמל חיפה אולם טרם החלה בהפעלה זו בפועל.

³⁹ שנתון סטטיסטי ספנות ונמלים 2021, רשות הספנות והנמלים (רספ"ן), משרד התחבורה, 2021, עמ' 101.

דעיכת הספנות הישראלית ואובדן הידע וכוח האדם בתחום הימי לכדי אוניות בודדות המניפות את דגל ישראל, וכמאה קציני ים ישראלים בלבד וללא מלחים ישראלים כלל, היא בעלת השפעות אסטרטגיות על המדינה בתחום הסחר הבין-לאומי בעת חירום, וסביר (לנוכח מקרי העבר) כי הספנות העולמית תימנע מלפקוד את נמלי ישראל. נוסף לכך, דעיכת הצי המסחרי של ישראל פירושה אובדן ידע ימי החיוני לניהול הנמלים והמרחב הימי של ישראל. פיתוח טכנולוגיות ימיות הוא כלי לרפיפי 'העיוורון הימי' שממנו סובלת ישראל, ולהחזיר את ההכרה בחשיבות התווך הימי לחיק הציבור בישראל.

הובלה טכנולוגית היא חלק משמעותי מהעוצמה הרכה של מדינה. חילופי טכנולוגיה וכלכלה הם פעמים רבות המטבע העובר לסוחר בעולם הדיפלומטי. מדינות בעלות עוצמה כלכלית וטכנולוגית יכולות להשפיע יותר על שחקנים אחרים במערכת הבין-לאומית כדי לקדם את מטרותיהן. בהקשר הישראלי ניתן לציין הובלה ישראלית בתחומים כגון חקלאות, טכנולוגיית מים ואנרגייה כתחומים המקדמים את מעמדה של ישראל במרחב ובעולם, ומאפשרים לה מרחב תמרון דיפלומטי.

הובלה טכנולוגית עולמית מאפשרת למדינה המובילה להגדיר תקנים בין-לאומיים המתאימים לתעשייה המקומית שלה, ובכך למנף את ההובלה במגזר מסוים לפיתוח כלכלי נוסף שבתורו משמר את מעמדה המוביל באותו התחום.

זאת ועוד, ייצוא טכנולוגיות מאפשר איסוף מידע רב היכול לשמש את המדינה או החברות המסחריות בפיתוחים עתידיים והשפעה כלכלית עתידית. לדוגמה, כוחה הפוליטי של פלטפורמת רשת חברתית עולמית – לאור המידע הרב שיש בה – גדול לאין שיעור מההיקף הכספי בלבד של הפעילות בה. דוגמה נוספת מתחומי התחבורה היא חברות כגון בואינג (Boeing) או איירבוס (Airbus) בתחום התעופה, מארסק (Maersk) בתחום הספנות, יצרניות הרכב הגדולות כגון טויוטה (Toyota) ועוד – כל אלו מחזיקות מידע רב על אודות מגמות עולמיות החורגות בהרבה מתחום התחבורה שבו הן פועלות, וזאת עקב היבטים גלובליים של פעילות חברות אלו. לאור החשיבות הרחבת של תחומי הסחר הימי, הספנות והביטחון הימי, הרי שנוכחות טכנולוגית עתידית ניכרת בתחומים אלו מביאה עימה גם יכולת איסוף מידע רב, ועימו השפעה גדולה יותר בזירה העולמית.

סיכום והמלצות

ככל הנראה יחלפו עוד שנים רבות עד שאוניות אוטונומיות לחלוטין וללא צוות כלל ישייטו ברחבי הימים. עם זאת נראה כי אנו בעיצומו של תהליך הצגת טכנולוגיות מתקדמות בתחום הספנות, ויש בהחלט לצפות לעלייה ברמת האוטומציה בכלי השיט וכניסת מערכות תומכות החלטה, שיקטינו מאוד את הצוותים על גבי האונייה. נוסף לכך ייתכנו אוניות המופעלות ומפוקחות מהחוף שהצוות מפעיל ומפקח על מספר אוניות בזמן, או ספינות וכלי שיט קטנים יותר ללא צוות המפליגים בנתיבים קבועים וברורים.

פיתוח טכנולוגיות ימיות הוא מנוע צמיחה לאומי כפי שקיים בתחומי החלל, הרכב והאוויר, וכן הוא יכול להיות מנוע צמיחה אזורי מרכזי באזור מפרץ חיפה כחלופה לתעשייה הפטרוכימית. פיתוח טכנולוגיות ימיות יכול לסייע בחיזוק היחסים עם קפריסין ואירופה, וכן עם מצרים, ויכול לסייע לישראל לתפוס מקום ראוי ומכובד בתחום הספנות העולמית. לישראל יש מורשת ימית, אולם בעשורים האחרונים אובד במדינה הידע הימי. למצב זה השלכות אסטרטגיות בין השאר על הסחר הבין־לאומי של המדינה בעת חירום וניהול המרחב הימי הישראלי.

כמו בתחומים רבים, הטכנולוגיה והמשפט מתקדמים יחד, ועולה הצורך באסדרה המאפשרת פיתוח טכנולוגי כגון עריכת ניסויים ימיים בישראל באופן סדיר כחלק מתשתית לפיתוח כלכלה כחולה. הדבר תואם מגמות עולמיות בפיתוח הכלכלה הכחולה כמו גם את מגמות הפיתוח הכלכלי בישראל המבוססות על יזמות וחדשנות.

עיקרי ההמלצות

1. יש לפעול לבניית תוכנית לאומית לקידום תחום הטכנולוגיות הימיות. ההכרזה על מרכז לאומי לכלכלה כחולה בחיפה, וההכרזה על תחום הכלכלה הכחולה כתחום עדיפות לאומי על ידי משרד החדשנות והמדע הן ללא ספק התקדמות ראויה לציון, אולם יש לפרוט הכרזות אלו לתוכניות פרקטיות המתוקצבות בהתאם ולקדם מסגרת רגולטורית מתאימה.
2. על הרגולטורים לתחום הימי לקדם את האסדרה שתאפשר ניסויים בטכנולוגיות מתקדמות לכלי שיט כגון כלי שיט אוטונומיים.
3. בנושא התקינה הבין־לאומית: מגמת הספנות האוטונומית היא מונחת תעשייה כלומר צומחת מלמטה. לפיכך יש משמעות גדולה ליכולות טכנולוגיות לצד תקינה. מומלץ לפעול לצורך הצבת מומחים ישראליים בתחומי התקינה הטכנולוגית לתחום הימי, ובעיקר נושא הסייבר הימי. לפיכך, יחד עם מכון התקנים, מומלץ לפעול לשלב מומחים טכניים מישראל תחת תחת הוועדה הטכנית מספר 8 לטכנולוגיות ימיות (ISO/TC 8 Ships and marine technology) לפעילות בקבוצות העבודה הבאות של ארגון התקינה העולמי.

