

הערכה אסטרטגית ימית רבתי לישראל 2022/23

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



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

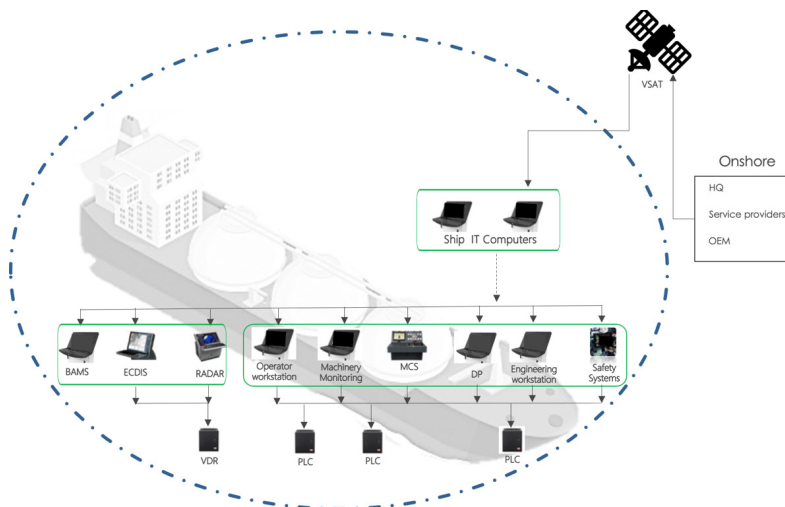
במהלך ארבעת העשורים האחרונים חלה התקדמות ניכרת בטכנולוגיות הנמצאות בשימוש על גבי פלטפורמות ימיות (כלי שיט מסחריים, אוניות נוסעים, אסדות קידוח, הפקה וכדומה) – מפלטפורמות שנבנו בתחילת שנות ה-80, והתבססו על טכנולוגיה פשוטה יחסית, דרך פלטפורמות שנבנו בתחילת המאה ה-21 שבהן רואים שימוש גובר בטכנולוגיות מבוססות 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 משמעותיות 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

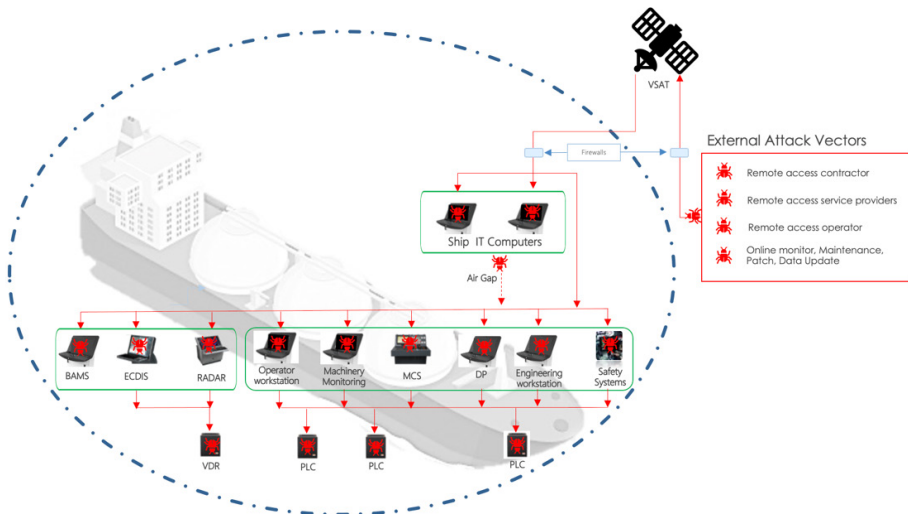
הנתיב השני, כפי שניתן לראות באיור 3, הוא נתיב התקיפה הפנימי (Internal Attack Vector) המשתמש בגורמים עם הרשאות גישה למערכות התפעוליות לצורך פעילות שגרתית (אנשי הצוות וטכנאים של היצרנים העובדים על הפלטפורמה) וללא ידיעתם, להחדרת הקוד הזדוני ממחשב מנהלתי למערכת תפעולית. דוגמאות לתקיפות שעשו שימוש בנתיב תקיפה 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

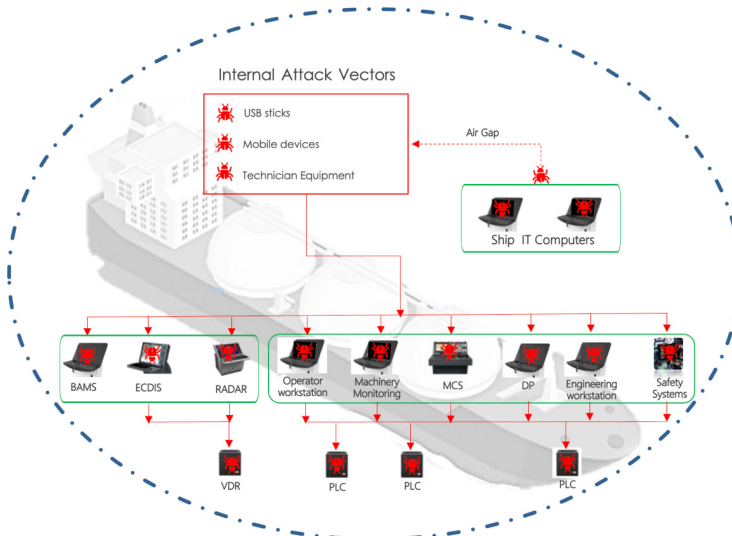
¹⁶ Zain Shauk, "[Malware on Oil Rig Computers Raises Security Fears](#)", *Houston Chronicle Energy*, February 23, 2013

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

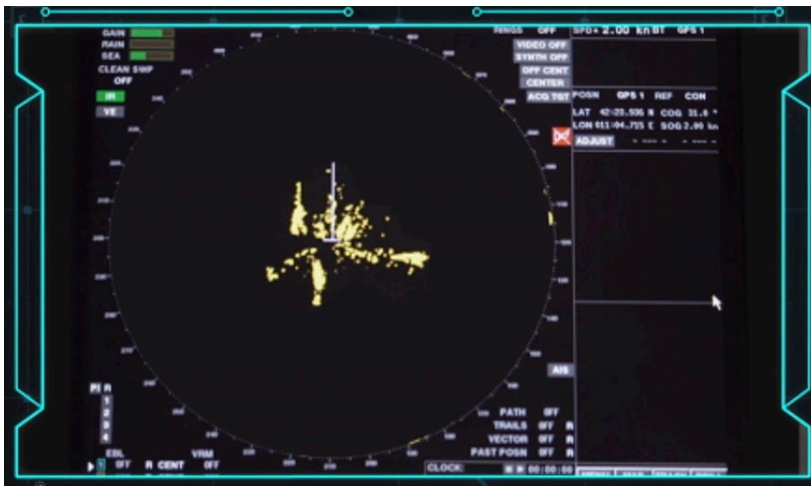


איור 3: נתיבי תקיפה פנימיים בכלי שיט והתפשטות הקוד הזדוני לכלל מערכות המחשוב התפעוליות

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 שהחלטות שיקבל בעניין תכנון ההפלגה ובטיחות השיט יהיו שגויות, ויובילו לסטייה מהמסלול המתוכנן ואף לתאונה.

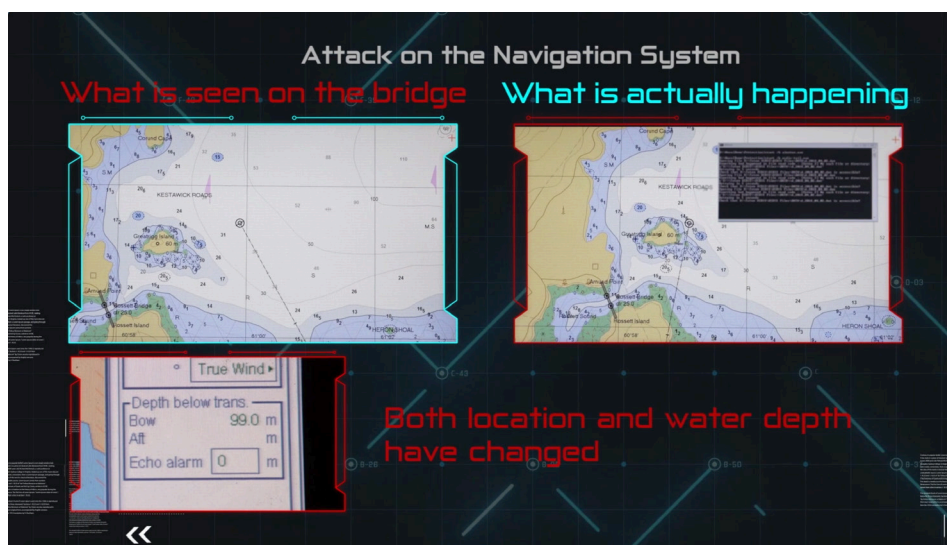
איור 7 מציג הדגמה של תקיפת מניפולציה על מערכת בקרת מכונה (MCS) השולטת על מנועי כלי השיט, מערכות היציבות, האיזון ומערכות נוספות שמאפשרות לקצין המכונה להפעיל ולבקר את פעולת מערכות כלי השיט.²⁴ בתקיפה זו ניתן לראות בחלונית השמאלית של האיור את מסך בקרת המכונה המציג משאבה אחת פועלת, למרות שבפועל, כפי שניתן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

²² Ibid.

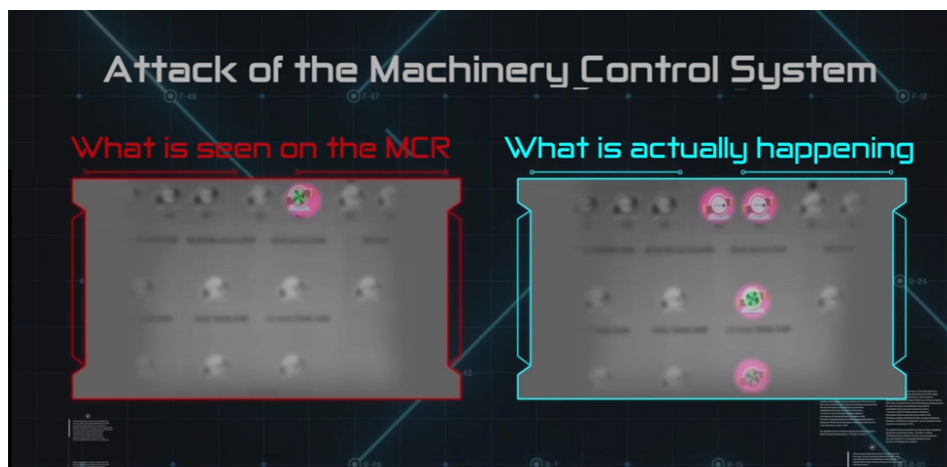
²³ [Ethical hackers demonstrate weaknesses in shipboard systems](#), *Digital Ship*, January 2, 2018.

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.



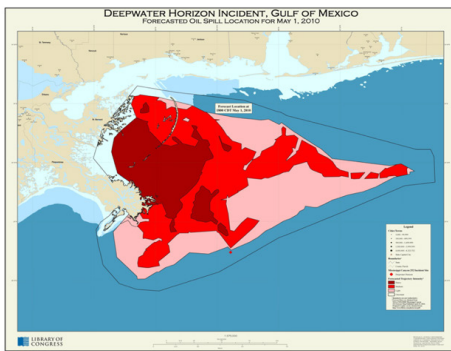
איור 6: תקיפת מניפולציה על מערכת ניווט (ECDIS)



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.

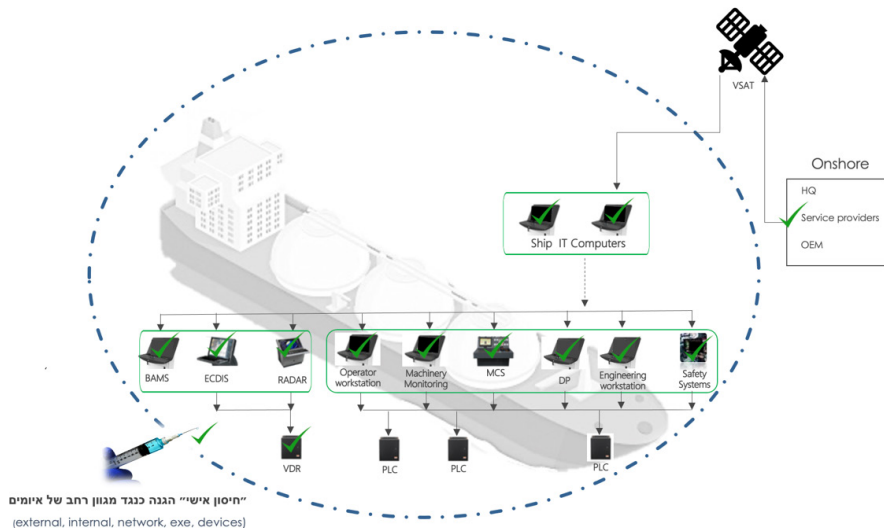
ניתן להצביע על שלוש תפיסות הגנה מרכזיות הנמצאות כיום בשימוש על גבי פלטפורמות ימיות אזרחיות במטרה להגן כנגד איום הסייבר על מערכות מחשוב תפעוליות: התפיסה הראשונה והמקובלת ביותר רואה בגורם האנושי אחראי מרכזי לשמירה על הפלטפורמה מפני איום הסייבר, ולכן מתמקדת בחינוך והדרכה של אנשי הצוות והטכנאים להיגיינת 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 הבינלאומית 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.

איתי סלע, דוקטורנט בבית הספר למנהל עסקים וחוקר במרכז לחקר מדיניות ואסטרטגיה ימית באוניברסיטת חיפה. איתי משמש כמנכ"ל-מייסד בחברת Naval Dome, העוסקת בזיהוי נקודות תורפה ובהגנה על מערכות מחשוב קריטיות על גבי פלטפורמות ימיות מפני תקיפות סייבר. פרש מצה"ל בדרגת סא"ל לאחר שירות של 25 שנה בחיל הים במגוון תפקידי פיקוד בשטח ובמטה. איתי מחזיק בתואר ראשון במדעי ההתנהגות מאוניברסיטת בר-אילן ותואר שני במינהל עסקים מאוניברסיטת בן-גוריון.