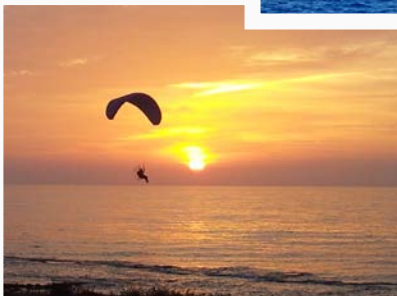
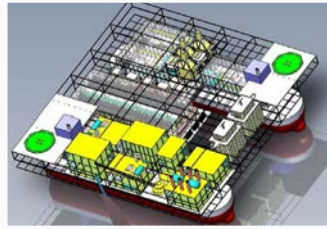


הערכה אסטרטגית ימית ל ישראל 2016/17

עורך ראשי: פרופ' שאול חורב
ערך והפיק: אהוד גונן



פרק 8: ההיבט הימי של לוחמת סייבר

איתן יהודה

כללי

לשליטה במרחבי היבשה, הים, האוויר והחלל התווסף בשנים האחרונות מרחב נוסף – המרחב הקיברנטי. התקפות הסייבר נפוצות מאוד ומתבצעות על ידי מגוון של גורמים כנגד כל סוגי הארגונים והמערכות ובכל הרמות.¹ ההתקפות מתבצעות כנגד גופים ממלכתיים ומשרדי ממשלה, גופים צבאיים, תשתיות ציבוריות ועירוניות (כמו ייצור חשמל, הובלת מים, מערכות רמזורים עירוניות, וכבישי אגרה), וגם נגד מטרות פרטיות כמו בנקים, חברות מסחריות ואנשים פרטיים.

התקפות סייבר נערכות על ידי ארגוני טרוך, מדינות עוינות, פעילים פוליטיים (כמו ארגונים אנרכיסטים והאקרים) וכמובן על ידי גורמים פליליים לשם רווח כלכלי. מטרות התקיפות עשויות להיות שונות ומגוונות; פגיעה או השבתה של מערכות מחשב, איסוף מידע, השתלטות על מערכת המחשב לצרכי כופה, או לצורך ביצוע התקפה נוספת בעתיד וכן כדי לפגוע בתשתיות לאומיות או בסדר ובמוראל הציבוריים.

גם אמצעי התקיפה מגוונים והם כוללים שימוש בטכנולוגיות שונות של העברה והדבקה, ו/או שימוש בגורם האנושי לצורך החדרה של התוכנה או של הקוד המזיק למערכות המידע המותקפות. בהקשר זה, פגיעותו של סקטור הנמלים והספנות למתקפות סייבר גדולה מאוד. התוצאות של התקפה כזאת עלולות להיות משמעותיות ברמה בלאומית, ולפיכך יש צורך להתייחס באופן ספציפי לנושא זה במסגרת האסטרטגיה הימית הכוללת של ישראל.

יעילותם של הנמלים ואיכות השירות החיוני שהם מספקים תלויים באופן מוחלט באיכות התקשורת, הלוגיסטיקה, ומערכות המידע והטכנולוגיה המופעלות על ידי הנמל. בין מערכות אלו ניתן לציין: מערכות הגנה ואבטחה היקפיות, מערכות לניהול ולניתוב מכולות ולאיתור מיקומן, מערכות לניהול מנופים ועגורנים, מערכות ERP לניהול של תקציב, מלאי וכוח אדם, מערכות בטיחות לתקשורת בין האוניות לנמלים ועוד.

גם לסקטור הספנות יש דרישות מחשוב גדולות. האוניות (הן אוניות סוחר והן אוניות נוסעים) נבנות יותר ויותר גדולות ותפעולן מבוסס לחלוטין על מערכות מחשוב מתקדמות

¹ SYMANTECH, 2016 Internet Security Threat Report; <https://www.symantec.com/security-center/threat-report>

כמו מערכות ניווט וגילוי, מערכות איזון וציפה, מערכות לניהול של פריקה וטעינה, בקרת מערכות מכניות (מנוע, גנראטור, היגוי), מערכות עגינה ועוד.

ההישענות ההולכת וגוברת על טכנולוגיות מחשוב מתקדמות מבוססות תקשורת (לוחיינית ואינטרנטית) יוצרת חשיפה של עולם הנמלים והספנות לסוג חדש של איום; תקיפות סייבר נגד נמלים ופלטפורמות ימיות.

נמלי ישראל

נמלי הים של ישראל מוגדרים כתשתית חיונית והם מהווים את 'צינור החמצן' של ישראל. כ-98% מנפח תנועת המטענים אל ישראל וממנה עוברים דרך נמלי הים, המשמשים, בנוסף, גם כחוליה מרכזית בשרשרת הלוגיסטית של המסחר הבינלאומי באזורנו.

נמלים מודרניים ונגישות לספנות הבינלאומית מהווים נדבך חיוני בכלכלה הישראלית, וזאת עקב התלות הגדולה של המשק הישראלי בייבוא מזון (מרבית צריכת הדגנים בישראל), ייבוא אנרגיה (כל הנפט הגולמי), וייבוא של חומרי גלם למשק ולתעשייה. בנוסף תעשיות ישראליות רבות תלויות בשוקי חו"ל, קרי בייצוא. כל פגיעה בתפעול הנמלים תגרום לפגיעה בתעשיות רבות בישראל, כמו התעשייה הכימית הישראלית, תעשיית הייצוא של שבבי אלקטרוניקה, ותעשיות נוספות.

בישראל קיימת היערכות 'משק לשעת חירום' (מל"ח) המוסדר בין השאר על פי 'חוק שירות העבודה בשעת חירום'. על פי הגדרת החוק 'מפעל חיוני' הוא:

...המפעל פועל או שאפשר להפעילו לצרכי הגנת המדינה או ביטחון הציבור או לקיום שירותים חיוניים. וכן כל מפעל או חלק ממנו שאפשר להפעילו לצרכי קיום המשק ושפעולתו חיונית לקיום הספקה או שירותים הדרושים לציבור או לייצוא.

הגדרה נוספת של החוק 'למפעל חיוני' היא:

... שירות אשר לדעת השר הפסקתו עלולה, בנסיבות העניין, לגרום לפגיעה רבה בכלכלה המשפיעה על המשק כולו.²

הרשות לשעת חירום אינה מפרסמת את רשימת המפעלים החיוניים מטעמים של ביטחון המדינה אולם ברור כי נמלי ישראל עומדים בהגדרות הנ"ל, וסביר להניח כי הם מוגדרים כמפעל חיוני ואף כמפעל למתן 'שירותים קיומיים'. גם מהגדרות אלו לשעת חירום ניתן להסיק על חשיבותן המכרעת של הנמלים למשק הישראלי.

2 חוק שירות עבודה בשעת חירום, תשכ"ז-1967, (תיקון מס' 1) תשל"ג-1973 (תיקון מס' 7) תשס"ח-2008.

סיכונים

ההתפתחויות הדרמטיות שחלו בשנים האחרונות בטכנולוגיות התקשורת והמידע השפיעו על הדרך בהן שחקנים מדינתיים ולא מדינתיים פועלים ויפעלו במרחב הימי. טכנולוגיות אלו יצרו הזדמנויות אך גם אתגרים לבעלי העניין בתחום הצבאי ובתחום המסחרי, וגם לבעלי עניין מעולם הפשע והטרור. הים הוא מרחב ענק שבו הפלטפורמות (בין אם אוניות או פלטפורמות אחרות) פועלות במרחק גדול מהחוף, בשל מורכבות פעילויות אלו נדרשת העברת מידע בלתי מופרעת ורצופה מכלי השיט לחוף ובחזרה. במרחב הימי המודרני טכנולוגיות מבוססות מחשב, הכוללות מערכות של הנחיה, חישה, בקרה, שליטה ותקשורת, כמו גם זיקה בין הפלטפורמות של כלי השיט לתשתיות החוף (כמו נמלים) חיוניות לשם יצירת תפוקה והגדלת היעילות.

מעבר לפגיעה החמורה בכלכלת המדינה או בחברת ספנות ספציפית, יש לפגיעה בנמלי מפתח או בשחקנים הגדולים של עולם הספנות פוטנציאל לפגיעה בסחר האזורי ואף הגלובלי. המבנה הגלובלי של ענף הספנות, כמו ההתבססות על שיטעון מכולות בין קווים עולמיים וקווי הזנה (feeder) יוצרים מצב שבו לפגיעה בנמל מסוים או בחברה מסוימת עלולה להיות השפעה גלובלית. לדוגמה, בשנת 2015 עברו 27.52 מיליון מכולות רק דרך נמלי המבורג, רוטרדם ואנטוורפן. מכולות אלו מהוות כ-8% מסך תעבורת הסחורות העולמית.³ בארה"ב נמל Long Beach לבדו נותן שירות לכ-2,000 אוניות מדי שנה, הנושאות 6.7 מיליון מכולות, המהוות בתורן חמישית מתעבורת המכולות בכל נמלי ארה"ב.⁴

ניתוח איום זה על ידי חברות הביטוח, הרגולטורים וציי הסוחר מעלה את ההכרה בעובדה שאם עד היום נדרשו הציים להתמודד עם אירועים נקודתיים של תקיפת סייבר על אוניה בודדת, הרי שתקיפה רחבה יותר עלולה להוביל לפגיעה מערכתית (פגיעה בצי שלם), עם השלכות קשות על הסחר העולמי ועל הסביבה.

להלן תיאור מקצת הסיכונים שעלולים להיגרם מתקיפות סייבר על נמלים, אוניות ואסדות אנרגיה:

סיכונים כלכליים

- פגיעה עד השבתה של תהליכי עבודה בנמלים ופגיעה בסחר החוץ של המדינה.
- פגיעה והרס מערכות מכניות של האוניה עד פגיעה בגוף האוניה עצמה (פגיעה בשרטון).

ENISA European Network and Information Security Agency 3

GAO United States Accountability Office 4

- פגיעה והרס התשתיות החופיות של הנמל (עגורנים, רציפים).
- נזק כלכלי לחברות הביטוח, ובעקיפין הגדלת תשלומי הפרמיות על ידי חברות הספנות ועליית עלויות הסחר הבינלאומי.
- השבתת תשתית חיונית מרכזית או אזורית, ופגיעה בשרשרת הלוגיסטית העולמית.
- פגיעה במוניטין של חברת הספנות.
- השבתת התהליכים של ייצור הגז ושל הולכת הגז מאסדות הקידוח הימיות, שיוביל לפגיעה במשק עקב פגיעה באספקת אנרגיה (גז או נפט).
- הברחות מסחריות העלולות לפגוע בכלכלה ובבטיחות הציבור.

סיכונים סביבתיים

- זיהום הסביבה הימית בנפט או בחומרים מסוכנים אחרים על ידי השתלטות על מערכות של מכלית נפט והתנגשות מכוונת בשרטון, או פתיחה של ברזי ההורקה במכלית ושחרור חומרים מסוכנים לים.
- פגיעה באסדות גז או בצנרת הימית, ושיבוש התהליכים של הקידוח וההולכה, שיגרמו לשחרור חומרים מסוכנים לים.

סיכונים ביטחוניים

- פגיעה בחוסן הלאומי של המדינה על ידי השבתת סחר החוץ לפרקי זמן ארוכים, ופגיעה באספקת מזון ודלק לאוכלוסייה האזרחית ולצבא.
- השתלטות מרחוק על מערכות הניווט של ספינה ושימוש בספינה עצמה ככלי לביצוע התקפה, כמו 'דריסה' של אסדת גז או חסימה של נמל, (לדוגמה על ידי שיבוש הנתונים וקבלת החלטות שגויות על ידי צוות הפיקוד של כלי השיט).
- היבטים ימיים של טרור כגון הברחת חומרי נפץ ולחימה, פיגועים כימיים על ידי חומרים מסוכנים ועוד.
- הברחת אנשים דרך הים והגירה בלתי חוקית.

התקפות סייבר נגד נמלים ואוניות אינן בגדר איום בלבד. התקפות כאלו כבר בוצעו בשנה האחרונה ובהיקפים גדולים:⁵

בשנת 2013 בוצעה התקפת סייבר על מערכות המידע של טעינת המכולות בנמל אנטוורפן שבבלגיה. סוחרי סמים השתלטו מרחוק במשך שנתיים על מערכת זו ושינו את תכולת המכולות ואת יעדן, דבר שאיפשר להם להבריח סמים בכמות אדירה למדינה.

התקפת סייבר שבוצעה על מכלית נפט מול חופי אפריקה גרמה למכלית לנטות על צידה עד השבתתה המוחלטת.

פיראטים סומלים במפרץ עדן העסיקו האקרים על מנת לזהות אוניות המובילות מטען יקר ערך שהאבטחה בהן מינימלית על מנת להשתלט על אותן ספינות.

חברת הספנות הלאומית של איראן 'אירסיל' הותקפה בשנת 2012. ההתקפה שיבשה את כל מערכות המידע הלוגיסטיות המטפלות בבקרה על תנועת המכולות ועל מיקומן. ההאקרים שחדרו למערכת המחשוב של 'אירסיל' מחקו את כל בסיסי הנתונים של החברה, כולל מערכות הגיבוי, כך שהחברה לא היתה יכולת התאוששות מאירוע זה.

המצב בישראל

מדינת ישראל נערכת כמובן לנושא ההגנה מפני התקפות סייבר. צה"ל, כמו שאר מערכת הביטחון, נדרש לנושא בשלב יחסית מוקדם, והטיפול בתחום הימי בתוך מערכת הביטחון זוכה לתשומת לב הולכת וגדלה.

בישראל הוקם 'מטה הסייבר הלאומי' שמטרתו לשפר את ההגנה על התשתיות הלאומיות החיוניות ולאבטח אותן, במידת האפשר, מפני התקפות סייבר. המטה מקדם בו זמנית את מעמדה של ישראל כמרכז לפיתוח טכנולוגיות מידע, תוך הידוק שיתוף הפעולה בין האקדמיה, התעשייה, המגזר הפרטי, משרדי הממשלה וקהילת הביטחון.⁶ המטה אחראי, בין השאר, על תיאום ההנחיות לנמלים לתשתיות החוף בישראל.

בתחום האזרחי, התשתית החוקית לרגולציה בתחום היא 'החוק להסדרת הביטחון בגופים ציבוריים', התשנ"ח-1998.⁷ החוק קובע סמכויות ואחריות לאבטחה פיזית, אבטחת מידע ואבטחת מערכות מחשוב חיוניות של גופים שונים, כולל כל הנמלים בישראל (הן נמלי חנ"י והם נמלי ומעגנות קצ"א וחברת החשמל) כמו גם חברות הספנות, האנרגיה והגז. בין השאר מחייב החוק מינוי 'ממונה ביטחון' בגופים האמורים, תחת הנחיות השב"כ או המשטרה, בהתאם לגוף הנדון. בתחום סמכותו של אותו ממונה נמצא מתן ההנחיות המקצועיות בנושאי אבטחה, אבטחת מידע ואבטחת מערכות מחשוב חיוניות בכל אחד מהגופים השונים.⁸

6 מטה הסייבר הלאומי, משרד ראש הממשלה <http://www.pmo.gov.il/BranchesAndUnits/Cyber/Pages/NationalCyber.aspx>

7 חוק להסדרת הביטחון בגופים ציבוריים, תשנ"ח-1998: https://www.nevo.co.il/law_html/Law01/111M1_001.htm

8 חוק להסדרת הביטחון בגופים ציבוריים, תשנ"ח-1998. תוספת ראשונה צו תשס"ז-2006, צו (מס' 2) תשע"ו-2016.

בשנתון הסטטיסטי שהתפרסם על ידי רשות הספנות והנמלים (רספ"ן)⁹, מתוארים בפירוט תפקידי הרשות וחשיבותן של נמלי הים לתהליכי המסחר של מדינת ישראל. בין השאר נכתב בשנתון כי: "ניתן לסכם ולומר שעתידה הכלכלי של מדינת ישראל תלוי בצורה רבה בפיתוח הנמלים, ביצירת תנאים לתחרות בין המשתמשים בהם מבית ומבחוץ, ובהגברת יעילותם".

בתחום מערכות המידע והטכנולוגיה מופיעים הנושאים הבאים:

- הקמה ותפעול של מערכות מידע לספנות ולנמלים.
- הקמה של מאגר מידע לאומי בנושא ספנות ונמלים.
- אחידות בתשתיות המחשוב בנמלים.
- איסוף, עיבוד והפצה של נתוני ספנות באופן שוטף.

עם זאת, אין אזכור כלל לנושא ההתמודדות עם איומי הסייבר על מערכות המידע והתקשורת של נמלי ישראל וחברות הספנות הישראליות זאת למרות חשיבותו של נושא זה וההנחיות שניתנו במסגרת החוק.

המבנה התפעולי והמשפטי של עולם הספנות מורכב מאוד עקב הפריסה הגלובלית של קווי הספנות; הימצאותם של הנמלים והתשתיות החופיות תחת ריבונות של מדינות שונות (ומכאן, היותן נתונות לחוקים לרגולציה, ולתקנות לא אחידים); רישומן של אוניות רבות תחת דגלי נוחות ועוד. לכן ניתן, באופן כללי, להפריד בין שלוש רמות ניתוח עיקריות: רמת המדינה ותשתיות החוף שלה; הרמה הבינלאומית; והרמה של חברת הספנות. שלושת רמות אלו מושפעות כמובן זו מזו ואף חופפות לעתים.

רמת תשתיות החוף והנמלים – זוהי כמובן תשתית לאומית הנמצאת בריבונות מלאה של המדינה החופית, שגם יכולה לקבוע עבור הנמל רגולציה מחייבת בנושא הסייבר. עם זאת, יש להביא בחשבון שעל תשתיות התקשורת של הנמל להתאים 'ולדבר' עם אוניות רבות, המחויבות בתקנים שונים, בהתאם למדינת הרישום שלהן. החמרה בתחום תקשורת הסייבר עלולה למנוע מהנמל את היכולת לתקשר עם האוניות באופן יעיל. הרגולציה שקובעת מדינת החוף נובעת בדרך כלל מהדרישות הבינלאומיות בתחום המהוות 'דרישות מינימום'. עם זאת – כמו במקרה הישראלי בנושא הסייבר – המדינה יכולה לקבוע לתשתיות החוף ולנמלים שלה רגולציה קפדנית והדוקה יותר מזו המקובלת בעולם.

גוף הביקורת של הקונגרס האמריקני (Government Accountability Office – GAO) פירסם בינואר 2015 דוח בנושא הסייבר בנמלי ארה"ב. על פי הדוח מטפלים הנמלים בארה"ב מדי

9 רספ"ן שנתון סטטיסטי לשנת 2015 (פורסם מרץ 2016): <http://asp.mot.gov.il/he/abstract>

שנה במטען בשווי של למעלה מ-1.3 טריליון דולרים. כל הפעילות הזאת נתמכת על ידי מערכות מידע ותקשורת הגישות להתקפות סייבר. כשלים במערכות אלו עלולים לפגוע או להפריע לפעילות בנמלים, ובכלל זה לזרימה של המסחר. המלצות הדוח הן שהמשרד להגנת מולדת יכוון את משמר החופים להעריך את הסיכונים הנוגעים להתקפות סייבר, וישתמש בהערכה זו כדי לסייע בפיתוח של הנחיות ביטחון למגזר הימי כולו. כמו כן, ממליץ הדוח, להקים מחדש את המועצה לתיאום איומים בסייבר במגזר זה.

הרמה הבינלאומית – קיימת כיום מחויבויות בינלאומיות של מדינות שונות לאמנות בינלאומיות ולקודים בינלאומיים בנוסף, במובלע או במפורש, כל אחת מהמדינות מחויבת לפרקטיקת פעילות הנובעת מהדרישות של השחקנים הגדולים בתחום, כמו חברות הביטוח הגדולות ועוד.

בקרב חברות הביטוח הגדולות נרשמת התעניינות הולכת וגוברת בנושא התקפות הסייבר. אחת לשנה מפרסמת חברת הביטוח העולמית Allianz דוח המסקר את ההפסדים ואת רמת הבטיחות של עולם הספנות בעולם. מניתוח הדוח האחרון¹⁰ עולה כי התייחסות ראשונה למודעות לנושא פורסמה רק בשנת 2013, ושמצא לא חלה התקדמות רצינית בנושא. הדוח האחרון מגדיר את עולם הסייבר כאחד 'האיומים המשמעותיים' לעולם הספנות ובעיקר למערכות הניווט (GPS), למערכות השליטה והבקרה (Electronic chart Display – ECDIS), ולמערכות הזיהוי האוטומטי (Automatic Identification System – AIS). יש להדגיש כי המערכות הנ"ל מקושרות לעולם האינטרנט ולמערכות תקשורת חיצוניות, ושכל פגיעה בהן עלולה לגרום להפסדים כספיים משמעותיים ולתביעות ביטוח.

איגוד הספנות העולמי, המייצג למעלה מ-2,200 בעלי אוניות (Baltic and International Maritime Council – BIMCO), פירסם בפברואר האחרון מסמך הנחיות לבעלי אוניות ומפעיליהם תחת הכותרת The Guidelines on Cyber Security onboard Ships¹¹. בהנחיות מתואר כיצד יש להיערך אול מול האיום החדש. לטענת BIMCO, הבנת האיום צריכה להתחיל ברמת ההנהלה הבכירה ולא להישאר נחלתם של אנשי המחשוב בלבד. במסמך מצוין שכל המערכות בספינה ובנמלים אשר מבוססות על טכנולוגיות מחשוב מתקדמות חשופות למתקפות סייבר, כולל רשתות האינטרנט המיועדות לרווחת אנשי הצוות ושל הנוסעים באוניות נוסעים. בדוח בוצע מיפוי של כלל המערכות, והוא כולל ניתוח מעמיק של מידת הנזק האפשרי שיכול להיגרם כתוצאה מפגיעה בהן, והמלצות על הפעולות

<http://www.agcs.allianz.com/insights/white-papers-and-case-studies/safety-and-shipping-review-2016> 10

https://www.marad.dot.gov/wp-content/uploads/pdf/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016.pdf 11

שצריכים לנקוט אנשי הצוות במקרה של השבתת מערכות אלו. ההמלצה המרכזית של הדוח היא לבצע ניתוח סיכונים וליצור תכנית התאוששות מאסון.

אם ניקח, כמקרה מבחן, את האיום של התקפות פיראטיות באזור מזרח אפריקה, נראה כי חברות הספנות והמדינות בעלות העניין השקיעו משאבים רבים על מנת להילחם בתופעה. עם הזמן, ועם ההשתכללות של הפעילות הפיראטית, החלו חברות הספנות וחברות הביטוח לנקוט באמצעי זהירות ומיגון כדי להפחית את הסיכון ולנטרלו. הגורם המשפיע ביותר על הירידה הניכרת בפעילות הפיראטית באזור זה מיוחס לפעילות של כוח המשימה הימי הבינלאומי של האו"ם, שבו חברות עשרים ושתיים מדינות. כאמור, הופצו הנחיות להתנהגות מונעת, לתקשורת ולדיווח בין הכוחות והארגונים השונים הפועלים במרחב במקרה של התקפה. במקביל, חלה עלייה במספר חברות האבטחה הפרטיות הנותנות מענה מקומי לחברות הספנות. כפועל יוצא של פעילות ענפה זו, ירדו מספר ההתקפות הפיראטיות באזור מזרח אפריקה לרמה זניחה. דוגמה זו ממחישה את הפער בין מתן מענה לאיום ממשי לבין איום הסייבר הקיברנטי, שאינו מוחשי, ולכן לא מושקעים בו משאבי הניהול והתקציבים המתאימים, חרף הסכנה הגדולה שהוא מהווה.

חברת הספנות – הירידה בעלויות השינוע הימי והשחיקה משמעותית ברווחים בתחום ההובלה הימית (חברת 'צים' לדוגמה הציגה בדוחות האחרונים של שנת 2015, הפסד חצי שנתי של 132 מיליון דולר). מקשים מבחינה כלכלית על חברות הספנות להשקיע בטכנולוגיות אבטחת מידע מתקדמות וגורמות להן לקחת סיכונים גדולים.

הנה כמה מהאתגרים שאיתן נאלצות חברות הספנות להתמודד בתחום זה:

- מחזור אורך החיים של מערכות טכנולוגיות והמספר הרב של יצרני חומרה ותוכנה לכלי שיט גורם להתיישנות מהירה של מערכות ההפעלה וזאת לפני הצורך בהחלפת המערכות כולן ומקל על הפריצה אליהן.
- התקשורת בין הנמלים לאוניות מתבססת על תווך גלוי ולא מוצפן שמטרתו לחסוך בעלויות השדרוג של המערכות למערכות מוצפנות.
- פיתוח המערכות והתוכנה בנמלים ובכלי השיט לא בוצעה תחת תפיסת 'פיתוח מאובטח' וכעת נדרשת השקעה עצומה כדי לבצע הסבה לתפיסה זו.
- מחסור באנשי מקצוע מיומנים בתחום.

בניגוד לתחומים אחרים בעולם הנמלים והספנות, כמו בטיחות השיט או הגנת הסביבה, אין כיום רגולציה או הנחיות ברורות ומחייבות. לכן אבטחת הסייבר נתונה ליוזמה מקומית של חברות הספנות ללא דירקטיבה לאומית או בינלאומית מחייבת.

סיכום והמלצות

נמלי ישראל מהווים את צינור החמצן שדרכו מגיע כ-98% מנפח הסחורות לישראל. לכן, מן הראוי לתת את הדעת על הגנה נאותה לאיום הקיברנטי החדש מולו ניצב סקטור הנמלים והספנות.

מניתוח הפעילות בארץ ובעולם עולה כי הגופים העוסקים בתחום הספנות והנמלים (מדינות, חברות ביטוח, איגודי ספנות), מודעים לנושא איום הסייבר, אך מודעות זו טרם הגיעה לבשלות שבכוחה להניע מהלכים מערכתיים קונקרטיים שיתמודדו עם האיום, וזאת בניגוד לנעשה בעולם הפיננסי או הביטחוני.

מכיוון שנמלי ישראל מהווים תשתית לאומית חיונית נדרש להגן עליהם בהתאם על מנת לאפשר רציפות תפקודית. בניית של מערך הגנה הולם שבכוחו להתמודד עם התקפות סייבר חייב להיות חלק מתכנית אסטרטגית שתכלול את הנושאים הבאים :

- קביעה ותיקוף של איום הייחוס של מערך הנמלים והספנות, נושא זה חייב להיכלל במתאר האיומים על תשתיות קריטיות במדינת ישראל.
- ניתוח סיכונים לכלל המערכות ותהליכי העבודה במערך הנמלים והספנות.
- דירוג הסיכונים בהתאם למידת ההשפעה שלהם על הפגיעה בתהליכי העבודה המרכזיים בנמלים.
- מינוי של גוף מרכזי שיוביל את הנושא ויספק לגורמי ממשלה ניתוח של האיומים, והמלצות כיצד להתמודד עם כל אחד מאיומים אלו. לגוף זה תהיה את הסמכות לתת הנחיות מחייבות לרספ"ן.¹²
- הגדרת תקינה להגנת סייבר מחייבת לכל הנמלים בישראל.
- ביצוע של תרגילי תקיפה שנתיים מתוכננים ותרגילי פתע שיתבצעו על ידי צוות 'אדום' של רשות הסייבר הלאומית כדי לבחון את יעילותה של ההגנה.
- הגדרה של חלק ממערכות המידע הקריטיות של מערך הנמלים כמערכות ליבה, ופיתוחן של מערכות ליבה אלו בתפיסה של 'פיתוח מאובטח'.
- הצפנת המידע שיוגדר כמסווג ובעל חשיבות ביטחונית למדינה וכן את תווך התקשורת בין הנמלים לאוניות.
- שיתוף פעולה עם מדינות ואיגודי ספנות בינלאומיים רלוונטיים על מנת להגיע לחתימה הדדית על הסכמים בנושא העברת מידע.

12 מרכז חיפה למחקרי מדיניות ואסטרטגיה ימית יסייע לגורם שיקבע בניתוח האיומים והמלצות לגבי פתרונות

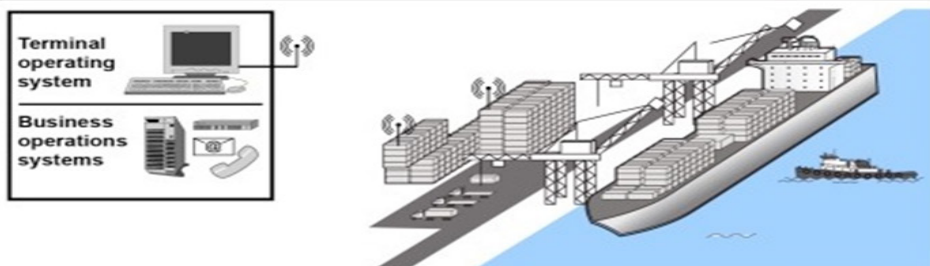
- הובלת תהליך לאומי של יצירת תקינת סייבר לעולם הספנות, שיתבצע יחד עם קבוצת מדינות ידידותיות ורלוונטיות, הובלה זו תסייע גם לחברות הישראליות בתחום.
- תקינה זו תגדיר את מענה ההגנה המיטבי של כל אוניה, ואת התקינה שבה עליה לעמוד על מנת לשמור על כשירותה התפעולית, וזאת בדומה לנהלים שמגדירים בטיחות שיט.

מכיוון שקיימת שחיקה מתמשכת במחירי ההובלה הימית וירידה משמעותית ברווחים של החברות, אנו עדים להשקעה הולכת ופוחתת בטכנולוגיות חדשות, כולל מערכות להגנת סייבר, שמהוות תקורה ואינן מוסיפות ליכולת התפעוליות של כלי השיט. ייתכן שהדרישה לתקינה בתחום תגיע דווקא מצדן חברות הביטוח ואיגודי הספנות, המגדירים את איום הסייבר כאיום משמעותי ורואות בו מרכיב סיכון גבוה.

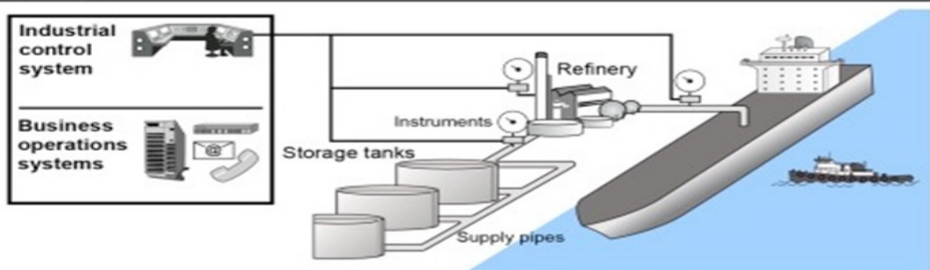
המלצות:

- ביצוע של ניתוח סיכונים למערכות המחשוב והתפעול, ויצירה של תכנית רציפות תפקודית בעת כשל באחת ממערכות אלו.
- ניתוח של תהליכי העבודה של כלי השיט בעת הפלגה, ובעיקר בנמל, וזאת על מנת לזהות נקודות כשל אפשריות עיקריות שיאפשרו פריצת סייבר (כמו תהליך התחזוקה מרחוק של מערכת כזו או אחרת בספינה, תהליכי פריקה וטעינה של מכולות וכיוצא בזאת).
- מיפוי של כלל המערכות, מבחינת גרסאות התוכנה והחומרה, וקבלת עדכוני אבטחה מהיצרנים.
- ניתוח כלל אמצעי התקשורת שיש לאוניה בים ובנמל ובנייה של מענה הגנה מתאים (כמו הצפנה של תווך התקשורת, חסימת התקנים ועוד).
- הדרכה, אימון ותרגול של צוות האוניה, החל מרמת המודעות לאיומי הסייבר (לדוגמה, הימנעות מהכנסה של התקנים חיצוניים, חיבור בין סוגי רשתות, עבודה נכונה ברשת האינטרנט), ועד דרכי ההתנהלות בעת זיהוי איום סייבר, והדרכים להכיל אירוע כזה.
- יצירה של מעטפת ביטחונית לאנשי הצוות באוניה, שכוללת בדיקות פרטניות לאנשי מפתח שיש להם גישה למערכות רגישות שלפגיעה בהן עלולות להיות השלכות הרסניות.

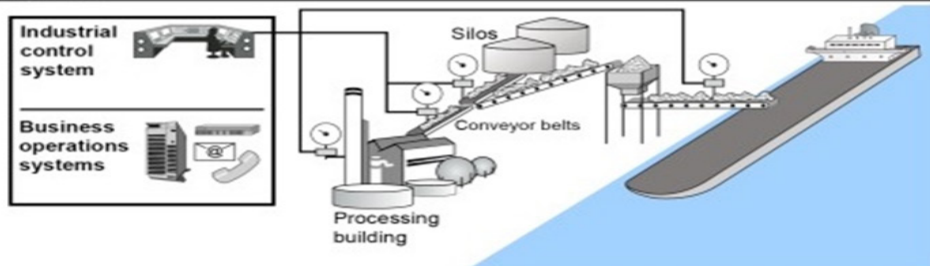
Container



Bulk liquid



Dry bulk



System descriptions

Terminal operating systems

Control container movement and storage in the maritime port, among other things. Examples of data that terminal operating systems could contain include shipping information, cargo categorization, and records of container movement.

Industrial control systems

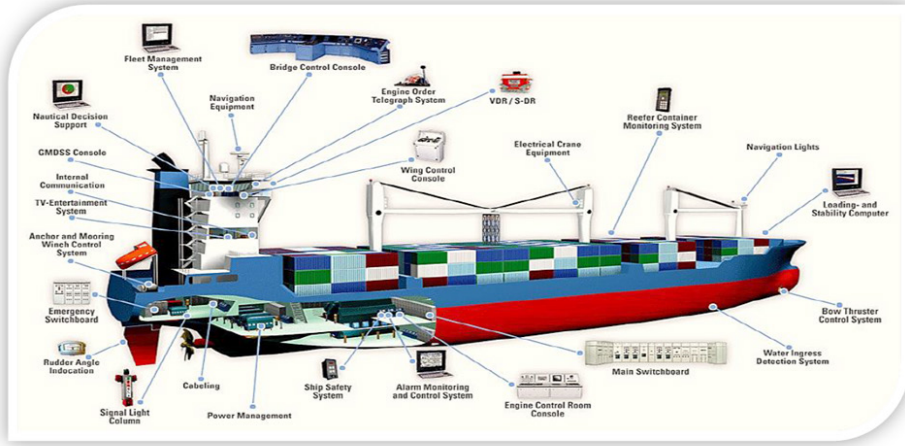
Facilitate the movement and processing of goods throughout the terminal, including the operation of motors, pumps, valves, signals, lighting, and access controls.

Business operations systems

Support the business operations of the terminal, such as communication with customers and preparation of invoices and billing documentation.

Source: GAO analysis of maritime sector information

איור 8.1 מערכות ממוחשבות לתקשורת בין ספינה לרציף



איור 8.2 מערכות מבוססות מחשוב באונייה



איור 8.3 מערכות מידע בנמלים