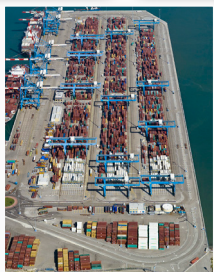


הערכה אסטרטגית ימית לישראל 2019/20

עורך ראשי: פרופ' שאול חורב

עורך והפיק: אהוד גובן



11. שיטות בשימוש במערכי ביטחון סייבר במגזר הימי האזרחי¹

אופיר כפרי

רקע

מאמר זה נועד להציג דוגמאות למספר שיטות שנעשה בהן שימוש במערכי ביטחון סייבר במגזר הימי האזרחי במדינות שונות. בשנים האחרונות חלה התפתחות במערכי ביטחון סייבר ימי אזרחי בחלק מהמדינות הנחשבות מתקדמות מבחינת ביטחון סייבר.² אירועים והתקפות סייבר במגזר הימי שגרמו להשפעה בינלאומית ומקומית רחבה וסיבות נוספות אחרות הובילו להתחזקות מגמה זו.³ ביטחון סייבר אף שולב באסטרטגיות הימיות של חלק מהמדינות המרכזיות הפועלות במרחב הימי.⁴

מדינות הקימו מערכי ביטחון סייבר במגזר הימי הכוללים מגוון כלים במטרה לנהל את הסיכונים לתשתיות קריטיות ואחרות במגזר. לדוגמה, הוקמו מרכזי ניהול אירועי סייבר ימי לנמלים ולמרחב הימי, פלטפורמות לשיתוף מידע ותיאום במגזר עצמו ועם מגזרים אחרים. רגולציית סייבר הכוללת את המרחב הימי נכנסה לתוקף במספר מדינות. דוגמאות נוספות הן תוכניות הכשרת כוח אדם והעלאת מודעות, פרסום הנחיות וקביעת סטנדרטים, הקמת תשתית מחקר ופיתוח, שיתוף פעולה בינלאומי ועוד.

- 1 פרק זה הוא חלק ממחקר הנכתב בסיוע מענק מחקר מטעם המרכז לחקר סייבר, משפט ומדיניות (CCLP) והמרכז לחקר מדיניות ואסטרטגיה ימית (HMS).
- 2 International Telecommunication Union (ITU), Global Cybersecurity Index (GCI) 2018 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
- 3 אירועי סייבר התרחשו בספינות, אסדות קידוח, תשתיות נמלים מסחריים, נמלי אנרגייה (דלק וגז), חברות ספנות, חברות שילוח בינלאומי ימי, חברות שירותי נמל וסוכני אוניות, רגולטורים ימיים ועוד. לדוגמה אנא ראו: United States Senate, Report of United States Senate Committee on Armed Services, inquiry into cyber intrusions affecting u.s. transportation command contractors, iii, 2014; Coast Guard Maritime Commons site, Lt. Jodie Knox, Coast Guard Commandant on Cyber in the maritime domain, June 15, 2015; The Columbian, Dameon Pesanti, Port of Vancouver meeting hindered by cyberattack, March 10, 2017; The New York Times site, Thomas Erdbrink, Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet, published April 23, 2012; Clarkson PLC Annual Report 2017, Page 19, 83; Danish Broadcasting Corporation news site, Michael Lund and Niels Fastrup, Fremmed stat spionerede mod dansk ministerium (Foreign State spied on Danish ministry), published September 21, 2014.
- 4 לדוגמה ראו מסמכי אסטרטגיה ימית של ארה"ב וצרפת: U.S.A Navy, Marine Corps, and Coast Guard, A Cooperative Strategy for 21ST Century Seapower, March 2015, page 33-34; France National strategy for the security of maritime areas, October 2015, page 23-24.

עקב קוצר היריעה יוצגו רק חלקים ממערכי ביטחון הסייבר הימי של מדינות עיקריות המוצגות במאמר והן ארה"ב, הולנד, דנמרק, קנדה וסינגפור. מדינות אלו נבחרו עקב היותן גורמים בעלי חשיבות במגזר הימי הגלובלי ו/או מפני שהן מפתחות מערכי סייבר ימי מדינתיים. יש לציין כי קיימים הבדלים מבחינת יכולות, איכות הפעילות והיעילות של המרכיבים במערכים של המדינות השונות. לסיכום יוצגו המרכיבים המרכזיים הקיימים במערכים שאף מומלצים על פי מדריכים בינלאומיים מרכזיים בתחום.

המרחב הימי של סינגפור

המגזר הימי האזרחי בסינגפור הוא גורם חשוב בכלכלת המדינה, והוא אחראי ל-7 אחוזים מהתוצר הלאומי הגולמי (GDP) בשנת 2017 וכ-170,000 מקומות עבודה.⁵ סינגפור שוכנת ליד מיצרי מלאקה וסינגפור (SOMS) הנחשבים לנתיב קריטי ואסטרטגי במערכת התעבורה הימית הגלובלית. דרך שני המיצרים עוברים כל שנה כמעט חצי מסך כל משקל המטען המסחרי הימי העולמי, ו-70 אחוז מיבוא הנפט לאסיה.⁶ אסטרטגיית הסייבר של סינגפור מדגישה את חשיבות ההגנה על הפעילות הימית, וזאת לאור היות נמל סינגפור השני בעולם בתעבורת מכולות.⁷ סוכנות אבטחת הסייבר של סינגפור (Cyber Security Agency of Singapore) פועלת להגנת המגזר הימי האזרחי בשיתוף עם רשות הים והנמלים של סינגפור (MPA Maritime and Port Authority of Singapore).

מרכז ניהול אירועי סייבר ימי (Maritime Cybersecurity Operations Centre) נפתח במאי 2019 בסינגפור. המרכז מבצע ניטור ותיאום של כלל תשתיות המידע הקריטיות במרחב הימי. למרכז אמורות להיות יכולות לזיהוי התקפות סייבר על ידי ניתוח תשתית מערכות המידע, גילוי חריגות ואיומים, ומתן תגובה לאירועי סייבר על ידי שימוש בפתרונות טכנולוגיים מגוונים.⁸ המרכז אמור לאפשר לרשות הים והנמלים של סינגפור (MPA) לעבוד יחד עם גורמי תשתיות מידע קריטיות כדי לחקור איומים ואירועי סייבר במרחב הימי. מרכז

Singapore Ministry of Trade and Industry, Enterprise Singapore, Industry Profile, 2018: <https://www.enterprisesg.gov.sg/industries/type/sea-transport/industry-profile> 5

Singapore Ministry of Defence, Fact Sheet: The Malacca Straits Patrol, 21 Apr 2015: <https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2016/april/2016apr21-news-releases-00134> 6

Singapore's Cybersecurity Strategy, Cyber Security Agency of Singapore, 10 Oct 2016: <https://www.csa.gov.sg/~media/csa/documents/publications/singaporecybersecuritystrategy.pdf> 7
Lloyds list, One Hundred Ports 2019: <https://loydslist.maritimeintelligence.informa.com/one-hundred-container-ports-2019>

Cyber Security Agency of Singapore, Singapore's Operational Technology Cybersecurity Masterplan 2019, 01 Oct 2019, page 41: https://www.csa.gov.sg/~media/csa/documents/publications/ot_masterplan/csa_ot_masterplan.pdf 8

הסייבר יקושר למרכז בקרת תפעול הנמל (Port Operations Control Centre) POCC של הרשות, וזאת על מנת לאפשר תגובה מהירה ומקיפה לאירועי סייבר.⁹

בתחום הכשרת כוח אדם מפותח קורס חדש ומקיף מזה הקיים שמטרתו להכשיר אנשי מקצוע במגזר הימי בנושאים בביטחון סייבר. הקורס מפותח בשיתוף פעולה עם אגודת הספנות של סינגפור (Singapore Shipping Association) ומוסד להשכלה מקצועית (Singapore Polytechnic), והוא אמור להכשיר כוח אדם, בין השאר, בתחום ניהול סיכונים ואמצעי-נגד בביטחון סייבר.¹⁰ בנוסף לכך מתקיימות פעילויות בשיתוף רשות הים והנמלים ואגודת הספנות של סינגפור שמטרתן להעלות מודעות לנושא ביטחון סייבר ימי דוגמת סמינרים הכוללים את המגזר הפרטי והציבורי.¹¹

חוק הסייבר החדש נכנס לתוקף במרץ 2018, והוא מעניק סמכויות רחבות היקף בתחום לממונה אבטחת סייבר של סינגפור (Commissioner of Cybersecurity) ובעלי תפקידים נוספים שימונו מטעמו או בידי השר האחראי. נקבעו, בין השאר, סמכויות המאפשרות איסוף מידע, חקירה, שיתוף מידע והתערבות באירוע סייבר. החוק קובע חובות בנוגע לביטחון סייבר בתשתיות שהוגדרו חיוניות במגזר הימי דוגמת ניטור וניהול תעבורת ספנות, תפעול טרמינלים לסווגיהם, תשתית תדלוק, פעילות חילוץ והצלה ועוד.¹²

תוכנית מחקר בתחום ביטחון סייבר ימי, הממוקדת בהגנת ציוד דיגיטלי בספינות, צפויה לפעול בשיתוף פעולה של רשות הים והנמלים עם מוסדות השכלה גבוהה בסינגפור והמכון הימי של סינגפור (Singapore Maritime Institute) SMI.¹³

Singapore Computer Emergency Response Team (SingCERT), Maritime, 08 Oct 2019: <https://www.csa.gov.sg/singcert/publications/maritime> 9

Maritime and Port Authority of Singapore, New 24/7 Maritime Cybersecurity Operations Centre to Boost Cyber Defence Readiness, 16 May 2019: <https://www.mpa.gov.sg/web/portal/home/media-centre/news-releases/detail/8a5114cf-8214-4b46-8999-2c6c42433b1e> 10

Maritime and Port Authority of Singapore, Shaping the Future of a Cyber-smart Maritime Industry, 24 April 2018: <https://www.mpa.gov.sg/web/portal/home/media-centre/news-releases/detail/0c373e30-7ff8-4a8a-a1d8-32bd3299ea4d> 11

Singapore Legislation Division of Attorney-General's Chambers, Cybersecurity Act 2018, 12 Mar 2018: <https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312>; Cyber Security Agency of Singapore, Cybersecurity Act, Explanatory Statement: https://www.csa.gov.sg/~media/csa/cybersecurity_bill/cybersecurity%20act%20-%20explanatory%20statement.pdf 12

Singapore Maritime Institute, About us: <https://www.maritimeinstitute.sg/about-us>; Maritime and Port Authority of Singapore, New 24/7 Maritime Cybersecurity Operations Centre to Boost Cyber Defence Readiness, 16.5.2019. 13

שיתוף פעולה בינלאומי מתקיים עם מספר מדינות, וכולל שיתוף מידע מקצועי בנוגע להגנת תשתיות קריטיות ונגישות לפעילות הכשרה. לדוגמה, בשנת 2016 נחתם מזכר שיתוף פעולה בביטחון סייבר עם הולנד.¹⁴ דוגמה אחרת היא אירוח כנס של פורום בינלאומי העוסק בביטחון השיט והגנת הסביבה במיצרי סינגפור ומאלקה שכלל ביטחון סייבר.¹⁵ הרשות לים ונמלים של סינגפור מתכננת הקמת רשת שיתופי פעולה בינלאומיים עם רשויות מקבילות וגורמים אחרים שמטרתה שיתוף במידע לגבי איומים ואירועי סייבר.¹⁶

תרגילי סייבר לאומיים המנוהלים על ידי סוכנות אבטחת הסייבר של סינגפור שילבו בשנת 2017 ו-2019 את המגזר הימי. התרגילים בחנו, בין השאר, את עמידות המרחב הימי לתרחישי סייבר מגוונים. התרגילים כללו מגזרים קריטיים אחרים במטרה לבחון מוכנות לאירועי סייבר משמעותיים תוך שיתוף פעולה בין-מגזרי.¹⁷

המרחב הימי של הולנד – נמל רוטרדם ונמל אמסטרדם

מספר גופי סייבר של הולנד דוגמת המרכז הלאומי לאבטחת סייבר (NCSC) מסייעים לגורמים במגזר הימי, ביניהם נמלי רוטרדם ואמסטרדם. חוק אבטחת רשתות ומערכות מידע העוסק באבטחת סייבר נכנס לתוקף בשנת 2018, והוא מתייחס לדירקטיבת האיחוד האירופי בתחום NIS Directive (EU) 2016/1148.¹⁸ החוק מחייב ספקי שירות חיוני, כולל מהמגזר הימי, בעמידה בדרישות אבטחת סייבר. בנוסף לכך מוענקות סמכויות למשרדי ממשלה שנקבעו בחוק או ל-Computer Security Incident Response (CSIRT)

14 Singapore and the Netherlands to Strengthen Cyber Security Cooperation, Cyber Security Agency of Singapore, 12 Jul 2016: <https://www.csa.gov.sg/news/press-releases/csa-signs-mou-with-the-netherlands-to-strengthen-cyber-security-cooperation>

15 MPA, 8th Co-operation Forum addresses key issues relating to Straits of Malacca and Singapore, October 2015: <https://www.mpa.gov.sg/web/portal/home/media-centre/news-releases/detail/c8c677d0-07d1-4d9c-b634-ac416c4c29e9>; Co-operative Mechanism on Safety of Navigation and Environmental Protection in the Straits of Malacca and Singapore, October 2015: https://www.soefartsstyrelsen.dk/Presse/Nyheder/Documents/Program_Co-operative%20Forum_Singapore.pdf

16 Maritime and Port Authority of Singapore, New 24/7 Maritime Cybersecurity Operations Centre to Boost Cyber Defence Readiness, 16.5.2019

17 Cyber Security Agency of Singapore site, 11 CII Sectors Tested on More Complex Cyber Attack Scenarios, 04 Sep 2019: <https://www.csa.gov.sg/news/press-releases/exercise-cyber-star-2019>

18 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016: <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>

(Team) הלאומי, בהתאם לנסיבות, לקבל דיווחים על אירועי סייבר. סמכויות נוספות שהוענקו נוגעות, בין השאר, לחקירה, ביקורת וסנקציות.¹⁹

נמל רוטרדם מדורג ראשון באירופה מבחינת תעבורת מכולות ואחד-עשר בעולם.²⁰ הנמל מהווה גורם חשוב בכלכלת הולנד ובפעילות תעבורה ימית מסחרית באירופה.²¹ בשנת 2017 כמעט מחצית מפעילות התעבורה המסחרית בנמל שירתה את אירופה, וכרבע את אסיה בחישוב של משקל מטען.²² הנמל מוגדר כספק שירות חיוני על פי חוק משנת 2018, ובעקבות כך הוא מחויב לעמוד במספר דרישות בתחום ביטחון סייבר. דוגמה לדרישה היא חובת דיווח על אירועי סייבר העומדים בתנאים מסוימים, לגורמי ממשל שנקבעו בחוק, ועמידה בדרישות סף הנוגעות לביטחון סייבר.²³

הנמל פועל בשיתוף פעולה עם המרכז הלאומי לאבטחת סייבר, ובנוסף לכך הוקמו בו מספר גופים בתחום אבטחת סייבר. לדוגמה דסק המקבל דיווחים בכל עת לגבי אירועי סייבר משמעותיים פועל במסגרת מרכז תפעול של הנמל משנת 2018. חברות הפועלות בנמל הכפופות לקוד ISPS²⁴ או לרגולציה של האיחוד האירופי²⁵ מחויבות לדווח לדסק, ולעיתים לגורמים נוספים, על אירועי סייבר משמעותיים. אירועים אלו מתייחסים למצבים

Netherlands Network and Information Systems Security Act (Wet beveiliging netwerk- en 19
informatiesystemen), Act of 17 October 2018:

https://wetten.overheid.nl/BWBR0041515/2019-01-01#Hoofdstuk4_Paragraaf1_Artikel5

World Shipping Council, Top 50 World Container Ports: <http://www.worldshipping.org/about-the-industry/global-trade/top-50-world-container-ports> 20

Erasmus University Rotterdam, Centre for Urban, Port and Transport Economics, The Rotterdam effect, 18 Dec 2018: <https://www.eur.nl/en/upt/news/rotterdam-effect>; W. Heijman et al, The impact of world trade on the Port of Rotterdam and the wider region of Rotterdam-Rijnmond, Case Studies on Transport Policy, 5 (2017) 351–354 21

Port of Rotterdam Authority, Facts and Figures, 2019: <https://www.portofrotterdam.com/sites/default/files/facts-and-figures-port-of-rotterdam.pdf> 22

Netherlands Network and Information Systems Security Act (Wet beveiliging netwerk- en informatiesystemen), Act of 17 October 2018; Decision on network and information security (Besluit beveiliging netwerk- en informatiesystemen), Decree of 30 October 2018: <https://wetten.overheid.nl/BWBR0041520/2019-01-01> 23

Safety of Life at Sea (International Ship and Port Facility Security) ISPS Code 24
(SOLAS Convention) מטרת הקוד היא לחזק את הביטחון בספינות ובתשתיות נמל. הצדדים שהתקשרו באמנה (Contracting Parties) מחויבים ליישם את הקוד. למידע נוסף ראו: International Maritime Organization (IMO), SOLAS XI-2 and the ISPS Code: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

Regulation (EC) no. 725/2004; Netherlands Port Security Act: <https://wetten.overheid.nl/BWBR0016991/2010-10-01> 25

שיש להם השפעה על ביטחון התעבורה בנמל, כניסות ויציאות של כלים ימיים, ויישום תוכנית הביטחון של הנמל.²⁶

בשנת 2016 מונה אחראי על חוסן בתחום ביטחון סייבר בנמל (Port Cyber Resilience Officer) ונקבעה תוכנית פעולה. תחום אחריותו כולל, בין השאר, העלאת מודעות, הכשרה וניהול סיכונים בתחום. לצורך כך הוקמו ועדות העוסקות בתחומים שונים של ביטחון סייבר דוגמת משפט, מודעות ותרגול ועוד. האחראי פועל בשיתוף פעולה עם גורמי אכיפת החוק, הרשות המוניציפלית והאגודה העסקית של חברות העובדות עם הנמל.²⁷ הנמל מבצע תרגילי סייבר, ומפעיל צוות של מומחי ביטחון סייבר האחראי להגן על תשתיות הנמל.

בתחום הכשרה והעלאת מודעות נערכו כנסי סייבר לעסקים הפועלים עם הנמל. תוכנית סיוע לעסקים קטנים בתחום ביטחון סייבר מופעלת בידי הנמל, ובמסגרתה מתקיימות פעילויות הכשרה אלקטרוניות, ומוצעים כלים המסייעים לזיהוי חולשות במערכות העסקים. הסיוע ניתן מתוך תפיסה שעסקים קטנים חשובים לפעילות הנמל, מחוברים למערכות חשובות שבו, אך אין להם משאבים לטפל בסוגיות סייבר מורכבות, ולכן יכולים להוות חולייה חלשה.²⁸

נמל אמסטרדם החל בתוכנית לשדרוג אבטחת הסייבר בשנת 2018. הוא הציג מודלים דיגיטליים ללמידה בתחום אבטחת מידע שנועדו להעלות מודעות לנושא בקרב העובדים וגורמים רלוונטיים אחרים. בשנת 2019 החלה תוכנית פיילוט שמטרתה העברה לתצורה אוטומטית של חלקים בתהליך הערכת הסיכונים הכולל גם ביטחון סייבר.²⁹

Port of Rotterdam, Policy document port cyber notification desk: https://www.portofrotterdam.com/sites/default/files/policy-document-port-cyber-notification-desk.pdf?token=waAgc_VH; Port Cyber Hotline operational, 11 June 2018: <https://www.portofrotterdam.com/en/news-and-press-releases/port-cyber-hotline-operational>

Port of Rotterdam site, Port of Rotterdam appoints Port Cyber Resilience Officer, 13 June 2016: <https://www.portofrotterdam.com/en/news-and-press-releases/port-of-rotterdam-appoints-port-cyber-resilience-officer>

Port of Rotterdam site, How the Port of Rotterdam is investing in cybersecurity, 06 December 2016: <https://www.portofrotterdam.com/en/news-and-press-releases/how-the-port-of-rotterdam-is-investing-in-cybersecurity>

:Port of Amsterdam Annual Report 2018, page 67, 72-73. Published on 6 May 2019 https://jaarverslag2018.portofamsterdam.com/wp-content/uploads/2019/06/Port-of-Amsterdam-Annual-Report-2018_final.pdf

הנמל גייס אחראי אבטחת מידע והקים דסק דיווח על אירועי סייבר. הדסק מקבל דיווחים וולונטריים ודיווחים שקיימת חובה משפטית לגביהם הנוגעים למקרים שבהם גורמים מעורבים כפופים לקוד ISPS,³⁰ ועומדים ברשימה של תנאים שהנמל פרסם.

שיתופי פעולה בתחום מתקיימים עם גורמים חיצוניים לנמל דוגמת מרכז אבטחת הסייבר הלאומי, נמל רוטרדם, מרכז הסייבר לעסקים של ממשלת הולנד Digital Trust Center ועוד. בנוסף לכך החלה לפעול בנמל תוכנית לשיתוף מידע וידע מקצועי המשלבת את המגזר הפרטי והציבורי, כולל גורמי אכיפת חוק ועוד. התוכנית פתוחה להצטרפות לגורמים רלוונטיים הקשורים לפעילות במרחב הימי של הנמל ואזור תעלת הים הצפוני, הכולל מתקנים נוספים. הנמל מקיים אירועים ציבוריים בתחום סייבר במטרה להעלות מודעות ולסייע במידע מקצועי.³¹

המרחב הימי של קנדה

מגזר התחבורה בקנדה, הכולל בתוכו את המגזר הימי, הוא אחד מעשרת המגזרים שהוגדרו כתשתית קריטית לאומית. משרד התחבורה אחראי לתיאום תגובה פדראלית במקרה של אירוע סייבר במגזר הימי. המשרד אחראי להקמת רשת וולונטרית לשיתופי פעולה הכוללת גורמים במגזר הימי. הרשת אחראית לתוכנית הערכת סיכונים מגזרית המעודכנת על בסיס שנתי.³²

פורום ממשלתי הנקרא פרויקט סיכוני סייבר ימי, מהווה בסיס לשיתוף פעולה הכולל עשרה גופים ממשלתיים שונים, ומטרתו להציע פתרונות לאיומי סייבר אפשריים במרחב הימי.³³ מרכז התגובה לאירועי סייבר של קנדה (Canadian Cyber Incident Response Centre) מפעיל פלטפורמה דיגיטלית להפצת מידע ולשיתוף פעולה למגזרי התשתיות הקריטיות. הפלטפורמה מאפשרת חלוקת מידע לפי רמות סיווג ביטחוני. המרכז זמין לעזור בניהול אירועי סייבר בתשתיות קריטיות, כולל במרחב הימי, והוא מפעיל תוכנית סיוע לביצוע הערכת סיכונים לגופים מהמגזר הפרטי.³⁴

30 ראה הערת שוליים מס' 24.

31 Port of Amsterdam, Cyber security in the North Sea Canal Area (NSCA): <https://www.portofamsterdam.com/en/port-amsterdam/organisation/cyber-security-nsca>

32 Canada Action Plan for Critical Infrastructure, Date modified: 2018-01-31: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/pln-crtcl-nfrstrctr/index-en.aspx#aB>

33 NATO Association of Canada, Canada's Cyber Security: A Discussion with Public Safety Canada, 22 August 2018: <http://natoassociation.ca/canadas-cyber-security-a-discussion-with-public-safety-canada>

34 Public Safety Canada, Fundamentals of Cyber Security for Canada's CI Community, Date modified: 2019-01-21: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx>

גופים הנמצאים תחת רגולציית ביטחון ימי חייבים לשלב אבטחת סייבר בהערכות ותוכניות הביטחון שלהם. במקרים מסוימים ישנה חובה לדווח על אירוע סייבר לגופי ממשל שנקבעו לצורך כך בחוק.³⁵

משרד התחבורה הקנדי פרסם בשנת 2016 חוברת בתחום אבטחת סייבר הכוללת שיטות עבודה מומלצות לגופים במרחב הימי.³⁶ יש לציין כי חוברות דומות פורסמו בשנים 2017-2016 מטעם בריטניה למגזר הימי. החוברות מציגות שיטות מומלצות באבטחת סייבר בתשתיות נמל ובספינות.³⁷ צרפת פרסמה אף היא סדרת חוברות בשנים 2016-2018 בנושא אבטחת סייבר במרחב הימי. החוברות התמקדו בשיטות מומלצות לאבטחת סייבר בספינות ואיומים אפשריים.³⁸

מופעלים מרכזים בתחום אירועי ביטחון ימי (MSOC Marine Security Operations Centers) האחראים על שליטה וניהול אירועים במרחב הימי. בשנים האחרונות התווסף גם תחום ביטחון הסייבר לפעילותם של המרכזים, ואלה מסייעים להערכות סיכונים לנמלים, כלים ומתקנים ימיים. כל שנה נעשות כ-7,000 הערכות סיכון לכלים ימיים הנכנסים למרחב הימי הקנדי.³⁹

במרכזים משולבים גופי ממשל שונים שהם רלוונטיים למרחב הימי. בנוסף לכך מתקיים שיתוף פעולה במשאבים דוגמת מידע מודיעיני. המרכזים מתמקדים בזיהוי ודיווח על

Transport Canada, Marine Security Operations Bulletin, No: 2014- 001: https://www.tc.gc.ca/media/documents/marinesecurity/MSOB_BSOM_2014-001-en.pdf 35

Transport Canada, Understanding Cyber Risk: Best Practices for Canada's Maritime Sector Page 16-17: http://publications.gc.ca/collections/collection_2016/tc/T86-21-2016-eng.pdf 36

UK Department for Transport & Institution of Engineering and Technology, Ports and port systems: cyber security code of practice, 16 August 2016: <https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice>; Ship security: cyber security code of practice, 2017: <https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice> 37

France Ministry of Environment, Energy and The Sea, Directorate-General for Infrastructure, Transport and the sea, Maritime Affairs Directorate, Cyber Security - Assessment and Protection of Ships, September 2016 Edition: <https://www.ecologique-solidaire.gouv.fr/sites/default/files/Guideline%20-%20Cyber%20security%20-%20Assessment%20and%20protection%20of%20ship.pdf>; Cyber Security – Reinforcing the Protection of Industrial Systems on a Ship, France Directorate-General for Infrastructure, Transport and the sea, Maritime Affairs Directorate, January 2017 Edition 38

Transport Canada, Transport Canada defends Canada's waterways and coastlines, 2019-03-07: <https://www.tc.gc.ca/eng/transport-canada-defends-waterways-coastlines.html> 39

פעילות ימית בעלת פוטנציאל איום על ביטחון ובטיחות.⁴⁰ נמל וונקובר, המדורג ראשון בהיקף הפעילות בקנדה, מקיים שיתופי פעולה עם מרכז MSOC ועם גורמים נוספים בעלי יכולות בתחום אבטחת סייבר.⁴¹

דנמרק – יישום אסטרטגיית ביטחון סייבר ימי

המגזר הימי הוא אחד מהתשתיות הקריטיות במדינה לפי אסטרטגיית הסייבר הלאומית. מסמך אסטרטגיית סייבר ספציפי למגזר הימי פורסם בינואר 2019, וחלק מהאמצעים המופיעים בו כבר יושמו.⁴² מטה קבוצת מולר-מארסק (A.P. Moller - Maersk), שהוא גם חברת הספנות הגדולה בעולם בתחום מכולות, פועל בדנמרק. התקפת סייבר משמעותית פגעה בחברות בקבוצה בשנת 2017, והשפיעה על פעילות נמלים במספר מדינות.⁴³

המרכז לאבטחת סייבר של דנמרק (Centre for Cyber Security) CFCS מספק סיוע לרשות הימית הדנית (Danish Maritime Authority) DMA. בנוסף לכך הוא אמור לשלב גורם מקצועי מהרשות הימית במרכז לאבטחת סייבר. עוד נקבע במסמך האסטרטגיה שהרשות הימית משמשת כנקודת קישור בין המגזר הימי למרכז לאבטחת סייבר. שיתוף הפעולה בין הגופים כולל ניתוח ומתן מידע על איומים וסיוע לפרסום של הערכת איומים למגזר הימי.⁴⁴ הערכה ראשונה פורסמה לציבור בשנת 2017, ואף כללה המלצות לאבטחת סייבר למגזר הימי.⁴⁵

ביוני 2018 הוקמה יחידה לביטחון סייבר ימי ברשות הימית הדנית, והיא אחראית ליישום האמצעים המופיעים במסמך האסטרטגיה. היחידה אמורה לשמש כגורם מייעץ, מרכז

Government of Canada, Marine Security Operation Centres, 2013-05-23: <https://www.tc.gc.ca/eng/marinesecurity/operations-269.html>; Canadian Coast Guard site, 2017-12-14: <http://www.ccg-gcc.gc.ca/eng/CCG/Maritime-Security/MSOC>

Port of Vancouver, Security and Emergency Management, Partners section: <https://www.portvancouver.com/about-us/security-emergency/partners>

Danish Ministry of Finance, Danish Cyber and Information Security Strategy 2018-2021, Page 8, 40: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf; Danish Maritime Authority, Cyber and Information Security Strategy for the Maritime Sector: <https://www.dma.dk/Documents/Publikationer/Cyber%20and%20Information%20Security%20Strategy%20for%20the%20Maritime%20Sector.pdf>

MAERSK Site, News Release, A.P. Møller - Mærsk A/S Cyber attack update, June 28, 2017: <http://investor.maersk.com/node/19831/pdf>

DMA, Cyber and Information Security Strategy for the Maritime Sector, page 8-9.

Denmark Threat Assessment Branch under the Centre for Cyber Security, The cyber threat against the maritime sector, March 2017: https://fe-ddis.dk/cfcs/CFCSDocuments/The_Cyber_Threat_to_the_Maritime_Sector_march.pdf

תקשורת למגזר הימי וגורם מומחה ברשות הימית. היחידה אחראית להכנת אירועים לציבור וריכוז תוכנית פעולה בשיתוף עם המגזר הימי בתחומים דוגמת רגולציה, הכשרה, העלאת מודעות ועוד.⁴⁶ היחידה משתתפת בפורום סייבר הכולל את כלל היחידות מהמגזרים הקריטיים של דנמרק המופעל בשיתוף המרכז הלאומי לאבטחת סייבר. מטרת הפורום היא לשתף במידע על היבטים מקצועיים, איומים ואירועי סייבר, ולקדם שיתוף פעולה בין המגזרים השונים.⁴⁷

צו בתחום ביטחון סייבר ימי פורסם על ידי הרשות ונכנס לתוקף בפברואר 2019. הצו מיישם על המגזר הימי חלקים מהדירקטיבה של האיחוד האירופי בתחום אבטחת סייבר (Directive (EU) 2016/1148) NIS Directive.⁴⁸ הצו מכיל מספר חובות שהושתתו על גופים שהוכרזו כחינוניים. לדוגמה, במקרים מסוימים חובה לדווח על אירוע סייבר לרשות הימית ולמרכז לאבטחת סייבר של דנמרק. חובה אחרת התקפה לגופים ימיים שנקבעו על ידי הרשות הימית היא עמידה בסטנדרט בינלאומי מוכר בתחום ביטחון סייבר, וזאת תוך תקופה של שנתיים מרגע קביעתם.⁴⁹

הרשות הימית פועלת ליצירת שיתוף פעולה עם מדינות אחרות בתחום.⁵⁰ פורום ביטחון סייבר המשותף לכלל הרשויות שיש להן השפעה ישירה על המגזר הימי בדנמרק אמור לקום בשנים 2020-2021. הפורום יפעל, בין השאר, להכנת תוכניות תגובה לאירועי סייבר וחירום, תיאום תרגילי סייבר במגזר ועוד.⁵¹

Danish Maritime Authority, Danish Maritime Cybersecurity Unit: 46

<https://www.dma.dk/SikkerhedTilSoes/Cybersikkerhed/Sider/default.aspx>

Center for Cyber Security, De samfundskritiske sektorer og CFCS drøfter 47
hændelsehåndtering og varsler: <https://fe-ddis.dk/cfcs/nyheder/arkiv/2019/Pages/tredje-moede-i-vidensdelingsnetvaerket.aspx>

New maritime regulation supports prevention of cyber attacks, Danish Maritime Authority, 48
31 January 2019: <https://www.dma.dk/Presse/Nyheder/Sider/New-maritime-regulation-prevention-of-cyber-attacks.aspx>

Danish Maritime Authority, Order no. 46 of 15 January 2019, Order on the security of network 49
and information systems of importance to the safety and navigation of ships: <https://www.dma.dk/Vaekst/Rammevilkaar/Legislation/Orders/Order%20on%20the%20security%20of%20network%20and%20information%20systems%20of%20importance%20to%20the%20safety%20and%20navigation%20of%20ships.pdf>

DMA, Cyber and Information Security Strategy for the Maritime Sector, page 6-7. 50

Ibid, page 9-10. 51

ארה"ב – המרחב הימי ונמל לוס אנג'לס

מערך ביטחון הסייבר הימי של ארה"ב הוא מורכב יחסית למערכים במדינות אחרות שהודגמו. משמר החופים של ארה"ב, הגוף הפדראלי שמונה לרכז את תחום ביטחון הסייבר במגזר הימי, פרסם בשנת 2015 אסטרטגיית סייבר למרחב הימי.⁵² בארה"ב קיימת רגולציה ענפה בתחום ביטחון סייבר ימי.⁵³ קיימת חובת דיווח בתנאים מסוימים שנקבעו ברגולציה על אירועי סייבר למשמר החופים המפעיל מצידי מרכז תגובה לאומי (USCG) NRC במשרד להגנת המולדת (National Response Center National Cybersecurity and Communications) NCCIC (Integration Center) מסייע לתשתיות קריטיות כולל למגזר התחבורה הכולל את המרחב הימי.⁵⁵ במרכז פועל צוות תגובה לאירועי סייבר (HIRT) העוזר, כולל בפעילות בשטח, לגופים שהותקפו ומבקשים את התערבותו.⁵⁶ בנוסף לכך הוקמה פלטפורמת שיתוף מידע (MPS-ISAO) במגזר הימי, שהיא מלכ"ר הפועל כשותפות של המגזר הפרטי והציבורי.⁵⁷

בנמל לוס אנג'לס, המדורג ראשון בפעילות מכולות בארה"ב, פועל משנת 2014 מרכז ניהול אירועי סייבר (CSOC) האחראי לתשתיות הנמל, והוא נחשב ראשון מסוגו במדינה.

Maritime Transportation Security Act of 2002, Executive Order 13636, Presidential Policy Directive 21, the Department of Homeland Security Blueprint for a Secure Cyber Future (2011), the 2014 DHS Quadrennial Homeland Security Review, the National Infrastructure Protection Plan of 2013, and the Department of Defense Cyber Strategy of 2015 52

Maritime Transportation Security Act of 2002, 107th Congress, PUBLIC LAW 107-295— NOV. 25, 2002: <https://www.congress.gov/107/plaws/publ295/PLAW-107publ295.pdf>; Electronic Code of Federal Regulations (e-CFR) Title 33. Navigation and Navigable Waters Chapter I. Coast Guard, Department of Homeland Security, Subchapter H. Maritime Security Part 104-106. Vessels: [Shttps://www.law.cornell.edu/cfr/text/33/part-104](https://www.law.cornell.edu/cfr/text/33/part-104); <https://www.govinfo.gov/app/details/CFR-2009-title33-vol1/CFR-2009-title33-vol1-part104> 53

Title 33 Code of Federal Regulations (CFR) §101.305 – Reporting, page 341-342: <https://www.govinfo.gov/content/pkg/CFR-2015-title33-vol1/pdf/CFR-2015-title33-vol1-sec101-305.pdf>; U.S. Coast Guard, Marine Safety Information Bulletin, Cyber Adversaries Targeting Commercial Vessels, May 24, 2019 54

U.S. DHS, National Cybersecurity and Communications Integration Center: https://www.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_NCCIC%20ICS_S508C.pdf 55

Marine Safety Alert, Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels, July 8, 2019: <https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5P/INV/Alerts/0619.pdf> 56

U.S. Coast Guard, The Maritime and Port Security Information Sharing & Analysis Center: <https://homeport.uscg.mil/Lists/Content/DispForm.aspx?ID=45422&Source=/Lists/Content/DispForm.aspx?ID=45422>; MPS-ISAO site: <https://mpsisao.org> 57

רשויות הנמל פרסמו בשנת 2019 כי הנמל הוא היחיד במדינה המוסמך לסטנדרט אבטחת סייבר ISO 27001.⁵⁸ תוכנית להקמת מרכז חוסן סייבר שישירת את כלל הגורמים הקשורים לפעילות הנמל החלה בשנת 2019. המרכז צפוי, בין השאר, לשמש פלטפורמה לשיתוף במידע וידע מקצועי, תיאום שיתופי פעולה ועוד.⁵⁹

סיכום ומסקנות

קיימים מספר נדבכים מרכזיים המרכיבים מערכי ביטחון סייבר מדינתיים במגזר הימי האזרחי, כפי שהוצג במאמר. סיכום קצר של נדבכים אלו מוצג בהמשך, אך זוהי אינה רשימה הממצה את כלל האפשרויות. קיימות וריאציות שונות שניתן להתאימן לתנאים ספציפיים של המדינה. שימוש מושכל בכלים השונים והקמת מבנה איכותי של מערך ביטחון סייבר במגזר הימי יכולים לסייע בניהול מיטבי של התחום.

כפי שצוין קיימים מספר מדריכים בינלאומיים מרכזיים המציגים תובנות מקצועיות שיכולות לסייע בהקמת מערך סייבר מגזרי. המערכים שהוצגו במאמר עושים, ברוב המקרים, שימוש בכלים דומים למוצג במדריכים אלו. מדריכים פורסמו, בין השאר, מטעם מרכז סייבר של נאט"ו (NATO CCDCOE), סוכנות האיחוד האירופי לאבטחת סייבר (ENISA) ואיגוד הטלקומוניקציה הבינלאומי (ITU).⁶⁰

להלן רשימה של נדבכים מומלצים למערך סייבר במגזר הימי האזרחי של מדינה המשמשים במערכים קיימים במדינות בעולם, ומוצגים במדריכים בינלאומיים מרכזיים בתחום:

מבנה מערך: גופים וגורמים מרכזיים

1. **גוף סייבר לאומי רב-מגזרי** – מהווה בסיס מקצועי המסייע לגורם האחראי על המגזר הימי. הגוף מספק מידע מקצועי, הכוונה וייעוץ, ניהול תרגילים רב-מגזריים, פלטפורמה לשיתוף פעולה חוצה מגזרים ועוד.

58 Port of Los Angeles, Port Proposes the Creation of a Cyber Resilience Center with Stakeholders, April 25, 2019: https://www.portoflosangeles.org/references/news_042519_cybersecurity

59 Port of Los Angeles Cyber Resilience Center, Request for Proposals, July 24, 2019: <https://kentic.portoflosangeles.org/getmedia/5d304eb8-71cf-4ba5-992c-86e311b5a682/RFP-Port-of-Los-Angeles-Cyber-Resilience-Center>

60 NATO Cooperative Cyber Defence Centre of Excellence, National Cyber Security Strategy Guidelines, 2013: https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf; European Union Agency for Cybersecurity, NCSS Good Practice Guide, November 14, 2016: https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport; International Telecommunication Union (ITU), Guide to Developing a National Cybersecurity Strategy, 2018: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

2. **גוף סייבר מגזרי ימי** – פועל לרוב כחלק מגורם ממשלתי שנקבע כאחראי על המגזר הימי האזרחי. גוף זה עוסק בפעילות מול הגורמים השונים במגזר הימי. תפקידו יכול לכלול, בין השאר, הפעלת תוכניות הכשרה והעלאת מודעות, ניהול תרגילים במגזר, סיוע וייעוץ, ביצוע הערכת סיכונים ואיומים מגזרית, פרסום הנחיות ועוד. מרכז ניהול אירועי סייבר CSOC (Cyber Security Operations Center) למגזר הימי יאפשר ניהול רציף ותגובה מהירה לכלל פעילות הסייבר במגזר. המרכז יספק תמונה מלאה על המתרחש במגזר, ירכז את המידע המתקבל מהגורמים השונים, ינהל תגובות לאירועי סייבר משמעותיים ועוד.
3. **גורמי אבטחת סייבר בתשתית וגופים ימיים חיוניים ולא חיוניים** – לדוגמה, בנמלים ומתקנים ימיים יקבע אחראי אבטחת סייבר ו/או צוות סייבר במידת הצורך, דסק סייבר או מרכז ניהול אירועי סייבר האחראי על אזור או מתקן וכדומה.

תוכניות הכשרה והעלאת מודעות

תוכניות הכשרה והעלאת מודעות לקבוצות שונות דוגמת עובדים בגופי ממשל הקשורים למגזר הימי, עובדי תשתיות חיוניות ופעילים במרחב הימי שאינם נכללים בקטגוריות האחרות. התוכניות מותאמות לרוב לקבוצות השונות ומבוצעות לכל קבוצה בנפרד.

תרגילים במגזר הימי ובמסגרת רב מגזרית

1. השתתפות גוף הסייבר המגזרי ו/או גורמים חיוניים בתרגילים לאומיים חוצי מגזרים.
2. תרגילים במגזר הימי הכוללים מספר גורמים או את כלל המגזר.
3. ביצוע תרגילים במתקני תשתית וגופים ספציפיים.

תוכניות שיתוף פעולה: תיאום, תכנון, הכוונה ושיתוף במידע

1. **פורום רב-מגזרי** – השתתפות בפורום לאומי, חוצה מגזרים, לתיאום ושיתוף פעולה שיכלול את נציגי הגוף האחראי על המגזר הימי.
2. **פורום גורמי ממשל ו/או גורמים חיוניים** – פורום לתיאום ושיתוף פעולה המשלב את כלל גופי הממשל והגורמים מתשתית קריטית במגזר הימי. במקרים מסוימים מומלץ על הקמת פורום ממשלתי שיכלול רק את גורמי הממשל הקשורים לביטחון סייבר ימי.
3. **פורום לכלל בעלי העניין במגזר הימי האזרחי** – פורום לתיאום, שיתוף במידע וביכולות המשלב את כלל הגורמים במגזר הימי.

שיתוף פעולה בינלאומי

שיתוף פעולה עם מדינות אחרות, גופים פרטיים וציבוריים ומוסדות בינלאומיים בתחומים דוגמת מחקר, הכשרה, תיאום פעילות, מודיעין ועוד.

תוכנית מחקר ופיתוח

תוכנית מחקר המשלבת גופי אקדמיה, ממשל ומגזר פרטי וציבורי בתחום ביטחון סייבר במגזר הימי.

רגולציה המספקת אמצעי אכיפה, יכולות וכלים

חקיקה המספקת כלים יעילים לניהול ביטחון סייבר במרחב הימי, זאת תוך כדי יצירת איזונים ובלמים מתאימים. חקיקה יכולה לכלול בסיס משפטי להקמת גופי סייבר במערך. בנוסף לכך היא תקבע חובות דוגמת חובת דיווח על אירועי סייבר מוגדרים לגורמי ממשל בתחום. עוד מומלץ שיהיו לגורם סייבר ממשלתי סמכויות, בין השאר, לאיסוף מידע, קביעת הנחיות ו/או סטנדרטים, פיקוח ובקרה, חקירה וניהול אירועי סייבר במקרים מסוימים ועוד.

תוכניות המשכיות והתאוששות

הכנה תוכניות המשכיות והתאוששות למגזר הימי בכללותו ובאופן ספציפי לגופים ותשתיות במגזר הימי. ביצוע בדיקה והתאמת התוכניות מחדש בהתאם לשינויים ומצב מדינתי ובינלאומי וכדומה.