מחשבה לעומק – השתנות אסטרטגית מול האיום הגובר בתווך התת ימי

תובנות מרכזיות מכנס Navy Tech 2025 בהלסינקי

שרון ארליכמן [1]

כנס Navy Tech 2025, שנערך בפברואר בהלסינקי, התקיים על רקע מתיחות גוברת באזור הים הבלטי ועליית חשיבותן של תשתיות תת-ימיות קריטיות במערב אירופה – החל ממערכות חשמל, דרך כבלי תקשורת, ועד צינורות גז. אירועים כמו הפגיעה בצינורות Nord Stream, תקלות מסתוריות בכבלים תת-ימיים, והתרחבות הפעילות הימית של רוסיה וסין, הפכו את המרחב התת-ימי מממד שקט ושולי – לאתגר אסטרטגי גלוי ומורכב.

הכנס, ביוזמת Defence Leaders הבריטית, ריכז נציגים בכירים מצבאות, תעשיות ביטחוניות, מוסדות מחקר וארגונים אזרחיים. בין הנושאים המרכזיים שנידונו: ניטור רציף של תשתיות תת-ימיות, פריסת מערכות בלתי מאוישות, פיתוח אמצעי התרעה מוקדמת, וגיבוש תגובה מבצעית מתואמת בין מדינות.

במאמר זה יוצגו התובנות המרכזיות של הכותב מהשתתפותו במושבי הכנס – תובנות המצביעות על הצורך בגיבוש תפיסה ביטחונית חדשה למרחב התת-ימי.

תקריות תת-ימיות במרחבים שונים בעולם

בשנים האחרונות הפך הים הבלטי לזירת עימות רגישה ורוויית מתחים. שורת תקריות בהן נקרעו כבלים תת-ימיים באופן מסתורי גרמה לשיבושים חמורים בתקשורת ובתשתיות מידע, והגבירה את תחושת האיום בקרב מדינות האזור. פינלנד, שוודיה ואסטוניה, בין היתר, החלו להקים כוחות ייעודיים לאבטחת תשתיות תת-מימיות, ובראשן כבלי תקשורת וצינורות גז.

האיום על תשתיות ימיות התעצם גם נוכח שינויים גיאופוליטיים משמעותיים – ובראשם הצטרפותה של פינלנד לנאט"ו. שינוי זה הטיל על הצי הפיני אחריות משותפת לאבטחת תשתיות אסטרטגיות בלב הים הבלטי ולשמירה על אינטרסים של הברית כולה. התפתחויות אלו יצרו גם פתח לשיתופי פעולה טכנולוגיים וביטחוניים חדשניים, במטרה לחזק את יכולות ההגנה באזור.

בין אוקטובר 2023 לפברואר 2025 התרחשו מספר תקריות מתוקשרות של פגיעה בתשתיות תת-ימיות בים הבלטי, שכללו נזק לכבלי תקשורת ולצינורות גז. באוקטובר 2023, צינור הגז Balticconnector בין פינלנד לאסטוניה נפגע, ככל הנראה בשל גרירת עוגן של ספינה סינית (Newnew Polar Bear), ויצא מכלל פעולה למשך חודשים. בדצמבר 2024, ניזוק כבל Estlink-2 כבל חשמל תת-ימי נוסף בין פינלנד לאסטוניה, וכן דווח על נזק לארבעה כבלי תקשורת באזור, שפגעו בקישורים בין פינלנד, שוודיה, אסטוניה וליטא, המשך ישיר לאירועים כמו הפגיעה

1 שרון ארליכמן מתאם מחקרים במכון למדיניות ואסטרטגיה ימית ו-CTO במרכז הלאומי לכלכלה כחולה. שירת בחיל הים הישראלי (סא"ל במיל') ובמשרד הביטחון (מפא"ת). בעל ניסיון בהובלת תוכניות בינלאומיות מורכבות, פרויקטים, מחקר ופיתוח טכנולוגיות ימיות.

המתוקשרת בצינורות Nord Stream בשנים קודמות. התקריות עוררו חשד לפעילות חבלה מכוונת ונענו בהגברת הסיורים, ניטור ימי מתוחכם, ופריסת כוחות בינלאומיים במסגרת מבצעי נאט"ו.

גם בזירה האסיאתית, ובפרט בדרום ים סין סמוך לטיוואן, התרחשו תקריות דומות. ספינות סיניות נחשדו בפגיעה מכוונת בכבלי תקשורת תת-ימיים. תקריות אלה ממחישות את הפגיעות ההולכת וגוברת של תשתיות תת-ימיות, ואת הצורך המיידי בהיערכות טכנולוגית ומודיעינית משותפת.

מאפיינים ואתגרים בהתמודדות עם האיומים התת-ימיים

הגנה על תשתיות תת-ימיות הפכה לאתגר אסטרטגי עבור ציים ברחבי העולם. כבלי תקשורת תת-ימיים וצינורות גז נפרשים לאורך אלפי קילומטרים בקרקעית הים – אך בשל מיקומם הנסתר ותפקידם החיוני הן לביטחון הלאומי והן לתפקוד הכלכלה הגלובלית, הם מהווים יעד מועדף לגורמים עוינים.

אחד הקשיים הבולטים בזירה זו הוא זיהוי מוקדם או בזמן אמת של פעילות חשודה. כבלי תקשורת תת-ימיים רגישים מאוד להפרעות – תזוזה לא מתוכננת של עוגן, כלי שיט שאינו מזדהה, או הצבת מתקני ריגול – עלולים כולם להסב נזקים חמורים. אמנם קיימות מערכות חישה אקוסטיות ואופטיות המותקנות לאורך חלק מהכבלים, אך טווח הגילוי שלהן מוגבל. לכן, ציים ברחבי העולם משקיעים כיום בטכנולוגיות מבוססות בינה מלאכותית, המסוגלות לנתח דפוסי תנועה, לזהות אנומליות ולתרגם אותן להתראות מבצעיות – גם באזורים נרחבים ועמוקים.

גם כאשר מזוהה איום, התגובה הצבאית המבצעית לאיומים מורכבת. המרחקים העצומים, התנאים הפיזיים של עומק הים, והצורך בזיהוי ודאי של גורם עוין – כל אלו מקשים על פעולה מיידית.
אחת הגישות המתפתחות היא פריסת כלי שייט בלתי מאוישים על ותת-מימיים שיכולים לשהות בקרבת תשתיות רגישות ולספק תמונת מצב רציפה. כלים אלו מתקדמים לעבר יכולות תגובה עצמאית, אך הפעלתם עדיין דורשת תיאום עם פלטפורמות מאוישות – ספינות, מרכזי שליטה ומודיעין. עיכובים בקבלת החלטות, או חוסר תיאום, עלולים לצמצם משמעותית את היעילות המבצעית.

האתגר בזירה התת-ימית איננו רק טכנולוגי – אלא בראש ובראשונה תפיסתי. כיצד ניתן להגן על תשתיות המשתרעות על פני אלפי קילומטרים, הרחק מעין אדם, מתחת לפני הים, ובתנאים פיזיים ועוינים של חוסר ודאות מבצעית?

גם כאשר מתגלה פגיעה – אם בזיהוי רעידות חריגות בכבל, אם בנתק בהעברת נתונים או באמצעות תצפית ישירה – ייתכן שיחלפו שעות ואף ימים עד להגעה למוקד האירוע. התגובה הצבאית עצמה אינה פשוטה. המרחקים, העומקים, והצורך בזיהוי ודאי של הגורם התוקף – מעכבים את המענה.

סיכונים חדשים – רגולציה מיושנת

חסם משמעותי בהגנה על תשתיות תת-ימיות הוא הפער בין טיב האיום לבין המסגרות החוקיות הקיימות. ברוב המקרים, תקיפות אינן מוגדרות כמעשה מלחמה אלא כ- "אירועים אזרחיים" או תקלות תחזוקה – מה שמונע תגובה צבאית מיידית או אף פעולת הרתעה.

נציגי האיחוד האירופי וגופי מודיעין הדגישו את הצורך לעדכן את הרגולציה הבינלאומית – להגדיר מחדש מהי תקיפה בזירה הימית, מהם גבולות הסמכות בתוך המים הכלכליים (EEZ) וליצור בסיס חוקי לפעולה במצבים של חבלה אסימטרית מצד מדינות או שחקנים לא-מדינתיים הפועלים ב"מרחב האפור".

קיימת משמעות רחבה לעובדה שהים העמוק כבר איננו רק תווך תעבורתי – אלא זירת לחימה טכנולוגית, רב-ממדית. תנאים פיזיים כמו עומק, זרמים, מליחות וטמפרטורה משפיעים ישירות על מערכות ניווט, תצפית ותקשורת. תופעות שבעבר היו נדירות – כמו צוללות לא-מאוישות, "מתקני תחזוקה" חשודים, ותנועות חריגות סמוך לתשתיות קריטיות – הפכו לשגרתיים.

לצד ההתפתחות הטכנולוגיות כגון חיישנים חכמים, מערכות התרעה רובוטיות וכלי שיט בלתי מאוישים – עולה צורך בשינוי תפיסתי עמוק. אין מדובר באבטחת כבל או תחנה בלבד – אלא בגיבוש תפיסה כוללת של "ביטחון תשתיתי תת-ימי".

אחת הדוגמאות מהעת האחרונה שיצרו דאגה בקרב גורמים רבים היא חשיפתה של סין של מכשיר אזרחי חדש לחיתוך כבלים תת-ימיים, המסוגל לפעול בעומק של עד 4,000 מטר – כפול מהטווח המבצעי של כבלי התקשורת המערביים. המכשיר, שפותח במרכז המחקר של סין לספינות ולצוללות מאוישות, מבוסס על גלגל השחזה מצופה יהלום בקוטר 150 מ"מ, המסתובב במהירות של 1,600 סל"ד – חזק דיו לריסוק פלדה מבלי לעורר מערבולות של משקעים. גורמים מערביים מזהירים כי מדובר בטכנולוגיה בעלת פוטנציאל צבאי מובהק, שיכולה לאיים על תשתיות אסטרטגיות.

שיתוף פעולה ורגולציה אזורית

האתגרים הרבים הביאו את מדינות נאט"ו להקים מסגרות רגולטוריות חדשות, המאפשרות תגובה מתואמת ומהירה יותר, כולל מרכזי שליטה אזוריים לניהול משברים ימיים. עם זאת, ההגנה בים הפתוח מורכבת במיוחד. כלי שיט עוינים פועלים לעיתים במסווה של פעילות מסחרית לגיטימית, ומשתמשים בטכניקות התחמקות מתוחכמות.

כמענה לאתגרים אלו, החלו מדינות נאט"ו לעשות שימוש בכלים המשלבים איסוף מודיעין צבאי ואזרחי ומאפשרים בנייה של תמונת מצב מרחבית. כלים אלו מסייעים בזיהוי דפוסים חריגים גם באזורים ללא נוכחות קבועה, ועתידים לאפשר תגובה מקדימה לאיומים.

שיתופי פעולה כאלו מסייעים גם בהתמודדות עם הקושי במימון ההגנה על תשתיות ימיות. הגנה אפקטיבית על תשתיות תת-ימיות מחייבת הקצאת משאבים עצומה – אתגר תקציבי שאינו מאפשר פתרונות מקיפים. התקנת מערכות ניטור לאורכם של כלל כבלי התקשורת התת-ימיים אינה מעשית מבחינת עלויות, ולכן רבות מהמדינות נאלצות להתמקד באזורים בעלי סיכון גבוה, תוך שימוש בגישות מבצעיות ממוקדות לאזורים אלו המסייעות בפתרונות מבצעיים חלקיים.

האיחוד האירופי שוקל שילוב של טכנולוגיות חלופיות כגון מערכות תקשורת מוצפנת ולווייני לייזר, המסוגלים להבטיח רציפות תקשורת גם במקרה של פגיעה פיזית בכבלים תת-ימיים. פתרונות מסוג זה עשויים לשפר את החוסן התשתיתי – אך עדיין נמצאים בשלבי ניסוי והערכה.

נושא נוסף שעלה בכנס הדורש שיתופי פעולה מחקריים הינו התמודדות עם שינויי האקלים והשפעתם על תשתיות תת-ימיות. מעבר לאיומים אנושיים, גם שינויי האקלים משפיעים באופן

ישיר על ביטחון תת-ימי. תנודות בטמפרטורה, זרמים חזקים יותר ורמות חמצן משתנות משפיעים לרעה על חיישנים ימיים ועל יכולת התפקוד של כלי שיט תת-ימיים. המציאות הזו מחייבת התאמות מתמידות במערכות התצפית, במיוחד באזורים רגישים מבחינה גיאולוגית כמו קווי שבר או אזורים מושפעים מהתחממות אוקיינית. בהתאם, כיול שוטף ושדרוג מתמשך של אמצעים טכנולוגיים הופכים להכרח בשגרה התפעולית של הציים.

תוכנית הפעולה של נאט״ו

לטובת התמודדות עם היבטים מבצעיים שונים, בתחומי המודיעין הימי ואכיפה, נאט״ו מגבירה את נוכחותה הימית, בעיקר באזור הים הבלטי, בניסיון ליצור הרתעה ולשמר את ביטחון התשתיות הקריטיות. מספר כלי השיט הצבאיים באזור גדל, וכולל כעת פריגטות וצוללות המוקצות למשימות סיור ואבטחת נתיבים.

מטוסי סיור מתקדמים מבצעים מעקב רציף אחר פעילות חריגה של כלי שיט, תוך שימוש באמצעים אלקטרו-אופטיים לאיתור ניסיונות חבלה. כחלק מהאסטרטגיה, נאט״ו מחמירה את מדיניות האכיפה כלפי כלי שיט חשודים. ספינות סחר מחויבות לדווח על מסלולן, מטענן והרכב הצוות. ספינות שאינן משתפות פעולה, עלולות להיעצר לבדיקה או אף להיות מוחרמות במקרים קיצוניים.

כוח המשימה Baltic Sentry מגלם את המעבר מהתבססות על נוכחות פיזית לטכנולוגיות חכמות. לאורך הכבלים התת-ימיים הותקנו חיישנים אקוסטיים ואלקטרומגנטיים מתקדמים, המסוגלים להתריע בזמן אמת על פעילות חריגה כמו גרירת עוגן או חיתוך מכוון.

בנוסף, נאט״ו מתכננת פריסת צי של כלים ימיים בלתי מאוישים, NATO TASK FORCE X, המצוידים במצלמות תרמיות, חיישני תנועה ומערכות סריקה תת-קרקעית. יכולות אלו יאפשרו תגובה מיידית והעברת תמונת מצב מבצעית בזמן אמת.

מרכיב מרכזי נוסף הוא השימוש ההולך וגובר בבינה מלאכותית. על רקע כמויות המידע האדירות הנאספות, מערכות AI מנתחות תנועות ימיות, מזהות דפוסים חריגים ומצליבות נתונים לצורך איתור מוקדם של איומים במיוחד סביב אזורי תשתית קריטיים.

לצד פעולות נאט״ו, גם האיחוד האירופי מחזק את מעורבותו בזירה הימית. מדינות מובילות כגון גרמניה, שוודיה וצרפת מקדמות שיתופי פעולה מודיעיניים, תיאום סיורים ימיים והקמה של מרכזי פיקוח מתקדמים למעקב אחרי תנועת כלי שיט חשודים.

האיחוד האירופי פועל להחמרת הרגולציה. חברות ספנות מחויבות בשימוש במערכות GPS מתקדמות, דיווח שוטף על יעדים ומסלולים, ובקרה על מטענים. הדגש הוא על אזורים מועדים לסיכון כגון הים הצפוני וים סין הדרומי – בהם נרשמה בעבר פעילות עוינת במסווה אזרחי.

שלושה כוחות מרכזיים פועלים כיום כאשר כל אחד מהם מביא עמו גישה ייחודית להתמודדות עם האתגרים הגאופוליטיים והטכנולוגיים באזורי הים הבלטי והים הצפוני.

Baltic Sentry – כוח משימה ימי חדש של נאט"ו

אחת ההתפתחויות המשמעותיות ביותר בשנים האחרונות היא הקמת Baltic Sentry, כוח משימה רב-לאומי בהובלת נאט"ו. הכוח משלב יכולות מודיעין, ניטור רציף, סיורים יומיים ויישום של טכנולוגיות אוטונומיות להגנה ממוקדת על תשתיות קריטיות.

בניגוד למענה תגובתי בלבד, מטרתו העיקרית של הכוח היא הרתעה באמצעות נוכחות רציפה. מדובר ב"מסך הגנה ימי" המנסה למנוע פגיעות עוד בטרם התרחשותן. הכוח פועל בשיתוף פעולה בין מדינות החוף של הים הבלטי, ומתבסס על שילוב של AI, רובוטיקה ימית ועיבוד אותות תת-ימיים, מה שמאפשר יצירת מערכת הלומדת ומגיבה.

NNCC – Northern Naval Capability Cooperation

ה- NNCC הוא מנגנון שיתוף פעולה אזורי, ולא כוח משימה מבצעי במובנו המסורתי. במסגרתו, מדינות צפון אירופה בהן פינלנד, שוודיה, נורבגיה, דנמרק, גרמניה והולנד פועלות יחד לחיזוק היכולות הטכנולוגיות והמודיעיניות בנוגע לתשתיות תת-ימיות.

הדגש ב- NNCC הוא על שילוב מערכות וידע. שימוש ברכבים תת-ימיים לאיסוף מידע, וחיישנים סונאריים למעקב מתמשך ומערכות בינה מלאכותית לזיהוי חריגות. המודל מאפשר תיאום בין ציים אזרחיים וצבאיים ותמיכה ישירה לכוחות נאט"ו והאיחוד האירופי, בעיקר במצבי חירום או חשש לפגיעה מכוונת.

JEF – Joint Expeditionary Force

כוח ה-JEF בהובלת בריטניה, הוא כוח משימה צבאי רב-לאומי שמאגד מדינות מפתח בצפון אירופה. פינלנד, שוודיה, נורבגיה, דנמרק, הולנד, אסטוניה, לטביה וליטא שותפות בכוח המשימה. הכוח הוקם בעקבות הצורך ביכולת תגובה מיידית למשברים ביטחוניים, תוך חיזוק היציבות באזורי עימות פוטנציאליים מהים הבלטי והים הצפוני ועד לאזור הארקטי.

ה- JEF פועל לצד Baltic Sentry ו- NNCC ומהווה שכבת פעולה מבצעית הכוללת סיורים ימיים, אבטחת נתיבי תקשורת, פריסת צוללות, מטוסי סיור ורובוטים תת-ימיים מתקדמים. כל אלה נועדו לאתר, לעקוב ולנטר איומים על רשתות קריטיות ולהגיב במהירות לכל תרחיש.

תובנות מרכזיות מן הכנס - שילוב טכנולוגיות, אתגרים ושיתופי פעולה

במהלך הכנס עלו שורה של תובנות מעשיות ואסטרטגיות, המהוות בסיס לעיצוב המדיניות הימית בשנים הקרובות:

- מעבר מגישת "הגנה מרחבית" למודל של "ניטור תשתיתי".

הוצגו פיתוחים מתקדמים מטעם חברות וציים שונים המשקפים מוקדי אבטחה הנעים מהמעטפת אל מוקדי התשתית עצמם. מערכות איסוף מידע תת-מימי אוטונומיות; פריסה של חיישנים פסיביים לאורך תוואי הכבלים; שימוש בבינה מלאכותית לאיתור אנומליות בזמן אמת.

- שיתוף פעולה בין-מדינתי בהגנת תשתיות.

הגנה על תשתיות תת-ימיות אינה יכולה להישען עוד על מדינה אחת, אלא מחייבת אינטגרציה עמוקה בין מדינות, ציים, תעשיות וגופי מודיעין. כמה מהאתגרים העיקריים שנותרו פתוחים הם סוגיות של אחריות משפטית, תאום בין מדינות, ורגולציה מקשה.

- שילוב כלים בלתי מאוישים בציים.

העתיד הימי יתבסס על שילוב בין מערכות מאוישות לבלתי-מאוישות, שכן הציים לא רואים החלפה מלאה של כלים מאוישים בעתיד הקרוב. עם זאת, קיים צורך לפתח פתרונות טכנולוגיים שיתמודדו עם מגבלות מזג אוויר, עומק וטווח פעולה, על מנת שכלים אלו יהוו חיזוק משמעותי – ולא רק תוספת טקטית.

- תהליכי פיתוח מהירים וגמישים.

הלקחים ממלחמת אוקראינה חשפו את הצורך בחדשנות גמישה. דוגמת בריטניה, שהציגה כיצד ניתן לצמצם מפרטים, לשלב AI בשלבים מוקדמים, ולספק פתרונות מבצעיים בסבבי פיתוח קצרים במיוחד עם קבלת תובנות מבצעיות מהלחימה בשטח תוך שבועות ולא שנים.

- שימוש בתשתיות אזרחיות קיימות.

רעיונות כמו שימוש בתשתיות DAS (Distributed Array Sonar) אזרחיות לניטור תת-ימי קיבלו במה משמעותית. היתרונות הם זמינות גבוהה, עלויות נמוכות, ותחזוקה פשוטה. אך נדרש עדיין פתרון לסוגיות משפטיות ורגולטוריות סביב השימוש בתשתיות אזרחיות לשימושים ביטחוניים.

- השפעת שינויי האקלים על ביצועים טכנולוגיים.

מערכות הגילוי הימיות צריכות להסתגל לתנאי סביבה משתנים. עלייה בטמפרטורות, ירידה באחוזי חמצן, וזרמים לא צפויים, כל אלו מציבים אתגר ישיר לדיוק החישה והבקרה.

- פיתוח טכנולוגיות דואליות.

חברות כמו FUGRO הדגימו כיצד טכנולוגיות אזרחיות קיימות של חישה, מיפוי, ורובוטיקה, ניתנות להסבה למטרות ביטחוניות. הדגש עבר ל"נגישות מבצעית" - כיצד מאפשרים לציים להשתמש ביכולות אלו בפועל.

- AI ככלי מודיעיני ולחימתי.

דוגמה אקטואלית ניתנה לגבי אוקראינה והמחישה כיצד ניתן להיעזר ב- AI ובמודלים כדוגמת ChatGPT לזיהוי חולשות אויב, סינון נתונים מודיעיניים, ותמלול נתונים מודיעיניים בהיקף רחב בזמן אמת. מדובר בשינוי תפיסתי ולא רק טכנולוגי.

לקראת תפיסת ביטחון ימי חדשה

הכנס Navy Tech 2025 שימש לא רק זירה להצגת טכנולוגיות – אלא ציון דרך בסיעור מוחות רב לאומי בתפיסת ההפעלה הימית.

המסר המרכזי הוא - יש לעבור מתפיסת "הגנה על טריטוריה" לתפיסת "הגנה על תווך". יש צורך בגישה כוללת בה כבלים, צינורות, תחנות קצה ותשתיות תת-ימיות אינם עוד רק "נכסים שיש לאבטח", אלא חלק ממערך אסטרטגי המחייב שילוב מודיעיני, משפטי, טכנולוגי ומדינתי.

בעידן של תחרות גאו-אסטרטגית חובקת עולם, התשתית התת-ימית הופכת לקו חזית חדש. לציים ברחבי העולם צפויה תקופה של השקעות מאסיביות ביכולות זיהוי, ניטור ותגובה – תוך שיפור מערכות AI, שימוש ברובוטיקה תת-ימית, וחיזוק המנגנונים הבינלאומיים לשיתוף פעולה ולרגולציה.