קול קורא לביצוע מחקר בנושא "סייבר בעולם הימי"

המרכז לחקר מדיניות ואסטרטגיה ימית (HMS) והמרכז לסייבר משפט ומדיניות (CCLP) מזמינים חוקרים/ות ותלמידי/ות מחקר להגיש מועמדות לקבלת מלגה עבור כתיבת עבודת מחקר בנושא "סייבר בעולם ימי".

המחקר יונחה ע"י פרופ' שאול חורב (מדעי המדינה, מרכז HMS), ופרופ' טל ז'רסקי (הפקולטה למשפטים). מטרת המחקר לבצע שילוב של בחינת יכולות טכנולוגיות והתאמה לרגולציה בתחום אבטחת הסייבר במרחב הימי, וכן, לגבש המלצות בדבר ההיערכות הנדרשת להתמודדות עם האתגרים הנמצאים על הפרק.

רקע:

נמלי הים של ישראל הם "צינור החמצן" של המדינה, דרכם עוברים כ-99% מתנועת המטענים אל ישראל וממנה, והם משמשים כחוליה מרכזית בשרשרת הלוגיסטית של המסחר הבינלאומי (ע"פ נתוני רספ"ן). יעילות הנמלים תלויה ישירות באיכות התקשורת, הלוגיסטיקה ובמערכות המידע והטכנולוגיה המתפעלים נמלים אלו. כמו כן, מרבית כלי השיט המפליגים כיום בעולם מתבססים על מערכות טכנולוגיות מתקדמות שמסייעות לאוניה לשוט בבטחה בים ולהוביל כמויות גדולות יותר של נוסעים וסחורות, כגון, מערכות ניווט וגילוי, איזון וציפה, בקרת מערכות מכאניות, ועוד. חלק ממערכות אלו מתבססות טכנולוגיות IoT, דוגמת בקרים ממוחשבים וחיישנים המייצרים מידע ומקבלים הנחיות ידניות או אוטומטיות.

בשנים האחרונות ישנה מודעות רבה בעולם המחשוב הארגוני לסכנות הנגרמות מתקיפות סייבר, ובתוך כך גם מתקיפות בתחום הימי. להלן תיאור מקצת הסיכונים שיכולים להיגרם מתקיפות סייבר על נמלים ואוניות: 1. פגיעה עד השבתה של תהליכי עבודה בנמלים; 2. פגיעה בחוסן הלאומי של המדינה עד השבתת תהליכי מסחר למשכי זמן ארוכים; 3. השתלטות מרחוק על מערכות הניווט של הספינה, שיבוש הנתונים וקבלת החלטות שגויה ע"י צוות הפיקוד של כלי השיט; 4. פגיעה עד הרס מערכות מכאניות של האוניה; 5. פגיעה סביבתית – זיהום מי ים; 6. פגיעת מוניטין; ו-7. נזק כלכלי לחברות הביטוח.

בשנת 2020 יפרסם ארגון הספנות הבינלאומי (IMO) נהלים המסדירים את דרישות הגנת הסייבר הנדרשות לצורך קבלת כושר שייט. על-מנת להיערך לאסדרה זו, ולבחון את הדרכים לשפר את רמת הגנת הסייבר של כלי שייט, **מרכז חיפה לחקר מדיניות ואסטרטגיה ימית והמרכז לסייבר משפט ומדיניות** מעוניינים לבצע מחקר שיכלול את הנושאים הבאים:

1. מיפוי איומי הסייבר בסביבה הימית.
2. כלים לאיסוף מידע מובנה ולא מובנה מחיישנים שונים בפרוטוקולי תקשורת שונים הנמצאים בשימוש בכלי שייט.
3. בניית data lake שיכיל את כלל המידע שנאסף.
4. הבנה של התנהגות תקינה מהחיישן למערכת הקולטת.
5. ניתוח אנומליות באמצעות כלים קיימים ופיתוח יכולת התרעה.
6. פיתוח מתודולוגית הגנה על מערכות משולבות IT, OT ומידת השפעתו על עולם ה-IOT.
7. התאמת המחקר לנהלי ה-IMO ועבודה משותפת עם גורמי המחקר.

על הבקשה למועמדות לכלול את המסמכים הבאים: קורות חיים ומכתב המפרט את העניין בתחום הסייבר הימי

לפרטים נוספים ומועמדות יש להגיש לכתובת דוא"ל: Zmeir@univ.haifa.ac.il