הדרך להבנה טובה יותר של מודיעין הסייבר

מתיאו א׳ בונפנטי

בדומה למונחים אחרים הקשורים לתחום הסייבר, אין כל הגדרה מגובשת למונח "מודיעין סייבר" ואין בנמצא די מחקרים המתמקדים באופן בו הוא נוצר. לאור זאת, מטרתו של מאמר זה היא לצייר תמונה ברורה יותר של ענף מודיעין הסייבר הנמצא בצמיחה, וזאת באמצעות סקירה של המחקרים האנליטיים הקיימים בנושא. המאמר סוקר את הספרות המדעית הזמינה העוסקת במודיעין הסייבר, דן במושג זה ובוחן כיצד הוא מגובש באמצעות "מעגל המודיעין" (בסייבר). המאמר מסתיים בהדגשת החשיבות של פיתוח הבנה ברורה ומשותפת לבעלי העניין הרלוונטיים בתחום הביטחון, ובייחוד בתחום אבטחת הסייבר, לגבי מודיעין הסייבר.

מילות מפתח: אבטחת סייבר, מודיעין, מודיעין סייבר, תהליך מודיעין סייבר, מודלים

מבוא

במהלך העשור האחרון גובר הלחץ לאימוץ גישות ופתרונות מבוססי מודיעין לצורך טיפול באיומי סייבר. לחץ זה מגיע מצד חברים בקהילת אבטחת הסייבר הבין־לאומית (הבלתי פורמלית), המורכבת מנציגים של מוסדות וסוכנויות על־לאומיים, גופים ציבוריים מקומיים, ארגונים פרטיים והאקדמיה. גורמים אלה יזמו, בין היתר, את אימוצם של תפיסות ופתרונות אד־הוק שמטרתם לספק "מידע/מודיעין על איומי סייבר" – מוצר המספק לצרכניו הבנה (טכנית) של מבצעים ופעילויות זדוניות ברשתות התקשורת ומאפשר להם לנקוט אמצעי תגובה על בסיס

ד"ר מתיאו א׳ בונפנטי הוא חוקר בכיר במרכז ETH ללימודי ביטחון בציריך.

הבנה זו.[1] עם זאת, "מודיעין על איומי סייבר" לא הוכיח עצמו כפתרון הולם שניתן להסתייע בו למניעה מראש של איומי סייבר,[2] עקב האופי הטכני והאופרטיבי שלו ("מבט מבפנים"). ניתן לומר באופן כללי כי "מודיעין על איומי סייבר" אינו בנוי לספק, וגם אינו מספק בפועל, ידע על ההקשר הרחב יותר שבמסגרתו מתהווים איומי הסייבר.[3] למעשה, מוצרי המודיעין על איומי הסייבר אינם מאפשרים הבנה טובה יותר של סביבת האיומים וגם אינם מאפשרים חיזוי שלהם ומניעתם מראש.

נציגים שונים של קהילת אבטחת הסייבר תומכים כיום באימוץ הרעיון לפיו ארגונים צריכים לעבור מעמדה של ניהול אבטחה תגובתי לצעדים פרו־אקטיביים. אותם גורמים מתנגדים לגישה המתייחסת לאבטחת הסייבר בעיקר כ"צעדים הננקטים לאחר האירוע" ו"הגנה היקפית סטטית", ודוגלים באימוץ תפיסות, כלים ופרקטיקות ליצירת מודיעין חובק כל על איומי סייבר ושיתופו.[4] מודיעין כזה אמור לאפשר לצרכנים להבין את ההקשרים המבצעיים, הטקטיים והאסטרטגיים של האיומים (סוכנים, יכולות, מוטיבציות, מטרות, השפעה והשלכות, לא רק מנקודת מבט טכנית), לחזות את ההתפתחויות בטווח הקצר, הבינוני והארוך ולקבל החלטות מודעות לגבי צעדי המנע הנדרשים. שילובו של מודיעין זה בתהליכי קבלת ההחלטות בנושאי אבטחה אמור לאפשר לארגונים העושים זאת לנקוט עמדה של "חיזוי" או "ראיית הנולד" במקום גישה מכוונת עבר – גישה שתהיה "דינמית במקום סטטית" ו"זריזה וניתנת להתאמה מהירה במקום קשיחה ומסתגלת" לסיכונים הקשורים לסייבר.

המודיעין המתואר לעיל מכונה לעיתים קרובות "מודיעין סייבר" (CYBINT), מתוך כוונה להבדיל בינו ובין "מודיעין על איומי סייבר", שכאמור הוא בעל אופי טכני וצר. הביטוי "מודיעין סייבר" משמש באופן כללי להעברת הרעיון של ידע נרחב

---

1 שיתוף מידע על איומים, דפוסי מתקפה עדכניים, נקודות תורפה בתוכנות וכיוצא באלה עברו תהליך של תיקנון באמצעות יצירת רשת של "צוותי תגובה לאירועי אבטחת מחשב" (CSIRT). הם זכו לחיזוק באמצעות יצירתן ופיתוחן של מספר יוזמות, כגון STIX/TAXII, CyBox ו־MISPs (פלטפורמה לשיתוף מידע על נוזקות). ראו, לדוגמה: http://stixproject.github.io/supporters/.

2 Brian P. Kime, "Threat Intelligence: Planning and Direction", *SANS Institute InfoSec Reading Room*, 2017, p. 3, https://www.sans.org/reading-room/whitepapers/threatintelligence/threat-intelligence-planning-direction-36857. כפי שמודגש על ידי המחבר, "סימנים מעידים לסכנה" (IOCs), כגון חתימות של וירוסים וכתובות IP, סולמיות ("האשים") של קבצי נוזקה, כתובות URL או שמות אתרים ושרתי שליטה ובקרה אינם מהווים כשלעצמם מודיעין, אלא נחשבים למידע שימושי לצורך הגנה סטטית של הרשת.

3 Michael Montecillo, "Why Context is King", *Security Intelligence*, April 22, 2014, https://securityintelligence.com/enterprise-it-security-context-king/.

4 פירוש המונח "פרו־אקטיבי" בהקשר הנוכחי הוא היכולת לתת מענה לאיומי סייבר פוטנציאליים באמצעות חיזוק אמצעי ההגנה והתגובה.

ואיכותי יותר על אירועים אמיתיים או פוטנציאליים הנוגעים למרחב הקיברנטי ועלולים לסכן את הארגון.

בדומה למונחים אחרים הקשורים לתחום הסייבר, אין כל הגדרה מגובשת או פרשנות אמיתית משותפת בקרב קובעי מדיניות, ארגונים העוסקים בתחום, חוקרים ודעת הקהל למונח "מודיעין סייבר" כתוצר ו/או כתהליך. אם בוחנים את המדיניות או המנגנונים הרלוונטיים שיושמו לאחרונה (בייחוד ברחבי אירופה) ומסמכים אחרים שפורסמו על ידי ארגונים פרטיים או ציבוריים, וכן במסגרת האקדמיה, מתברר כי המונח "מודיעין סייבר" לא תמיד זוכה להגדרה כוללנית ומקיפה, אלא יש לו מגוון של פירושים והגדרות.[5] חרף השימוש ההולך וגובר בביטוי זה או אחר על ידי התקשורת, וכן על ידי חוקרים ואנשים העוסקים בתחום זה (במיוחד ספקים בתחום אבטחת הסייבר), החשיבה הקיימת בנושא הינה מוגבלת ואינה מפותחת דַיָה. הדבר נכון במיוחד כאשר בוחנים את העבודות האקדמיות או את המחקרים האחרים שנכתבו עד היום באותו נושא באירופה.[6] למעשה, אין כיום באירופה אף מחקר מעמיק שיתמקד בנקודת המבט התיאורטית והמעשית כאחת של נושא זה.

בניגוד לאירופה, החשיבה של המעורבים בתחומי האבטחה ואבטחת הסייבר בארצות הברית בסוגיית מודיעין הסייבר הינה מתקדמת יותר, הן במישור האקדמי והן במישור המעשי.[7] ייתכן כי הדבר נובע מאימוץ מוקדם יותר של תפיסות, פרקטיקות ופתרונות טכנולוגיים הקשורים למודיעין הסייבר על ידי ארגונים שבסיסם הוא בארצות הברית.[8] עם זאת, הדחף לאימוץ תוכניות הקשורות במודיעין

---

5 Matteo E. Bonfanti, "Another INT on the Horizon, Cyber Intelligence is the New Black", Paper Presented at the Intelligence in the Knowledge Society Conference, Bucharest, October 26-27, 2017 (אנתולוגיה של מאמרים מהכנס צפויה להופיע ב־2018).

6 נראה כי זה המקרה לפחות בחלק מן הספרות שנבחנה לצורך כתיבת מאמר זה. ראו, לדוגמה:
Mario Caligiuri, *Tra libertà e sicurezza* (Roma: Donzelli, 2016); Mario Caligiuri, "Cyber Intelligence, la Sfida dei Data Scientist", June 2016, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/cyber Intelligence-la-sfida-dei-data-scientist.html; Antonio Teti, "Cyber Intelligence e Cyber Espionage. Come Cambiano i Servizi di Intelligence nell'Era del Cyber Spazio", *Gnosis, Rivista Italiana d'Intelligence* 3 (2013):95-121; Umberto Gori and Luigi S. Germani, *Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia* (Bologna: Franco Angeli, 2012).

7 בנוסף לספרות המצוטטת להלן, ראו גם דיון שנערך על ידי בעלי עניין בתחום אבטחת הסייבר בארצות הברית ב־*Cyber Intelligence Blog* בכתובת https://cyberintelblog./wordpress.com.

8 ראו, לדוגמה: "The National Intelligence Strategy of the United States of America", *Office of the Director of National Intelligence*, 2014, https://www.dni.gov/files/documents/2014_NIS_Publication.pdf. לפי אותה אסטרטגיה, ההגדרה של מודיעין סייבר היא כדלקמן: "איסוף, עיבוד, ניתוח והפצה של מידע מכל המקורות המודיעיניים על התוכניות, הכוונות, היכולות, המחקר והפיתוח, הטקטיקה, הפעילויות המבצעיות והסימנים

הסייבר נמצא במגמת עלייה גם בקרב המעורבים בתחום אבטחת הסייבר שאינם מארצות הברית, מצב המצדיק את הרחבת הדיון בנושא. בהקשר זה, מן הראוי לבחון בפירוט רב יותר את המושג "מודיעין סייבר" ולנסות להבין את ההשלכות על סוכנויות וארגונים לאומיים שיעשו שימוש בגישות, במתודולוגיות, בכלים ובמסגרות לשיתוף פעולה שיהיו מבוססים על מודיעין סייבר.

מאמר זה מבקש לתרום תרומה ממוקדת לדיון על מודיעין הסייבר. במסגרת זו הוא מנסה לשרטט תמונה ברורה יותר של ענף מתפתח זה באמצעות סקירה של העבודה המחקרית הקיימת בנושא. המאמר סוקר את הספרות המדעית הזמינה העוסקת במודיעין הסייבר, דן במושג "מודיעין סייבר" ובוחן כיצד הוא נוצר, וזאת באמצעות הפריזמה של "מעגל המודיעין" (בסייבר). המאמר מסתיים בהדגשת החשיבות שבפיתוח הבנה ברורה ומשותפת של בעלי העניין הרלוונטיים בתחום הביטחון, ובמיוחד בתחום אבטחת הסייבר, לגבי מודיעין הסייבר.[9]

על שרמינולוגיה ומושגים (משותפים)

המונח "מודיעין סייבר" משמש בשפת היומיום בעיקר כביטוי מקיף וחובק כל. לפיכך, השאלה היא מהי ההגדרה המדויקת של מודיעין סייבר? בהיותו הן תוצר והן תהליך, יש לשאול האם מדובר במודיעין **הנובע** מהמרחב הקיברנטי, במודיעין **על** מרחב זה, במודיעין **במסגרת** המרחב או במודיעין **עבורו**, או שמדובר בשילוב של כל אלה? בנוסף לכך יש לשאול באיזו מידה מתמקד מודיעין הסייבר רק במרחב הסייבר ובאיזו מידה הוא מכסה אירועים/תופעות המתרחשים במרחב הפיזי? וכן, מהם המקורות העיקריים של מודיעין הסייבר וכיצד הוא נוצר? שאלות נוספות הן האם "מעגל המודיעין" "המסורתי" חל גם על מודיעין הסייבר ומהן הסוגיות הקשורות ביצירתו של מודיעין זה ובשיתופו? התשובות לשאלות אלו ולשאלות ספציפיות אחרות אינן מובנות מאליהן.

היעדר הסכמה כוללת סביב המונח "סייבר" מונע כל אפשרות להגיע להסכמה על מושג מקיף ואחיד של "מודיעין סייבר". בעוד שאין כמעט מחלוקת באשר למושג "מודיעין" (כתוצר וכתהליך), הגדרתו בהקשר למרחב הקיברנטי קשה יותר

המעידים של שחקנים זרים בתחום הסייבר; השפעתם הפוטנציאלית על הביטחון הלאומי, מערכות מידע, תשתיות ומאגרי נתונים; אפיוני רשת או מבט לתוך המרכיבים, המבנים, השימוש ונקודות התורפה של מערכות מידע זרות", שם, עמ' 8; ראו גם: "Resilient Military Systems and the Advanced Cyber Threat", *US Department of Defense Science Board*, January 2013, pp. 46, 49, http://www.dtic.mil/docs/citations/ADA569975; "The Department of Defense Cyber Strategy", *Department of Defense Science US Board*, April 2015, p. 24, https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

9 המאמר מבוסס על מחקר מקדים המתבצע כעת כחלק מפרויקט מחקר בן שלוש שנים שהוגדר ומנוהל על ידי המחבר.

ויוצרת אתגר לא פשוט. באופן כללי ניתן לקבוע כי החשיבה על מודיעין סייבר כוללת תפיסות, מסגרות מושגיות ומינוחים הנובעים מהמערכת המודיעינית, תוך החלתם והתאמתם למרחב הקיברנטי.[10] הדבר נראה הגיוני, במיוחד בהתחשב בעובדה שחלק מהתפיסות מבוססות מספיק, ולכן אין כל צורך "להמציא את הגלגל מחדש ". ניתן לתהות, עם זאת, על היקף תחולתן של תפיסות אלו על מרחב הסייבר, הנבדל כאמור מן המרחבים המסורתיים והמוכרים. הסייבר הוא סביבה מעשה ידי אדם, המתפתחת בקצב מהיר, מעוצבת באופן טכנולוגי וכזו שאי אפשר לחוש אותה במלואה. על רקע זה, ייתכן שיש לפרש אותה באמצעות פרדיגמות אחרות. למעשה, האינטראקציות בין סביבת הסייבר ובין המרחב הפיזי/ממשי עדיין אינן ברורות לחלוטין.

זאת ועוד, מודיעין הסייבר הינו ענף חדש יחסית, הטעון עדיין מידה רבה של בחינה, הערכה ופיתוח. אין לפי שעה מספיק ניסיון משותף היכול להגדיר את הדרך בה הוא פועל ומהן היכולות הטובות ביותר הדרושות כדי לעשות בו את השימוש האפקטיבי ביותר. גם מצב זה מקשה על כל ניסיון ליצור מודל מקיף שיפרש את המושג "מודיעין סייבר".

הניתוח והשיקולים דלעיל חשובים להבנת המושג והבעייתיות סביבו. הם גם מסייעים להבין מדוע לא קיימת עדיין הגדרה מוסכמת ומגובשת של מודיעין הסייבר. כל מי שמבקש לאמץ גישה פחות מוטה מראש או יותר ודאית לחקר מודיעין הסייבר חייב להתחשב בשיקולים אלה.

מודיעין סייבר: ידע המאפשר פעולה, המופק מהסייבר או מיועד עבורו

קיימות שתי דרכים להתבונן על מודיעין הסייבר או לפרש אותו. זאת, בהתאם להיקף הפעילות לאיסוף המידע, האמצעים בהם נעשה שימוש כדי לבצע פעילות זו והמטרה הסופית אותה היא משרתת.[11] דרך אחת היא לחשוב על מודיעין הסייבר כמודיעין המגיע מהסייבר, כלומר, ידע המופק באמצעות הניתוח של כל המידע הערכי הנאסף "במסגרת" או "באמצעות" המרחב הקיברנטי. זהו מודיעין סייבר במובן הצר של המילה. מנקודת מבט זו, המונח "סייבר" מתייחס הן למרחב ממנו מגיעים הנתונים, או במילים אחרות, אותו מאגר דיגיטלי עצום של מידע הניתן

10 Robert M. Lee, "An Introduction to Cyber Intelligence", *Tripwire*, January 16, 2014, https://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/; Stephanie Helm, "Intelligence, Cyberspace and National Security", paper given at EMC Chair Symposium.

11 Matthew M. Hurley, "For and From Cyberspace Conceptualizing, Cyber Intelligence, Surveillance and Reconnaissance", *Air & Space Power Journal* 26, no. 6 (2012): 12-33.

לשליפה או לעיבוד, והן לכלים/טכניקה/אמצעים המשמשים לאיסוף נתונים אלה (לדוגמה, באמצעות טכנולוגיות וטכניקות לניצול רשתות מחשבים).[12] בהתאם לפרשנות זו, יש ביכולתו של מודיעין הסייבר לתמוך עקרונית בקבלת החלטות בכל תחום, ולא רק בתחום ההתמודדות עם איומי סייבר. מודיעין הסייבר יכול אז לתמוך במגוון רחב של משימות במסגרת הממשלתית, התעשייתית והאקדמית, לרבות קביעת מדיניות, תכנון אסטרטגי, משא ומתן בין־לאומי, ניהול סיכונים וכן תקשורת אסטרטגית בתחומים המצויים מעבר לאבטחת סייבר.[13] במילים אחרות, מודיעין הסייבר עשוי לפעול "באופן בלתי תלוי ואינו צריך בהכרח לתמוך במשימת אבטחת הסייבר".[14] עם זאת, בהתחשב בעובדה כי מודיעין הסייבר נדון לעיתים קרובות בהקשר לאבטחת סייבר או למניעה של איומי סייבר ותגובה להם, ברור שאלו הן המטרות העיקריות (אם כי לא הבלעדיות) שלו.

דרך שנייה לפרש מודיעין סייבר היא לראות בו מודיעין המיועד "עבור" הסייבר, כלומר, תובנה הנובעת מפעילות מודיעין הכוללת את כל סוגי המקורות ומתרחשת הן במסגרת המרחב הקיברנטי והן מחוצה לו. זהו מודיעין סייבר במובן הרחב של המילה. המודיעין "עבור" סייבר יכול במצב זה גם לכלול (או להתבסס על) מודיעין "הבא מן" הסייבר. למעשה, מודיעין כזה עשוי לשאוב מידע מכל דיסציפלינה מודיעינית המספקת מידע חיוני, ללא קשר לזהות המקור, השיטה או האמצעים בהם נעשה שימוש לצורך גיבושו.

מודיעין הסייבר עשוי, אפוא, לנבוע משילוב של מודיעין ממקורות גלויים (OSINT), מודיעין אותות (SIGINT), מודיעין גיאו־מרחבי (GEOINT), מודיעין מרשתות חברתיות (SOCMINT) ומודיעין אנושי (HUMINT).[15] מנקודת מבט זו, מודיעין הסייבר הינו פחות בגדר דיסציפלינה כשלעצמה ויותר בגדר פרקטיקה אנליטית המסתמכת על מידע/מודיעין הנאסף גם באמצעות דיסציפלינות אחרות ומיועד לאספקת מידע למקבלי ההחלטות בסוגיות המתייחסות לפעילויות בתחום

---

12 Ross W. Bellaby, "Justifying Cyber-Intelligence?", *Journal of Military Ethics* 15, no. 4 (2016): 299-319; Hurley, "For and From Cyberspace", p. 13.
ניצול מערכות מחשבים או ניצול סייבר מתייחס לאיסוף ולשכפול חשאי של נתונים דיגיטליים ממחשבים או מרשתות.

13 Troy Townsend, Melissa K. Ludwick, Jay McAllister, Andrew O. Mellinger and Kate A. Sereno, "SEI Innovation Center Report: Cyber Intelligence Tradecraft Project: Summary of Key Findings", January 2013, pp. 2.01-2.20, spec. 2.5, https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_40212.pdf.

14 שם.

15 Aaron F. Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision Making* (Athens GA: University of Georgia Press, 2016), Ch. 7, pp. 103-108, 116-121.

הסייבר.[16] מה שהופך סוג זה של מודיעין ל"סייבר" הוא המטרה לשמה הוא מגובש: תמיכה בקבלת החלטות בסוגיות הקשורות למרחב הקיברנטי.

שתי נקודות המבט על מודיעין הסייבר – מודיעין "המופק" מן הסייבר ומודיעין "עבור" הסייבר – נדחסות לעיתים קרובות לתוך מושג אחד כולל. זאת, גם בשל העובדה כי מודיעין "עבור" הסייבר כולל בתוכו למעשה גם את המודיעין "המופק" מהסייבר. התוצאה היא מושג נרחב יותר של מודיעין סייבר הכולל את האיסוף, העיבוד, ההערכה, הניתוח, האינטגרציה והפרשנות של מידע הזמין "בתחומי" המרחב הקיברנטי, "באמצעותו" ו/או "מחוץ" לו, וכל זאת לשם שיפור תהליך קבלת ההחלטות בנושא האיומים הקשורים לסייבר.

ראוי לציין, כי כאשר בוחנים את הדיסציפלינות המודיעיניות "המסורתיות" הנכללות במושג "מודיעין סייבר" במובנו הרחב, רואים כי השלכותיהן על המרחב הקיברנטי הובילו להתפתחות מושגים וגישות אד־הוק, כמו אלו המכוונות לעיתים קרובות בשם HUMINT וירטואלי, OSINT וירטואלי או מבוסס אינטרנט, COMINT וירטואלי וכן הלאה. שם התואר "וירטואלי" מציין פעילויות מודיעיניות המבוצעות בתחומי המרחב הקיברנטי או באמצעות כלים הנוצרים באמצעות מחשב. החיבור בין תפיסות ופרקטיקות "וירטואליות" לתפיסות ופרקטיקות "מסורתיות" של מודיעין מתייחס לאימוץ השיטות, הגישות והכלים בהם נעשה שימוש בפרקטיקות המסורתיות, תוך התאמתן למרחב הקיברנטי.[17] SOCMINT הוא מושג שונה במעט מן המושגים שצוינו לעיל, ולדברי מספר חוקרים ואנשי מקצוע, הוא דיסציפלינה עצמאית שיש לה מאפיינים ספציפיים.[18]

מידע המיועד ליצור מודיעין סייבר עשוי לכלול נתוני רשת טכניים (לדוגמה, נתוני חומרה ותוכנה), נתונים על ארגונים עוינים ויכולותיהם, נתונים על פעילויות

16 "Operational Levels of Cyber Intelligence", *Intelligence and National Security Alliance*, September 2013, pp. 1-14, https://www.insaonline.org/operational-levels-of-cyber intelligence; "Cyber Intelligence: Setting the Landscape for an Emerging Discipline", *Intelligence and National Security Alliance*, September 2011, pp. 1-20, https://www.insaonline.org/cyber-intelligence-setting-the-landscape-for-an-emerging-discipline. לעניין הדיסציפלינות המודיעיניות הקיימות, ראו, בין היתר: "Understanding and Intelligence Support to Joint Operations", Joint Doctrine Publication 2-00, *UK Ministry of Defence*, August 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.

17 לדוגמה, גישת ה־HUMINT הווירטואלי מיועדת לאיסוף מודיעין טקטי/מבצעי מן המידע הנוצר על ידי חברים בקהילות וירטואליות.

18 David Omand, Jamie Bartlett and Carl Miller, *#Intelligence* (London: Demos Publishing, 2012); Matteo E. Bonfanti, "Social Media Intelligence a Salvaguardia dell'Interesse Nazionale. Limiti e Opportunità di una Pratica da Sviluppare", in *Intelligence e Interesse Nazionale*, eds. Umberto Gori and Luigi Martino (Rome: Aracne, 2015), pp. 231-262.

סייבר נמשכות, או כל נתון רלוונטי אחר על אירועים גיאו־פוליטיים.[19] סוג זה של נתונים, כמו גם סיווגם, אינם ייחודיים למושג "מודיעין סייבר". נתונים כאלה יכולים להגיע באופן גולמי או בצורה של מידע שכבר עבר עיבוד; הם יכולים להתקבל באופן חוקי או באמצעות פעולות חדירה/ניצול בלתי חוקיות, הן ממקורות גלויים, הן ממקורות שהם קניין של גורם כלשהו והן ממקורות מסווגים אחרים.[20]

כפי שעולה מן הספרות המקצועית, נדרשים מקורות מידע מרובים כדי לפתח הבנה הוליסטית יותר של סביבת האיום ולגבש מודיעין סייבר מקיף.[21] ההיבט החשוב ביותר של הנתונים הוא היכולת שלהם לקבל תוקף וממשות. ניתוח המידע צריך לאפשר למקבלי ההחלטות לזהות, לעקוב ולחזות יכולות, כוונות ופעילויות בתחום הסייבר המחייבות פעולה מצידם.[22] זהו למעשה המאפיין העיקרי של מודיעין הסייבר. מטרתו היא לספק לצרכנים תובנות על פעילויות עוינות פוטנציאליות העלולות להתרחש במרחב הסייבר, כאלו שעלולות להתבצע באמצעותו של מרחב זה או כאלו שעלולות להתבצע נגדו, וכן לאפשר להם לתכנן צעדי מנע (פרו־אקטיביים) או אמצעי נגד (תגובתיים).

מודיעין סייבר עשוי להיות אסטרטגי, טקטי או אופרטיבי, בהתאם להיקפו או למידת היכולת לפעול על פיו.[23] לא קיימת הסכמה באשר לרמות השונות של מודיעין הסייבר. על פי הספרות הקיימת, מודיעין הסייבר עוסק בטווח הארוך, סוקר מגמות ואיומים מתפתחים ובוחן הזדמנויות להכלתם. הוא משמש לקבלת החלטות בדרגים הגבוהים ביותר, שמטרתן היא מימוש משימותיו של הארגון וקביעת כיוונו ויעדיו. מודיעין סייבר אסטרטגי מכסה את אופק האיומים ברמת המאקרו (איומים פוליטיים, חברתיים וכלכליים) המשפיעים על הארגון ומזהה את הגורמים המאיימים, מטרותיהם והאופן בו הם עלולים לנסות להשיגן. מודיעין הסייבר האסטרטגי עשיר במידע הֶקשֶרי.[24]

---

19 Jung-ho Eom, "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace", *International Journal of Software Engineering and Its Applications* 8, no. 9 (2014): 137-146. המאמר עוסק במודיעין סייבר למטרות צבאיות.

20 Robert M. Lee, "Cyber Intelligence Collection Operations", February 25, 2014, https://www.tripwire.com/state-of-security/security-data-protection/cyber-intelligence-collection-operations/.

21 "Cyber Intelligence: Setting the Landscape for an Emerging Discipline", p. 1.

22 Townsend et al., "SEI Innovation Center Report".

23 ראו לדוגמה: Randy Borum, "Getting 'Left of the Hack': Honing Your Cyber Intelligence Can Thwart Intruders", *InfoSecurity Professional*, September/October 2014, https://works.bepress.com/randy_borum/63/.

24 Randy Borum, John Felker, Sean Kern, Kristen Dennesen and Tonya Feyes, "Strategic Cyber Intelligence", *Information & Computer Security* 23, no. 3 (2015): 317-332; "Strategic Cyber Intelligence", *Intelligence and National Security Alliance*, March 2014, pp. 1-16, https://www.insaonline.org/strategic-cyber-intelligence/.

מודיעין סייבר טקטי עוסק במה שמתרחש ברשת. בנוסף לכך הוא בוחן את החוזקות ואת נקודות התורפה של הארגון, וכן את הטקטיקה, הטכניקות והנהלים המשמשים את הגורמים המאיימים עליו.[25] עקב אופיו והטווח שלו, קיימת ככלל הלימה בין מודיעין סייבר טקטי למודיעין העוסק באיומי סייבר.[26] מודיעין הסייבר הטקטי, בהיותו בדרך כלל בעל אופי טכני יותר, משמש מקור מידע לצעדים ולפעולות מבוססי רשת אותם יכול הארגון לנקוט לצורך הגנה על נכסיו, שמירה על רציפות פעילותו וחידושה.

מודיעין סייבר אופרטיבי מורכב מידע על איומים מיידיים או ישירים על הארגון. מודיעין זה מאפשר את הפעילויות והתפוקות היומיומיות ותומך אותן. ברמה זו, מודיעין הסייבר בוחן את התהליכים הפנימיים בארגון ואת נקודות התורפה שלו.[27]

ראוי לחזור ולציין כי האבחנה המתוארת בין הרמות השונות של מודיעין הסייבר הינה לצורך אקדמי בעיקרו. בפועל, לא קיימת הבחנה ברורה בין רמה אחת של מודיעין סייבר לרמה האחרת, ולעיתים קרובות הן חופפות או אף משולבות ביניהן. יתרה מזאת, קרוב לוודאי כי משמעות המושגים "אסטרטגי", "טקטי" ו"אופרטיבי" תשתנה בין ארגון לארגון עקב גודלם, מורכבותם, משימתם ומאפייניהם.[28] כך או כך, חשוב שלארגון תהיה יכולת להביא בחשבון את הרמות השונות של מודיעין הסייבר ולעצב את המודיעין בדרך שתאפשר לו להבין את האתגרים וההזדמנויות בהם הוא עשוי להיתקל בסבירות גבוהה בטווחים הקצר, הבינוני והארוך. בכל מקרה, נראה כי אין בנמצא מתכון קבוע להצגת המוצר הסופי של מודיעין הסייבר בפני מקבלי ההחלטות.

תהליך יצירתו של מודיעין הסייבר: מודלים חלופיים מול מודלים מסורתיים

כמו במקרה של דיסציפלינות ומוצרים מודיעיניים אחרים, מודיעין הסייבר נוצר באמצעות מערך של פעילויות/פונקציות, המוצא את ביטויו ומוסבר באופן מסורתי באמצעות המודל של "מעגל המודיעין".[29] מודל זה נלמד, נבחן והועמד בספק מספר

25 "Tactical Cyber Intelligence", *Intelligence and National Strategic Alliance*, December 2015, pp. 1-16, https://www.insaonline.org/strategic-cyber-intelligence/.

26 שם.

27 "Operational Levels of Cyber Intelligence", *Intelligence and National Security Alliance*, September 2015, pp. 1-16, https://www.insaonline.org/strategic-cyber-intelligence/.

28 "Strategic Cyber Intelligence", p. 4.

29 "מעגל המודיעין" מופיע בכמה צורות. הנפוצות שביניהן מורכבות מחמש פעולות נפרדות: תכנון והכוונה, איסוף, עיבוד, ניתוח והפצה. חלק מפעולות אלו עשויות לכלול פעולות משנה, ובכך ליצור מעגל המורכב מתכנון והכוונה, איסוף, בחינה והשוואה, הערכה, ניתוח, אינטגרציה, פרשנות והפצה. לגבי "מעגל המודיעין" ראו: Mark Phythian, ed. *Understanding*

פעמים על ידי אנשי מקצוע ואנשי אקדמיה, עד שהוצעו לו מודלים חלופיים.[30] אותם ספקות לגבי התקפות והתחולה של "מעגל המודיעין" המסורתי קיימים גם בהקשר של מודיעין הסייבר. כפי שציין אחד המומחים הבולטים, "ככל שהמודיעין הופך ליותר דיגיטלי ו'סייברי' (בנושאי הטיפול, בשיטותיו ובצורותיו), הבנה כי 'מעגל המודיעין' הוא למעשה אמצעי למידה ולא חלק מתהליך הבנייה של המודיעין, עשויה לאפשר לעוסקים בנושא לחשוב על המודיעין בדרכים חדשניות יותר".[31] חוקרים ומומחים אחרים שותפים גם הם להשקפה זו. הם מדגישים כי מודל "מעגל המודיעין" חל רק בצורה מוגבלת על מודיעין הנוצר "מסייבר" ו"עבור הסייבר" ומצביעים על חוסר יכולתו של המודל לייצג ולהסביר את הליך יצירתו של מודיעין הסייבר. המודל המסורתי, שנועד לשמש כמעגל לינארי החוזר ונשנה, אינו מדגיש את ההדדיות של הפעולות מהן מורכב תהליך יצירתו של מודיעין הסייבר (תכנון, איסוף, עיבוד וכן הלאה) ואת הרלוונטיות שלהן האחת לשנייה. במילים אחרות, מודל "מעגל המודיעין" מתעלם מהתלות ההדדית ומההשפעות ההדדיות הקיימות בין פעולות אלו.

המבקרים המצוטטים לעיל מסתמכים למעשה על טיעונים המשמשים נגד "מעגל המודיעין" באופן כללי, ללא קשר לדיסציפלינה מודיעינית ספציפית.[32] על רקע זה, מתעוררת השאלה האם יש צורך במודל פרשני נפרד שיסביר את תהליך מודיעין הסייבר, ובמילים אחרות, האם תהליך מודיעין הסייבר הינו כה שונה מהתהליכים הנכללים בדיסציפלינות מודיעיניות אחרות, עד כדי כך שהוא דורש מודל חלופי שיתאר אותו. מתן תשובות משמעותיות לשאלות אלו מחייב הבנה ברורה, מקיפה ומעמיקה של מודיעין הסייבר כתפיסה, ומעל הכל כפרקטיקה בפני עצמה. אלא שקשה להגיע להבנה כזאת נוכח היעדר דיון וניסיון מספיקים בנושא מודיעין הסייבר. לפיכך, קביעת מודל ייחודי למודיעין הסייבר מהווה בשלב הנוכחי בעיקר סוג של תרגיל או ניסוי אינטלקטואלי, שתוצאותיו מחייבות עדיין תיקוף.

---

the Intelligence Cycle (London and New York: Routledge, 2013); Philip H. J. Davies, Kristian Gustafson and Ian Ridgen, "The Intelligence Cycle is Dead, Long Live the Intelligence Cycle", ibid., p. 56.

30 החסרונות של "מעגל המודיעין" המסורתי כמייצג את תהליך המודיעין נדונים בשורה של מאמרים בספר *Understanding the Intelligence Cycle*. ראוי לציין כי המודלים אינם מדויקים, משום שהם מנסים לפשט מציאות מורכבת. בנוסף לכך, מודלים אינם תהליכים אלא ביטויים מצומצמים שלהם. לפיכך, אין טעם לצפות מהמודל של "מעגל המודיעין", או מכל מודל פוטנציאלי אחר, לייצג את תהליך המודיעין באופן הוליסטי, חובק כל ומפורט לחלוטין. מודלים כאלה יהיו מסובכים וערכם המעשי יהיה נמוך.

31 Michael Warner, "The Past and Future of the Intelligence Cycle", in *Understanding the Intelligence Cycle*, p. 19.

32 *Understanding the Intelligence Cycle.*

אף על פי כן, נראה כי יש מספר טיעונים המצדיקים הגדרה של מודל אד־הוק שיסביר את תהליך גיבושו של מודיעין הסייבר.

המאפיין העיקרי של מודיעין הסייבר טמון בעובדה כי הוא "ממורכז סייבר", כלומר, עוסק בידע על סוגיות הקשורות לסייבר. מודיעין סייבר כרוך בניתוח של מידע הנאסף מן המרחב הקיברנטי, וכן ממקורות אחרים, לצורך השגת מטרות הקשורות לסייבר. ברמה הבסיסית ביותר, המושג "סייבר" מתייחס לתחום שהוא מעשה ידי אדם, תחום המתפתח במהירות, מעוצב באופן טכנולוגי ולא לגמרי מוחשי.[33] זהו תחום בו המידע נוצר, מעובד, מופץ, משותף, נשמר, עובר שינוי, נצרך ומושמד על ידי מספר רב של שחקנים ובקצב מהיר.[34] קשה לחזות את ההשלכות של קבלת החלטות מוכוונות מטרה על סוגיות הקשורות לסייבר ועל התחומים הווירטואלי והפיזי כאחד. מצב זה משפיע על אופן היצירה של מודיעין הסייבר וצריכתו ומאתגר את פונקציות הליבה של התהליך המודיעיני, קרי האיסוף, ההערכה, הניתוח, האינטגרציה, פירוש המידע והפצת המודיעין.

כאשר מדובר באיסוף ובהערכה, מודיעין הסייבר מסתמך גם על מידע המגיע ממקורות בלתי מבוקרים, דוגמת האינטרנט.[35] מידע זה דורש סינון, הערכה ותיקוף (במידה מסוימת). חשיבות מכרעת יש לסינון המידע, כדי שניתן יהיה לבחור מתוך המרחב הקיברנטי את פריטי המידע המשמעותיים בלבד. גם ההערכה היא משימה מאתגרת, וזאת עקב ההפכפכות הרבה, האנונימיות וחוסר הוודאות של הנתונים הזמינים במרחב הקיברנטי וההטרוגניות של מקורות המידע. מכאן, שכדי לתקף נתונים, יש חשיבות רבה לאימות המידע המופק ממקור אחד אל מול מידע המופק ממקורות אחרים, ועדיף שלפחות אחד ממקורות אלה יהיה מבוקר.

סינון, הערכה ותיקוף מיועדים למתן את מה שמכונה בשם "אנרכיית המידע", הנוצרת מן השילוב בין הנפח הגדל של הנתונים הזמינים ובין היעדר הבקרה עליהם. העובדה שתהליך היצירה של מודיעין הסייבר עשוי להתבסס גם על מידע/מודיעין המופק באמצעות דיסציפלינות אחרות, גורמת לכך שהשילוב בין כל החלקים

---

33 תחום זה הינו גם מרכיב וגם תוצר של המהפכה הדיגיטלית. ראו: Luciano Floridi, *Information: A Very Short Introduction* (Oxford: Oxford University Press, 2010); Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford: Oxford University Press, 2016).

34 Warner, "Past and Future of the Intelligence Cycle", p. 16.

35 ניתן להגדיר איסוף כניצול מקורות ואספקת מידע המופק מהם לצורך עיבודו וניתוחו. מקור יכול להיות אדם, אובייקט, תהליך או מערכת מהם ניתן להשיג מידע. מקורות הינם בלתי מבוקרים כאשר הם אינם נמצאים תחת פיקוח והכוונה רשמיים של ארגון. דוגמה לכך הוא מידע הנוצר על ידי משתמשי אינטרנט או שחקנים אחרים במרחב הקיברנטי. הערכה ניתנת להגדרה כשלב בפונקציית הניתוח בו מתבצעת הערכה של המידע במה שנוגע לאמינות המקור ולמהימנות המידע. ראו, לדוגמה: "Understanding and Intelligence Support to Joint Operations", Joint Doctrine Publication 2-00, pp. 3-14, 3-20.

הרלוונטיים של הידע והפיכתו למוצר עקבי אחד יוצרת תופעה מאתגרת. זאת, עקב השוני בצורה, באופי ובמידת אי־הוודאות של המידע והמודיעין המתקבלים מהמרחב הקיברנטי (לדוגמה, מידע או נתונים טכניים אחרים המגיעים מרשתות חברתיות, פורומים ברשת וכן הלאה) בהשוואה למקורות "בלתי וירטואליים" אחרים.[36] מידת אי־הוודאות משפיעה גם על הפרשנות הניתנת למידע המעובד, כלומר, על הסקת המסקנות המבוססת עליו, הנכללות בדרך כלל במסגרת המוצר הסופי של מודיעין הסייבר. אי־ודאות זו צריכה להיות מובהרת גם לצרכן של מודיעין הסייבר, שחייב להיות מודע למגבלותיו העיקריות, ובעיקר בכל מה שנוגע לרמת הדיוק שלו.

היבט רלוונטי נוסף אותו יש להביא בחשבון בעת הגדרת מודל פרשני עבור תהליך מודיעין הסייבר הוא לוח הזמנים הצפוף הנדרש לעיתים תכופות לשם ביצוע משימות מודיעיניות. הדבר מחייב שהפעולות המודיעיניות יתבצעו בו־זמנית, או לחילופין שיימצאו קיצורי דרך כדי להוציאן אל הפועל. במילים אחרות, הפעולות הכרוכות במודיעין הסייבר אינן נעשות בצורה מעגלית, אלא מהוות "רשת רב־ערוצית" שלהן עצמן.[37]

נראה כי התנאים ליצירת מודיעין הסייבר שנדונו לעיל והאתגרים הכרוכים בהם מזרזים את הצורך בהגדרה של מודל ספציפי שיתן ביטוי טוב יותר לייחודיות של תהליך זה. צוות של מומחים ואנשי אקדמיה מן המכון לתוכנה ולהנדסה (SEI) של אוניברסיטת "קרנגי־מלון" בחן לפני מספר שנים את הספרות הקיימת בנושא זה והציע מודל המבוסס עליה.[38] המודל של SEI נבדל מ"מעגל המודיעין" המסורתי במינוח בו הוא עושה שימוש, בלוגיקה הבלתי לינארית והתוצאתית של הפעולות מהן מורכב התהליך, בחלוקה של פעולת הניתוח לשתי התמחויות נפרדות (ניתוח טכני או פונקציונלי וניתוח אסטרטגי) וביכולת של מודיעין הסייבר לתת מענה הן למטרות הטכניות "הצרות" של אבטחת הסייבר והן למטרות "הרחבות יותר" של מניעת איומי סייבר. המודל החדש מפרש את מודיעין הסייבר כתהליך אנליטי המסתמך על מידע/מודיעין הנאסף גם באמצעות דיסציפלינות אחרות ומיועד לספק מידע למקבלי ההחלטות בסוגיות המתייחסות לפעילויות בתחום הסייבר.[39]

המודל של SEI מורכב מחמש פונקציות: (1) הגדרת "הסביבה" שעל פיה נקבע היקף המאמץ להשגת מודיעין הסייבר, והמשפיעה גם על טיב המידע הנדרש

---

36 ניתן להגדיר אינטגרציה כפונקציה במסגרת התהליך המודיעיני, שבה המידע ו/או המודיעין המנותחים מנופים ומשולבים בתוך תבניות בתהליך יצירתו של מודיעין נוסף, שם, עמ' 3–22.

37 ראו, לדוגמה: Davies, Gustafson and Ridgen, "The Intelligence Cycle is Dead, Long Live the Intelligence Cycle" p. 64 ff.

38 Townsend et. al., "SEI Innovation Center Report".

39 שם.

כדי להשיגו;[40] (2) "איסוף הנתונים", או חקר המקורות ואיסוף וסינון של מידע באמצעות שימוש בכלים אוטומטיים ועתירי עבודה;[41] (3) "ניתוח פונקציונלי", כלומר ביצוע ניתוח טכני המותאם למשימה (לרוב, לצורך תמיכה במשימת אבטחת סייבר), שמטרתו היא להפיק את ה"מה" וה"איך" של איומי הסייבר;[42] (4) "ניתוח אסטרטגי", הכרוך בסקירה של מודיעין הסייבר הפונקציונלי, בשילובו עם מידע בעל הקשרים דומים ובהבהרה נוספת שלו, וזאת במטרה לענות על השאלות "מי" ו"מדוע";[43] (5) "דיווח ומשוב", כלומר הפצת מודיעין הסייבר למקבלי ההחלטות וקבלת משוב מהם.[44]

להלן פירוט של התחומים העיקריים שבהם קיימות תלות הדדית והשפעות הדדיות בין הפעולות השונות הכרוכות ביצירת מודיעין הסייבר: איסוף הנתונים מתבצע בהתאם להגדרת הסביבה, וזו מצידה מושפעת מן ההחלטות המתקבלות על ידי הארגון על בסיס מודיעין הסייבר שנצרך על ידו. המודיעין המתקבל מן הניתוח הפונקציונלי יכול לשמש כבסיס לקבלת החלטות בדבר פעולות שיינקטו ברמה הטכנית של רשת הארגון, שמצידן ישפיעו על הגדרתה של הסביבה הפנימית. אותו כלל חל גם על מודיעין המתקבל מן הפונקציה האסטרטגית, המשפיע על הסביבה הפנימית והחיצונית כאחת. הפונקציה האסטרטגית הופכת את המודיעין

40 שם, עמ' 2.9. המונח "סביבה" מתייחס לסביבה פנימית וחיצונית כאחת. הגדרת הסביבה הפנימית כוללת את חקר הנוכחות של הארגון בעולם הסייבר, את התשתית הנגישה באמצעות האינטרנט ואת הגדרת הנתונים אותם יש לאסוף כדי לשמור על ערנות באשר למתרחש ברשת. לצורך הגדרת הסביבה החיצונית יש לדעת אילו גופים הינם בעלי יכולת להשפיע על הרשתות של הארגון. הארגון חייב לגלות ולמפות את נקודות התורפה של המערכת, את כיווני החדירה או המתקפה עליה ואת הטקטיקה, הטכניקות, הנהלים והכלים המשמשים את הגורמים הרלוונטיים המאיימים עליה. כפי שנטען על ידי טאונסנד ואחרים, "השקעת הזמן והאנרגיה להגדרת הסביבה אפשרה לארגונים לשפר במידה משמעותית את פעולת איסוף הנתונים שלהם, וכתוצאה מכך להפוך את תוכניות מודיעין הסייבר ליעילות ולאפקטיביות יותר".

41 שם, עמ' 2.11. על איסוף המידע לכלול הן מקורות פנימיים (זרימת מידע ברשת, יומני תנועות, נתונים דמוגרפיים על המשתמשים) והן מקורות חיצוניים (ספקי מודיעין מצד שלישי, מידע ממקורות גלויים, רשתות חברתיות). על האיסוף להתמקד בסיכונים הרלוונטיים ובצרכים האסטרטגיים אשר זוהו במהלך לימוד הסביבה בה פועל הארגון. איסוף נתונים אפקטיבי צריך להתבסס על הגדרה של הסביבה. עליו להיות מכוון לנתונים הדרושים לצורך ביצוע ניתוח משמעותי של איומי סייבר קריטיים.

42 שם, עמ' 2.13. פונקציה זו כוללת אימות/תיקוף של נתונים על בסיס איכות המקור, היסטוריית הדיווח שלו ואימות בלתי תלוי באמצעות מקורות מאמתים אחרים.

43 שם, עמ' 2.15. ניתוח אסטרטגי מוסיף פרספקטיבה, הֶקשר ועומק לניתוח הפונקציונלי. הוא נטוע בסופו של דבר בנתונים טכניים, אך כולל גם מידע המגיע מחוץ למקורות הטכניים המסורתיים. הניתוח האסטרטגי מתאר פרופילים של גורמים מאיימים, יוצר את הערנות הנדרשת באשר למתרחש ברשת ומספק למקבלי ההחלטות מידע על ההשלכות האסטרטגיות של איומי הסייבר על ארגונים, תעשיות, כלכלות ומדינות.

44 שם, עמ' 2.17.

המתקבל מן הניתוח הפונקציונלי לשימושי יותר עבור מקבלי החלטות בכירים, שייתכן שהם נעדרים רקע טכני. מנקודת מבט זו, מדובר בסוג של יישום נוסף התורם לגישור על פערי התקשורת בין החוקרים בארגון ובין מקבלי ההחלטות בו. האחרונים מספקים משוב על המודיעין שהתקבל, ומשוב זה מסייע לעצב את הפעילות המחקרית של הארגון ולהסדיר ולכוון את דרכו. בכך משפיעים הבכירים בארגון על הסביבה.

מאמר זה לא מטפל בשאלת "תקפותו" של המודל של SEI. המודל גובש והוצג בעקבות עבודה אמפירית למיפוי והערכה של פרקטיקות קיימות בתחום מודיעין הסייבר בארצות הברית. הוא מבוסס על נתונים ומהווה את "המילה האחרונה" אצל ארגונים נבחרים שבסיסם הוא בארצות הברית. המודל הוא גם בעל השפעה נורמטיבית, כלומר, הוא מתאר כיצד תהליך גיבושו של מודיעין הסייבר אמור לפעול כדי שיהיה אפקטיבי. יתרה מזאת, יתרונו הוא בהיותו פשוט יחסית, ובה בעת מייצג את הפרקטיקות שאומצו על ידי ארגונים מסוגים שונים, כגון תאגידים קטנים, תעשיות גדולות יותר וסוכנויות ממשלתיות. יחד עם זאת, מידת הייצוג של מודל SEI צפויה להתפוגג ברמה הנמוכה ביותר וברמה הגבוהה ביותר של תהליך מודיעין הסייבר, כלומר ברמת הפרט מצד אחד וברמת השותפים המרובים, או הרמה העל־לאומית, מצד שני. סביר להניח כי המורכבות הארגונית/המוסדית ברמה העל־לאומית ומרובת השותפים הופכת את המודל המודיעיני של SEI לבלתי מתאים לרמה ארגונית זו. בנוסף לכך, יש להניח כי פיתוחים טכנולוגיים חדשים בתחום הסייבר ישפיעו על מודל זה ויחייבו הכנסת שיפורים שוטפים נוספים בו.[45] לפי המודל של SEI, האיסוף והניתוח הם תהליכים המתבצעים באופן עוקב, כלומר, שלב הניתוח יכול להתחיל רק לאחר השלמתו של שלב האיסוף. אלא שבפועל, קיימת אינטראקציה בין שתי הפונקציות והן יכולות להתרחש בו־זמנית. חרף האמור, יש להכיר בעובדה שהמודל המוצע על ידי המכון לתוכנה ולהנדסה הינו ניסיון מבוסס ראשוני להסביר בצורה טובה יותר את תהליך היווצרותו של מודיעין הסייבר ואת הדרכים העדיפות לגיבושו.[46]

מסקנות

יש חשיבות רבה להבנת התהליך של מודיעין הסייבר. הבנה כזאת יכולה לסייע לבעלי עניין לשמור על עקביות בכל הנוגע לקידום תוכניות או לנקיטת פעולות

45 מקדמיו של המודל מכירים בצורך זה במיוחד כשמדובר ביכולות האנליטיות: "מכיוון שהטכנולוגיה משתנה בקצב כה מהיר, הליך הפקתו של ניתוח מודיעין הסייבר צריך להיות דינמי דיו כך שיוכל להסתגל לכלים חדשים, ליכולות ולתחכום של היריבים המתפתחים במהירות".

46 דיון מעמיק יותר בתהליך מודיעין הסייבר ובגיבושו של מודל חלופי יתקיים במסגרת פרויקט המחקר.

הקשורות למודיעין הסייבר, וזאת ברמת המדיניות, ברמה המשפטית, במישור המבצעי ובתחומים נוספים. כדי להבין את תהליך מודיעין הסייבר יש להתבסס תחילה על הגדרה ברורה של המושג "מודיעין סייבר". המסגרת המושגית תשמש כשלד ליצירת הבחנות מושגיות, לארגון רעיונות ולקישור ביניהם, דבר שיאפשר הבנה מקיפה וכוללת של מודיעין הסייבר. אימוצה של מסגרת כזאת גם יהווה מרכיב חשוב בהפיכתו של מודיעין הסייבר לדיסציפלינה, כלומר, לתחום לימוד או פעילות מודיעיניים ספציפיים.

מרבית הספרות המקצועית מתייחסת כבר היום אל מודיעין הסייבר כאל דיסציפלינה מבוססת, או כזו שתתבסס בקרוב, אך נראה כי הדבר אינו כך. הבוסריות של הניתוח התיאורטי של מודיעין הסייבר, לצד הניסיון המוגבל יחסית בתחום זה, מקשים על ראייתו כתחום או כענף מודיעיני מוכר. במילים אחרות, אין לראות בשלב זה במודיעין הסייבר דיסציפלינה, משום שהוא עדיין אינו מוגדר דיו מבחינה תיאורטית ולא נוסה מספיק באופן מעשי. יתר על כן, אופיו של מודיעין הסייבר ותהליך יצירתו, כפי שתוארו לעיל, הופכים אותו לפרקטיקה אנליטית יותר מאשר לדיסציפלינה – פרקטיקה המסתמכת על מידע/מודיעין הנאסף גם באמצעות דיסציפלינות אחרות. יחד עם זאת, אין דבר שצריך למנוע ממודיעין הסייבר מלהפוך לדיסציפלינה, שתהליך גיבושה יעשה שימוש במשאבים טכניים או אנושיים ספציפיים לה.

תנאי מוקדם ליצירת מנגנוני שיתוף פעולה בתחום מודיעין הסייבר הוא הבנה משותפת של בעלי העניין לגביו. מדובר בהיבט חשוב, שכן תהליך יצירתו של מודיעין הסייבר דורש שיתוף פעולה הדדי ושיתוף ידע. כדי ששיתוף פעולה כזה יהיה אפקטיבי ומלא, עליו להתבסס לפחות על שפה משותפת ועל הבנת המושגים והמרכיבים של מודיעין הסייבר ושל תהליך גיבושו.

מאמר זה תורם להגדרת המושג "מודיעין סייבר" הן במובנו הצר והן במובנו הרחב (על בסיס הידע שכבר קיים בנושא), לזיהוי והבנייה של רכיבים מושגיים שלו ולפירושם באמצעות מסגרת תיאורטית בסיסית (וראשונית) ביותר. אין ספק כי יש להרחיב מסגרת תיאורטית זאת כדי שתכיל היבטים שונים נוספים של מודיעין הסייבר ותאפשר לפרקטיקה צומחת זו להתבסס ולהמשיך להתפתח.