פיתוח וסיווג "רשתות" סייבר מודיעיניות – הזדמנויות לקהילת המודיעין

על בסיס מאמרם של ג'ורי פסקל קלקמן ולוטה ויסקאמפ[1]

שירה כהן[2]

הקדמה

המאמר "Cyber Intelligence Networks: A Typology" פורסם באפריל 2019 בכתב העת The International Journal of Intelligence, Security and Public Affairs ונכתב על ידי Jori Pascal Kalkman ו-Lotte Wieskamp. המאמר ממפה ארבעה סוגים שונים של רשתות (Networks) סייבר מודיעיניות ועומד על מאפייניהן הייחודים. במילים אחרות, **רשתות סייבר מודיעיניות משמעותן סוג של קהילות העוסקות במודיעין-סייבר ואבטחת מידע**. לטענת כותבי המאמר, סוג הרשת משפיע על האתגרים והתוצאות של שיתופי הפעולה המודיעיניים בתחום הסייבר.

בעוד שמחקרים רבים דנים בשיתופי פעולה מודיעיניים בתחום הסייבר במונחים כללים או מנתחים מקרים בודדים, כותבי המאמר מבקשים לספק תובנה על המגוון הקיים של רשתות סייבר מודיעיניות. על סמך מחקר איכותני של רשתות מודיעין-סייבר בהולנד, זיהו חוקרי המאמר ארבעה סוגים שונים של רשתות: **רשתות מרכזיות** (Centralized networks); **רשתות עסקיות** (Business networks); **רשתות מבצעיות** (Operational networks); **ורשתות מקומיות** (Local networks). רשתות אלה נבדלות זו מזו במקור היוזמה שלהן, בפעילותן, במבנה שלהן, בתדירות התקשורת, בקונצנזוס הרשתי בנוגע ליעדיהן, במחויבות המשתמשים ובתוצאות המתקבלות מעצם קיום הרשת. בהתאם לתוצאות המחקר, כותבי המאמר מבקשים להרחיב את מעורבות המגזר הפרטי ברשתות מודיעין-סייבר אלה, וכן תומכים בעידוד יוזמות בגישת Bottom-Up בתחום המודיעין-סייבר, שיעודדו את שיתופי הפעולה בתחום.

מהו מודיעין בהקשרי אבטחת סייבר?

בעזרת הגדרת המונח 'מודיעין', ניתן לבחון מהו המודיעין בהקשרי אבטחת סייבר. אנו נתייחס להגדרת המונח 'מודיעין' הבאה: "תהליך של איסוף וניתוח מידע במטרה לספק התרעה ולסייע למקבלי ההחלטות בעיצוב המדיניות על מנת להגן או לשפר את היתרון היחסי"[3]. בהתאם להגדרה זו, בהקשרי סייבר ניתן להתייחס למונח 'מודיעין' כצורך בהבנה וניתוח יכולות, כוונות ופעילויות של יריבים ומתחרים פוטנציאליים, ככל שהם מתפתחים, כדי לצפות ולהגן מפני איומי סייבר. באמצעות מודיעין סייבר, גופים ציבוריים ופרטיים יכולים לחזק את אבטחת הסייבר שלהם ולהגן על פרטיות דיגיטלית, רכוש ותשתיות קריטיות.

---

[1] ג'ורי פסקל הינו דוקטורנט ב-Netherland Defense Academy שחוקר שיתופי פעולה בין ארגונים צבאיים לארגונים אזרחיים. לוטה ויסקאמפ היא יועצת לאבטחת סייבר ופרטיות ובעלת תואר שני מאוניברסיטת VU באמסטרדם.

[2] עוזרת מחקר במכון לחקר המתודולוגיה של המודיעין.

[3] Gill, P., & Phythian, M. (2016). What is intelligence studies? The International Journal of Intelligence, Security, and Public Affairs, 18(1), 5–19. Retrieved November 5, 2019, from: https://bit.ly/2WHlJjf.

כיום, ארגוני מודיעין מגדירים את אתגר הסייבר כאחד מאיומי הליבה העיקריים על מדינתם, דבר שמחייב את הממשלות וארגוני המודיעין לשדרג את מערך אבטחת הסייבר שלהם. כך למשל, בארה"ב במסמך ה-National Intelligence Strategy, שמתפרסם אחת לארבע שנים על ידי ה-DNI (Director of National Intelligence), "איום הסייבר" הופיע לראשונה ב-2009 וחשיבותו במדרג האיומים עולה בכל פעם. הכוונה ב"איום הסייבר" היא שכמעט כל המידע, התקשורת, המערכות, התשתיות הקריטיות והרשתות הלאומיות החיוניות צפויות להיות בשנים הבאות תחת סיכון לתקיפת סייבר מצד יריבותיה של ארה"ב.[4]

<u>מדוע יש צורך בשיתוף פעולה מודיעיני בתחום הסייבר?</u>

המורכבות והמהירות של איומי סייבר הופכת את ההתמודדות עמם לכמעט בלתי אפשרית עבור ארגונים הפועלים באופן עצמאי, משום שבדרך כלל אין להם את כלל הכלים כדי להתמודד עם האתגר המשתנה במהירות. מכאן, שבתחום אבטחת הסייבר נדרשת מידה הולכת וגוברת של שיתופי פעולה מודיעיניים הן בין-ארגוניים והן בין-המגזרים השונים, שהמפתח אליהם הינו **פתיחות**. כיום, ישנה הבנה רווחת כי שיתוף פעולה שכזה יהיה יעיל כאשר הוא מצליח לפרוץ את המחסומים והגבולות הארגוניים ולכלול שחקנים גם מהמגזר הציבורי וגם מהמגזר הפרטי. בתוך כך, ישנן ממשלות שביקשו להקים שותפויות ורשתות חוצות מגזרים בתחום המודיעין-סייבר:

- **בקנדה**, הוקמה הרשת הציבורית-פרטית ה-CCIRC (Canadian Cyber Incident Response Centre) על מנת לשפר את השיתוף בין הסקטור הציבורי והפרטי במידע סייבר שנאסף ומנותח. הרשת מתאמת את שיתוף פעולה זה בין הסקטורים השונים ופועלת כסוג של מסלקה עבור ארגוני וחברות מודיעין.[5]
- **בבריטניה**, הוקם ה-NISCC (National Infrastructure Security Co-ordination Centre) שהינו מרכז תיאום לביטחון תשתיות לאומי שמפגיש גורמים ממגזרים שונים להגנה על תשתיות קריטיות מפני איומי סייבר.[6]

יחד עם זאת, יישומה בפועל של הבנה זו עדיין נתקל במכשולים בקרב ארגוני המודיעין שנוטים לפנות יותר לשותפויות עם ארגוני מודיעין ובמידה פחותה עם חברות סייבר במגזר הפרטי. על מנת להמשיך ולבחון את מידת שיתוף הפעולה של ארגוני המודיעין בתחום הסייבר הן עם המגזר הציבורי והן עם המגזר הפרטי, טוענים חוקרי המאמר כי יש להבחין בין סוגי רשתות מודיעין סייבר שונות על מנת להבחין בין סוגי שיתופי הפעולה השונים.

<u>שאלת המחקר ומתודולוגיה</u>

<u>שאלת המחקר</u>: באילו סוגי "רשתות", קרי קהילות, מודיעין סייבר ניתן להבחין ומהם מאפייניהם?

במחקר זה נבחנו רשתות מודיעין-סייבר בהולנד. בדומה למדינות מערביות אחרות, הולנד הינה מדינה מתקדמת מבחינה טכנולוגית בה ארגונים ציבוריים ופרטיים כאחד תלויים יותר ויותר

---

4 Director of National Intelligence. (2019). **National Intelligence Strategy 2019**. Retrieved February 14, 2019, from: http://bit.ly/2L86quv.

5 Shore. J.J.M. (2015). An obligation to act: Holding government accountable for critical infrastructure cyber security. **International Journal of intelligence and CounterIntelligence**. 28 (2), 236-251. Retrieved November 12, 2019, from: https://bit.ly/33Hx2L5.

6 Trim, P.R.J. (2003). Public and private sector cooperation in counteracting cyberterrorism. **International Journal of Intelligence and CounterIntelligence**. 16 (4), 594-608. Retrieved November 12, 2019, from: https://bit.ly/2qJ3H4e.

במערכות מידע ותשתיות דיגיטליות. המדינה ניצבת כיום בפני איומי אבטחת סייבר משמעותיים שהובילו לקונצנזוס רחב בדבר הצורך בשיתוף פעולה מודיעיני בתחום הסייבר.

מתודולוגיית המחקר הינה איכותנית כאשר מקורות המידע בהם נעשה שימוש הינם: ראיונות עם דמויות מרכזיות מכל המגזרים בתחום המודיעין-סייבר בהולנד; מסמכים פנימיים של ארגונים הנוגעים לתחום המודיעין-סייבר, שכללו יעדי רשת ודרישות כניסה וכן מרשמים להתנהגויות של משתתפי הרשת; ומידע גלוי, בפרט מאתרים ממשלתיים ומדוחות.

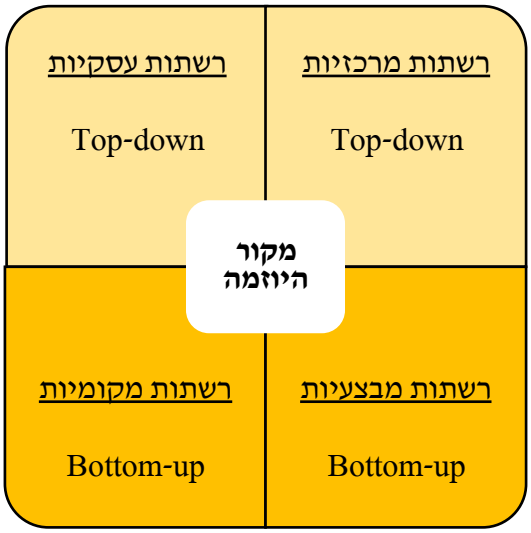
במסגרת המחקר זוהו 4 סוגים של רשתות סייבר:

1. רשתות מרכזיות (Centralized networks) – רשת **בינונית** בגודלה, שבדרך כלל הינה יוזמה של המגזר הציבורי. מטרת רשת מסוג זה היא **לרכז ולשפר** את השיתוף המודיעיני בתחום הסייבר בין **ארגונים ציבוריים ופרטים** בסקטורים ייעודיים.
2. רשתות עסקיות (Business networks) – רשת **בינונית** בגודלה שמטרתה **לבסס את חילופי** המודיעין בתחום הסייבר ואת המומחיות בתחום בין הגורם המבקש שירות, שעשוי להיות **מכלל המגזרים**, לבין ארגונים פרטיים המספקים שירותים בתחום. יצוין, כי מכיוון שהגורם המבקש משלם בתמורה לשירותים שהוא מקבל, הוא למעשה גם יגדיר את אופי שיתוף הפעולה, הופעתו וסיומו האפשרי.
3. רשתות מבצעיות (Operational networks) – רשת **קטנה** יחסית בה חברים מומחי מודיעין סייבר של ארגונים **ציבוריים** שונים, אשר מזהים אתגרים מבצעיים משותפים ומחליטים להקים רשת שתסדיר את שיתוף הפעולה ביניהם.
4. רשתות מקומיות (Local networks) – רשת **גדולה** יחסית של ארגונים **פרטיים** מקומיים המכירים באינטרס משותף, למרות התחרות ביניהם, ומחליטים לשתף בשיטות עבודה בנושאי אבטחת סייבר באופן שלאורך זמן יוצר רשת מודיעין סייבר.

במסגרת המחקר, נבחנו מספר היבטים לבחינה ההבדלים בין רשתות הסייבר השונות, שנבחרו על בסיס סקירת הספרות והנתונים שנאספו: (1) מקור היוזמה, (2) פעילויות, (3) מבנה הרשת, (4) תדירות תקשורת, (5) קונצנזוס על יעדים, (6) מחויבות המשתמשים ו-(7) תוצאות שהתקבלו.

תוצאות המחקר

1. מקור היוזמה – רשתות הסייבר יכולות להופיע בתהליך של **Top-down** או של **Bottom-up**. כלומר, בתהליך Top-Down הרשתות נוצרות על בסיס רצון של גוף ניהולי (ממשלה או מנהלי חברה) לשיפור אבטחת הסייבר של השירותים הציבוריים/הפרטיים; בתהליך Bottom-up הרשתות הן תוצר של מומחי מודיעין סייבר או של קבוצת ארגונים פרטיים מקומיים המזהים אתגר או אינטרס משותף ומחליטים להקים רשת שתסדיר את שיתוף הפעולה ביניהם.

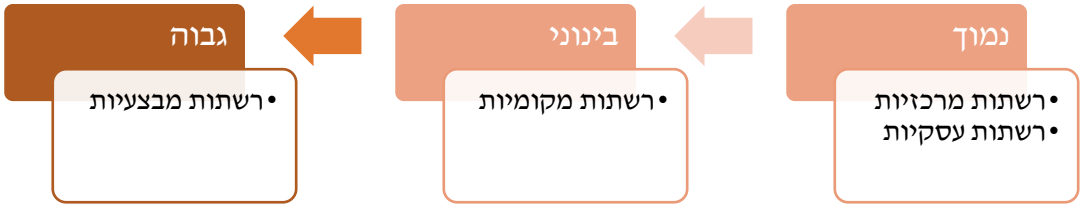


2. <u>פעילויות</u> – אופן פעולתן של הרשתות נחלק לשניים: (1) **שיתוף מודיעיני**, כלומר עיקר הפעילות ברשת מורכב מ"חילופי מודיעין". למשל מתבצע שיתוף מידע אודות איומי סייבר ואירועי סייבר שהתרחשו, שיתוף בחוויה בה מנגנוני אבטחת הסייבר של הארגון הוכחו כיעילים או לא וכן מתן וקבלת ייעוץ כיצד להגביר את חוסן הסייבר של ארגוניהם; (2) **פעולות איסופיות**, כלומר הרשת מתמקדת באיסוף מידע מודיעיני בתחום הסייבר, שכולל בין היתר גם שיתוף בשיטות עבודה מומלצות ויישומים אפשריים להגברת היעילות והעמידות של המערכת.

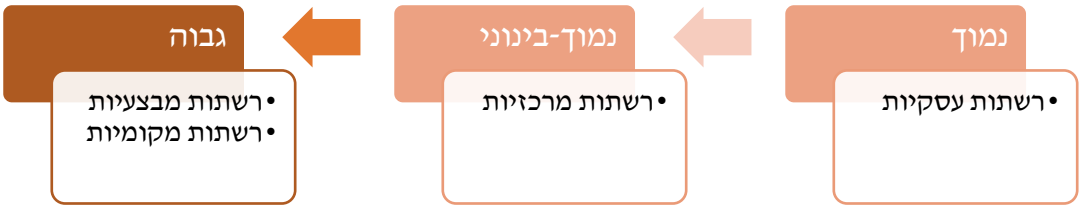
3. <u>מבנה הרשת</u> – תחת מאפיין זה ישנן שלוש קטגוריות: (1) **מבנה ניהולי**, כלומר ישנו מנהל שעומד בראש הרשת, האחראי על פיקוח ושמירה שיתופי הפעולה, אך אין למנהל כוח פורמלי כיוון שהשותפים ברשת שואפים לשוויון בסמכויות ובקבלת ההחלטות; (2) **מבנה היררכי**, כלומר הארגונים ברשת אינם שוויוניים. (3) **מבנה משותף**, כלומר מבנה רשת שטוח ומבוזר במסגרתו קיימת ועדת היגוי למטרות מעשיות, אך החברים ברשת ממונים על עצמם ועל ההחלטות המבצעיות.

<u>המאפיינים הבאים שנבחנו מוגדרים על סקאלה שבין נמוך-בינוני-גבוה:</u>

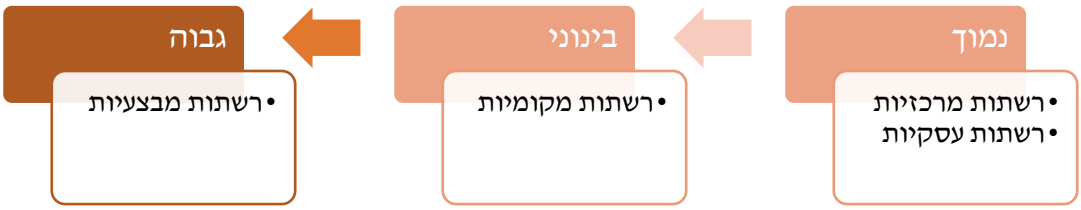
4. <u>תדירות תקשורת</u> – באיזו דחיפות מתקיימות פגישות פנים מול פנים פורמליות ולא פורמליות ברשת המודיעין-סייבר?



5. <u>קונצנזוס על יעדים</u> – באיזו מידה קיימת הסכמה על מטרות ויעדי הרשת בקרב הארגונים השונים המרכיבים את הרשת?

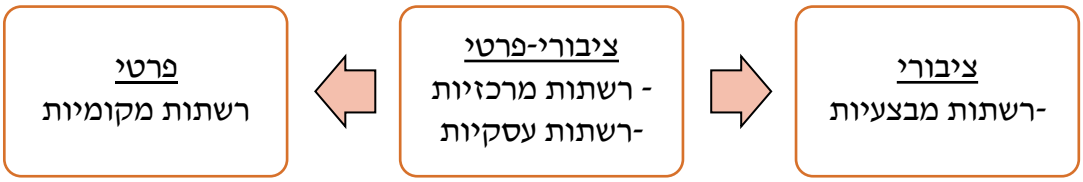


6. <u>מחויבות המשתתפים</u> – באיזו מידה מחויבים הארגונים השונים ברשת לרשת המודיעין-סייבר בה הם חברים?



7. <u>תוצאות שהתקבלו</u> – באיזו מידה תופסים חברי הרשת את תוצאות שיתוף הפעולה של הרשת כמועילות?

תוצאות המחקר למעשה משקפות סקאלה הנעה בין 'ציבורי' לבין 'פרטי' מבחינת סוג הרשת:



<u>מסקנות המחקר</u>

הדמיון והשוני שבין ארבעת רשתות הסייבר שזוהו מאפשרים להסיק מספר מסקנות בנוגע לשיתוף פעולה מודיעיני במרחב הסייבר. ראשית, משום שרשתות המודיעין בתחום הסייבר בעלות מאפיינים שונים לא ניתן לאחד את מאמצי שיתוף הפעולה בתחום ניהול אבטחת סייבר לסוג רשת אחד, קרי לקהילה מודיעינית אחת משותפת בתחום. לטענת כותבי המאמר, ההבחנה בין הסוגים השונים דווקא תאפשר להתמודד עם מגוון האתגרים המתהווים במרחב הסייבר. כלומר, סוג הרשת משפיע באופן ישיר על האתגרים והתוצאות של שיתוף פעולה מודיעיני בתחום הסייבר. יצוין, כי ייתכן כי סוגי רשתות נוספים יתווספו בעתיד בהתאם להתפתחות מרחב הסייבר.

שנית, המחקר ממקד את תשומת הלב של סוכנויות המודיעין בתחום הסייבר בשיתוף פעולה עם שחקנים מהמגזר הפרטי. כפי שעולה מן המחקר, אחת מרשתות הסייבר המודיעיניות שזוהו במחקר זה הינה רשת ה'מקומיות' שמורכבת רק מגורמים וארגונים מהמגזר הפרטי. הארגונים הפרטיים המקומיים המרכיבים רשת זו מכירים באינטרס משותף באופן שיוצר רשת מודיעין-סייבר. בנוסף, הן רשתות המודיעין-סייבר מסוג 'עסקיות' והן מסוג מרכזיות' משלבות בתוכן גורמים רבים מהמגזר הפרטי. הנוכחות הרחבה של המגזר הפרטי ברשתות המודיעין-סייבר השונות, המשאבים העומדים לרשות החברות הפרטיות והאפשרות להתמקד בבעיות מצומצמות ולא רחבות ורבות, כפי שנאלצים להתמודד ארגוני המודיעין, מגבירה את הצורך לבחון את המאמצים המתרחשים בקרב חברות הסייבר במגזר הפרטי. זאת, על מנת לבחון האם הקהילות הללו והחברות הפרטיות מפתחות ידע שעשוי להיות רלוונטי עבור המגזר הביטחוני.

שלישית, שיתופי פעולה ציבוריים-פרטים מתרחשים בדרך כלל מיוזמות Top-Down, כפי שנמצא **ברשתות ה'ריכוזיות' וה'עסקיות'**. כלומר, היוזמה משקפת את רצון הממשלה להשתמש במומחיות מובחנת. יחד עם זאת, המחקר הראה כי **רשתות 'מבצעיות' ורשתות 'מקומיות'** הפעולות מיוזמות Bottom-Up נתפסו כמוצלחות יותר במספר ממדים ובהם במחויבות המשתתפים לרשת, בתפיסת פעולות הרשת כמועילות, בתדירות התקשורת ברשת ובקונצנזוס על היעדים. לצד הצלחתן של רשתות מסוגים אלו ישנם גם חסרונות ובהם חוסר יציבות, מכיוון שלרוב חסרים נהלים והסכמים רשמיים, וחוסר יכולת לקבץ קבוצה גדולה של ארגונים תחת קורת גג אחת.

לאור היתרונות והחסרונות היחסיים של כל אחת מרשתות הסייבר שזוהו במחקר, כותבי המאמר מבקשים לאפשר לכלל סוגי הרשתות, קרי הקהילות, להתקיים במקביל ואף לחפוף זו לזו בהתאם לצורך באופן שישרת את צורכי המדינה בצורה המיטבית להתמודדות במרחב הסייבר המתהווה.

<u>משמעויות עבור קהילת המודיעין בישראל</u>

סיווג קהילות ידע שונות איננה תופעה ייחודית לעולם הסייבר וניתן לראות אותה גם בקרב קהילות ידע מודיעיניות, שעוסקות בפיתוח ידע, איסוף וכו'. כך למשל, קהילת המודיעין בישראל ביקשה לייצר קהילות ידע ומרחב משותף לגורמי המחקר והאיסוף ביחידות השונות באמצעות הפלטפורמה הדיגיטלית "טרייסבוק", שהינה רשת חברתית מודיעינית שפותחה בהשראת Facebook. אומנם, מהלך זה לא נחל הצלחה אך הוא משקף את מגמת "שבירת החומות" של המעגל המודיעיני, שהחלה כבר ב-2009, באופן שיאפשר יצירת קשרי גומלין, חיבורים רשתיים ושילוביות בין גופים שהיו בלתי תלויים אחד בשני.[7]

ניתן לייצר קהילות ידע ופיתוח משותפות בתחומי מודיעין נוספים, למשל קהילה המחברת בין יכולות איסוף שונות, זאת באופן שמשלב גם את המגזר הפרטי וחברות היי-טק אשר מפתחות ידע בתחום זה. דוגמא נוספת, הינה קהילה המחברת את גופי המודיעין לארגונים וחברות הן מהמגזר הציבורי והן מהמגזר הפרטי העוסקים ב'פייק ניוז', תודעה והשפעה. יצוין, כי גם במגזרים כמו האקדמיה ומכוני מחקר ניתן לפתח קהילות ידע משותפות, שיעסקו בין היתר בנושאי מודיעין.

כיום במרחב המודיעיני בישראל קיימים גופים רבים ומגוונים מכלל המגזרים העוסקים בפונקציות מודיעיניות שונות. ריבוי הארגונים העוסקים במודיעין עשוי לאפשר לבחון ולסווג את הקהילות

---

7 גליק. א. (דצמבר 2018). החומות לא נשברו – הסיפור של טרייסבוק. <u>בין הקטבים</u>, גיליון 18. אוחזר בתאריך 18 בנובמבר 2019, מתוך: https://bit.ly/32YE8cE.

השונות הקיימות, באופן שיסייע בשלושה ממדים: ראשית, בבחינת וסיווג אילו שיתופי פעולה מודיעיניים מתקיימים **כיום** ומה מידת יעילותם. שנית, הדבר יאפשר לבחון שיתופי פעולה מודיעיניים **עתידיים** בין המגזרים השונים, שיאפשרו להתמודד באופן יעיל ורציף עם האתגרים המתהווים. לבסוף, עבור ארגון מהמגזר הציבורי או מהמגזר הפרטי סיווג הרשתות השונות אליהן הם שייכים יכולים לסייע עבורם **להעריך את הסיכונים וההזדמנויות** כחלק מאותה הרשת בה הם לוקחים חלק ובתוך כך לפעול בהתאם ולהיערך לאתגרים.

לסיכום, חשיבותו של מחקר זה טמונה בהפניית תשומת הלב לתחום שבדרך כלל לא נחקר – איך מקימים קהילות מודיעיניות? כיצד משמרים אותן? מה עושים בהן? מה היתרונות והחסרונות הגלומים בהם? מהו העתיד בתחום זה? וכיצד "הרשתות" המודיעיניות הללו עשויות לסייע לקהילת המודיעין אל מול האתגרים המתהווים?

נספח – גרף סיכום ממצאים

	רשתות מרכזיות	**רשתות עסקיות**	**רשתות מבצעיות**	**רשתות מקומיות**
מקור היוזמה	Top-Down	Top-Down	Bottom-up	Bottom-up
פעילויות	שיתוף מודיעיני	פעולות איסופיות	פעולות איסופיות	שיתוף מודיעיני
מבנה הרשת	ניהולי	היררכי	משותף	ניהולי
תדירות תקשורת	נמוך	נמוך	גבוה	בינוני
קונצנזוס על יעדים	נמוך-בינוני	נמוך	גבוה	גבוה
מחויבות המשתתפים	נמוך	נמוך	גבוה	בינוני
תוצאות שהתקבלו	נמוך	בינוני	גבוה	גבוה
דפוס לפי המחקר	**ציבורי-פרטי**	**ציבורי-פרטי**	**ציבורי**	**פרטי**