"What is New is Old" – אנלוגיות בין התפתחותו של מרחב הסייבר לבין עבודת המודיעין "הקלאסית"

1. במאמר "Intelligence in Cyber – and Cyber in Intelligence" שפורסם באוקטובר 2017 ע"י Michael Warner, המשמש כהיסטוריון של פיקוד הסייבר בארה"ב, מבקש הכותב לבחון **אנלוגיות בין מרחב הסייבר לבין התפתחותו של המקצוע המודיעיני, כאמצעי לבחינת החלתן של תפיסות מודיעין קיימות גם במרחב הסייבר וכאמצעי לבחינת דילמות חדשות שהתפתחותו של מרחב זה מעלה.**
2. המאמר פורסם בקובץ מאמרים של אוניברסיטת ג'ורג'טאון בארה"ב הנקרא – "Understanding Cyber Conflicts – 14 analogies", הבוחן **אנלוגיות בין מרחב הסייבר לבין תחומים שונים.** חשיבותו, לטענת הכותבים, נובעת מכך שאנו יוצרים אנלוגיות כל הזמן כדי **להסביר את ה"לא מוכר" באמצעות ה"מוכר" וכדי לבנות טיעונים לוגיים מבלי לבחון האם האנלוגיות שיצרנו נכונות או דורשות התאמות.** קונקרטית, בנוגע למרחב הסייבר מציינים הכותבים כי יצירת אנלוגיות בינו לבין תחומים אחרים עשויה לסייע **לגורמי מדיניות** שעבורם מרחב הסייבר הוא אתגר חדש יחסית ולא מוכר; כמו גם **לאנשי הסייבר** אשר ככל-הנראה אינם בקיאים באירועי עבר או במקרי בוחן מהם ניתן להשליך גם על ההתנהלות במרחב הסייבר.

יומינט וסייבר

3. האנלוגיה הראשונה אותה בוחן הכותב היא **בין מודיעין אנושי, הנחשב לאחד מאמצע המודיעין העתיקים ביותר לבין מרחב הסייבר.** כך, הסייבר בדומה ליומינט שקדם לו באלפי שנים מאפשר **מרחב פעולה חשאי.** חשיפת סוכן של מדינה זרה, בדומה לחשיפת פעילות סייבר **מעוררת הד תקשורתי רחב,** אך **אינה מהווה עילה לפתיחת מלחמה.** במהלך השנים מדינות יצרו **פרוטוקולים להתמודדות עם ריגול מצד מדינות/גופים זרים.** אף שאלה עדיין לא נוצרו כדי להתמודד עם פעילות קיברנטית כותב המאמר מעריך כי אלה יתפתחו בשנים הקרובות[1].

מודיעין מסכל וסייבר

4. מבצעי מודיעין מסכל (Counterintelligence) בעבר כללו **"שתילת" סוכנים במדינות היעד** אשר תפקידם היה **להעביר מידע,** ולעיתים גם **ליצור מהומה,** וכן **לחשוף פעילויות מתוכננות. מאפיינים דומים ניתן למצוא גם במרחב הסייבר.** כך, למשל, מציין הכותב כי ה-FBI **מגייסים פושעי סייבר** הפועלים בחשאי במרחב הקיברנטי (תוך שימוש ב-Darknet לדוגמה). "המגויסים" ממשיכים לנהל קשרים עם הקבוצה

---

[1] דוגמה להתפתחות "כללי משחק" ניתן למצוא בצו (Executive Order) עליו חתם הנשיא אובאמה בשנת 2015 המתיר הטלת סנקציות על גורמים שהיו מעורבים בפעילות סייבר כנגד ארה"ב - https://apps.washingtonpost.com/g/documents/world/executive-order-obama-establishes-sanctions-program-to-combat-cyberattacks-cyberspying/1502/.

אליה השתייכו, ובמקביל לכך מוסרים מידע ל-FBI. מבצעים אלה כוללים שיתופי פעולה עם מדינות נוספות, וכאשר נחשף מספיק מידע המאפשר את חשיפת הרשת כולה מבצעות המדינות המעורבות **מבצעי פשיטה מתוזמנים.** "המגויסים" זוכים להגנה מצד המדינה ולעיתים חיים תחת זהות חדשה.

5. זהו למעשה **יישום של שיטות העבודה בתחום המודיעין המסכל במרחב הסייבר.** ההבדל המרכזי הינו **בהיקפי הפעילות, כשמרחב הסייבר מאפשר פעילות בהיקף משמעותי יותר** מזה שהתאפשר במבצעי מודיעין מסכל מסורתיים.

מודיעין, הצפנה ואבטחת מידע

6. השימוש בטכנולוגיות תקשורת (communication technologies) כחלק מעבודת המודיעין החל בתחילת המאה ה-20 עם השיפורים שחלו בטלגרף, וביתר שאת לאחר הופעת הטלגרף האלחוטי והרדיו. בהיבט הצבאי גברו הדרישות **לציוד חדש** המאפשר העברת מידע **ולמערכות הצפנה** המאפשרות את אבטחת המידע המועבר. המידע המתקבל בזמן אמת יצר **מהפכה בעניינים צבאיים** (RMA, Revolution in Military Affairs), **אפשר למפקדים לסנכרן בין מגוון של אמצעים צבאיים** ובפועל יצר **תלות בטכנולוגיות התקשורת וביכולת לצרוך מודיעין בזמן אמת** (C4ISR – Communications, Computers, Intelligence, Surveillance, Reconnaissnace).
7. עם התפתחותן של טכנולוגיות התקשורת התפתחו גם **מערכות ההצפנה ותפיסות** המבחינות בין רמות הצפנה שונות **כתלות ברגישות המידע** המועבר. כאשר החלה תעשיית המחשבים להתפתח – החל להתפתח גם תחום **אבטחת המידע.** מומחיותו של ה-NSA בתחום השפיעה על התפתחותן של **תפיסות** אבטחת מידע ועל **הדילמות** בתחום זה. מבין הדילמות שהתחדדו היו **מידת מעורבותה של הממשלה בהגברת איכות ההצפנה** (פתרונות הצפנה נתפסו כסודות צבאיים); **האופן בו יש להגן על מידע רגיש**; **הצורך באיזון בין אבטחת המידע והזכות לפרטיות לבין צרכי ביטחון לאומי** (אחד הביטויים למתח זה הינו השארת פרצות אבטחה במכוון כדי לאפשר לגופי ביטחון לנצלן בעת הצורך על-חשבון אבטחת מידע מיטבית).
8. לצד זאת, כותב המאמר טוען כי אנלוגיה נוספת בין הסייבר לבין עבודת המודיעין "הקלאסית" ניתן למצוא בכך **שהתפתחות תפיסת אבטחת המידע נובעת במידה רבה מהלקחים שנלמדו ממבצעי מודיעין** במלחמת העולם השנייה ולאחריה, בזמן המלחמה הקרה. כך למשל, כאשר הקונגרס האמריקני בחן (בשנת 1976) את ההגנה על המחשבים הוא שיבח את ה-CIA על הנחת היסוד שעמדה בבסיס אבטחת המידע שביצע לפיה **לא רק שניתן לפרוץ את מערכות ההגנה** (היכולת קיימת), **אלא סביר גם שייעשו ניסיונות לפרוץ אותן** (ישנם כוונה/אינטרס).
9. השינוי שיצר מרחב הסייבר בעניין אבטחת מידע היה **בצורך להגן על המידע באופן תמידי**– **בהעברתו ובאחסונו**, שכן המידע הפך חשוף יותר בפני מבצעי איסוף ותקיפה בפרט לאור פעילותם של שחקנים שונים במרחב – ממדינות עד האקרים פרטיים.

רדיו וסייבר

10. התפתחות הרדיו מציעה אנלוגיה נוספת למרחב הסייבר – מאפיינים מסוימים של הרדיו דומים למאפייניו של מרחב הסייבר ואכן **חלק מהטרמינולוגיה המשמשת במרחב הסייבר נבעה מהטרמינולוגיה ששימשה בהתפתחות הרדיו** בתחילת המאה ה-20 (מונחים כמו: רשת, רוחב פס, אל-חוטי). מעבר לכך, **קליטת אותות רדיו, גם אם התוכן שהועבר לא פוענח, שימשה כאמצעי איסוף מודיעין.** זאת, כמובן, בדומה לשימוש במרחב הסייבר.
11. לצד זאת, ניתן למצוא הקבלה נוספת **בשימוש ברדיו ובסייבר במבצעי הונאה ובלוחמת מידע,** ע"י **שיבוש** פעילות היריב או **שתילת מסרים** בהם. עם זאת, ניתן להבחין בין לוחמה אלקטרונית לבין סייבר – לוחמה אלקטרונית "מסורתית" נועדה לכוון מערכות נשק או להגן עליהן, אך נותרה **מרכיב חיצוני בפעילותם.** מרחב הסייבר לעומת זאת מכיל פעילות של הרבה ממערכות הנשק האלה ומהווה **חלק אינטגרלי מפעילות מערכות הנשק.**

שיפור ביכולות מודיעין וסייבר הנובעים מצרכים מבצעיים

12. היבט נוסף בקשר שבין המודיעין לבין הסייבר נעוץ בעצם העובדה כי שיפורים רבים שחלו בתעשיית המחשבים **נבעו מצרכים צבאיים שנגעו להפיכתם של אמצעי הלחימה ל"חכמים" יותר**, כך שיהיו בעלי **דיוק משופר**, יעבירו **מידע מפעילות מבצעית ויוזנו ממודיעין המתקבל בזמן אמת.** שיפורים אלה באמצעי הלחימה **חייבו גם שיפורים בטכנולוגיות התקשורת המשמשות את הצבא** ובהמשך הביאו **לשיפור בתעשיית המחשבים כולה.**

המאמר בוחן **אנלוגיות בין מרחב הסייבר לבין התפתחותו של המקצוע המודיעיני** ובכך מתמקד בעיקר בשימוש בסייבר **לצרכי איסוף מודיעין** או **כחלק מפעילות תודעתית,** תוך התייחסות מצומצמת לאפשרות להסב נזק ע"י תקיפות סייבר. האנלוגיות המוצגות מציעות כי התפתחותו של מרחב הסייבר הנתפס לעיתים כ"חדש" הוא למעשה **אבולוציה של המודיעין** שהחל בפעילותם של **מרגלים אנושיים,** עבור בשימוש **בטכנולוגיות תקשורת** (כמו הרדיו והטלגרף) ועד **לשימוש ברשתות מחשבים.** אם כן, כותב המאמר סבור כי התפתחותו של מרחב הסייבר תרמה לשיפור ביכולות המודיעין וליכולת להוציא לפועל מבצעי מודיעין בהיקפים משמעותיים יותר מכפי שהתאפשר בעבר.

לצד זאת, האנלוגיה בין הסייבר לבין **אמצעי איסוף מודיעין קודמים וטרמינולוגיה קיימת** – מאפשרת להחיל, או לכל הפחות לבחון את התאמתן של תפיסות קיימות הנוגעות **לתפקיד המודיעין, לפרקטיקה המודיעינית ולאבטחת המידע.** זאת, תוך ביצוע **ההתאמות הנדרשות** בהתאם למאפייניו הייחודיים של מרחב הסייבר: היקף הפעילות המתאפשר בו, האיום התמידי על המידע לאור הקישוריות הגוברת (Interconnectivity), פעילות של מגוון רחב של שחקנים והפעלת יכולות שבעבר היו נכס של מדינות בלבד.

חרף נקודות הדמיון הרבות בין עבודת המודיעין לבין המאפיינים של מרחב הסייבר והפעילות בו יש לבחון גם את **השוני** בן השניים ובמיוחד **את מאפייניו הייחודיים של מרחב הסייבר, בהם כותב המאמר כמעט ולא עסק.** כך, הופעתו של מרחב הסייבר מאפשרת למשל **להגדיר מחדש מונחים כמו גבולות וזמן,** שכן במרחב הסייבר משמעותם של גבולות גיאוגרפיים הינה מצומצמת עד כדי אפסית, ופעילות במרחב מתאפשר בקצבים מהירים מאוד.