היומינט בעידן הקיברנטי: משחקים בשני עולמות

אבי טל ודודי סימן טוב

עידן הסייבר מחולל שינוים עצומים בעולמות המודיעיניים והאיסופיים. מאמר זה דן בשאלות האם יש מקום למקצוע היומינט בעולם שבו הסייבר מהווה מרחב איסוף ופעולה מרכזי? באם יש מקום ליומינט, אילו משימות מוטלות עליו והאם נוצרות הזדמנויות לשיטות פעולה חדשות בעידן הסייבר? המאמר בוחן את מהות הדיסציפלינה היומינטית בעידן זה, ובתוך כך את האתגרים שמציב הסייבר בפני דיסציפלינה זו. בנוסף לכך הוא דן בתרומה הפוטנציאלית של היומינט בעידן הקיברנטי ומעלה את השאלה האם מדובר בדיסציפלינה מודיעינית־איסופית חדשה.

החלק הראשון במאמר מציג את היומינט עד לעידן הסייבר. חלקו השני דן ביומינט בעידן הקיברנטי, תוך שימת דגש על ההזדמנויות, הסיכונים והשינויים שחלו בו, ומציג הצעה לתפיסה חדשה באשר למקצוע היומינט בעידן הקיברנטי.

מילות מפתח: יומינט, מודיעין, איסוף מודיעיני, סייבר, קהילת המודיעין, יומינט קיברנטי, אוואטר.

מבוא

הסייבר הפך את העולם לכפר גלובלי. הוא מנגיש בו עמיתים ויריבים, אויבים וידידים, תוך גישור על גבולות ושפות. בסייבר עובר מידע גלוי וגם מסווג ומוצפן, והוא גם הפלטפורמה המרכזית לבקרה ולשליטה על מערכות וכלים. פלטפורמה זו מייצרת איומים של מתקפות קיברנטיות, שלעיתים יכולות להיות להן גם תוצאות קינטיות. הרשתות החברתיות, הבלוגוספירה והמדיה החדשה הפכו לבמה המרכזית

דודי סימן־טוב הינו חוקר של תחום המודיעין במכון למחקרי ביטחון לאומי, אבי טל הוא בכיר לשעבר במגזר הערבי בשב"כ

של ההמונים לשיח ולפעולה בכל תחומי החיים.[1] הרשתות החברתיות גם הפכו לפלטפורמה מרכזית להתארגנויות שונות, דוגמת "האביב הערבי", וכן להסתה, כמו זו שהובילה לגל הסכינאות העכשווי ברחבי ישראל. כמעט לכל אחד יש כיום דף בית אישי באינטרנט, וכמעט כולם נותנים בו במה לעמדותיהם ולרצונותיהם בנושאים אישיים ומקצועיים. המידע הגלוי עצום ורב ונמצא בעלייה מתמדת; לצידו קיימים אזורים קיברנטיים הקשים לחדירה.[2]

עידן הסייבר מחולל שינוים עצומים בעולמות המודיעיניים והאיסופיים. אלה מעוררים שאלות כגון: האם יש מקום ליומינט בעולם שבו הסייבר מהווה מרחב איסוף ופעולה מרכזי? ואם יש מקום כזה, האם נוצרות הזדמנויות לשיטות פעולה חדשות? מטרת המאמר היא לבחון מהם מאפייני היומינט בעידן הקיברנטי, תוך שימת דגש על השינויים שחלו בתפיסות ובשיטות ההפעלה שלו בהשוואה למקצוע היומינט הקלאסי. החלק הראשון במאמר מציג את היומינט עד לעידן הסייבר. חלקו השני דן ביומינט בעידן הקיברנטי, מדגיש את ההזדמנויות, הסיכונים והשינויים שחלו בו ומציג הצעה לתפיסה חדשה באשר למקצוע היומינט בעידן הסייבר.

היומינט הקלאסי

משחר ההיסטוריה ועד תחילת המאה העשרים התבססו גורמי המודיעין באופן בלעדי על מידע ממקורות אנוש. סון טסו, מצביא סיני מהמאה השישית לפני הספירה, כתב בספרו "אמנות המלחמה" על המרגלים וחשיבותם במלחמה.[3] יש הרואים במקצוע היומינט – המודיעין האנושי (Human Intelligence) – הקלאסי הוא אמנות משום שהוא דורש מהאדם העוסק בו יכולת תקשורת בין־אישית גבוהה, ידע כללי רחב, רב־גוניות ויכולת לשחק תפקידים שונים, לצד היכרות עם התחום הפסיכולוגי־פילוסופי של ההתנהגות האנושית, יכולת השפעה ושכנוע, וכמובן הנעה לפעולה.

קיימים שלושה שלבי מפתח במקצוע היומינט: הראשון הוא אתירה ובחירה, קרי איתור ובחירת האנשים הנדרשים לגיוס על בסיס כישורים אישיים וייעודיים, מניעים (קיימים ופוטנציאליים) ונגישות (לגיוס ולהפעלה); השלב השני הוא מִבצע הגיוס, שיכול להתבצע בשיטות שונות ומגוונות – גיוס מתוכנן, גיוס ישיר, גיוס עקיף באמצעות סייען ובכיסוי, גיוס מזדמן וגיוס מתנדבים;[4] השלב השלישי הוא הפעלה ומִבצעים. פגישה פיזית חשאית היא בעלת חשיבות רבה ליצירת אמון וזיקה אישית עם הסוכן ולהיבטים המבצעיים הקשורים בהפעלתו (מבחן אומץ, מתן אמצעים, הדרכות והכשרות ייעודיות ועוד).

היומינט הקלאסי היה בתחילת דרכו פעילות אנושית פשוטה.[5] הגיוס וההפעלה התבססו בעיקר על פגישות פיזיות, בשל היעדר כמעט מוחלט של נגישות מרחוק. תהליך האתירה נעשה על בסיס מודיעין מצומצם וחסר יחסית, ולכן

המאתרים ויכולת הבחירה האיכותית היו מוגבלים. בעולם פיזי זה, ככל שמִבצע הגיוס וההפעלה חייבו פעולה בכיסוי מול המגויס והסביבה, היה צורך בהתאמה מלאה של מערך ההפעלה למגויס ולסביבתו, וזאת בהתאם לסיפורי הכיסוי. אלה היו חייבים לעמוד במבחן הפיזי: דמות המפעיל, השחקנים המסייעים, ובכללם האבטחה, המקום, התפאורה, השפה ועוד. מצב זה יצר סיכונים רבים לביטחון המִבצע, למפעילים וגם לסוכן. ציוד הסוכן באמצעים לפעולה חשאית הגביר את הסיכון והיווה חותמת מפלילה.

מעמדו של המודיעין האנושי בקהילות המודיעין במערב נמצא בדעיכה משנות השבעים של המאה העשרים ואילך.[6] הסיבות לכך היו ההתפתחויות הטכנולוגיות ומעבר מסיבי של המין האנושי והצבאות לשימוש במרחב האלקטרומגנטי. אלה הביאו לעלייתו של האיסוף הטכנולוגי, לעלייה בתרומת המודיעין הגיאו־מרחבי באמצעות לוויינים וסייבר, וכן לעלייה עצומה בכמות המידע הגלוי (אוסינט).

מסקנות ועדות החקירה שחקרו את הפיגועים במגדלים התאומים בארצות הברית ב־11 בספטמבר 2001 ואת כישלון המודיעין האמריקאי בעיראק, היוו נקודת מפנה בקהילת המודיעין האמריקאית. מסקנות אלו הצביעו על היעדר מידע מדויק על ארגון "אל־קאעדה", מהסוג האינטימי שמערך היומינט אמור לספק. בעקבות זאת החל ניסיון להחזיר את היומינט למרכז העשייה המודיעינית בארצות הברית. דוגמה לתרומה אפקטיבית של היומינט לאיסוף המודיעיני האמריקאי ניתן למצוא במצוד אחר מנהיג "אל־קאעדה", אוסמה בן לאדן, כאשר ה־CIA גייס רופא פקיסטני שנתן חיסון מזויף לבן לאדן, ובאותה הזדמנות הפיק ממנו את הדנ"א שלו.

היומינט בעידן הקיברנטי

בשיח על האיסוף המודיעיני בעידן הקיברנטי קיימת גישה, לפיה לא נכון להתבסס על הסייבר כמקור איסופי כמעט בלעדי. לפי גישה זו, אין תחליף ליומינט כדי להבין את תמונת המודיעין השלמה, במיוחד כשמדובר בארגונים דוגמת דאע"ש וחמאס, שחתימתם בסייבר נמוכה, והסתמכות על מודיעין טכנולוגי בלבד כדי להגיע למידע מדויק עליהם הינה חסרה ובעייתית.[7] בהמשך לכך, קיימת גישה הגורסת כי דווקא בעידן הנוכחי, כאשר מתבררת מידת החדירה האיסופית לכלל תחומי החיים, מדינות וארגונים שואפים להפחית את רמת החתימה המודיעינית שלהם ולפעול באמצעות שליחים ופגישות עבודה.

בדיון התיאורטי על היומינט בעידן הקיברנטי יש המציעים להרחיב את מושג היומינט ולהוסיף לו את המושג "הנדסה חברתית" שבמסגרתו יוצרים זהות בדויה לשם גיוס מקורות אנושיים על מנת להשפיע עליהם לפעול באופן הרצוי. קיימות הצעה לבצע מיזוג בין היומינט ובין תחום ההנדסה החברתית, אולם נראה שמהלך כזה עלול להחמיץ את היתרונות הקיימים של דיסציפלינת היומינט ולתעל אותה

לתחום אחד בלבד שהוא תחום אבטחת המידע. וכך להחמיץ את הפוטנציאל הגלום בתחום היומינט הקיברנטי ההתקפי.

התפתחות היומינט הקיברנטי החלה באמצע העשור הקודם, על ידי הכוונת סוכנים לעשות שימוש בכלים קיברנטיים, ובראשם האינטרנט, כלומר הפניית הסוכנים לפורומים ברשת, שם הם יפעלו בשמם או בשם בדוי. השלב הבא היה יצירת דמויות מדומיינות, שמאחוריהן עמד צוות שהורכב ממספר אנשים מדיסציפלינות שונות. אלה הפנו את הדמויות המדומיינות לפורומים שונים, שבהם הן פעלו בזהות בדויה, ושם הן גם חדרו לאזורים שאין סבירות שסוכנים קיימים יפעלו בתוכם. שלב זה היה פועל יוצא של ההתפתחות הטכנולוגית המואצת של השנים האחרונות, שאפשרה יצירת דמויות באופן טכנולוגי וללא הגבלה. בהקשר הישראלי, שיטה זו יכולה לאפשר מעבר מפעילות של פיקוח וניטור של "טרור הסכינים" – סוג הפעילות הנהוגה כיום, שהאפקטיביות שלה מוטלת בספק – לפעילות אקטיבית ופרו אקטיבית שמטרתה להביא לצמצום ההסתה שמובילה לסוג זה של פיגועים וכן להשפיע על דעת הקהל.

לכאורה, קיימת סתירה פנימית בין מקצוע היומינט הקלאסי של הפעלת סוכנים ובין היומינט המבוסס על הפעלת סוכנים דרך הסייבר. היומינט הקלאסי כולל פגישות אישיות ליצירת אמון וזיקה אישית, היכרות קרובה, אינטימית וארוכת שנים ויצירת יחסי מרות הדומים ליחסי עובד־מעביד וכוללים מתן תגמולים חומריים ולא חומריים. כל זאת, יחד עם תוכנית לפיתוח ההפעלה בראייה ארוכת טווח, בדיקות מהימנות, הכשרות, ציוד באמצעים ועוד. לעומת זאת, היומינט הקיברנטי מתבסס על יחסים שאינם בהכרח קבועים, המחויבות והנאמנות הן ברמה נמוכה יותר, והקשרים בין המפעיל למקורותיו אינם עמוקים ואינם מתבססים על חיבור אנושי בלתי אמצעי.

ביומינט הקלאסי מתקיים מגע אנושי אינטימי, המאפשר שפה בלתי אמצעית ורגשית, שיוצרת חיבור וקירבה החורגים מעֵבר למפגש האינטרסים. ההפעלה ביומינט הקיברנטי מבוססת על אינטרסים מצטלבים. כתוצאה מכך, רמת המחויבות ביומינט הקלאסי גבוהה יותר, והסוכן אף עשוי לבצע מהלכים שיסכנו אותו; לעומת זאת, בהפעלה הקיברנטית רמת הסיכון לסוכן נמוכה הרבה יותר. זאת ועוד, המפגש הפיזי הבלתי אמצעי עם סוכנים מהווה מרכיב חשוב, ולעיתים קריטי, ליצירת הזיקה האישית, שהיא בעלת חשיבות רבה כמעט בכל היבט הפעלתי ומבצעי. המגע הפיזי, האכילה והשתייה המשותפות יוצרים חיבור מיוחד התורם לתחושת המוטיבציה של הסוכן. הסייבר, מצידו, מאפשר לקיים מפגש וירטואלי ברמה הקרובה למפגש פיזי, אך לא מפגש פיזי של ממש, שכל הנדרש במסגרתו הוא לבצע אותו במינימום סיכונים וחתימות מפלילות.

בעידן היומינט הקיברנטי, המאתרים לגיוס הינם מגוונים וכמעט בלתי מוגבלים. ניתן לקבל במהירות מודיעין הדרוש לאתירה, יכולת הבחירה היא מרובה, ואיתה גם הנגישות. זאת ועוד, הסייבר מאפשר לבצע את שלבי הגיוס וההפעלה בסיכון קטן יחסית וכמעט ללא עלות וללא מאמץ, באמצעות התחזות או אנונימיות, ובכלל זה פגישות במולטימדיה. ניתן גם להקים קשר עם יחידים וקבוצות ו/או להשתייך אליהם בלי סיכונים פיזיים. הדבר מאפשר פריצת גבולות ומשפר משמעותית את היכולת של אנשי היומינט להגיע לקהלי יעד רחוקים וקשים לגיוס. הסייבר גם תורם לאנשי החקירות על ידי פעולות לבדיקת מהימנותם של סוכנים וחקירתם של חשודים. כך, למשל, בחינת מהימנות של נחקר יכולה לעשות שימוש בנתונים שהוא שיתף בפייסבוק. דומה שסוגיית המקורות האנונימיים שזהותם אינה ידועה למפעיל הינה פחות משמעותית כאשר המידע נועד למחקר ולהבנת זרמי עומק חברתיים; לעומת זאת, שאלה זו מקבלת משמעות אקוטית כאשר המידע נדרש לפעולה סיכולית או אחרת, העלולה לסכן חיי אדם.

עידן הסייבר מאפשר להיעלם באוקיינוס הגדול של המידע ובתוך משחקי הזהויות והתפקידים, ובכך הוא מאפשר להגביר בצורה משמעותית את התקשורת הבטוחה עם הסוכנים. היכולות להעביר מידע בסייבר הן מגוונות, וניתן לעשות זאת במהירות ובנפחים גדולים. כתוצאה מכך, הסייבר משפר את אפשרויות התקשורת עם סוכנים וסייענים, ובכלל זה העברה מהירה של מידע בנפחים גדולים. בעבר, סוכנים היו צריכים למלא תיקים, מזוודות או ארגזים בחומר ולהעבירם למפעיליהם, תוך סיכון גבוה לשני הצדדים. כיום, די בשימוש בהחסן נייד כדי לאפשר לסוכנים להעביר כמויות גדולות של מידע במולטימדיה ובאיכות גבוהה אף יותר. בכך מצמצם הסייבר את הצורך במפגשים פנים אל פנים ומקטין את הסיכון לשני הצדדים. יחד עם זאת, לפעילות מודיעינית אקטיבית בסייבר יש חתימה, שעלולה להוות איום בטווח הקרוב או הרחוק. במקביל, קיימים סיכונים עקיפים בסייבר, המתגברים והולכים ככל שגוברות פעילויות של פיקוח, ניטור וגילוי.

היומינט הקיברנטי יכול לחדור למרחב הקיברנטי בו עושה היריב שימוש, כמו פורומים פתוחים או סגורים, ולהשתלב בהם בצורה פסיבית (לאיסוף מידע) או אקטיבית. ההשפעה האקטיבית של הסוכנים הקיברנטיים יכולה לבוא לידי ביטוי בגיוס סוכנים של היריב לטובת איסוף מידע, בהכוונה של סוכנים פיזיים לפעול בעולם הפיזי, או בהשפעה של סוכנים קיברנטיים על דעת הקהל (למשל, יצירת דעת קהל נגדית בתחום הדה־לגיטימציה של ישראל בפורומים רלוונטיים). כיוון נוסף שניתן לעשות בו שימוש בעולם הקיברנטי הוא יצירת שמועות שקריות על אדם שמעוניינים לפגוע בו – מעין "סיכול קיברנטי" (shaming). בנוסף, הפוטנציאל של יומינט קיברנטי מאפשר לסוכן הקיברנטי להיות מוביל טכנולוגי של פורום באינטרנט, ובכך להשפיע באופן רב יותר על המתרחש בו.

הפוטנציאל של יומינט קיברנטי להשפיע ולעצב את המרחב הקיברנטי של היריב הוא רב, ונובע מהאופי האזרחי הפתוח של עידן הסייבר. חשוב להדגיש בהקשר זה כי ארגוני מודיעין רבים פועלים כבר כיום בעולם הקיברנטי, וכי ניתן לאתר דמויות קיברנטיות של ארגונים אלה. הדבר מאפשר ליצור שיתופי פעולה וסינרגיה הדדית עם ארגוני מודיעין זרים בעלי אינטרסים משותפים. במקביל, יש לקחת בחשבון שגורמים עוינים או יריבים יעשו שימוש מניפולטיבי במרחב הקיברנטי וינסו להחדיר באמצעותו "סוכנים קיברנטיים כפולים" ולהזין גופי מודיעין במידע כוזב.

בעולם האזרחי המוביל את הסייבר פותחה דמות ה"אוואטר" (AVATAR), שהינה ייצוג של משתמש בסייבר באמצעות אייקון גרפי בדמות או בדמויות מדומיינות, כמו שחקן בהצגה או בסרט קולנוע. אייקון זה מאפשר לעשות שימוש במספר בלתי מוגבל של זהויות וליצור מצג וכיסויים כמעט לכל תרחיש שייבחר, וזאת בהיקפים גדולים, במהירות וללא צורך במבצעים מורכבים ועתירי משאבים.

המודיעין האמריקאי הזהיר מפני השימוש ב"אוואטרים" לצורכי טרור, דוגמת "אוואטר" של אוסאמה בן לאדן לגיוס המוני של טרוריסטים.[8] רוברט אוהארו, כתב ה"וושינגטון פוסט", המדבר על הפיכתו של שדה הקרב של המרגלים לווירטואלי, נותן כדוגמה "אוואטר" של איש עסקים בעולם המשחקים, ומציין כי אנשי מודיעין מצביעים על הפוטנציאל של "אוואטר" זה לשמש לצורכי טרור ופשיעה.[9]

יש מקום מרכזי להפעלת "אוואטרים" מסוגים ובהיקפים שונים ביומינט הקיברנטי, ובכלל זה להשתמש ב"אוואטרים המפותחים בחברות אזרחיות, כמו סוכן "אוואטר" לבדיקת אמת,[10] מכשיר לבדיקת אמת על בסיס קול[11] ואפליקציות של פוליגרף,[12] לצורכי סיוע בחקירות ובבדיקות מהימנות.

כיווני פעולה לבחינה בקהילות המודיעין

תחום היומינט הקיברנטי משלב בין המאפיינים ההפעלתיים של מודיעין אנושי ובין עולם הסייבר. שילוב זה מזַמן הזדמנויות חדשות ופורץ גבולות, שעולם היומינט המסורתי תחם לעצמו. מוקדם לדעת האם מדובר בדיסציפלינה חדשה, אך יש בשילוב זה מאפיינים חדשים של תפיסה ופעולה המחייבים סינרגיה חדשה בין הסביבה החשאית ובין הסביבה האזרחית־מסחרית. בכך טמון פוטנציאל גדול, הן להשגת מודיעין מקהלים חדשים, בזמנים קצרים יותר ובהיקפים רחבים יותר, והן להשפעה ברשתות החברתיות ובמרחב הסייבר של היריב.

היומינט בעידן הקיברנטי חווה שינוי מהותי, ובראשו כניסה של תת־מקצוע חדש, שהוגדר במאמר זה כיומינט קיברנטי. הסיבה להגדרתו ככזה היא, שלצד הזדקקותו לעקרונות הדומים לעקרונות יומינטיים מסורתיים לצורך הפעלה בתווך הקיברנטי, נוצר כאן מקצוע בעל מאפיינים חדשים, אשר אינו מחייב מגע ישיר עם

המקורות. הבנה זו מחייבת התארגנות בכלל ההיבטים של בניין הכוח המודיעיני, בדגש על תחום הכשרת כוח האדם המודיעיני, אשר לצד רגישות אנושית צריך לסגל לעצמו גם רגישות חברתית.

במאמר זה הצגנו את עקרונות מקצוע היומינט מהתקופה שקדמה לעידן הקיברנטי, כמקצוע מודיעיני־איסופי קלאסי. בהמשך הצגנו את ההתפתחות שחלה במקצוע זה בעידן הסייבר, בדגש על השונות והחדשנות שקיימות בעידן הנוכחי. בחַנו את שאלת הסתירה, לכאורה, שקיימת בין שתי הפנים של מקצוע היומינט – הקלאסי והקיברנטי – והצבענו על שורה של הבדלים ביניהם:

א. ביומינט הקלאסי נדרשים קירבה ומפגש בלתי אמצעי עם המקור. לעומת זאת, ביומינט הקיברנטי ניתן להפעיל מקורות בלי לדעת מה זהותם (עד גבול מסוים).
ב. ביומינט הקלאסי יש מגבלה על היכולת לעבור גבולות. לעומת זאת, ביומינט הקיברנטי ניתן לפרוץ גבולות ולהפעיל מקורות גם בעולמות רחוקים.
ג. היומינט הקלאסי מתמקד באיסוף מידע. ביומינט הקיברנטי ניתן גם להשפיע על דעת הקהל של היריב (באמצעות לוחמה פסיכולוגית).
ד. ביומינט הקלאסי המאתרים הם מוגבלים ויש קושי להשיג מידע על המועמדים לגיוס. לעומת זאת, ביומינט הקיברנטי המאתרים כמעט בלתי מוגבלים ומרבית האנשים מנדבים מידע וחושפים את עצמם מרצונם החופשי.
ה. ההפעלה ביומינט הקלאסי כרוכה בסיכון רב למפעיל ולמופעל. לעומת זאת, הפעלה קיברנטית היא לכאורה בטוחה יותר ואינה כרוכה בסיכון (זאת, למרות שגם הפעלה קיברנטית מותירה חתימות).
ו. בהפעלה הקלאסית המרחב הפיזי של היריב הינו נתון. לעומת זאת, בהפעלה קיברנטית ניתן להשפיע ולעצב את המרחב הקיברנטי של היריב.
ז. היומינט הקלאסי התבסס על מקורות אנושיים ועל מפעילים אנושיים. לעומת זאת, היומינט הקיברנטי מתבסס, לצד ההפעלה האנושית, גם על דמויות מדומיינות בשני הצדדים ועל מכונות היוצרות דמויות המוניות.

בעידן הסייבר התחזקה השילוביות בין הדיסציפלינות האיסופיות. הסייבר והסיגינט מספקים מודיעין ליומינט לצורכי אתירה וגיוס, לנגישות והפעלה ולהזדמנויות מבצעיות, וזאת לצד מטריה מפקחת ומאבטחת לפעילותו. היומינט מספק לסיגינט ולסייבר קצות חוט ו/או מודיעין המאפשר להם ליירט ולנטר באמצעותו מודיעין, וכן נגישות לאפיקי מידע ולמאגרי מידע וציוד קצה שאינם מחוברים לרשת, וכל זאת באמצעות סוכנים מזן חדש.

חשוב שהדיסציפלינה היומינטית בקהילת המודיעין תעקוב אחרי הנעשה בתעשיות ובחברות האזרחיות המובילות את המחקר והפיתוח בתחום הקיברנטי, וגם חודרות לעולם ההפעלה בסייבר,[13] ותתאים את מקצוע היומינט לאתגרי המציאות החדשה. בנוסף, חיוני שקהילת המודיעין תקיים שיח רציף עם התעשיות

והחברות האזרחיות העוסקות בתחום זה. שיח כזה יגדיל באופן משמעותי את יכולות ההתמודדות היומינטיות עם האתגרים שבפתח, משום שלפי הבנתנו קיימות טכנולוגיות ויכולות יומינט משמעותיות שנוצרו במגזר הפרטי, שהמערכת הביטחונית יכולה וצריכה ללמוד מהן, במקום לנסות לפתח את כלל הכלים והשיטות אצלה בבית.

הערות

1 Andrew Shapiro, "Is the Net Democratic? Yes – and No," Berkman Center for Internet and Society at Harvard University, http://cyber.law.harvard.edu/shapiroworld.html

2 Amit Steinhart, "The future is behind us? The human factor in cyber intelligence: Interplay between Cyber-HUMINT, Hackers and Social Engineering," Cyber Guard, 2014, http://diplomacy.bg/archives/1190?lang=en

3 Sun Tzu, The Art of War, Translated by Lionel Giles, XIII: The Use of Spies, The Internet Classic Archives, 1994-2009, http://classics.mit.edu/Tzu/artwar.html

4 מתנדבים מהווים סיכון/הזדמנות, כי טיבם אינו ידוע וכוונותיהם לא נבדקו. אלה יכולים להיות נוכלים ושרלטנים, כאלה הפועלים ממניעים אמיתיים ומגוונים, או כאלה שהם שליחי היריב המתכוונים לחדור לשורותינו כסוכנים כפולים. הם יכולים להפוך לסוכנים הטובים ביותר, ובאותה מידה יכולים להעביר אותנו אל עברי פי פחת. מאמר של החוקרת קתרין ל' הרביג, שפורסם על ידי משרד ההגנה של ארצות הברית, מנתח את השינויים בשיטות הריגול בארצות הברית בשנים 1947–2007:
K.L. Herbig, "Changes in Espionage by Americans: 1947-2007," March 2008, https://www.fas.org/sgp/library/changes.pdf

5 יהושפט הרכבי, **המודיעין כמוסד ממלכתי**, **הספר הגנוז**, הוצאת מערכות, 2015, עמ' 173.

6 Julien Babanoury, "Where does Humint fit in with 21st Century Intelligence Community," September 8, 2014, http://www.secuinsight.fr/2014/03/03/where-does-humint-fit-in-with-the-21st-century-intelligence-community-by-julien-babanoury-ceis/

7 גבי סיבוני, "מודיעין זה לא רק סייבר", **הארץ**, 1 ביולי 2014.

8 Sara Malm, "A threat for the digital age – an avatar Osama Bin Laden: U.S. intelligence warned terrorists could create virtual jihadist to 'preach and issue fatwas for hundreds of years," MailOnline, January 9, 2014, http://www.dailymail.co.uk/news/article-2536440/A-threat-digital-age-avatar-Osama-bin-Laden-U-S-intelligence-warned-terrorists-create-virtual-jihadist-preach-issue-fatwas-hundreds-years.html; David Kravets, "US intel: Bin Laden avatar could recruit terrorists for hundreds of years," Wired, January 9, 2014, http://www.wired.co.uk/news/archive/2014-01/09/osama-bin-laden-avatar

9 Robert O'Harrow Jr., "Spies' Battleground Turns Virtual," *The Washington Post*, February 6, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/02/05/AR2008020503144.html

10 **AVATAR** – Automated Virtual Agent for Truth Assessments in Real-Time, University of Arizona, 2015, http://borders.arizona.edu/cms/projects/avatar-automated-virtual-agent-truth-assessments-real-time

11 Amir Liberman, The LVA (Layered Voice Analysis) Technology, nemesysco, http://www.nemesysco.com/technology-lvavoiceanalysis.html

12 Android apk Polygraph Lie Detector version 1.0 Free Download, 2014, http://appdownload.m5f.net/apk/com.ciberdroix.polygraph.html

13 למשל, חברת מודיעין סייבר ישראלית המפעילה "אוואטרים": https://www.sensecy.com