מודיעין מסכל בארצות המערב והביג דאטה*

ד"ר אבנר ברנע[1]

הקדמה

מערכות מידע של ביג דאטה[2] התפתחו בעולם העסקי משנות ה־2000 ואילך כתוצאה מצורך לטפל באופן יותר אפקטיבי בכמויות המידע העצומות הנאספות על ידי חברות עסקיות, במיוחד בעידן המדיה החברתית. בהמשך, ארגוני מודיעין מסכל[3] (להלן, ממ"ס) כמו גם ארגוני מודיעין בתחומים אחרים, הפנימו את תרומת הביג דאטה לפעילותם. הסיבה הראשית לשיהוי בתגובה היא שמרנות וחוסר היכרות של היכולות המתפתחות בעולם העסקי. האתגרים החדשים בהתמודדות עם סיכול טרור וסייבר דחפו את ארגוני הממ"ס, להטמיע בקרבם מערכות ביג דאטה כדי לשפר את האפקטיביות שלהם. עם זאת, מידע על שימוש שעושה הממ"ס בכלי ביג דאטה כמעט אינו מתפרסם ובכך מקשה על הפיקוח הציבורי על פעולות אלה.

התפתחות השימוש בכלי מערכות מידע מתקדמים בממ"ס

את חמישים השנים האחרונות בתחום הממ"ס (counter intelligence) ניתן לחלק לשלוש תקופות:

- הראשונה, שנמשכה עד שנת 1989, מועד קריסתה של ברית המועצות ושחרור מדינות מזרח אירופה ('ברית ורשה') מהמשטר הקומוניסטי, התאפיינה בכך שהנושא הדומיננטי בתחום הממ"ס היה סיכול ריגול. בתקופת ה'מלחמה הקרה', הקדישו ברית המועצות וגרורותיה במזרח אירופה מאמצים עצומים לאיסוף חשאי בעיקרו של מידע על ארצות המערב בהנחה כי מודיעין איכותי יסייע להן לשפר את היכולות הצבאיות ויתרום לסגירת הפערים הטכנולוגיים מארצות המערב.
- התקופה השנייה היא בשנים 1989–2001, תקופת ביניים, שבה פג האיום הסובייטי, אך טרם הובהר באילו נושאים יתמקדו שירותי המודיעין בארצות המערב.
- התקופה השלישית היא מסוף שנות ה־90 וביתר שאת מאז 9.11 (2001) ועד עתה. אנו נמצאים בתקופה השלישית שבה האיומים המרכזיים הם הטרור האסלאמי ואיומי סייבר. ארגוני המודיעין נדרשים לפתח יכולות חדשות ומשמעויות לסיכול איומים אלה, השונים מהותית ממה שהיה מקובל בתקופה הראשונה שהתאפיינה בריגול קלסי.

התקופה הראשונה במודיעין מסכל: סיכול ריגול

תקופה זאת אופיינה במאבק הבין־גושי בין ארצות המערב בראשן ארצות הברית, לבין ברית המועצות וגרורותיה הקומוניסטיות. באותה עת, קיבל הריגול עדיפות גבוהה אצל שני הצדדים וכך גם הפעילות לסיכולו. עדיין לא היו ברשות הממ"ס כלי מערכות מידע מתקדמים וגם כמויות

*** ראו רשימת המקורות בסוף המאמר**

המידע היו קטנות יחסית בהשוואה להיום. רוב המידע הביטחוני שנאסף הושג בדרכים חשאיות. האיסוף הגלוי בקרב שני הצדדים היה בעדיפות נמוכה יחסית. הגישה המקובלת בקרב ארגוני הממ"ס למידע הייתה במידה רבה אינטואיטיבית,[4] ונתנה עדיפות למידע שהושג בחשאי, ללא בחינה השוואתית של מידע דומה שניתן להשיגו באיסוף גלוי.

חיפוש מידע באופן ידני וכמעט ללא אוטומציה אפיין את אותה תקופה. אז היו לאנשי הממ"ס ספקות ביחס לתהליכי טיפול אוטומטיים במידע שנתפסו כבלתי מדויקים וללא תרומת התבונה האנושית. האתגר היה איתור מידע במאגרי מידע פנימיים של ארגוני המודיעין והיה קושי ניכר לאתר מידע שלא היה שלם בהעדר מערכות אוטומטיות יעילות. לכן, התחום הראשון שאליו נכנסו מערכות מידע בממ"ס, היה זיהוי חד־ערכי של אנשים וארגונים, בעיקר של יעדי הממ"ס, כדי לשפר את ההערכה לגבי מסוכנותם.

בתקופת המאבק הבין־גושי קיבל הריגול עדיפות גבוהה אצל שני הצדדים וכך גם הפעילות לסיכולו. עדיין לא היו ברשות הממ"ס כלי מערכות מידע מתקדמים וגם כמויות המידע היו קטנות יחסית בהשוואה להיום כאשר רוב המידע הביטחוני שנאסף הושג בדרכים חשאיות

באותה עת, מערכות מידע אוטומטיות היו בראשית דרכן, הרבה לפני שאנשי מודיעין חשבו במונחים של ביג דאטה, ולארגוני ממ"ס היה יחס דו־ערכי כלפיהן: מחד גיסא, הורגש צורך בכלים מתקדמים ומאידך גיסא היה חשש ביטחוני מפני חשיפת פעילות הממ"ס במיוחד בפני מומחי מערכות מידע חיצוניים. היה גם חוסר אמון במידת האפקטיביות של כלים אלו. רבים מאנשי הממ"ס האמינו במערכות ידניות ובזיכרון האנושי כאשר כמויות המידע עדיין לא הגיעו לכלל התפוצצות. הגישה השלטת בקרב אנשי הממ"ס הייתה ביטחון מופרז במומחיותם ונטייה לחשוב כי התרומה של מערכות אוטומטיות זניחה.

מי שהוביל את עולם מערכות המידע (אז ועתה), היו חברות מסחריות שפיתחו כלים עבור התחום העסקי בעולם תחרותי. באותה עת היו ארגוני מודיעין שהאמינו כי ביכולתם לפתח בעצמם כלים מתקדמים וגם חששו לחשוף את עצמם, וניסיונות אלה לוו בהשקעות כספיות גבוהות מאוד, ללא הצדקה. מסוף שנות ה־80 חדרה ההכרה שארגוני מודיעין אינם יכולים להתמודד עם היכולות המתקדמות שמפתחות ומובילות חברות מִחשוב בעולם העסקי והדרך הנכונה היא לרכוש כלים אלו ולהתאימם לצורכיהם.

השלב הבא היה התמודדות עם אחזור מידע טקסטואלי. מאחר שלמערכות המידע היו אז יכולות מוגבלות בתחום זה, נעשה שימוש ב'מילות מפתח'. אולם עד מהרה התברר כי 'מילות מפתח' הוא תחום בעייתי מאחר שמספרן הלך וגדל במהירות והיה קושי לבצע אחידות בחיבור בין המידע שהתקבל לבין הכנסת מילת המפתח הרלוונטית. בראייה לאחור, מערכות המידע האוטומטיות של שנות ה־70 וה־80 קידמו את יכולות הממ"ס אך לא עמדו בציפיות לתת לארגונים אלה יתרון

משמעותי על פני יריביהם. עברו שנים רבות בטרם נכנס האינדוקס האוטומטי לעבודת המודיעין שעשה את 'מילות המפתח' לכמעט לא רלוונטיות.

התקופה השנייה במודיעין המסכל: תקופת הביניים

מסוף שנות ה־80 ועד 2001 הייתה תקופת הביניים שאופיינה בקיצוץ משמעותי בתקציבי ארגוני המודיעין במערב, במיוחד במודיעין האמריקאי, והמאמץ המודיעיני עבר ממיקוד בברית המועצות ובגרורותיה למאמץ גלובלי ומבוזר, על פי איומי אד הוק שעלו. קהילת המודיעין האמריקאית נדרשה להיות יותר גמישה בהיענות לצרכים משתנים, שינוי שהתקשו להסתגל אליו[5] גם בארגוני מודיעין מערביים אחרים.

המאמץ המודיעיני הושפע גם ממסקנות שעלו מגישתו של פרנסיס פוקוימה בספרו "קץ ההיסטוריה והאדם האחרון" (1992),[6] שבו העלה את האפשרות כי נפילת הגוש הקומוניסטי לא הייתה עוד מהלך בהיסטוריה האנושית הארוכה של סכסוכים בין השקפות, אידיאולוגיות וצורות משטר, אלא סימנה את קיצה של היסטוריה זו, ומעבר לתקופה שבה השלום והדמוקרטיה הלי־ברלית ישררו בעולם, מבלי שאידיאולוגיה אחרת תקרא עליה תיגר, וסכסוכים בין מדינות יהיו מוגבלים לכיסים נקודתיים. כתוצאה מכך התפתחה הערכה בקרב מקבלי החלטות במערב שבע־תיד יהיה פחות צורך בארגוני ביטחון ומודיעין ובכללם ארגוני הממ"ס. עד מהרה יצא ההיסטוריון סמואל הנטינגטון בתיאוריה שונה לחלוטין וב־1993 הציג את "התנגשות הציביליזציות".[7] הנטי־נגטון ראה בעידן שלאחר ה'מלחמה הקרה' את הציביליזציות ככוח מניע ראשי במערכת היחסים הבין־לאומיים. אולם מאחר שהציביליזציות נבדלות זו מזו בערכיהן ובהשקפותיהן הבסיסיות, צפויה במהרה התנגשות ביניהן ולהערכתו, הכוח המניע להתנגשויות תהיינה הדתות.

למרות אי־הבהירות לגבי כיווני ארגוני המודיעין, החל במקביל להתפתח תהליך אחר - הת־פתחות האינטרנט שהביאה לגידול מהיר בכמויות המידע הגלוי הפתוח לכל. החלה להתחזק הדעה כי המידע הגלוי והזמין יכול לתת מענה טוב גם בתחום הביטחוני-מודיעיני ולהשלים את האיסוף החשאי. עדיין, ארגוני ממ"ס רבים היו במצב של הכחשה לגבי התרומה הפוטנציאלית של האיסוף הגלוי והמשיכו לתת עדיפות עליונה ולעיתים קרובות גם בלעדית, לאיסוף באמצעים חשאיים. יצוין כי בארצות הברית דחפו ועדות המודיעין של הקונגרס להגברת יכולות האיסוף הגלוי עוד משנות ה־90 של המאה שעברה[8] וציינו כי לעיתים קרובות הוא איכותי לא פחות ממידע שהושג בחשאי וכך גם ניתן לצמצם את תקציבי ארגוני המודיעין.[9]

לאחר תום המלחמה הקרה וכניסת האינטרנט החלה להתחזק הדעה כי המידע הגלוי והזמין יכול לתת מענה טוב גם בתחום הביטחוני-מודיעיני אולם ארגוני הביון המשיכו להכחיש את התרומה הפוטנציאלית של האיסוף הגלוי למשימת הממ"ס

בתקופה זו נמשכה ההתפתחות המחשובית של ארגוני המודיעין בכללם הממ"ס, שבהמשך הובילה לשימוש בכלי ביג דאטה, אך האתגרים

ברובם לא נראו מהותיים ועלות המחשוב הייתה עדיין גבוהה מאוד, כך שהכנסת מערכות מידע אוטומטיות נמשכה אך לא בהשקעה גדולה, אף שבתחום העסקי הושגה התקדמות משמעותית בתחום זה. בתחום העסקי היה ברור כי המחשוב הוא המהפכה הבאה למרות התפוצצות בועת 'הדוט קום' בסוף שנות ה־90. התפתחות המחשוב של הממ"ס בישראל, הייתה מהירה יותר מאשר ברוב ארצות המערב בגין הבעיות הייחודיות של ישראל, שעבורהסיכול טרור הפך לנושא מרכזי של הממ"ס מאז 1967, שלא כמו בארצות המערב.

לקראת סוף התקופה השנייה, החלו להתפתח בעולם העסקי עשרות מנועי חיפוש, שפותחו כדי לאסוף מידע מהאינטרנט, וגם יכולות וכלים לסיוע בניתוח מידע והבנת משמעותו באמצעות קישור בין פרטי מידע הנקרא link analysis.[10] אלה פותחו במקור עבור מחקרים במדעי החברה ומדעי המחשב, והיו הבסיס לפיתוח יכולות מחשוב אנליטיות חשובות בהמשך, בעיקר בתחום סיכול הטרור.

המאה ה־21 כנקודת מפנה - התקופה השלישית: סיכול טרור ואיומי סייבר

התקופה השלישית בתחום הממ"ס מתחילה ממתקפת הטרור על ארצות הברית ב־11.9.2011. אם בתקופת המלחמה הקרה התפתח המודיעין בתחום האסטרטגי: התרעות ותחזיות ארוכות טווח[11] ועימו שיפור ניכר ביכולות איסוף[12] וסיכול ריגול, בהמשך ובמיוחד מאז 9.11, היה על הממ"ס להתאים עצמו במהירות למצבים חדשים ולהתמקד יותר בנושאי התרעה טקטיים והתמודדות עם טרור[13] של ארגונים לא מדינתיים שמהווים איום שונה מזה שהמודיעין הכיר. יצוין כי לארגוני המודיעין לקח זמן להתאים עצמם למצב החדש.[14] החל מתקופה זו היה ברור כי סיכול הטרור הופך לאתגר העיקרי של הממ"ס ובהמשך התפתח תחום חדש לגמרי – איומי סייבר (Cyber security). שני נושאים נוספים שהם חלק מהדיסציפלינה של הממ"ס: סיכול חתרנות מדינית וסיכול ריגול נמצאים בעידן זה בעדיפות נמוכה יותר בקרב הממ"ס בארצות המערב.

לאחר 11.9 החלו ארגוני המודיעין במערב במאמץ אינטנסיבי לאיסוף מידע על איומי טרור בתוך מדינות וברמה הגלובלית כדי לסכלם בעוד מועד. הדבר התאפשר כתוצאה ממדיניות "המלחמה בטרור" שלוותה בחקיקה שהקנתה לממשל האמריקאי יכולות ששינו לחלוטין את האיזון בין חופש הפרט לבין אינטרסים ביטחוניים

אחד הלקחים החשובים של 11.9 היה שלא היה חוסר במידע. ועדת החקירה שבדקה את האירועים שקדמו למתקפה[15] הגיעה למסקנה כי בידי המודיעין האמריקאי היה מידע התרעתי איכותי על כוונות ארגון אלקאעדה לתקוף יעדים אמריקאיים בתוך ארצות הברית כולל מועד אפשרי למתקפה זו. הכשל המרכזי של קהילת המודיעין האמריקאי היה חוסר היכולת לגבש תמונת איום ברורה, כתוצאה מכך שלאף

אחד מארגוני המודיעין הרלוונטיים בארצות הברית לא הייתה תמונה שלמה על אודות האיום של אלקאעדה, והמודיעין הרלוונטי היה מפוזר בין ארגוני המודיעין השונים, בעיקר כתוצאה מחוסר שיתוף פעולה רב־שנים ומידור שלא לצורך. הוועדה המליצה על שינוי הגישה לתחומי המידור וביטחון המידע וקבעה סטנדרטים לשיתוף במידע בקהילת המודיעין האמריקאית[16] וכן במסגרת מרכזי היתוך (fusion centers) ברחבי ארצות הברית, המתאמים פעילויות ביטחוניות שונות, בעיקר בסיכול טרור, בין ארגוני המודיעין, המשטרות השונות[17] וארגונים אחרים. העדיפות שניתנה לסטנדרטים האלה על פני ערכים שמרניים של מידור מופרז, ושמירת מידע בלעדית ברשות כל אחד מארגוני המודיעין, היו הבסיס התפיסתי להטמעת כלי מידע מתקדמים ביותר לצורכי הממ"ס: מערכות ביג דאטה.

המודיעין האמריקאי עם ארגוני מודיעין בארצות המערב, החלו במאמץ אינטנסיבי לאיסוף מידע על איומי טרור בתוך מדינות, כולל בתוך ארצות הברית, וכן ברמה הגלובלית, כדי לסכלם בעוד מועד. הדבר התאפשר, בין היתר, כתוצאה ממדיניות חדשה שזכתה לכינוי "המלחמה בטרור" (War on Terror) שלוותה בחקיקה חדשה ומהירה שהקנתה לממשל האמריקאי יכולות ששינו לחלוטין את האיזון בין זכויות האדם וחופש הפרט ובין אינטרסים ביטחוניים של מדינות המבקשות להגן על ריבונותן ואזרחיהן.[18] התפתחו יכולות מתקדמות ביותר בתחום האיסוף האינטרנטי (OSINT) וכן יכולות לניטור מידע כתוצאה מהמעבר למערכות תקשורת דיגיטליות. התוצאה המיידית הייתה כמויות מידע עצומות שנאספו וקשיים רבים בטיפול במידע זה כדי לזהות חשודים ופעילי טרור פוטנציאליים,[19] שחיזקו עוד את הצורך במערכות מידע מתקדמות ביותר.

אדאורד סנודן הדגיש כמה אתגרים לעבודת הממ"ס בהקשר לסיכול טרור: הוא ציין את כמויות המידע העצומות ואת הקושי באגירת המידע. הוא ציין גם את הקושי הגדול לסנן ולמקד מתוך כמויות המידע את היעדים המסוכנים והציג מידע פנימי המצביע על הקשיים להיות אפקטיבי במצב כזה.

באותן שנים עלה גם בתחום העסקי הצורך בשיפור דרמטי של מערכות המידע. עד אמצע שנות ה־ 2000 היו בארגונים עסקיים מערכות מידע מגוונות שכל אחת מהן שירתה גורם מסוים בארגון. לדוגמה, מערכת מידע לצורכי שיווק, מערכת מידע של תחום המכירות, משאבי אנוש, תפעול, כספים וכולי. היה קושי ארגוני בניהול כל אחת ממערכות אלה שלא תקשרו ביניהן והצריכו מיומנויות מיוחדות כדי להפעילן. השימוש במידע שכבר היה במערכות אלה לא היה ממצה, בגין הקושי להפעילן, אך עיקר הבעיה הייתה שמערכות אלה עמדו כל אחת בפני עצמה ובפועל לא אפשרו לארגונים לבצע פעולות חוצות מערכות במטרה לטייב את היכולות העסקיות שלהם. מכאן עלה הצורך בפיתוח מערכות שמסוגלות לטפל בכמויות מידע גדולות בתחומים שונים בארגון על ידי חברות מחשוב מובילות כגון אורקל, IBM, SAS, SAP ועוד, ולפלטפורמות אלה ניתן בהמשך השם Big Data.[20]

הנחת המוצא הייתה כי כלים חדשים אלו שיודעים לטפל במידע מכל סוג, מעבר למידע כתוב (טקסטים), כולל קול, וידיאו, זיהוי מיקומים של יעדים (location intelligence- LI) בעיקר בגין הדיגיטליות של המידע, יסייעו למצות טוב יותר מידע שכבר מצוי בארגונים. ההנחה הסמויה שעמדה בלב פיתוח ושיווק מערכות אלה הייתה כי הן יסייעו לארגונים לקבל החלטות טובות יותר על סמך המידע שמצוי בתוך המערכות הפנים־ארגוניות[21] בתחומי מחקר שיווקי, ניתוח מתחרים, ניהול מערכי הארגון ועוד. חברות מובילות בעולם החלו להתקין מערכות ביג דאטה ובתוך שנים ספורות הפכו מערכות אלו לסטנדרט בחברות גדולות ובינוניות.[22] ההנחה כי מערכות אלו יהפכו ארגונים ל"חכמים" יותר עומדת בבסיס השימוש במערכות אלה כמערכות Business Intelligence – BI[23] וכך נכנס לתחום העסקי המינוח data driven organizations המתייחס לארגונים העושים שימוש נבון במערכות ביג דאטה לפעילותם השוטפת.

בעוד השימוש במערכות ביג דאטה בתחום העסקי נחקר באופן שוטף וניתן ללמוד ממנו על אופן השימוש בכלים אלה ומידת התועלת מהם, כולל גם ביקורת ניכרת על היכולות האנליטיות הלא מספקות של מערכות אלה,[24] מצב השימוש בהן בתחום הממ"ס שונה וכמעט אין על כך מחקר שיטתי. עם זאת, ידוע שארגוני מודיעין כולל ממ"ס הבינו את התרומה האפשרית של כלי הביג דאטה הרבה אחרי שמערכות מתקדמות אלה פעלו כבר בהצלחה בעולם העסקי.[25] הדבר נובע מכמה סיבות: שמרנות והיסוס בכניסה לתחומים חדשים, היכרות לא מספקת של העולם העסקי שבו התפתחויות מהירות של כלים שונים בעיקר בגלל סביבת התחרות וכן חשש ביטחוני של חשיפת מידע רגיש במערכות שעלולות להיות לא מספיק מוגנות ובטוחות, הצורך להתאים מערכות מסחריות של ביג דאטה לצרכים הייחודיים של ארגוני הממ"ס. ידוע שכלי הביג דאטה בתחום העסקי יותר מגוונים מאלו שבתחום המודיעין, כולל הממ"ס,[26] בגלל המגוון הרחב של פעילויות בתחום העסקי.

לפי אדוארד סנודן, שעזב את ה־NSA ב־2013, מערך האיסוף חובק העולם של המודיעין האמריקאי והבריטי[27] שכוון בעיקר למטרת סיכול טרור, עשה כברת דרך ניכרת בתחום הביג דאטה. גילוייו אפשרו הצצה למערכת האיסוף ושמירת המידע הענקית שקמה אחרי 11.9 כולל השימוש בכלי ביג דאטה.[28] סנודן הדגיש שני צדדים לעבודת הממ"ס בהקשר לסיכול טרור: כמויות המידע העצומות שנאספות, והיכולות העצומות באגירת המידע במערכות ביג דאטה ובאחזורו היעיל. הוא ציין גם את הקושי הגדול לסנן ולמקד מתוך כמויות המידע את היעדים המסוכנים והציג מידע פנימי המצביע על הקשיים להיות אפקטיבי במצב כזה. יצוין כי קושי דומה קיים גם במערכות אלה בתחום העסקי.

מקובל לייחס למערכות ביג דאטה בתחום הממ"ס יכולות לקלוט מאות אלפי יחידות מידע בשנייה ובאמצעות שימוש בכלים אנליטיים לבצע ניתוח המצביע על חשודים ולהתריע על אירועי טרור שצפויים להתרחש. אולם ניתוח המצב בתחום העסקי של מערכות ביג דאטה, שהוא פחות מורכב מעולם המודיעין, מראה שכמות הכשלים בניתוח איכותני (ולא כמותי) גבוהה למדי וניתן לשער כי המצב בתחום הממ"ס אינו שונה.[29] מסקנה זו קיבלה חיזוק ניכר מגילויי סנודן שהוסיפו באופן משמעותי לדברים דומים שהועלו לפניו על ידי אנשי מודיעין לשעבר[30] בכך שאיסוף המידע הגיע לסדרי גודל עצומים ולדעת רבים, בלתי סבירים,[31] עם קשיים באפקטיביות של פעילות זו וכן

היבטים אתיים כתוצאה מהיקף האיסוף וחוסר השקיפות בדבר היקפו.[32]

אף שסנודן עצמו לא השתמש במושג ביג דאטה בהקשר לכלי המחשוב שבהם משתמש ה־NSA לאגירת ואחזור המידע, לפי מה שמסר, כולל מצגות מקוריות של ה־NSA שהועלו לאינטרנט, ניתן להבין את השימוש הנרחב במערכות אלה. המושגים שמופיעים במצגות ה־NSA שמסר סנודן: bulk data, dragnet, massive surveillance יותר מרומזים על כך.[33] מגילויי סנודן התפתח גם המושג "Big data and surveillance" שמשמעו שלא ניתן לבצע מעקב (surveillance) יעיל אחר אנשים, קבוצות וארגונים, כולל יכולת לזהות בודדים בתוך אוכלוסיות גדולות, ללא שימוש במערכות ביג דאטה. מושג זה, surveillance, התפתח ונקרא גם actionable intelligence שלפיו ניתן לזהות באמצעות מידע האגור במערכות ביג דאטה בודדים המהווים סיכון ולפעול כנגדם נקודתית.[34] סנודן דיבר הרבה על מושג ה־Metadata שמשמעותו שכדי לזהות חשודים בודדים או קבוצות קטנות יש צורך באיסוף רחב ממדים ממגוון גדול של מקורות שמקורו בדרך כלל בתקשורת.[35] לדוגמה, תוכנה שפיתח ה־NSA בשם "Co-Traveler" המסוגלת לקשר בין טלפונים סלולריים שקשורים לחשודים ולמפות את הקשרים ביניהם ובמידת הצורך לנטר את התקשורת ביניהם. הדברים שסנודן חשף היו ידועים במידה מסוימת גם קודם לכן,[36] אך הוא הציג לראשונה חומרים מקוריים של ה־NSA ובכך נתן לדברים משנה תוקף, כולל הערכות לא רק בדבר היקף הפעולות שנעשו אלא באשר למידת האפקטיביות שלהן. סנודן מסר גם כיצד חברות תקשורת בארצות הברית ביניהן, Apple, Facebook, Google, Microsoft, Skype, Yahoo, YouTube ואחרות, כולל ספקי השירות האינטרנטי (ISP), שיתפו פעולה עם ארגוני המודיעין אף שהיו יכולות שלא לעשות כן, ועד כמה היה שיתוף פעולה בין הממשל לבין ספקי התקשורת מקיף, דבר שלא פורסם לפני כן.

החשיפות של סנודן מלמדות עד כמה נפגעה הפרטיות של רבים מאוד בארצות הברית, בבריטניה וברחבי תבל, בגין ההיקף של הפעולות שנעשו, שבדרך כלל לא היה להן כל קשר לטרור.[37] יובל נח הררי מייחס את הדברים ל"נטייה אוניברסלית זו להגזים בגודל האיום היא בעייתית תמיד, כי היא גורמת לבזבוז משאבים יקרי ערך".[38] על כך התעוררה ביקורת ציבורית גדולה בארצות הברית שהביאה להחמרת הפיקוח הציבורי על ה־NSA של ועדות המודיעין של הקונגרס, וגם לחקיקה שדורשת אישורים מיוחדים שמקשה על ביצוע איסוף מידע גורף כלפי אזרחים חפים מכל חשד.[39] הנשיא אובמה התייחס לנושא ב־2014 כאשר קרא להגנה על הפרטיות - "comprehensive review of Big Data and privacy" בעקבות גילויו של סנודן.[40]

כאשר השימוש בביג דאטה בתחום המודיעין הלאומי, בעיקר לצורכי ממ"ס, הולך וגובר ומשתכללים הכלים שבהם נעשה שימוש, בתחום העסקי מתקיים ויכוח על תרומת הביג דאטה לשיפור היכולות הארגוניות להיות יותר תחרותיים ולהשיג יתרון על פני מתחרים. רוב הביקורת אינה על היכולות הטכנולוגיות של כלי הביג דאטה אלא על מידת הניצול הנכון של מידע שברשות הארגונים. קיימת טענה נפוצה למדי לפיה החברות המפתחות ביג דאטה לא פיתחו כלים אנליטיים טובים שיסייעו בניתוח המידע המתקבל מכלים אלו.[41] כך גם טוענים ג'ונס וסילברז'אן, חוקרים בולטים בתחום מערכות מנהל עסקים ומודיעין.[42] שיפורים שהוכנסו בכלים אלו בשנים

האחרונות, בעיקר בתחום האנליטי יחד עם כניסת מקצועות חדשים בתחום המידע -Data an alyst ו־Data scientist[43] מביאים לכך שהחלה התקדמות בניצול המידע האגור במערכות ביג דאטה עסקיות.[44] כיום לא ניתן לראות פעילות עסקית בתחומי המסחר, הרפואה, הפיננסים, המדיה החברתית וגם במודיעין,[45] ללא מערכות ביג דאטה. אחד מבכירי ה־CIA ציין לאחרונה כי בארגון הוקם אגף Digital Innovation שהוא, לדבריו, "השינוי הארגוני הגדול ביותר בארגון ב־50 השנים האחרונות".[46]

לביג דאטה תרומה חשובה גם בתחום סיכול איומי הסייבר.[47] פיתוח יכולות איסוף גלוי על המדיה החברתית (Socmint) שהיא זירת המודיעין החדשה, מגיע מהמגזר העסקי[48] וממנו זלג גם לתחום הממ"ס, בעיקר בהקשר לסיכול טרור וזיהוי איומי סייבר בעוד מועד, ולא ניתן לטפל בו ללא תרומת מערכות ביג דאטה.[49] נראה כי תרומתן של מערכות אלה בתהליך האנליטי מחייבת שיפור ובינתיים הן מסייעות יותר בעיבוי הערכות שכבר גובשו.[50]

סיכום

המודיעין האמריקאי נע בין ניסיונות רצופים ולא תמיד מוצלחים לתת מענה לאיום ביטחוני לבין תגובות חסרות רסן שמטרתן לתת מענה ביטחוני אד הוק. לדוגמה, כפי שקרה במעצר ההמוני של אזרחי ארצות הברית ממוצא יפני לאחר מתקפת פרל הרבור (1491) מחשש שיהיו בקרבם מי שיעסקו בחבלה וריגול נגד ארצות הברית. לאחר ההלם מאירועי 11.9, התרחשה פעילות איסוף חסרת תקדים על סמך חקיקה מהירה ובלתי מאוזנת, שעלתה ביתר שאת לדיון ציבורי לאחר גילויו של סנודן.[51] כתוצאה מכך, חודד שיח זכויות הפרט והקשר שלו לשיח הביטחוני יחד עם עלייה במשקל שניתן לזכויות הפרט בעידן הדיגיטלי. נדרש מארגוני ממ"ס בארצות מערביות, וגם בישראל, להיות ממוקדים בזיהוי מדויק יותר של האיומים עם פגיעה קטנה ככל הניתן בזכויות הפרט והפרטיות. השיפור שיושג ביכולות האנליטיות של מערכות ביג דאטה והתמקצעות האנליסטים שמפעילים כלים אלו יסייעו ביצירת שינוי זה. עם זאת, לפי המתפרסם בדמוקרטיות מערביות אחרות, גם בישראל יש מקום לדיון ציבורי בדבר האיזון בין דרישות הביטחון לשמירת זכויות הפרט וכיצד דואגים לכך שהכוח הקיים בידי הממ"ס יהיה מבוקר יותר.

מקורות

1 עמית מחקר במרכז לחקר הביטחון הלאומי, אוניברסיטת חיפה. ראש המגמה לסייבר, אבטחה, מודיעין תחרותי וניהול משברים, תכנית MBA, המכללה האקדמית נתניה, בכיר לשעבר בשב"כ.

2 הגדרת ביג דאטה מקורה בתחום העסקי: "Big data is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation".
https://www.gartner.com/it-glossary/big-data
מרק לוונטל מראשי ה־CIA לשעבר הגדיר ביג דאטה כך:
"The ability to amass and manipulate large amounts of data on computers offers, to some, tantalizing possibilities for analysis and forecasting".
https://www.afcea.org/content/big-data-way-%E2%80%A8ahead-intelligence

3 מודיעין מסכל – פעילות מודיעין חשאית שיעדיה הם סיכול טרור, סיכול חתרנות פוליטית קיצונית ומניעת ריגול על ידי מדינות זרות. ביטחון סייבר הופך לחלק מהממ"ס. ראו הגדרה מרחיבה בהוראת ממשלת ארצות הברית: Executive Order 12333, as amended, United States Intelligence Activities: https://www.cia.gov/about-cia/eo12333.html
עוד בנושא זה:
Shulsky, A., & Scmitt, G. (2002). *Silent warfare: Understanding the world of intelligence, Potomac* Books Inc. pp. 99-128.

4 טברסקי, ע' ובהנמן, ד' (2005). שיפוט בתנאי אי וודאות: יוריסטיקות והטיות, בתוך רציונליות, הוגנות, אושר דניאל בהנמן ואחרים, מיה בר הלל, עורכת, אוניברסיטת חיפה. בעניין זה ראו עוד: כהנמן ד' (2013). לחשוב מהר לחשוב לאט, הוצאת מטר, תל אביב, עמ' 136.

5 Marrin, S. (2012). *Improving intelligence analysis: Bridging the gap between scholarship and practice*, London, Routledge.

6 פוקויאמה, פ' (1993). קץ ההיסטוריה והאדם האחרון, הוצאת אורעם, תל אביב.

7 הנטיגטון, ס' (2003). התנגשות הציביליזציות, הוצאת שלם, ירושלים.

8 Best, R., & Cumming, A. (2007). Open source intelligence (OSINT): Issues for congress", *Congressional Research* Service, https://fas.org/sgp/crs/intel/RL34270.pdf.

9 Steele, D. (2008). The open source orogram: Missing in action", International Journal of *Intelligence and Counterintelligence*, Vol. 21. No. 3. pp. 609-619.

10 Barnea, A. (2005). Link analysis as a tool for competitive intelligence, *Competitive Intelligence Magazine*, Vol. 8, No. 4, July-August.
ראו בהקשר להיבטים מודיעיניים אופרטיביים של שימוש ב־Link analysis:
Barnea, A. (2017). The "Lone Wolf" Phenomenon - New challenges in the era of overload of information, *International Journal of Intelligence and Counterintelligence,*.

11 Davis, J. (2007). Intelligence analysts and policy makers: Benefits and dangers of tensions in relationships, in Johnson, L. (Ed.) *Strategic Intelligence: The Intelligence Cycle*, Praeger Security International, New York, pp. 143-165.

12 Fingar, T. (2011). "Analysis in the U.S. Intelligence Community: Missions, Masters, and Methods", in *Intelligence Analysis, Behavioral and Social Scientific Foundation*s, Baruch Fischhoff & Cherie Chauvin, Editors. National Research Council of the National Academics, The National Academies Press, Washington, D.C.

13 **הגדרת טרור לפי מחלקת המדינה של ארצות הברית:** "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."
Byman, D. (2017). Should we treat domestic terrorists the way we treat ISIS? Foreign Affairs, October 3.https://www.foreignaffairs.com/articles/united-states/2017-10-03/should-we-treat-domestic-terrorists-way-we-treat-isis?cid=nlc-fa_twofa-20171005

14 Cavelty, M. & Mauer, V. (2009). Postmodern intelligence: Strategic warning in an age of reflexive *intelligence, Security Dialogue*, vol. 40, No. 2, pp. 123-144.

15 "The 9/11 Commission Report", (2004).http://www.9-11commission.gov/report/911Report.pdf

16 **ראו גם בספרו של היועץ ללוחמה בטרור בבית הלבן ריצ'רד קלארק:**
Clarke, R. (2004). *Against all enemies, inside America's war on terror*, Free Press, a subsidiary of Simon & Schuster.

17 de Castro Garcia, A. Matei, F. & Bruneau,T., (2017). Combatting terrorism through fusion centers: Useful lessons from other experiences? *International Journal of Intelligence and Counter Intelligence*, v.30 #4, 723-742.

18 ב־18 ספטמבר 2001, כשבוע לאחר מתקפת 11.9, אישר נשיא ארצות הברית להשתמש בכוח צבאי נגד האחראים למתקפה זו, כולל אומות, ארגונים ויחידים ברחבי עולם ולאחריו חוקק USA patriot act שנתן הרשאה רחבה ביותר, ללא תקדים בדמוקרטיות המערביות, ליירוט ושיבוש פעולות טרור כולל בתוך ארצות הברית, שזכה בהמשך לביקורת גדולה על הסמכויות האינסופיות כמעט שהוא מעניק לרשויות אכיפת החוק.

19 Lim, K. (2015). Big data and strategic intelligence, *Openbrief*. https://www.openbriefing.org/publications/report-and-articles/big-data-and-strategic-intelligence/

20 ב־1999 השתמשו לראשונה במושג Big Data בספרות האקדמית על אודות מערכות מידע ומשם השם התגלגל למערכות מידע רלוונטיות שהתפתחו בהמשך:
Bryson, S. Kenwright, D. Cox, M. Elsworth, D. & Haimes, R. (1999). Visually exploring gigabyte data sets in real time, *Communication of the ACM*, Vol. 42, Iss. 8, pp. 82-90.

21 Jones, M. & Silberzahn, P. (2013). Three reasons why big data doesn't make you smarter :Lessons from the world of intelligence, Forbes, Feb. 7..https://www.forbes.com/sites/silberzahnjones/2013/04/11/play-it-like-steve-jobs-three-questions-for-business-leaders-to-ask-when-surprise-hits/#27c33ad4765d

22 לפי דוח של חברת הייעוץ מקינזי מ־2011, לכל חברה בארצות הברית שבה מועסקים מעל 1,000 עובדים יש מידע אגור במערכותיה בגודל של כ־200 טרהבייט:
https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation

23 ראוי לעשות הבחנה בין מערכות BI אשר המיקוד שלהן הוא בטיפול במידע הנמצא בתוך ארגונים, לבין המושג Competitive Intelligence – CI שהוא התחום העוסק בניטור איומים וזיהוי הזדמנויות לחברות עסקיות בסביבת התחרות באמצעות איסוף מידע גלוי.

24 Court, D. (2015). Getting big impact from big data. *McKinsey Quarterly*, January. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/getting-big-impact-from-big-data

25 לדוגמה, רק ב־2013 מסר ה־CIA על הסכם שנחתם עם גורם עסקי בנושא cloud computing שהוא הכרחי בתחום מערכות ביג דאטה. http://www.businessinsider.com/cia-presentation-on-big-data-2013-3

26 Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique, *Big Data* & Society, July–December, 1–13.

27 Greenwald, G. (2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. June 6. Available at: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

28 Lyon, 2014 . ב־2015 הודתה שרת הפנים הבריטית דאז תרזה מיי (כיום ראשת הממשלה) באיסוף מידע פרסונלי בהיקפים גדולים מאוד על ידי קהיליית המודיעין הבריטית ודיברה על Bulk power שמשמעותו היא שימוש במערכות ביג דאטה:
Mathieson, S. (2015). How MI5 and MI6 gather your personal data for surveillance, *ComputorWeekly*, 17 June, http://www.computerweekly.com/news/450298621/How-MI5-and-MI6-gather-your-personal-data-for-surveillance

29 Moore, S. (2015). "How to Prevent Big Data Analytics Failures", *Gartner*, December 18. http://www.gartner.com/smarterwithgartner/how-to-prevent-big-data-analytics-failures

30 ראו, לדוגמה, את ספרו של איש ה־NSA לעבר ג'יימס באמפורד מ־2009:
anchor Bamford, J. (2009). The Shadow factory: The NSA from 9/11 to the *eavesdropping on America*, NY, first books.
בעניין זה ראו גם סקירה מקיפה על דמוקרטיה, אתיקה ומודיעין: Konstanopoulos, I. (2016). Democracy and ethics vs. intelligence and Security: From Wikileaks to Snowden, in George Bitros, Nicholas Kyriazis (eds.) *Democracy and an Open –Economy World Order*, Springer International Publishing.pp. 3-24.

31 Jeffreys-Jones, R. (2017). We Know all About You: *The Story of Surveillance in Britain and America*, Oxford University Press.

32 בעניין זה ראו מאמר מקיף על דמוקרטיה, אתיקה ומודיעין: Konstanopoulos, I. (2016). Democracy and ethics vs. intelligence and security: From Wikileaks to Snowden, in George Bitros, Nicholas Kyriazis (eds.) *Democracy and an open economy world order,* Springer International Publishing. pp. 3-24.

33 Sotteck, T. and Kopstein, J. (2013). Everything you need to know about PRISM, The Verge, July 17, https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

34 Gandy, O. (2012). Statistical surveillance: Remote sensing in the digital age. In: Ball KS, Haggerty K and Lyon D (eds) *Routledge Handbook of Surveillance Studies*. London and New York: Routledge, pp. 125–132.

35 Friedman, G. (2014). Keeping the NSA in perspective, *Stratfor*, 22 April, http://www.stratfor.com/weekly/keeping-nsa-perspective.

36 Andrejevic, M. and Gates, K. (2014). Big Data surveillance: Introduction. surveillance & society, 12 (2): 185–196. Ball, K.S. and Snider, L. (eds) (2013) The Surveillance-Industrial *Complex: A Political Economy of Surveillance*. London: Routledge.

37 Brown, M. (2015). "NSA Mass Surveillance: Biggest Big Data Story", Forbes, Aug 25 . https://www.forbes.com/sites/metabrown/2015/08/27/nsa-mass-surveillance-biggest-big-data-story/#578b4e092c13

38 הררי, י' (2009) טרור מהו? מימי-הביניים ועד למאה העשרים ואחת, זמנים, 108, סתיו.

39 Hattam, J. (2016). Spying after Snowden: What's changed and what hasn't, *The Hill*, 15th December, http://thehill.com/policy/technology/310457-spying-after-snowden-whats-changed-and-what-hasnt

40 White House, (2014). "Big Data and the future of privacy". Available at: https://obamawhitehouse.archives.gov/blog/2014/01/23/big-data-and-future-privacy

41 Gilad, B. (2015). "Your Big Data Analytics Can't Save your Company", Academy of Competitive Intelligence, Available at: http://www.academyci.com/2015/01/06/big-data-analytics-cant-save-company/

42 Jones and Silberzahn, 2013.

43 הגדרת המקצוע חדש זה היא בלהלן: A data scientist is a professional responsible for collecting, analyzing and interpreting large amounts of data to identify ways to help a business improve operations and gain a competitive edge over rivals.
http://searchbusinessanalytics.techtarget.com/definition/Data-scientist
ה־CIA פונה באתר שלו ומחפש בעלי מקצוע זה לעבודה אצלו:
https://www.cia.gov/careers/opportunities/science-technology/data-scientist.html

44 ישנם מחקרים רבים בנושא מערכות ביג דאטה, בדרך כלל של חברות הייעוץ המובילות בעולם. כגון מקינזי: (https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/how-companies-are-using-big-data-and-

https://www.accenture.com/t20160106T194441__w__/fi-en/_acnmedia/Accenture/) :Accenture ,(analytics
Conversion-Assets/DotCom/Documents/Global/PDF/Digital_1/Accenture-Global-Operations-Megatrends-
http://www.ey.com/Publication/vwLUAssets/EY_-Big_data:_changing_the_) ,(Study-Big-Data-Analytics-v2.pdf
:וגם מחקרים באקדמיה בגון (way_businesses_operate/%24FILE/EY-Insights-on-GRC-Big-data.pdf
.MacAfee, A. & Brynjolfsson, E. (2012). Big Data: the management revolution, *Harvard Business Review*, October
45 קצין הטכנולוגיה הראשי (CTO) של ה־CIA, Ira Hunt, התייחס ב־2012 לנושא זה באתר האינטרנט של ה־CIA והצביע על האתגר
של הארגון בגיוס אנליסטים לתחום הביג דאטה. -https://www.cia.gov/news-information/featured-story-archive/2012
featured-story-archive/big-data-at-the-cia.html
46 Konkel, Frank. "How the CIA Is Making Sense of Big Data." Nextgov, 16 Mar. 2016.
http://www.nextgov.com/big-data/2016/03/how-cia-making-sense-big-data/126722/

47 O'Brien, S. (2017). Challenges to cyber security and how Big Data analytics can help, *Datameer*, May 4, https://
www.datameer.com/company/datameer-blog/challenges-to-cyber-security-and-how-big-data-analytics-can-
help/
48 Scaachi, M. (2017). Competitive intelligence and unstructured Data, *Competitive Intelligence* Magazine, Vo. 20,
.No. 1, Spring
49 Murdock, J. (2017). Spies in the age of social media: Ex-CIA experts reveal challenges of modern espionage,
International Business Times, July 19, http://www.ibtimes.co.uk/spies-age-social-media-ex-cia-experts-reveal-
challenges-modern-espionage-1631042
50 .Lim, 2015
51 העיתון 'ניו יורק טיימס' יצא בינואר 2014 במאמר מערכת שבו קרא לראות בסנודן חושף שחיתויות (rewolbeltsihw) בגלל
גילוייו החשובים, והציע לאפשר לו לחזור לארצות הברית ולקבל חנינה: sptth://www.semtiyn.moc/4102/10/20/noinipo/
lmth.rewolb-eltsihw-nedwons-drawde