



מרכז בגין-סאדאת למחקרים אסטרטגיים

הסוד הבלתי מסווג

מאת ד"ר נתנאל פלמר וסא"ל (מיל') ארז מגן

מבט מבס"א, מס' 2,238, 26 בנובמבר 2023

תקציר: מתקפת חמאס ב-7 באוקטובר התבססה על מודיעין שחלק מרכזי ממנו הוא מידע אזרחי או מידע צבאי שאינו מסווג בהכרח. המאורע משקף תופעה רחבה בהרבה שמוגדרת במאמר כ"סוד הבלתי מסווג" - מידע שאינו מוגדר כמסווג, אך בפועל הוא ערכי, לפעמים מאוד, לאויב. על בסיס הגדרת התופעה, מנותחים קווים ראשוניים להתמודדות עמה, שהיא מורכבת שכן בשל היותו של המידע גלוי או זמין לאיסוף, הוא דורש התייחסות מיוחדת שמאזנת בין היבטים דמוקרטיים של חופש המידע וזכות הציבור לדעת לבין צרכי ביטחון.

בבסיס תפיסת אבטחת המידע וההגנה בסייבר של כל ארגון מתקדם קיים מנגנון לניהול סיכונים, שמשקלל בין הסבירות להתממשות איום מודיעיני וטכנולוגי לבין עוצמת הנזק כתוצאה מדלף מידע. ניהול הסיכונים מאפשר להתמקד בהגנה על נכסים משמעותיים ולהבטיח, ככל שניתן, שהתממשות האיומים על אלו לא תצלח. האלטרנטיבה הפחות טובה היא "להגן על הכל", דבר שיבטיח חוסר אפקטיביות בשל מרחב יריעה אין סופי ומשאבים מוגבלים.

מאמר זה מבקש לתאר תופעה אותה אנו מכנים "הסוד הבלתי מסווג", כלומר מידע שהוא בלתי מסווג בהגדרתו, אך עדיין יש בו ערכיות לאויב שמבקש לעשות בו שימוש כדי לפגוע במדינה או בגוף נגדה הוא נלחם. בחברה דמוקרטית ופתוחה חופש המידע וזרימתו הם יסודות בסיסיים. היכולת של אנשים בחברה להחליף מידע ולשתף אותו חיונית כדי לאפשר לחברה להתקדם ולהתפתח, כמו גם לתת את התשתית לאזרחים להיות מעורבים, לפקח על רשויות השלטון, לבקר אותן ולגבש דעה עצמאית מתוך בחירה חופשית ומושכלת. באופן זה, מידע אזרחי, או מידע ביטחוני שהוגדר כבלתי מסווג, נגישים לעין הכל – במיוחד ככל שהפלטפורמות להפצתו ולהנגשתו הולכות ומתפתחות. למידע זה נגישים לא רק אנשי המדינה, אלא גם גורמים מבחוץ, לרבות אויביה.

אירועי ה-7 באוקטובר עוד יחקרו ויבדקו, אך כבר כעת ניתן לומר כי חמאס החזיק בתמונת מודיעין טובה על מרכיבי ההגנה של מדינת ישראל שעל גדר הגבול - דבר שאפשר לו לנטרל חלק מהסנסורים ויכולות הגילוי, למנוע יכולת לשלוט באירועים וכן לפעול באופן אפקטיבי בתוך הבסיסים, המוצבים והיישובים אליהם חדרו אנשיו. לצד המידע הצבאי, היה ברשות חמאס מידע אזרחי, פרטי ומנהלתי שאפשר לו לממש את כוונותיו ולפעול בצורה אפקטיבית בתוך היישובים שתקף. מלבד מפות שזמינות לעין כל, ניכר כי לחמאס היה מידע על אתרים מסוימים בתוך היישובים, אשר חלקו ניתן לאיסוף ברשת האינטרנט (דוגמת כתובות של בכירים) וכן מידע אשר ניתן לאסוף בהפעלה

אנושית (יומינט) של אזרחים ללא נגישות צבאית, כמו מיקום כיתות הכוננות, מוקדים מרובי חיילים ואזרחים, מעטפת ההגנה של היישובים ועוד.

התבוננות על המידע הביטחוני על ישראל שנאסף על-ידי חמאס לאורך השנים, יגלה שחלק משמעותי מהצי"ח - ציון ידיעות חשובות - של חמאס, הינו על מידע שאינו מסווג בהגדרה. למשל, מרבית גורמי האיסוף האנושי (יומינט), אשר גויסו על-ידי חמאס לאסוף מידע התבקשו "לדקור" איתורים ברחבי ישראל, כאלה שכל אזרח יכול לראותם בעין בלתי מזוינת. מידע שנאסף על-ידי חמאס מהתקשורת הישראלית כלל מידע רב על החברה הישראלית, על סוגיות הנוגעות למרחב עוטף עזה, ואמצעי לחימה שמידע על אודותם פורסם באופן רשמי.

עובדה זו מציפה תופעה מאתגרת במיוחד, אותה אנו מבקשים לכנות כ"סוד בלתי מסווג". מדובר במידע אזרחי או כזה שהוגדר על-ידי הגורמים המוסמכים לכך כבלתי מסווג, אך הוא ערכי לגורמים חורשי רעה שאוספים אותו לצרכיהם. כשמדובר בארגון טרור כמו חמאס ובמתקפה כמו זו שהוציא אל הפועל - מידע טקטי ומיקרו-טקטי שחלקו מוגדר כבלתי מסווג, כמו גם מידע אזרחי שהוא בהגדרה חשוף לעין כל - הופכים להיות ערכיים ביותר, במיוחד כשהפרטים מצטרפים לתמונה שמשלים אותה איסוף ממקורות מודיעיניים שאינם גלויים, אותם מפעיל חמאס או כל ארגון אחר. במיוחד במקרה של ארגון טרור, שמידע אזרחי שנתפס לעיתים כזניח הוא ערכי עבורו ביותר - המרחב הבלתי מסווג מכיל "סודות" שנדרש להתייחס אליהם.

בנקודה זו הייתה יכולה לעלות הטענה: אם מדובר במידע שהוא ערכי עבור האויב, מדוע הוא מוגדר כ"בלתי מסווג"? למעשה, השאלה העמוקה יותר שמתעוררת היא עד היכן ניתן למתוח את הגדרת המושג "מידע מסווג". סיווג מידע מבטא את פוטנציאל הסיכון והנזק כתוצאה מחשיפתו לגורם בלתי מורשה, וכנגזרת ההגדרה הבסיסית של המושג היא מידע שהגעתו לידי גורם שאינו מוסמך עשויה להביא לנזק לביטחון המדינה או יישות אחרת שמחזיקה בסוד. אך נזק לביטחון המדינה באיזה מובן? לצורך העניין, מפות ישראל ב-Google Earth, בתרחיש של פשיטת מחבלים על יישובים הן מידע ערכי עבור המחבלים. נדמה שברור לכל בר דעת שלא ניתן, בגלל הפוטנציאל של המידע הזה להוות תשתית למתקפת טרור, להסיר אותו מרשת האינטרנט.

הקיצון השני, הוא להגיד שהסוד הבלתי מסווג הוא גזירת חיים של חברה דמוקרטית ופתוחה, בעיקר במרחבי סיכון ובסמוך לקו גבול עוין, ושאינו שום דבר שניתן לעשות כדי לצמצם את הסיכון שבתופעה. למול שתי עמדות הקיצון, אשר נראה כי האמת המלאה לא נמצאת באף אחת מהן, נכון להגדיר כמה עקרונות מובילים במציאות שבה מתקיימת בצורה נרחבת התופעה של הסוד הבלתי מסווג, אך כזה שיש בו ערך ביטחוני לאויב.

הסוד הבלתי מסווג נדרש להיות נדון ברמה המערכתית בהקשרי השפעות המידע האזרחי על מרכיבי הביטחון המאפשרים לאויב ניצולם למטרות מבצעיות בעלות משמעויות למערכת הביטחון. המרחב ה"בלתי מסווג" נדרש לקבל מענה במסגרת הערכות המצב, תוך הפנמת ערכו לצד השני.

לאור כך, נכון להתייחס ל"סלי מידע" אזרחי בהם נדרש להשקיע בהגנה, פיקוח ובקרה, וביניהם:

- מרכיבי ביטחון אזרחיים - כיתות כוננות, יחסי גומלין מול הצבא ומערכת הביטחון, מעטפת ההגנה האזרחית על יישובים, תגבורי כוחות בעת אירוע.
- מוקדים הומי אדם שיכולים לשמש יעד מרכזי לתקיפה - קבועים וארעיים (תחנות תחבורה ציבורית, אולמות אירועים, פארקים וכו').
- כתובות מגורים של גורמים בכירים, גורמים מבצעיים, מנהיגים מקומיים וכו'.
- משטחי תקיפה טכנולוגיים (אתרים, שרתי אחסון, מצלמות וכו') במרחב האזרחי.

בתוך כך, המגמה צריכה להיות צמצום קלות ההשגה של מידע אזרחי שאינו חיוני, כגון: הגנה על מאגרים בהתאם לתקני הגנת הפרטיות, הגדרת קהלי יעד האסורים בחתימה רשתית גבוהה על אודות פרטים אישיים, ניטור חריגות ומתן התרעה לשם מניעה והפחתת נזק וכן החלת צנזורה על חריגות. גם בהקשרי מידע צבאי שמפורסם, לאור צרכים שונים, על-ידי גורמי הביטחון, נדרשת חשיבה מחודשת על נקודת האיזון, שכן במקרים רבים המידע הופך להיות "סוד בלתי מסווג", כלומר מידע שאושר לפרסום אך מועיל לאויב.

לשם המחשה, בהקשר האיום האנושי למשל, אל מול תרחיש שבו חמאס מתאמן ומצהיר בפומבי במשך שנים על כוונתו לתקוף את היישובים בעוטף עזה – צריכה להביא לחשיבה מחדש על מניעת אפשרות שפועלים מרצועת עזה, או כאלו בעלי פוטנציאל לקשר לגורמי כח ברצועת עזה, יעבדו ביישובים אלו ויקבלו גישה ל"סוד הבלתי מסווג". באופן דומה, נדרשת עירנות יתר לגבי פעילות איסוף של אזרחים בסביבת אתרים ביטחוניים והומי אדם.

מטבע הדברים, הממשק בין המרחב הביטחוני לבין המרחב האזרחי ובין המרחב הלא מסווג לבין הסוד, מציב אתגר גדול לשם מתן מענה הולם ומאוזן לאיום הנשקף מהסוד הבלתי מסווג. לפיכך, גיבוש מרכיבי הביטחון בהקשר זה מורכבים ודורשים קשב, הקצאת משאבים, חקיקה ושיתוף פעולה רב מערכתי. הצורך לשמור על חופש מידע מירבי, אך גם להכיר באילוצי ביטחון, שמלווה דמוקרטיה בעולם כולו, וביניהן ישראל, ימשך ללוות אותנו, תוך שהאתגר ילך ויתעצם.

נכון לומר שגם אחרי גיבוש קווי המדיניות ומימושם, הנחת העבודה הסבירה היא שהאויב יחזיק במידע ערכי. לכן יש להתייחס בכל היערכות ותפיסת הגנה, מבצעית או אזרחית, למטען הידע שיש לצד השני גם בנושאים שאינם מסווגים בהגדרה אך יכולים לשרתו. בהתאמה, נדרש מענה הגנתי או התקפי משלים. המערכה על הסוד הבלתי מסווג כאן כדי להישאר.

ד"ר נתנאל פלמר הוא מרצה בכיר במחלקה ללימודי המזרח התיכון באוניברסיטת בר-אילן וחוקר בכיר במרכז בס"א. חוקר מודיעין, טרור ומערכות א-סימטריות במזרח התיכון. סא"ל (מיל') ארז מגן הוא מומחה אבטחת מידע והגנת בסייבר, מייסד Magen Cyber אשר מספקת לגופי ביטחון וחברות בארץ ובעולם פתרונות הגנה.