על מיקור חוץ בקרב סוכנויות המודיעין וגופי הביטחון: סיכון המוביל לעלייה בתפוצת נשק הסייבר?

עמרי וקסלר

תקריות רבות של דליפת חומרים מסווגים השייכים לסוכנויות מודיעין הובילו לטענה כי עובדי קבלן העובדים עבור סוכנויות המודיעין והביטחון מוּעדים לפורענות וכי הם הסיבה לתקריות אלו בשל חוסר נאמנותם או היותם לוקים ברשלנות. לצד זאת, דליפות של מידע מסווג, שכללו רכיבים ותוכנות פריצה, הובילו לשאלה האם האיום הפנימי בקרב סוכנויות המודיעין והביטחון מוביל גם להגברת התפוצה של נשק סייבר מתוחכם ולהעברתו לידיהם של שחקנים שאינם בעלי יכולת לפתחו מלכתחילה. מקרה בוחן בולט מהשנים האחרונות הוא דליפתו של רכיב הפריצה EternalBlue של הסוכנות לביטחון לאומי (NSA) של ארצות הברית, והשימוש בו לצורך התפשטותה של מתקפת הסייבר הגלובלית WannaCry, שפגעה במחשבים ב־150 מדינות ויוחסה לצפון קוריאה. הבנת האיום הפנימי והקשר שלו לתפוצת נשק סייבר, לצד פירוט היתרונות והחסרונות של העסקת חברות קבלן, הינם חיוניים לצורך מזעור האיום וההתמודדות איתו, ובדרך זו למניעת פגיעה בביטחון הלאומי והידרדרות נוספת של היציבות במרחב הסייבר.

מילות מפתח: מיקור חוץ, תפוצת נשק סייבר, מודיעין, חברות קבלן, ביטחון מידע.

מבוא

רבות דובר על החסרונות שבמיקור חוץ ובהפרטה של פונקציות ושירותים ביטחוניים לא קיברנטיים, ביניהם בעיות אתיקה ואחריות הנובעות מהעברה לידיים פרטיות

עמרי וקסלר הוא ראש מוקד מחקר סייבר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון ובמרכז למחקר סייבר בינתחומי ע"ש בלווטניק, אוניברסיטת תל אביב.

של הסמכות לעשות שימוש בכוח. מספר תקריות של הדלפת חומרים מסווגים, שחלקן הסתיימו בזליגה של קודים לתוכנות תקיפה, הביאו בשנים האחרונות לשורה של התבטאויות מצד בכירים בארצות הברית, שהדגישו את הסכנה הנובעת מהעסקתם של עובדי קבלן בענפים ביטחוניים רגישים, בכללם ענף הסייבר.

מי שהיה ראש ה־CIA ושר ההגנה של ארצות הברית, ליאון פָּנֶטָה, אמר לאחר דליפת ה־Vault 7, שכללה קודי מקור של כלי פריצה של ה־CIA, כי השימוש בעובדי קבלן טומן בחובו סיכונים וכי ייתכן שלעובדים אלה אין את אותה נאמנות לארגון שיש לעובדיה הקבועים של הסוכנות.[1] הסנאטור הרפובליקני בן סס (Ben Sasse) טען, לאחר דליפה נוספת, כי על ה־NSA לפתור את בעיית ההדלפות שמקורה בקבלנים של הסוכנות.[2] התבטאויות אלו מצביעות על כך שעובדי קבלן בסוכנויות המודיעין האמריקאיות נתפסים כבעייתיים יותר מאשר עובדי הממשל הקבועים.

הנחת היסוד של מאמר זה היא שקיים קשר בין תופעת מיקור החוץ והשימוש בחברות קבלן ובין הדלפות הגורמות להגברת התפוצה של נשק מתוחכם. מטרת המאמר היא להציע דרכים להתמודדות עם סיכון זה ולמזעור השלכותיו.

השימוש בקבלנים, שאינם חלק מצבא סדיר ואינם נמנים על אנשי השלטון או הממשל, לצורך מילוי תפקידי לוחמה או ריגול, אינו חדש, ומקורו כבר בעת העתיקה. תופעת מיקור החוץ לתפקידי לוחמה, איסוף מודיעין, לוגיסטיקה, פיתוח אמצעי לחימה, אבטחה וייעוץ, הייתה נורמה לכל אורכה של ההיסטוריה הצבאית הגלובלית. תופעה זו הולכת ומתרחבת כיום. דוגמה לכך ניתן לראות במלחמת עיראק השנייה (2003), כאשר לצד 165,000 חיילים אמריקאים, נשלחו גם כ־200,000 עובדי קבלן הנמנים על חברות פרטיות.[3]

עם הופעתו של הסייבר והפיכתו לזירת לוחמה ואיסוף מודיעין, החלה תופעת מיקור החוץ להתפשט גם לתחומי הסייבר. את הסיבות לצמיחתה של תופעת מיקור החוץ בתחומי איסוף המודיעין, פיתוח נשק הסייבר וביצוע מבצעי סייבר ניתן לייחס לקיצוצים בכוח אדם ובתקציבים ולהתקדמות הטכנולוגית המהירה בתחום טכנולוגיות המידע והתקשורת במגזר האזרחי – דבר שהֵקנה לשוק הפרטי יתרון טכנולוגי מובהק על פני ממשלות. הדלפות של נשק סייבר, בין אם כתוצאה מרשלנות ובין אם בזדון, עלולות להוביל לכך שנוזקות מתקדמות, המגיעות לידי

1 Andrea Mitchell and Ken Dilanian, "Wikileaks Release already Damaging U.S. Intelligence Efforts", *NBC News*, March 10, 2017, https://www.nbcnews.com/news/us-news/wikileaks-release-already-damaging-u-s-intelligence-efforts-n731531.

2 Eric Geller and Cory Bennet, "NSA Contractors Back in Spotlight after Reported Russian Theft", *Politico*, May 10, 2017, https://www.politico.com/story/2017/10/05/nsa-contractors-russia-hackers-surveillance-tools-243509.

3 Alan Axelrod, *Mercenaries: A Guide to Private Armies and Private Military Companies* (Thousand Oaks, California: CQ Press, 2014), pp. 3-8.

מדינות עניות או בעלות יכולת טכנית נמוכה, ארגוני טרור או גורמים עבריינים, יעברו הסבה מחדש ויקנו לתוקפים אלה יכולות מתקדמות שלא היו ברשותם לפני כן.[4]

מאמר זה מתמקד במקרים של הדלפת תוכנות פריצה ונשק סייבר מהשנים האחרונות, שייתכן והובילו לעלייה בתפוצה של נשק זה, ובוחן האם ניתן לקשור הדלפות אלו לחברות הקבלן. המאמר בוחן האם תוכנות או קודים נגנבו, נמכרו ללא אישור או דלפו, והאם הם עלולים לשמש לאחר מכן לצורך מתקפות. כמו כן בוחן המאמר מקרי רשלנות שבהם היה פוטנציאל לגניבה או להדלפה של רכיבים שעלולים לשמש לצורך מתקפות. לפיכך, תפוצה של נשק סייבר מוגדרת בו כ"מכירה מטעם גורמים לא מורשים, גניבה או הדלפה של רכיבי פריצה, מידע על חולשות יום־אפס וקודים זדוניים, אשר גרמה או עלולה לגרום באופן פוטנציאלי להגעתו לידי שחקנים אחרים".

המאמר מסביר את תופעת מיקור החוץ בקרב קהילת המודיעין ועושה זאת באמצעות התמקדות בקהילת המודיעין האמריקאית, וכן בוחן את יתרונותיה וחסרונותיה של תופעה זו. מטרת המאמר אינה לפסול את תופעת מיקור החוץ, שכן מתברר כי גם מוסדות ממשלתיים נפרצים, מה שמאפשר גניבה או הדלפה של נשק סייבר או חומרים מסווגים גם מארגונים השייכים לממשלה.

מטרה נוספת של המאמר היא להגביר את המוּדעוּת לצורך בפיקוח ממשלתי ובהטלת אחריות על גופי ממשלה, או על חברות פרטיות הפועלות עבור ממשלות. המאמר טוען כי פיקוח, שמירה על נהלים, הטלת אחריות ורגולציה, לצד עזרים טכנולוגיים, יוכלו לסייע לגופי ממשל לפקח על עובדי הקבלן. עוד טוען המאמר כי תמריצים כלכליים יכולים לסייע לחברות הקבלן לשפר את אבטחת הסייבר שלהן ולעודד אותן להעניק הכשרות בהיגיינת סייבר לעובדיהן ולפקח טוב יותר על פעילותם.

תופעת מיקור החוץ בתחום המודיעין ויכולות הסייבר ההתקפיות מוצאת ביטוי במספר מישורים. במקרים רבים מתקיימת הפרטה של פונקציות מחקר ופיתוח לצורך קבלת גישה לטכנולוגיה מתקדמת ופיתוח מהיר של אמצעי לחימה. במקרים אחרים קיימת הפרטה של מִבצעי סייבר, המאפשרת לממשלות מרחב הכחשה ויכולת להסיר מעצמן אחריות מרגע זיהוי מקור המתקפה ולהימנע בדרך זו מנזק תדמיתי או מתגובת נגד. יש להבחין בין מיקור חוץ של מִבצעים ולוחמת סייבר ובין הפרטה המתרחשת במדינות המערב הכוללת פעילויות תמיכה במִבצעים, כגון מחקר, פיתוח, איסוף ועיבוד מידע.

---

4 דניאל כהן ואביב רוטברט, "תפוצת נשק קיברנטי במרחב הסייבר", **צבא ואסטרטגיה**, כרך 5, גיליון 1, אפריל 2013, עמ' 49.

מקרים רבים שהתרחשו בשנים האחרונות, בהם נגנבו כלי פריצה, נוזקות ותוכנות רוגלה ממחשבים של עובדי סוכנויות המודיעין וגופי הסייבר או חברות הקבלן, לצד התבטאויות ודיון נרחב סביב תפקידן של חברות הקבלן, מדגימים את הסיכון הפוטנציאלי הקיים בהפרטה של פעילויות תמיכה במבצעים. דוגמאות מהעולם הפיזי מצביעות על האפשרות שמגמת ההפרטה בתחום הסייבר עלולה לזלוג גם לפעילויות המוגדרות "ממשלתיות בלבד", כגון ביצוע מבצעים התקפיים במרחב הסייבר, אפילו בקרב ממשלות במערב.

מיקור חוץ והפרטה של שירותי מודיעין וסייבר – מסגרת תיאורטית

חלק זה של המאמר מציע מסגרת תיאורטית הכוללת את היתרונות והחסרונות של מיקור חוץ של פונקציות ופעולות השמורות לגופי הסייבר והמודיעין, תוך שהוא עושה שימוש בדוגמאות הלקוחות מקהילת המודיעין וגופי הסייבר בארצות הברית. מיקור החוץ בתחום הסייבר הוא חלק מתופעה נרחבת יותר של מיקור חוץ בתחומי המודיעין והביטחון. חשוב לציין כי ממדי התופעה שונים ממדינה למדינה ותלויים לרוב בהקשר היסטורי ובתרבות הארגונית. עם זאת, ישנם מספר יתרונות וחסרונות מובנים לתופעה זו, שראוי לקיים עליהם דיון.

מדוע מפריטות ממשלות שירותי מודיעין וסייבר?

תקציב וכוח אדם

מיקור חוץ היא פרקטיקה שנועדה, בראש ובראשונה, להגביר את יעילות הארגון תוך הפחתת עלויות. התמריץ להוציא פעילויות מידי הארגון ולהעבירן לחברות או לעובדים חיצוניים התבסס על המחשבה שארגונים אינם יכולים לבצע את כל פעולותיהם באופן מיטבי, ועל כן, כדי להגביר את היתרון התחרותי שלהם, עליהם להתמקד בפעולות הליבה שלהם ובמה שהם מצטיינים בו ולמסור את כל הפעולות שאינן ליבה לחברות חיצוניות.[5]

התיאוריה של מיקור חוץ מתייחסת גם אל תחום המודיעין והסייבר. אמנם, ארגוני מודיעין אינם צריכים לשמר יתרון תחרותי בשוק, ולכן במקרה זה מיקור החוץ משמש בעיקר להפחתת עלויות ולייעול. זאת ועוד, מיקור החוץ וההפרטה של פיתוח אמצעי לוחמת סייבר הפכו לשיטת התמודדות עם קיצוצים בתקציבים של גופי המודיעין ועם מחסור בכוח אדם. בעיית המחסור בכוח אדם עלולה לנבוע מקיצוצים בתקציב, ממכסות וממגבלות כוח אדם המוטלות על ידי הגופים

5 Ian McCarthy and Angela Anagnostou, "The Impact of Outsourcing on the Transaction Costs and the Boundaries of Manufacturing", *International Journal of Production Economics* 88 (2004): 62.

המפקחים על גופי המודיעין, מעזיבת כוח אדם מיומן לטובת השוק הפרטי, או משילוב של כל השלושה. קיצוצים במשאבים או בכוח אדם מובילים לכך שגופי המודיעין נאלצים להעסיק פחות כוח אדם פנימי ואינם יכולים להציע שכר גבוה כדי למשוך כוח אדם מוכשר ומיומן. מצב זה מביא להקמת חברות פרטיות המסוגלות להציע תנאי העסקה גבוהים, אשר מתורגמים לגיוס כוח אדם איכותי.

דוגמה לצורך בהתמודדות עם קיצוצי כוח אדם ותקציבים ניתן לראות במקרה האמריקאי: תום המלחמה הקרה ונפילת הגוש הסובייטי הביאו לכך שהיריב העיקרי שמולו נבנה מערך המודיעין האמריקאי העצום במשך מספר עשורים התפרק. בעקבות זאת נתקלו גופי המודיעין בקיצוצי תקציבים נרחבים ונאלצו לפטר עובדים רבים ולהוציא אחרים לגמלאות. הקיצוצים בתקציבים ובכוח האדם של גופי המודיעין האמריקאיים בשנים 1990־1995 עמדו על כ־16 אחוזים מהתקציב וכ־20 אחוזים מכוח האדם של קהילת המודיעין כולה. מבין כל סוכנויות המודיעין האמריקאיות, ה־NSA ספגה את הקיצוצים המשמעותיים ביותר: כשליש מתקציב הסוכנות קוצץ בשנים אלו, וגרר אחריו קיצוץ בשיעור דומה במצבת כוח האדם שלה. למרות זאת, תוך זמן קצר צצו אתגרים חדשים ושלל איומים גלובליים בפני גופי המודיעין של ארצות הברית, ובהם החשש מפני זליגה של נשק גרעיני מהמדינות הפוסט־סובייטיות החדשות, לצד תופעות של סחר בסמים, פשע מאורגן, טרור וסכסוכים אתנו־פוליטיים.

יכולת התמודדות עם עליה חדה בפעילות (Surge capacity)

מיקור חוץ מתגלה כפרקטיקה יעילה להתמודדות עם מצב אפשרי של חוסר התאמה בין מבנה הכוח בסוכנויות המודיעין, ומאוחר יותר בקרב גופי הסייבר בתוך מערכת הביטחון, ובין הדרישות המבצעיות הנובעות ממספר המטרות או האיומים. מיקור חוץ מאפשר גמישות ויכולת להפנות כוח אדם מיומן ומשאבים כדי לכסות לפי הצורך כמות גדולה של איומים בו־זמנית.[6] הצורך בגמישות הינו תוצר של התפתחות סביבת האיומים על הביטחון הלאומי והופעתם של תרחישים שונים שחרגו מההתמקדות בעימותים בין מדינות ועסקו בסוגיות כגון טרור, תפוצת נשק להשמדה המונית, ארגוני פשע בין־לאומיים, רצח עם, עימותים על רקע אתני, ובשנים האחרונות גם איום הסייבר.[7] הצורך בגמישות תקף גם לעידן הסייבר: מוצרים חדשים בשוק, כגון מערכות הפעלה, מכשירי טלפון ניידים ואפליקציות

6 Glenn James Voelz, *Managing the Private Spies: The Use of Commercial Augmentation for Intelligence Operations* (Joint Military Intelligence College, 2016), p. 2.

7 Bruce Berkowitz and Allan Goodman, *Best Truth: Intelligence in the Information Age* (New Haven and London: Yale University Press, 2010), pp. 51, 56.

חדשות, מחייבים התמקדות בחיפוש ובמחקר של חולשות אבטחה ושל תוכנות המנצלות אותן.

שינויים טכנולוגיים מהירים בתחום התקשורת והמידע

גורם נוסף המקנה יתרון לשוק הפרטי הם השינויים המהירים בטכנולוגיית המידע והתקשורת, המעניקים יתרון משמעותי ליכולות העיבוד והניתוח של שוק זה ושל החברות המסחריות. מאז שנות השבעים של המאה העשרים, ובאופן הולך ופוחת עד תחילת שנות התשעים, רווחה בקרב גופי מודיעין האמונה שלממשלות יש את הגישה הטובה ביותר למחקר ולפיתוח של טכנולוגיות מתקדמות ולפיתוח מערכות איסוף וניתוח. אמונה זו הלכה ונשחקה ככל שמידע הפך להיות זמין וזול יותר.[8]

החיבור לאינטרנט והנגישות הגוברת אליו מאז שנות התשעים הובילו לצמיחה חדה ומעריכית במספר המשתמשים העושים שימוש ברשתות לצורך אינטראקציות וחילופי מידע, שיתופי פעולה ועוד. שינויים אלה תקפים לא רק למחשבים, אלא גם לכל מכשיר אלקטרוני המתַקשר עם מכשירים אחרים, כגון לווייניים, מערכות בקרה ושליטה ועוד. הופעתן של טכנולוגיות כמו טלפונים סלולריים ותקשורת לוויינית, חיישנים מתקדמים, מעבדים בעלי עוצמה, תוכנות הצפנה ועוד, הקנתה לשוק הפרטי יתרון טכנולוגי משמעותי על פני המערכות מהדור הקודם (legacy systems), הנמצאות לעיתים בשימושם של גופי ממשלה, צבא ומודיעין עד היום.

שינויים אלה גם הביאו לשינויים התנהגותיים ותרבותיים הנוגעים להתנהלות אל מול מידע זמין ונגיש. המידע היה בעבר משאב נדיר ויקר ונחשב לנחלתם של גופי המודיעין, אך מהפכת המידע והטכנולוגיה הביאה לכך שמידע ונתונים הפכו לזמינים מִתמיד. המנגנון התחרותי של השוק הפרטי, לפיו חברות טכנולוגיה מפַתחות טכנולוגיות ומוצרים חדשים ומשיקות אותם בקצב מהיר, מקנה לשוק זה יתרון כמעט תמידי בתחומי המחקר והפיתוח ובמהירות ההשקה של שירותים ומוצרים חדשים.[9] כמו כן, השוק הפרטי מגיב טוב יותר לשינויים ולהתפתחויות טכנולוגיות, מאפשר תגובה מהירה יותר ונותן שירותים טובים יותר. על אחת כמה וכמה הדבר נכון כשמדובר בניצול טכנולוגיות מידע. בתנאים אלה, האתגר של גופי המודיעין אינו נובע מהשאלה האם יש צורך לפנות לשוק הפרטי לצורך קבלת גישה לטכנולוגיה מתקדמת, לשירותים חדשים ולפיתוח ומחקר, אלא מהשאלה כיצד לנצל את יתרונותיו של השוק הפרטי לצרכים ביטחוניים.

במקרה האמריקאי ניתן להצביע על פיתוחים טכנולוגיים בתחום טכנולוגיות התקשורת והמידע והמעבר של מדינות כמו לוב, עיראק, סוריה, אירן וצפון קוריאה משימוש במעגלי רדיו לתשתיות תקשורת הקבורות מתחת לאדמה ולסיבים

8 Ibid, p. 23.
9 Ibid, pp. 18-23.

אופטיים. כל אלה הציבו אתגר ליכולות הסיגינט של המודיעין האמריקאי וחייבו אותו להשקעה מתמדת בטכנולוגיה.[10]

מיקור חוץ של פעולות סייבר התקפיות וריגול מקשה על ייחוס המתקפה למדינה

אחד האתגרים המוכרים של לוחמת סייבר ואחד היתרונות הגדולים של מדינות העושות שימוש התקפי במרחב הסייבר הוא הקושי לייחס את המתקפה לַתוקף. בניגוד למתקפות קינטיות, במרחב הסייבר קיים קושי לעקוב אחר מקור המתקפה ולאתר אותו, וגם כאשר התגלה המחשב שממנו היא הוצאה לפועל, קשה לדעת האם מדובר במחשב השייך לתוקף, או שמדובר במחשב שנפרץ ונעשה בו שימוש לצורך המתקפה ללא ידיעת בעליו. כמו כן, לתוקפים במרחב הסייבר יש כלים רבים המאפשרים להם לכסות או למחוק את עקבותיהם, להטעות את החוקרים ולהשמיד ראיות.[11]

העברת הביצוע של מִבצעי סייבר התקפיים לידיים פרטיות מקשה עוד יותר על ייחוס המתקפה, שכן גם אם הצד המותקף יצליח להתחקות אחר התוקפים, יהיה עליו להוכיח את הקשר בינם ובין המדינה. על כן, העברת פעילויות סייבר התקפיות לידיים פרטיות יכולה להגדיל את מרחב ההכחשה של המדינות ולמַזער את הסיכוי לתגובה מטעם המדינה המותקפת.

ייצוא פעולות שאינן עולות בקנה אחד עם החוקה או חוקי המדינה

ייצוא של פעולות לפיתוח תוכנות תקיפה ומִבצעי סייבר עלול להעלות סימני שאלה בעניין האחריות והפיקוח, כאשר פעולות אלו מתבצעות תחת סמכותה ובאישורה של המדינה אך מחוץ לתחומי השיפוט והפיקוח של גופי ביקורת ופיקוח פורמליים, כמו ועדות פרלמנט, גופי רגולציה ועוד. חברות פרטיות (צד שלישי), העורכות מִבצעי סייבר התקפיים וריגול עבור גופי המודיעין, אינן כפופות לגופי הרגולציה ולא חל עליהן פיקוח שעלול לעכב או למנוע מבצעים הנתפסים כהכרחיים ושסודיותם ומהירות הביצוע שלהם חיוניים לצורך השגת מטרתם. מרכיב זה, שיש לו יתרונות אך גם חסרונות, נדון בעבר בהקשר לחקירות של חשודים בטרור, אך הוא מקבל משנה תוקף כשמדובר בצורך לנצל פרצות וחולשות כדי לפרוץ למחשבים ולרשתות במסגרת מבצעי הגנה אקטיבית, ריגול נגדי או פריצה למחשבים של ארגוני טרור במטרה למנוע פיגועים.

10 Matthew Aid, *The Secret Sentry* (New York: Bloomsbury, 2010), pp. 196-198.

11 Bruce Schneier, "Attack Attribution in Cyberspace", *Schneier On Security*, January 8, 2015, https://www.schneier.com/blog/archives/2015/01/attack_attribut.html.

הסיכונים והחסרונות של מיקור חוץ בתחומי הסייבר והמודיעין

תופעת מיקור החוץ בתחומי הסייבר טומנת בחובה גם סיכונים וחסרונות. חלק מסיכונים וחסרונות אלה נדונו בהקשרים של מיקור חוץ בתחומי הלחימה הפיזית, ניהול חקירות וסיוע למִבצעי סיכולים ממוקדים. מרחב הסייבר הינו תחום לוחמה חדש יחסית, ההולך ומתהווה כממד לחימה נוסף שייחודיותו מתאפיינת במרחב תקיפה נרחב, בספקטרום רחב של תוקפים בעלי אינטרסים שונים הכוללים גם גורמים אזרחיים כגון עבריינים או חברות עסקיות, בחוסר תלות במרחק גיאוגרפי, בהיעדר גבולות פיזיים ובהיעדר הגדרה ברורה של מה חוקי ומה אינו חוקי. מאפיינים אלה של הסייבר, בשיתוף הסיכונים והחסרונות שבתופעת מיקור החוץ בתחומי הביטחון, הצבא והלוחמה, הופכים את הסיכון שבמיקור חוץ לרלוונטי גם לאזרחים, לחברות, לגופי ממשלה ולארגונים הרחוקים משדה הקרב ואינם מעורבים בלחימה. סיכון נוסף הכרוך במיקור חוץ הוא שפעולות הנתונות תחת סיווג ביטחוני עלולות לפתוח פתח לניצול לרעה ולשחיתויות.

תחרות בין השוק הפרטי לגופי המודיעין

מיקור חוץ של פעילויות ממשלתיות מוביל להיווצרותו של שוק פרטי עבור פעילויות אלו. צמיחתו של שוק זה יוצרת אפקט של "היזון חוזר": הוצאת עוד ועוד פעילויות מידיהם של הגופים הממשלתיים מביאה לצמיחתו של השוק הפרטי ולעלייתן של המשכורות המוצעות בו. הדבר גורם לארגונים ממשלתיים, ובהם גופי המודיעין, להימצא במצב של תחרות אל מול השוק הפרטי, שהופך להיות מוקד משיכה עבור העובדים בגופים אלה ועבור כל בעלי כישרון הזמינים בשוק.

השכר הגבוה והתנאים הטובים יותר המוּצעים בשוק הפרטי מובילים לתופעה של "דלת מסתובבת", הידועה בארצות הברית תחת השם "Bidding Back", כאשר עובדי סוכנויות המודיעין עוזבים אותן לטובת השוק הפרטי וחוזרים לעבוד עבורן בתור יועצים פרטיים ובשכר גבוה יותר. תופעה זו עלולה ליצור נהירה של עובדי סוכנויות המודיעין וגופי הסייבר לשוק הפרטי, ועל ידי כך לגרום לבריחת מוחות שתחמיר את בעיית כוח האדם הממשלתי, אותה ניסו לפתור מלכתחילה באמצעות מיקור החוץ.[12]

דוגמה לכך ניתן לראות בשוק הפרטי האמריקאי. שוק זה צמח בשנות האלפיים בשיעור חד עקב התפוצצות בועת הדוט־קום,[13] שיצרה מאגר כוח אדם זמין עבור

12 Patrick Radden Keefe, "Don't Privatize Our Spies", *The New York Times*, June 25, 2007, https://www.nytimes.com/2007/06/25/opinion/25keefe.html.

13 בועת הדוט־קום הייתה בועה כלכלית שצמחה בשנים 1997־2001, במהלכה הוקמו חברות אינטרנט רבות שהתבססו על צמיחת האינטרנט ואימוצו על ידי עסקים ולקוחות, בשילוב

גופי הביטחון. מספר חברות, שהוקמו על ידי יוצאי מערכת הביטחון ושכרו את שירותיהם של אנליסטים ואנשי צבא ומודיעין שפרשו, הקימו חטיבות ומחלקות שעסקו בתחילה במודיעין ולאחר מכן בסייבר והיו היחידות שלעובדיהן היו גם ניסיון מספיק וגם סיווג ביטחוני. גם ענקיות הייצור הביטחוני, כגון "בואינג", "לוקהיד מרטין" ו"נורת'רופ־גרומן", הקימו מחלקות העוסקות בסייבר ובפיתוח תוכנות פריצה.

נתונים על היקף מיקור החוץ הכולל בתחומי המודיעין והסייבר הם מידע מסווג, מה שמקשה על למידה מסודרת של היקף התופעה. עם זאת, ב־2007 דובר על כך שכ־70 אחוזים מתקציב המודיעין של ארצות הברית הוקצב לחברות פרטיות.[14] לפי הערכות גסות של סוכן CIA לשעבר במאמר שנכתב עבור מגזין "טיים", עובדי חברות קבלן מהווים כ־50 עד 60 אחוזים מכוח העבודה של ה־CIA.[15]

חוסר פיקוח, ניטור ושליטה

גופי המודיעין, הביון והסייבר נתונים לפיקוח חלקי מטעם ועדות פרלמנטריות וגופי קונגרס. לעומתם, פעולות ההפרטה, מיקור החוץ וההעברה של פעולות רגישות לידיים פרטיות נעשות ללא פיקוח ושליטה של ממשלות, ולגופי הרגולציה אין יכולת לבחון את מידת חוקיותן כשהן מבוצעות על ידי גורמים פרטיים. זאת ועוד, חברות פרטיות עלולות להרגיש פחות מחויבות למסור מידע מלא ואמין לגופי הרגולציה והפיקוח. בנוסף לכך, במדינות רבות ישנם חוקים המנחים את גופי הביטחון והמודיעין כיצד לערוך מכרזים, לחתום על חוזים עם גופים פרטיים ולבצע רכש של מוצרים או שירותים, אך חוקים אלה אינם כוללים, ברוב המקרים, הגדרה מדויקת וברורה של תהליכי פיקוח על ההעסקה של החברות או ניטור התנהלותן והתנהלות עובדיהן. אחת ההשפעות של חוסר הפיקוח היא היעדר תחרות בין חברות הקבלן עצמן. דוגמה לכך היא חוסר התחרות במיקור החוץ בקרב גופי המודיעין והסייבר האמריקאיים. הדבר נובע מהדרישה לפיה עובדי קבלן בתחום הסייבר יעמדו בתנאי סף של סיווג ביטחוני – תהליך שבארצות הברית הינו ארוך ואיטי ומושפע מוויכוחים על תקציבים בין משרד ההגנה למשרד לניהול כוח אדם. גופי הסייבר במערכת הביטחון האמריקאית זקוקים ליכולת להעסיק עובדים חדשים

עם צמיחה מהירה של מחירי מניות, ספקולציות לגבי ערכן וזמינות של כספי השקעות. עם התפוצצות הבועה, חברות אינטרנט רבות הפכו לחדלות פירעון ונסגרו.

14 Simon Chesterman, "'We Can't Spy…If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Function'", *European Journal of International Law*, Vol. 19, no. 5 (November 2008): 1056, https://doi.org/10.1093/ejil/chn055. מקור הנתון הוא במצגת שהוכנה במאי 2007 במשרד ראש המודיעין הלאומי של ארצות הברית (ODNI).

15 Robert Baer, "Just Who Does the CIA's Work?", *Time Magazine*, April 20, 2007, http://content.time.com/time/nation/article/0,8599,1613011,00.html.

במהירות, ואילו התהליך האיטי של מתן סיווג ביטחוני הוביל לעלייה בביקוש לעובדים לשעבר בעלי סיווג ביטחוני וגרם למצב של חוסר תחרות.[16]

המצב כיום הוא שכ־80 אחוזים מכ־45,000 עובדי הקבלן המועסקים בתחום המודיעין בארצות הברית שייכים לחמישה תאגידים פרטיים: Booz Allen Hamilton, CSRA, SAIC, CACI International ו־Leidos. כל חמשת התאגידים ממוקמים במדינת וירג'יניה ועוסקים גם בפיתוח כלי פריצה ולוחמת סייבר.[17]

דוגמה לחוסר התחרות בשוק הפרטי סביב פיתוח אמצעי מודיעין וסייבר ניתן לראות במכרז לפיתוח מערכת Trailblazer לכריית מידע מתקשורת סלולרית ותכתובות דוא"ל עבור ה־NSA. חברת SAIC זכתה ב־2002 במכרז לפיתוח מערכת Trailblazer, בסך של 280 מיליון דולר. עד שנת 2005 זינקה עלות הפרויקט ליותר ממיליארד דולר, והוא הוגדר לאחר מכן ככישלון חרוץ. עם זאת, כשהכריזה ה־NSA על תוכנית ExecuteLocus, שמטרתה הייתה להחליף את מערכת Trailblazer, ניתן החוזה בשנית לחברת SAIC.[18]

סוגיה נוספת המתעוררת בשאלת מיקור החוץ קשורה לאופן הגדרת פונקציות השמורות לגופי הממשלה והביטחון בלבד ואלו פונקציות ניתן להפריט.[19] דוגמה לכך ניתן לראות בחוזה לשירותי תרגום שפות שנחתם עם חברת הקבלן CACI International, שבמסגרתו סיפקה החברה חוקרים למשטרה הצבאית שהייתה אחראית על חקירות עצירים עיראקים במהלך הפלישה לעיראק ב־2003. מחקירה שנפתחה ב־2008 בעקבות תביעה שהוגשה כנגד CACI עלה כי חוקרים מטעם החברה התעללו בעצירים והפרו זכויות אדם.[20] בעייתיות נוספת היא היעדר פיקוח על אופי הפעילויות שניתן להפריט ועל היקפן, מה שעלול להוביל את חברות הקבלן המבַצעות את עבודות המחקר, הפיתוח, האיסוף, ולעיתים גם מִבצעים רשתיים, לשנות, מתוך אינטרסים מסחריים, את התמריץ לפעילותן. אינטרסים מסחריים אלו, כגון מקסום רווחים או הארכת חוזה, לצד תנאים המנוגדים לתנאי

16 Chesterman, "'We Can't Spy…If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Function'", pp.1068-1069.

17 Tim Shorrock, "Why does WikiLeaks keep Publishing U.S. State Secrets? Private Contractors", *The Washington Post,* March 16, 2017, https://www.washingtonpost.com/posteverything/wp/2017/03/16/the-reason-wikileaks-receives-so-many-u-s-state-secrets-private-contractors/?utm_term=.55e8187baf23.

18 Chesterman, "'We Can't Spy…If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Function'", p. 1058.

19 Voelz, *Managing the Private Spies: The Use of Commercial Augmentation for Intelligence Operations*, p. 23.

20 James Lesher, "Outsourcing Cyberwarfare: Drawing the Line for Inherently Governmental Functions in Cyberspace", *Journal of Contract Management* (Summer 2014): 7.

השוק החופשי, כגון היעדר מידע וחוסר תחרות, עלולים לפגוע בפעילות ובתוצריה. לדוגמה, אינטרסים מסחריים עלולים להוביל לניתוח מודיעין והסקת מסקנות מוטה כדי לרצות גורמים פוליטיים או גורמים בגופי המודיעין עצמם. בשנה שלפני הפלישה לעיראק, המרכז לניתוח ולטכנולוגיה נגד־טרור,[21] שנוהל על ידי חברת הקבלן SAIC, הפיק דוחות מודיעיניים בדבר קיומו של נשק להשמדה המונית בעיראק ובדבר כוונתה של עיראק לפתוח במלחמה. עם הפלישה לעיראק, זכתה SAIC בחוזים עבור פעילויות מודיעיניות וביטחוניות על אדמת עיראק.[22]

תוצאה אפשרית נוספת של היעדר פיקוח היא התנהלות לקויה בתחום ביטחון המידע. איום התפוצה של נשק סייבר עלול לגדול משמעותית עקב חוסר פיקוח על התנהלות עובדים בעלי גישה לקודי מקור של תוכנות או של פרויקטי פיתוח. היעדר פיקוח ושליטה של ממשלות עלול להביא להעסקתם של אנשים שאינם מתייחסים לעבודתם כמשימה לאומית, מה שיכול להוביל לרשלנות או להעסקה של אנשים בעלי אידיאולוגיות הפוגעות באופן שבו הם ממלאים את תפקידם. מצבים כאלה עלולים להוביל לזליגה ודליפה של מידע מסווג, של רכיבי פריצה ותקיפה ועוד.

רבות דובר על איומי הסייבר הנשקפים לתשתיות חיוניות, למגזרים כלכליים ולחברות וממשלות במערב מצד מדינות כמו רוסיה, סין, צפון קוריאה ואיראן. עם זאת, אבטחת מידע לקויה, או קבלת מועמדים לא מתאימים למשרות ביטחוניות, לצד מחסור בפיקוח ובאחריות, עלולים להוביל למצב שבו נשק סייבר שפותח על ידי טובי המוחות יודלף או ייגנב מהאחראים לפיתוחו, יגיע לידי גורמים עוינים וינוצל נגד אותן המדינות שפיתחו אותו מלכתחילה, או נגד בעלות בריתן. בעיה זו מחריפה נוכח הקושי לנטר תוכנות ולפקח עליהן.

הדלפה של נשק סייבר יכולה לאפשר למדינות בעלות יכולת טכנית נמוכה יחסית, ארגוני טרור או ארגוני פשע לבצע הנדסה לאחור (Reverse Engineering) או להעתיק חלקי קוד של נוזקות מתוחכמות ולהסב את הנשק הגנוב לשימוש חוזר.[23] דוגמה לכך ניתן לראות בדיווחים, על פיהם תולעת "סטקסנט" (Stuxnet), ששימשה במקור למטרת חבלה במתקני הגרעין של איראן, הועתקה ושימשה למתקפות על מערכות שליטה ובקרה בכ־15 תחנות חשמל ומפעלים כימיים בגרמניה.[24]

---

21 Center for Counterterrorism Technology and Analysis

22 Donald Barlett and James Steele, "Washington's $8 Billion Shadow," *Vanity Fair*, March 2007, https://www.vanityfair.com/news/2007/03/spyagency200703

23 כהן ורוטברט, "תפוצת נשק קיברנטי במרחב הסייבר", עמ' 50, 59.

24 Nicole Goebel, "Report says Stuxnet Computer Virus Hits German Firms", *Deutsche Welle*, October 2, 2010, https://www.dw.com/en/report-says-stuxnet-computer-virus-hits-german-firms/a-6069500.

בהינתן מצבים אלה, ולצד הסיווג והמידור הנהוגים בקרב גופי הסייבר, ארגונים או גופים ממשלתיים עלולים לא להיות מודעים לבעיות שפורטו לעיל, או שלא יהיה ביכולתם לכפות מדיניות או תקני אבטחה על חברות הקבלן, והם עשויים להעדיף את החיסכון הפיננסי בלבד. בסיכומו של דבר, בחינת היתרונות והחסרונות של תופעת מיקור החוץ בתחומי המודיעין והסייבר מראה כי מצד אחד קיימים יתרונות רבים לתופעה, אך מצד שני קיימים גם חסרונות, שרבים מהם נסובים סביב שאלת הפיקוח והאחריות המוטלת על חברות הקבלן.

יתרונות וחסרונות של מיקור חוץ בתחום המודיעין והסייבר

יתרונות	חסרונות
התמודדות עם קיצוצי תקציב ומכסות כוח אדם	תחרות בין השוק הפרטי ובין גופי המודיעין
התמודדות עם איומים משתנים וחדשים	חוסר תחרות בין חברות הקבלן
גישה לטכנולוגיה מתקדמת ולפיתוח מהיר	חוסר פיקוח על סוג התהליכים והפעילות המופרטים
הרחבת מרחב ההכחשה (בעת שימוש בקבלנים לטובת מבצעי ריגול או תקיפת סייבר)	פוטנציאל לפוליטיזציה של תהליכים ופעולות
מתן יד חופשית – פעילות ללא מגבלות חוקיות	רשלנות או זדון בהתנהלות עם ביטחון מידע וחומרים מסווגים

דליפת נשק סייבר וחומרים מסווגים – מקרי בוחן בקהילת המודיעין האמריקאית

פרשת אדוארד סנודן

רקע: המקרה הידוע והמפורסם ביותר של הדלפת חומר מסווג בשנים האחרונות הוא פרשת סנודן. אדוארד סנודן הועסק ב־2013 על ידי חברת הקבלן Booz Allen Hamilton ועבד כאנליסט עבור ה־NSA. כארבעה חודשים אחרי תחילת העסקתו ב־Booz Allen, במאי 2013, טס סנודן להונג קונג, וכחודש לאחר מכן חשף מאות אלפי מסמכים מסווגים של ה־NSA. אלה פורסמו בעיתונים "וושינגטון פוסט" ו"גארדיאן", ולאחר מכן ב"דר שפיגל" וב"ניו יורק טיימס".

הקשר בין המקרה ובין תפוצת נשק סייבר: הדלפותיו של סנודן חשפו יכולות וטכניקות מעקב של ה־NSA אחר תקשורת סלולרית ותכתובות דוא"ל. במסגרת זו נחשפה תוכנית PRISM, שאפשרה ל־NSA לגשת למרכזי נתונים של "גוגל" ו"יאהו" ולדלות מידע על אזרחים בכל רחבי העולם, כולל אזרחים אמריקאים.[25]

25 Barton Gellman and Ashkan Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say", *The Washington Post*, October 30,

מלבד PRISM, חשפו מסמכי סנודן מאגרי מידע שנאסף על אזרחים, מידע על כלים אנליטיים לאיסוף מידע מתעבורת רשת ומידע על שיתופי פעולה של ה־NSA עם חברות תקשורת ועם גופי מודיעין של בעלות בריתה של ארצות הברית.[26] רוב המסמכים שהדליף סנודן כללו מידע על תוכניות המעקב של ה־NSA, אך לא את קודי המקור של הרכיבים ששימשו אותן. למרות זאת, פרשת סנודן הפכה למקרה המדגים את הסיכון שבחוסר הפיקוח על קבלנים.

המניע: במספר ראיונות שהעניק לאחר הדלפת המסמכים טען סנודן כי עשה זאת מתוך אמונה שפעילות המעקב של ה־NSA אינה חוקית ומפרה את זכויותיהם של אזרחים אמריקאים. כמו כן, הוא האשים את ממשל אובמה בכך שהעלים עין מתוכניות הריגול שהחלו בזמן ממשל בוש הבן.[27] על רקע זה ניתן להגדיר את מניעיו של סנודן כמניעים אידיאולוגיים, מה שמעורר שאלות בנוגע לתהליך הגיוס וההשמה של עובדים לחברות הקבלן המועסקות על ידי המודיעין של ארצות הברית.

הרולד מרטין ודליפת ה־Shadow Brokers

רקע: הרולד מרטין נעצר באוגוסט 2016 בחשד שלקח לביתו ללא אישור חומרים מסווגים של ה־NSA, ה־CIA ופיקוד הסייבר האמריקאי, בהיקף שהוערך בכחמישים טֶרה־בייט. מרטין עבד במשך שני עשורים כעובד קבלן עבור שבע חברות קבלן שביצעו פרויקטים עבור משרד ההגנה, ה־CIA וה־NSA, ובתפקידו האחרון היה עובד קבלן עבור חברת Booz Allen Hamilton (שעבורה עבד, כזכור, גם אדוארד סנודן). על פי כתב האישום, מרטין החל לגנוב חומרים מסווגים בשנת 1996 והמשיך בכך עד מעצרו שני עשורים לאחר מכן. בין החומרים שגנב נכללו רכיבי

2013, https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.dc6eea63ee4c.

26 Glenn Greenwald, "XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'", *The Guardian*, July 31, 2013, https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data; Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily", *The Guardian*, June 6, 2013, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Scott Shane and Ravi Somaiya, "New Leak Indicates Britain and U.S. Tracked Diplomats", *The New York Times*, June 16, 2013, https://www.nytimes.com/2013/06/17/world/europe/new-leak-indicates-us-and-britain-eavesdropped-at-09-world-conferences.html.

27 Barton Gellman and Jerry Markon, "Edward Snowden Says Motive behind Leaks was to Expose 'Surveillance State'", *The Washington Post*, June 10, 2013, https://www.washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html?noredirect=on&utm_term=.207834dcb16d.

פריצה, מסמכים המתארים טכניקות פריצה לרשתות זרות ומסמכים המתארים יכולות סייבר התקפיות, תהליכים ושיטות לביצוע גישה לרשתות ולהגנה על רשתות ומערכות ממשלתיות.[28]

הקשר בין המקרה ובין תפוצת נשק סייבר: במהלך החקירה סביב הפרשה נמצא כי חומרים רבים שגנב מרטין נמצאו מאוחר יותר בין הקבצים שהדליפה קבוצת ההאקרים The Shadow Brokers.[29] קבצים אלה פורסמו בתחילת אפריל 2017 באתר Medium, וכללו מידע על פרצות אבטחה במערכות וביישומים, לצד פרטים על אמצעי מעקב אחר מערכות מחשב, טלפונים, התקנים ניידים ואתרי אינטרנט.

הרכיב הבולט ביותר שעל פי החשד נגנב ממחשבו של מרטין הוא רכיב הפריצה EternalBlue. EternalBlue הינו קוד המנצל חולשה בפרוטוקול SMB (Server Message Block), אשר משמש לגישה מרחוק במערכות הפעלה מסוג Windows. מאז דליפתו, שימש רכיב זה לצורך התפשטותה של מתקפת הסייבר הגלובלית WannaCry, שפגעה בלמעלה מ־230,000 מחשבים ביותר מ־150 מדינות במאי 2017.[30] רכיב EternalBlue ממשיך להיות נפוץ ברחבי העולם. על פי דוח של הארגון לשיתוף מודיעין על איומי סייבר – Cyber Threat Alliance – האקרים ממשיכים לעשות שימוש ברכיב זה כדי לכרות מטבעות דיגיטליים.[31] בהקשר זה תצוין גם מתקפת הסייבר הגלובלית NotPetya, אשר התפשטה באמצעות רכיב נוסף של ה־NSA בשם EternalRomance.[32]

דוגמה נוספת של כלי פריצה שהודלף על ידי ה־Shadow Brokers, וככל הנראה נגנב לראשונה על ידי מרטין, הוא נוזקת ה־DarkPulsar, המייצרת "דלת אחורית" ומאפשרת התקנת נוזקות נוספות. באוקטובר 2018 טענה חברת קספרסקי כי זיהתה כחמישים קורבנות מענפי האנרגיה הגרעינית, התקשורת, ה־IT, התעשייה האווירית והמחקר והפיתוח ברוסיה, באיראן ובמצרים, שנדבקו ב־DarkPulsar.[33]

---

28 Richard Chirgwin, "Ex-NSA Contractor Harold Martin Indicted: He Spent 'Up to 20 Years Stealing Top-Secret Files'", *The Register*, February 8, 2017, https://www.theregister.co.uk/2017/02/08/us_grand_jury_indicts_harold_martin_nsa/.

29 Scott Shane, Nicole Perlroth and David Sanger, "Security Breach and Spilled Secrets Have Shaken the N.S.A. to its Core", *The New York Times*, November 12, 2017, https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.

30 "EternalBlue – Everything there is to Know", *CheckPoint*, September 30, 2017, https://research.checkpoint.com/eternalblue-everything-know/.

31 "The Illicit Cryptocurrency Mining Threat", *Cyber Threat Alliance*, p. 14.

32 Iain Thomson, "Everything you Need to Know about the Petya, er, NotPetya Nasty Trashing PCs Worldwide," *The Register*, June 28, 2017, https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/.

33 Catalin Cimpanu, "Kaspersky Says it Detected Infections with DarkPulsar, Alleged NSA Malware", *ZDNet*, October 19, 2018, https://www.zdnet.com/article/kaspersky-says-it-detected-infections-with-darkpulsar-alleged-nsa-malware/.

המניע: בעת כתיבת שורות אלו עדיין מתנהל משפטו של מרטין, שהוגדר על ידי עורכי דינו כאגרן כפייתי (Compulsive hoarder), וטרם הוכח האם הוא מכר את החומרים שאסף או שמא הם נגנבו ממחשבו האישי. עם זאת, לאור העובדה שמרטין לקח חומרים לביתו במשך שנים, אפשר להעריך שמדובר בהרגל ובהתנהלות רשלניים ולקויים בכל הנוגע לביטחון מידע. בהקשר זה מתעוררים סימני שאלה רבים באשר לצעדי האבטחה של Booz Allen Hamilton, שלא גילתה את מעשיו של מרטין גם לאחר שהגבירה כביכול את אמצעי ותהליכי האבטחה בעקבות הדלפותיו של אדוארד סנודן.

דליפות ה־Vault 7 וה־Vault 8 מה־CIA

רקע: ב־7 במארס 2017 החל אתר "ויקיליקס" לפרסם סדרת מסמכים המפרטים טכניקות, כלים ויכולות של ה־CIA לביצוע מעקב אלקטרוני ולוחמת סייבר. הסדרה זכתה לכינוי Vault 7, והמסמכים שהיא כללה פורסמו ב־24 חלקים בין החודשים מארס לספטמבר 2017. בנובמבר אותה שנה החלו מייסדי "ויקיליקס" להדליף אוסף נוסף של מסמכים, שזכה לכינוי Vault 8.

באוגוסט 2017 נעצר ג'ושוע שוּלְטֶה, כחלק מחקירה של ה־FBI על תפוצה של תכנים פדופיליים. בפשיטה על דירתו החרימו החוקרים מחשבים, התקנים ניידים ושרתים שהכילו חומרים פדופיליים, וכן חלק מחומר מסווג שלקח לביתו ממקום עבודתו. שולטה עבד כמהנדס תוכנה עבור יחידה של ה־CIA שאחראית על פיתוח קודים לתוכנות רוגלה ומבצעי גישה. למרות הערכות קודמות, שולטה לא היה עובד קבלן. במהלך החקירה התברר כי שולטה העלה, החל מ־2013, מספר פרויקטים וקודים שכתב עבור ה־CIA לחשבון ה־GitHub הציבורי שלו, ובנוסף לכך שמר עוד חומר על שרתים ציבוריים לשיתוף קבצים.[34]

הקשר בין המקרה ובין תפוצת נשק סייבר: בהדלפות ה־Vault 7 לאורך שנת 2017 נחשפו רכיבי פריצה למערכות הפעלה מסוג Linux ו־MacOS X לצורכי ריגול וגניבת מידע, וכן רכיבים המשמשים ליירוט תקשורת, לניתוב תעבורת רשת ולשיתוק מצלמות אבטחה.[35] דליפות ה־Vault 7 כללו בעיקר מסמכים המתארים

34 Jason Koebler, "Alleged CIA Leaker has some of the Worst Opsec I've ever Seen", *Motherboard*, May 17, 2018, https://motherboard.vice.com/en_us/article/qvn83q/joshua-schulte-cia-vault-7-wikileaks-opsec; John Walcott and Mark Hosenball, "CIA Contractors Likely Source of Latest WikiLeaks Release: U.S. Officials", *Reuters*, March 8, 2017, https://www.reuters.com/article/us-cia-wikileaks-idUSKBN16F2AP.

35 Pierluigi Paganini, "Wikileaks – CIA Developed OutlawCountry Malware to Hack Linux Systems", *Security Affairs*, July 1, 2017, http://securityaffairs.co/wordpress/60584/breaking-news/cia-outlawcountry-hack-linux.html; Sooraj Shah, "WikiLeaks Reveals CIA Tool Acting as SMS Proxy on Android", *Infosecurity-Magazine*, July 14, 2017, https://www.infosecurity-magazine.com/news/wikileaks-highrise-cia-android/; Swati

טכניקות פריצה ומסמכים המנחים את הסוכנים כיצד לעשות שימוש ברכיבי הפריצה. לעומת זאת, דליפת ה־Vault 8 כללה קודי מקור ורישומי פיתוח של פרויקט Hive – מרכיב ששימש את ה־CIA לשליטה מרחוק בתוכנות נוזקה ולקבלת מידע ונתונים שנגנבו ממחשבים, ושעצם קיומו נחשף כבר בדליפת ה־Vault 7.[36]

המניע: כתב האישום נגד שולטה מייחס למעשיו כוונת זדון וניסיון לפגוע בביטחון הלאומי של ארצות הברית. נטען בו כי שולטה ביצע גישה לא מאושרת למחשבי ה־CIA שבהם אוחסנו החומרים, העביר אותם מרצונו לצד שלישי, טשטש את עקבותיו, חסם את גישתם של אחרים למערכת ושיקר לחוקריו.[37] בניגוד למרטין, שולטה הכחיש את מעשיו וטען כי עזב את ה־CIA כתוצאה מחוסר יכולת להמשיך לתפקד, וכי בעקבות זאת מייחסת לו הסוכנות רגשות מרמור והופכת אותו ל"שעיר לעזאזל".[38] נכון לכתיבת שורות אלו, לא ניתן לדעת בוודאות מה היה המניע של שולטה, אך ניתן להעריך כי היה לו תפקיד פעיל בהדלפת החומר שפורסם.

פרשת קספרסקי והדליפה מה־NSA

רקע: ניה הואנג פו עבד כמפתח עבור יחידת TAO (Tailored Access Operations) לפיתוח אמצעי פריצה של ה־NSA משנת 2006 עד שנת 2015. פו הואשם בכך שבמשך חמש שנים לקח מסמכים וחומרים דיגיטליים מסווגים לביתו. פעילותו התגלתה לאחר שהאקרים ישראלים פרצו למחשבי חברת קספרסקי וזיהו קודים לתוכנות של ה־NSA שאוחסנו עליהם. החקירה העלתה כי על מחשבו של פו הייתה מותקנת תוכנת אנטי־וירוס של קספרסקי, הסורקת את המחשב ומנטרת

Khandelwal, "3 New CIA-Developed Hacking Tools for MacOS & Linux Exposed", *The Hacker News*, July 27, 2017, https://thehackernews.com/2017/07/linux-macos-hacking-tools.html.

36 Swati Khandelwal, "Vault 8: WikiLeaks Releases Source Code for Hive – CIA's Malware Control System", *The Hacker News*, November 9, 2017, https://thehackernews.com/2017/11/cia-hive-malware-code.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+TheHackersNews+(The+Hackers+News+-+Security+Blog)&_m=3n.009a.1620.op0ao09m9g.z6u.

37 "Joshua Adam Schulte Charged with the Unauthorized Disclosure of Classified Information and other Offenses Relating to the Theft of Classified Material from the Central Intelligence Agency", *Department of Justice*, June 18, 2018, https://www.justice.gov/opa/pr/joshua-adam-schulte-charged-unauthorized-disclosure-classified-information-and-other-offenses.

38 Matt Zapotosky, "Ex-CIA Employee Charged in Major Leak of Agency Hacking Tools", *The Washington Post*, June 18, 2018, https://www.washingtonpost.com/world/national-security/ex-cia-employee-charged-in-major-leak-of-agency-hacking-tools/2018/06/18/dadd40ac-7352-11e8-b4b7-308400242c2e_story.html?noredirect=on&utm_term=.79c76a6ece55.

קודים זדוניים. קודים לתוכנות פריצה של ה־NSA שלקח פו לביתו זוהו על ידי התוכנה כזדוניים ונשלחו לתיקיית ענן המשמשת את החברה לצורכי מחקר.[39]

הקשר בין המקרה ובין תפוצת נשק סייבר: פו עבד, כאמור, עבור יחידת TAO המפתחת קודים לתוכנות פריצה. הקודים שנאספו ממחשבו על ידי תוכנת קספרסקי היו שייכים לפרויקטים עליהם עבד במסגרת עבודתו באותה יחידה וזוהו על ידי התוכנה כקודים זדוניים. מהחקירה עלה, שבניגוד לטענותיה של חברת קספרסקי, המידע שנאסף ממחשבו של פו הגיע לידי גורמים במודיעין הרוסי. יש שלוש תיאוריות מרכזיות לאופן שבו המידע זלג מקספרסקי לידי המודיעין הרוסי. תיאוריה אחת גורסת כי האקרים רוסים ניצלו חולשות אבטחה בתוכנת קספרסקי. שתי התיאוריות האחרות גורסות כי האקרים רוסים יירטו את המידע בעת העברתו לשרת של קספרסקי במוסקבה, או שחברת קספרסקי פעלה מטעם ממשלת רוסיה, ומרגע גילוי החומרים על מחשבו של פו פעלה כדי לגנוב אותם ולהעבירם לגורמי ממשל רוסיים.[40]

המניע: פו הודה במעשיו וטען במכתב שהגיש לבית המשפט כי הוא סובל מבעיות חברתיות וכי לקח את החומרים לביתו מתוך רצון לעבוד עליהם מחוץ לשעות העבודה ולשפר את ביצועיו בעבודה ואת הציון השנתי שניתן לעובדי ה־NSA על ביצועיהם.[41] המקרה של פו מלמד על רשלנות ועל ביטחון מידע לקוי ולא על כוונת זדון או מניע אידיאולוגי.

דרכי התמודדות ומענים לחסרונות של מיקור חוץ

בהינתן ההיקף ההולך וגדל של תופעת מיקור החוץ ויתרונותיה הרבים, סביר להניח שהיא תלך ותתרחב. על כן, יש להתמקד בפתרונות למזעור ההשפעות השליליות של התופעה.

כדי להתמודד עם בעיית ההדלפות של עובדים בגופי הסייבר של מערכות הביטחון ושל עובדי קבלן העובדים עבורן, יש צורך במענה הגנתי מצד ממשלות ותעשיות של אבטחת סייבר. מענה כזה צריך להיות מסוגל להתמודד עם הדלפת חולשות, פרצות אבטחה ונשקי סייבר שפותחו עבור גופי המודיעין או נמצאים

39 Nicole Perlroth and Scott Shane, "How Israel Caught Russian Hackers Scouring the World for U.S. Secrets", *The New York Times*, October 10, 2017, https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html.

40 Zack Whittaker, "What is Kaspersky's Role in NSA Data Theft? Here are Three likely Outcomes", *ZDNet*, October 9, 2017, https://www.zdnet.com/article/what-role-did-kaspersky-play-in-nsa-data-theft/.

41 Sean Gallagher, "NSA Employee who Brought Hacking Tools Home Sentenced to 66 Months in Prison", *Ars Technica*, September 26, 2018, https://arstechnica.com/tech-policy/2018/09/nsa-employee-who-brought-hacking-tools-home-sentenced-to-66-months-in-prison/.

בשימוש של חברות קבלן. בנוסף, יש להנהיג פיקוח הדוק יותר על הגופים האחראים לתחום הסייבר במערכות הביטחון, כמו גם על החברות הפרטיות הפועלות עבורם, תוך שימת דגש על הרקע והזהות של העובדים, על אבטחת הסייבר של המערכות ועל נוהלי האבטחה. יש גם להחיל בדיקות רקע, שניתן לעשותן באופן תקופתי, אשר יכללו ראיונות אישיים ובדיקת רשומות ציבוריות, וכן בדיקות ברשת של מידע על העובדים, שיבדקו בין השאר את התנהגותם ברשתות החברתיות. מידע כזה עשוי לשפוך אור על תפיסות אידיאולוגיות או פוליטיות של עובד, שעלולות לפגוע בתהליכי ביצוע עבודתו. בנוסף על כל אלה יש לבצע בדיקות רפואיות ופסיכולוגיות תקופתיות של העובדים. בדיקות כאלו יוכלו למנוע התנהלות לא תקינה שלהם עם תוכנות פריצה או עם רכיבים התקפיים.

שיפור נהלים והנהגת שיטות עבודה מומלצות לשמירה על היגיינת סייבר יכולים לסייע במזעור תופעת הרשלנות, המובילה לדליפות בלתי רצוניות בקרב עובדים. כדי לשפר את היגיינת הסייבר של עובדים המפתחים או מפעילים תוכנות פריצה ורכיבי סייבר התקפי, יש לחייב את עובדי הקבלן ואת עובדי קהילת הביטחון וגופי הסייבר לעבור הכשרות ומבחנים תקופתיים בזיהוי סיכונים לביטחון מידע ואיומי סייבר. זאת, לצד חידוד נהלים להתנהלות עם מידע מסווג, ובכלל זה עם קודי מקור ותוכנות תקיפה. בנוסף, ובהמשך למגמה שכבר החלה בארצות הברית, יש לאסור על עובדים הנמצאים במגע עם אמצעי סייבר לעשות שימוש במוצרים של חברות הנמצאות בקשר עם ממשלות זרות. דוגמאות למוצרים כאלה הם מוצרי האנטי־וירוס של חברת קספרסקי, וכן מכשירים וציוד תקשורת של חברות תקשורת סיניות, כגון Huawei ו־ZTE, המחויבות על פי החוק הסיני להיענות לבקשות סיוע של גופי המודיעין של סין.[42] ניתן להתנות מתן סיווג ביטחוני או הארכתו בעמידה בנהלים ובתהליכים אלה.

מענה נוסף למזעור תופעת הרשלנות ודליפות המידע הוא טכנולוגי. דוגמאות למענה טכנולוגי שיכול לסייע בשיפור הפיקוח על היגיינת הסייבר של עובדים בגופי הסייבר, או של חברות הקבלן הפועלות עבורם, הן תוכנות לסריקה וניטור של התקני אחסון חיצוניים המחוברים למחשבי סוכנות הסייבר או החברה החיצונית, וסריקת חיבורי USB המשמשים להפָרות ביטחון מידע ולקיחת חומרים הביתה. גם ניטור תנועות של קבצים ברשתות וניטור חשבונות דוא"ל של עובדים עשויים לשפר את יכולות הפיקוח ולסייע לשמור על היגיינת סייבר.

---

42 Arjun Kharpal, "Huawei Says it would Never Hand Data to China's Government. Experts Say it wouldn't have a Choice," *CNBC*, March 4, 2019, https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

כדי להיאבק בהתנהלות לקויה של עובדי קבלן, ניתן לקדם ולכלול תמריצים כלכליים בחוזים הנחתמים עם חברות הקבלן, ובכך לעודד אותן לעקוב, לנטר ולפקח על עובדיהן ופעילותם ולנהל תהליכי גיוס כוח אדם קפדניים ומעמיקים יותר. ניתן לכלול תמריצים אלה כתנאי להשתתפות במכרזים עתידיים או כתנאי להפסקת חוזה.

נראה כי גם לאחר הטמעתן של הצעות אלו לא ניתן יהיה למנוע לחלוטין התרחשותן של דליפות. לדברי ראש המרכז הלאומי לביטחון ומודיעין נגדי, הכפוף למשרד ראש המודיעין הלאומי בארצות הברית, ויליאם איווינה, יש להתמקד בדרכים לזהות את הדליפות במהירות האפשרית ולמזער את נזקיהן מרגע הגילוי.[43] על כן, על הגופים האחראים על תחום הסייבר במסגרת גופי המודיעין והביטחון לקיים הערכות סיכונים, שיכללו תרחישים של דליפת קודי מקור של נשק סייבר, וכן לפעול להבנת עומק הנזק וההשפעה של הדליפות הפוטנציאליות על מִבצעים עתידיים, לצד היקף ההשפעה הפוטנציאלית שלהן על היציבות במרחב הסייבר. משדלפו תוכנות שעלולות לשמש למתקפות גלובליות נרחבות, על קהילת גופי הסייבר להיות ערוכה לחשוף את חולשות האבטחה ליצרנים בהליך מהיר וחשאי.

סיכום ומסקנות

סקירה של מקרי הבוחן מראה כי בעוד שעובדי קבלן היו קשורים למקרים של ביטחון מידע רעוע, רשלנות, היגיינת סייבר לקויה ואף דעות או רקע אידיאולוגי שאינם תואמים את אופיו הביטחוני של התפקיד, גם עובדים פנימיים של קהילת גופי הסייבר היו אחראים לתפוצה בלתי חוקית של נשק סייבר. לפיכך, רשלנות, חוסר פיקוח והעסקה של עובדים בעלי רקע בעייתי, או כזה שאינו מתאים לאופי התפקיד, ניתן למצוא גם בקרב חברות הקבלן וגם בקרב קהילת גופי הסייבר במערכות הביטחון.

למיקור חוץ בתחום הסייבר יתרונות רבים. זאת ועוד, מגמת מיקור החוץ בתחום זה צפויה להתרחב, ואף לכלול ביצוע מבצעי סייבר התקפיים. למרות היתרונות שבמיקור החוץ, אין להתעלם מההשלכות השליליות של התופעה, בין אם מדובר בדליפה של יכולות סייבר התקפיות ובקודים של תוכנות פריצה, ובין אם מדובר במסמכים מסווגים החושפים יכולות, שיטות או מבצעים. גם פעולות הגנתיות המבוצעות על ידי חברות פרטיות עבור גופי ממשלה, כגון ניטור תעבורת רשת ובדיקת חדירות (penetration testing), עלולות לשמש לצרכים זדוניים, בהינתן חוסר פיקוח או רשלנות של כוח אדם.

---

43 Patrick Tucker, "Can the NSA Stop the Next Snowden?", *The Atlantic*, September 18, 2016, https://www.theatlantic.com/international/archive/2016/09/nsa-snowden/500345/.

כדי לתת מענה לבעיות אלו, יש צורך במציאת פתרון הגנתי מצד ממשלות ותעשיות אבטחת סייבר, שיוכל להתמודד עם הדלפת חולשות, עם פרצות אבטחה ועם נשקי סייבר שפותחו או שנמצאים בשימוש של חברות הקבלן הפועלות עבור גופי המודיעין. פתרון כזה אמור לכלול הנהגת פיקוח הדוק על התנהלותם של עובדים העוסקים בפיתוח והפעלה של נשק סייבר, שימת דגש על בדיקות רפואיות ופסיכולוגיות תקופתיות שלהם, בדיקות רקע מקיפות, מתן הכשרות וקיום מבחנים בזיהוי והתנהלות מול איומי סייבר, וכן איסור על שימוש במוצרי חברות המקיימות קשרים עם ממשלות זרות, במיוחד כאלו המהוות יריבות אסטרטגיות ומעורבות בריגול סייבר. גם שימוש בעזרים טכנולוגיים יכול למַזער את ההשפעות השליליות של התופעה.

למרות כל זאת, נראה כי לא ניתן למנוע לחלוטין דליפת חומרים מסווגים, ובכללם נשק סייבר. על כן, קהילת גופי הסייבר חייבת להיערך טוב ככל הניתן לזיהוי דליפות ולהתמודדות עם הנזקים הפוטנציאליים שלהן מהרגע שבו הן מתגלות.