מאחורי מבצעי השפעה בסייבר - מתקפות כופר כמקרה מבחן

מיכאל גנקין[1]

הופעת האינטרנט ועלייתו של מרחב הסייבר הובילו לפיתוח שיטות חדשות להקרנת כוח ולהשפעה אסטרטגית, ואחת מהן היא מבצעי סייבר התקפיים. מאמר זה דן בשימוש שמדינות עושות במבצעי סייבר התקפי, ובפרט מתקפות כופר, כחלק ממבצעי השפעה, דרך ניתוח שני מקרי בוחן שהתרחשו באלבניה וישראל ומיוחסים לאיראן. המאמר כולל ניתוח תיאורטי של מושגי מפתח בעולם הסייבר ההתקפי, ובכלל זה מבצעי השפעה במרחב הסייבר. כחלק ממבצעי ההשפעה, נעשה שימוש במתקפות כופר להעברת מסרים אסטרטגיים. אלבניה הגיבה למתקפה בתגובה דיפלומטית חריפה, ושילבה שיתוף פעולה בין־לאומי בניסיון להרתיע מפני מתקפות עתידיות, ואילו המקרה הישראלי מדגים תפיסה ייחודית להגברת חוסן מול מבצעי השפעה העושים שימוש בפעילויות הסייבר התקפי.

מבוא[2]

האינטרנט, שפרץ כרשת עולמית עם חדירה בין־לאומית רחבה,[3] הפך במהירות להיות מרכיב יסוד בסביבת המידע המודרנית[4] ואִפשר את צמיחתו של מרחב הסייבר.[5] בתוך זמן קצר זיהו שחקנים בין־לאומיים את חשיבות מרחב הסייבר לסביבת המידע, את משמעותו הכלכלית, ואת חשיבותו ליצירה העוצמה הלאומית ולמימושה.[6] בחתירה למימוש מטרותיהם הפוליטיות והאסטרטגיות, שחקנים אלה מבקשים לנצל את כל מקורות העוצמה הלאומית שלהם כדי להשפיע על המדיניות ועל קבלת ההחלטות של מדינות אחרות, ולכן מפתחים שיטות חדשות ומקוריות לשימוש במרחב הסייבר כמחולל השפעה.[7]

המיקוד בתכונותיו של מרחב הסייבר אשר הופכות אותו לכר פורה עבור מבצעי השפעה[8] (ובניצול תוצאות המבצע להרחבת ההשפעה), הביא לכך שצורות אחרות של הקרנת כוח במרחב הסייבר זכו לפחות תשומת לב. אחת מהן היא מה שמכונה מבצעי סייבר התקפיים (OCO).[9] לאור השכיחות של מבצעי סייבר התקפיים, ובמיוחד מתקפות כופר,[10] מאמר זה מבקש לתת מענה לפער

1 מיכאל גנקין הוא עמית אורח במחלקה ללימודי ביטחון באוניברסיטת קינגס קולג' לונדון וחבר במכללת המומחים של ה־OCWG.

2 המחבר מבקש להודות לא"ש ולע"ש על הערותיהם המועילות והחשובות במהלך מפגשי סיעור המוחות שהובילו לעבודה זו.

3 Ani Petrosyan, Internet and Social Media Users in the World 2024, *Statista*, January 31, 2024, https://www.statista.com/statistics/617136/digital-population-worldwide/.

4 Ahmad Alzubi, The Evolving Relationship between Digital and Conventional Media: A Study of Media Consumption Habits in the Digital Era, *The Progress: A Journal of Multidisciplinary Studies 4*, no. 3 September 30, 2023: 1–13, https://hnpublisher.com/ojs/index.php/TP/article/view/25.

5 Marco Mayer et al., How Would You Define Cyberspace, *First Draft Pisa* 19 (2014): 2014.

6 Daniel T. Kuehl, From Cyberspace to Cyberpower: Defining the Problem, in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (University of Nebraska Press, 2011), https://doi.org/10.2307/j.ctt1djmhj1; William J. Lynn III, Defending a New Domain, *Foreign Affairs*, September 1, 2010, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain; Tomáš Minárik, NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit, NATO CCDCOE, 2016, https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/.

7 See, for example, Marie Baezner and Sean Cordey, Influence Operations and Other Conflict Trends, in *Cyber Security Politics* (Routledge, 2022), 17–31; Pascal Brangetto and Matthijs A. Veenendaal, Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations, in *2016 8th International Conference on Cyber Conflict (CyCon)* (IEEE, 2016), 113–26, https://doi.org/10.1109/cycon.2016.7529430; Sean Cordey, Cyber Influence Operations: An Overview and Comparative Analysis, (ETH Zurich, October 31, 2019), https://doi.org/10.3929/ETHZ-B-000382358; Herbert Lin and Jaclyn Kerr, On Cyber-Enabled Information Warfare and Information Operations, in *The Oxford Handbook of Cyber Security*, ed. Paul Cornish (Oxford University Press, 2021), 250–272, https://doi.org/10.1093/oxfordhb/9780198800682.013.15; Peter Pijpers and P.A.L. Ducheine, Influence Operations in Cyberspace - How They Really Work, Amsterdam Law School Legal Studies Research paper No. 2020-61, *Amsterdam Center of International Law,* 2020-31 (2020), https://doi.org/10.2139/ssrn.3698642.

8 המונח משמש כאן במקביל למונח 'מבצעי מידע' (Information operations), כמקובל בספרות הכללית.

9 מבצעי סייבר התקפיים הם בעיקר מבצעים צבאיים שנעשים במרחב הסייבר, ונועדו לשלול, לפגוע, לשבש, להרוס או לעשות מניפולציות כדי להשיג השפעות בעולם הפיזי בתוך שמירה על מרחב הבחשה, ראו: US Joint Chiefs of Staff, *Joint Publication 3-12: Cyberspace Operations*, US Department of Defense, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

10 על שכיחות מבצעי סייבר התקפיים, ראו: Jakob Bund et al., EuRepoC Cyber Conflict Briefing - 2023 Cyber Activity Balance, *European Repository of Cyber Incidents*, January 31, 2024, https://eurepoc.eu/wp-content/uploads/2024/01/EuRepoC-Cyber-Conflict-Briefing-2023-Cyber-Activity-Balance.pdf; על השכיחות של מתקפות כופר, ראו, בין היתר: C. David Hylender et al., Verizon 2023 Data Breach Investigations Report, The Verizon DBIR Team, 2023, https://verizon.com/dbir/; Ani Petrosyan, Global Firms Targeted by Ransomware 2023, *Statista*, March 28, 2024, https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/; The State of Ransomware 2023, Sophos, May 2023, https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf; The 2024 Crypto Crime Report, *Chainalysis*, February 2024, https://go.chainalysis.com/rs/503-FAP-074/images/The%202024%20Crypto%20Crime%20Report.pdf.

הקיים בספרות, ולבחון כיצד מבצעי סייבר התקפיים משמשים ותומכים במבצעי השפעה.

כדי לדון בשימוש שנעשה במתקפות כופרה לצורך מבצעי השפעה, יציע מאמר זה מסגרת אנליטית לניתוח מבצעי השפעה, יציג את מתקפות הכופרה כמבצעי סייבר התקפיים בתוך המסגרת האנליטית המתוארת, ויביא שני מקרים שידגימו כיצד מרחב הסייבר מנוצל למבצעי השפעה באופן זה.

מבצעי השפעה בתוך מרחב הסייבר ובאמצעותו

מבצעי השפעה הם פעולות המתרחשות בתוך סביבת המידע ובאמצעותו, במטרה להשפיע על עמדות, התנהגויות וקבלת ההחלטות של קהל מסוים, וכדי לקדם את מטרותיו של התוקף מבלי להזדקק להפעלת כוח קטלני. מבצעי השפעה מתרחשים בין המשפיע למושפע, ובנויים בדרך כלל מרצף שלבים הכולל הכנה, ביצוע ומינוף ההצלחה. שלב ההכנה מורכב מהגדרת היעד ובחירת נרטיב אסטרטגי מתאים. נרטיב זה הוא מבנה המתאר עתיד משותף ורצוי, שעימו המשפיע והמושפע יכולים להזדהות, ולאחר מכן מתורגם למסגור מתאים.[11] מסגור זה נועד לנצל הִיוריסטיקות קוגניטיביות של קהל היעד, באופן שיגרום למושפע לקבל את ההחלטות הרצויות על ידי המשפיע.

בשלב הביצוע, המסר הממוסגר שהוכן מוחדר לתוך סביבת המידע באמצעות התקשרות ישירה עם קהל היעד או באמצעות גורמים מתווכים.[12] פעולות שהצליחו מחייבות מינוף, כמו למשל, באמצעות כלים שיווקיים שיחזקו את הנרטיבים שהוחדרו או על ידי בחירת מטרות חדשות שיחזקו את הלגיטימיות הנתפסת של הנרטיב.[13] "הצלחה" מושגת כאשר סביבת המידע של המושפע מתעצבת באופן שמוביל אותו לשנות את התנהגותו או כאשר יעדיו הפוליטיים משתנים באופן שעולה בקנה אחד עם כוונותיו של המשפיע.

נהוג לתאר את מרחב הסייבר כמורכב משלוש שכבות: שכבת הרשת הפיזית, השכבה הלוגית והפרסונה הווירטואלית. שכבת הרשת הפיזית של מרחב הסייבר כוללת מרכיבים גאוגרפיים לצד מרכיבים רשתיים ואת הקשרים הפיזיים ביניהם. התוצאה היא רשת עתירת חיבוריות של רשתות, חופפות לעיתים, המשמשת כתווך הנתונים במרחב הסייבר. השכבה הלוגית כוללת אלמנטים לא מוחשיים, כמו נתונים או קוד ("אפס ואחד"), שהם הפשטה של שכבת הרשת הפיזית, כלומר הצורה שלהם והיחסים ביניהם אינם קשורים לנתיבים או לצמתים ספציפיים הקיימים בשכבת הרשת הפיזית.

לדוגמה, מערכות הפעלה, פרוטוקולים, יישומים, רכיבי תוכנה ונתונים נוספים. שכבת הפרסונה הווירטואלית מייצגת רמה גבוהה עוד יותר של הפשטה מהשכבה הלוגית. היא עושה שימוש בכללים החלים בשכבה הלוגית כדי ליצור ייצוג זהות דיגיטלי לאדם או לישות במרחב הסייבר. כך, אנשים וארגונים אמיתיים יכולים לגשת לרמה הלוגית של מרחב הסייבר באמצעות מזהים כגון כתובות דואר אלקטרוני או חשבונות בפלטפורמות מדיה חברתית. הזהויות בשכבת הפרסונה הווירטואלית עשויות להיות שונות מאוד מאלה שבתחום הפיזי, שכן יחידים ומדינות יכולים לשנות את התכונות שלהם באמצעות מניפולציה של השכבה הלוגית והפיזית ברשת. אפשר לעשות זאת דרך טכנולוגיות של "אנונימיזציה", כגון רשת TOR.[14] השכבה הלוגית ושכבת הפרסונה הווירטואלית מרכיבות ביחד את הממד הווירטואלי של מרחב הסייבר, אשר גם חופף לממד הווירטואלי של סביבת המידע.

כאשר דנים במבצעי השפעה מבוססי סייבר או בפעולות סייבר התומכות במבצעי השפעה, מפתה להתמקד רק בממד הווירטואלי של סביבת המידע. חשיבות השכבה הלוגית של מרחב הסייבר למבצעי השפעה ברורה. שכבה זו מייצגת את המידע המאוחסן במרחב הסייבר שמבצעי ההשפעה מבקשים לנצל באמצעות פגיעה בסודיות או בשלמות המידע של אדם, ארגון או ממשלה.[15]

---

11 George Lakoff, Chapter 1, in *The Political Mind: A Cognitive Scientist's Guide to Your Brain and Its Politics* (Penguin, 2008), 22.

12 Lin and Kerr, *On Cyber-Enabled Information Warfare and Information Operations:* Pijpers and Ducheine, *Influence Operations in Cyberspace - How They Really Work*.

13 Robert B Cialdini, Social Proof: Truths Are Us, in *Influence: The Psychology of Persuasion*, vol. 55 Collins New York, 2007, 114.

14 Roger Dingledine, Nick Mathewson, and Paul Syverson, Tor: The Second-Generation Onion Router, in *In Proceedings of the 13th Usenix Security Symposium*, 2004, https://doi.org/10.21236/ADA465464.

15 לפעמים מכונה גם "doxfare", "doxing" או "פריצה והדלפה" - כאשר ידוע שהמידע שדלף נגנב בעבר באמצעות אירוע פריצה. ראו, למשל, Baezner and Cordey, *Influence Operations and Other Conflict Trends*; Brangetto and Veenendaal, *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations*; Lin and Kerr, *On Cyber-Enabled Information Warfare and Information Operations*; Pijpers and Ducheine, *Influence Operations in Cyberspace - How They Really Work*. לדוגמה על ניצול מוצלח של פגיעה בשלמות נתונים או סודיות נתונים לצורך השפעה, ראו: Nikolay Koval, Revolution Hacking, *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (2015), 55–65, https://www.ccdcoe.org/uploads/2018/10/Ch06_CyberWarinPerspective_Koval.pdf; Heidi Moore and Dan Roberts, AP Twitter Hack Causes Panic on Wall Street and Sends Dow Plunging, *The Guardian*, April 23, 2013, https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall.

פעולות אלו נועדו לזרוע בלבול ולשחוק את אמון האזרחים על ידי חשיפת מידע שלא נועד לצריכה ציבורית והפניית תשומת לב לא פרופורציונלית אליו.

הניצול של שכבת הפרסונה הווירטואלית מציע הזדמנות נוספת למבצעי השפעה. הוא מאפשר מיקוד בקהל יעד ספציפי ותקשורת ישירה עימו, וכך יכול התוקף להחדיר את מסרי ההשפעה ללא תלות בגורמי התיווך או פילטרים של המדיה המסורתית. זו דרך נפוצה לנצל רשתות חברתיות שכן הן מאפשרות הפצה חופשית ובלתי מוגבלת על ידי המשאבים הזמינים למשפיע של הודעות, ויכולת להבליט מסרים שבאופן טבעי לא היו מובלטים. התוצאה היא הוספת נופך של אמינות למסר, בתוך מינוף ההטיות הקוגניטיביות של תאימות ואישוש חברתי,[16] והכפלת יעילותן פי כמה. המסרים המוגברים יכולים להשפיע בזכות עצמם,[17] וכך הם יכולים לשמש דוגמה למבצעי השפעה שאפשר להוציא לפועל בשכבת הפרסונה הווירטואלית בלבד. לחלופין, אפשר לנצל את שכבת הפרסונה הווירטואלית כדי למנף פעולות סייבר מוצלחות שהתרחשו בשכבה הלוגית.[18]

אפשר להסביר את הנטייה להשתמש במרחב הסייבר לצורך מימוש מבצעי השפעה בעובדה שרובם של המבצעים הללו הם יחסית לא מתוחכמים, ולכן גם בעלי עלות מימוש נמוכה מאוד.[19] נוסף על כך בשל האנונימיות האופיינית במרחב הסייבר מחד גיסא, והיעדרן של מסגרות משפטיות מתקדמות מספיק מאידך גיסא, קיים סיכוי נמוך לזיהוי טכני של מבצע הפעולה,[20] ופירוש הדבר שהסיכון להסלמה או לתגובת נגד - נמוך. מעניין לציין כי אף שרבים ממקרי הבוחן שנהוג לצטט (כגון מתקפות מניעת שירות/DDoS) הם של מתקפות נגד שכבת הרשת הפיזית בסייבר, הספרות על מבצעי השפעה מעדיפה להתמקד באופן השימוש במתקפות הללו לניצול הממד הווירטואלי. העדפה זו נובעת ממנגנוני ההשפעה שמקרים כאלה מנצלים דרך הממד הווירטואלי, וספציפית דרך השכבה הלוגית של מרחב הסייבר. הסבר אפשרי נוסף הוא ההנחה שמתקפות המנצלות את שכבת הרשת הפיזית נעדרות יכולת להחדיר מסרים ונרטיבים, ולכן אינן מועילות למבצעי השפעה.

חריגה מעניינת ממגמה זו היא עבודה עדכנית של דולב וסימן-טוב, שבדקה שורה של מתקפות כופר בישראל שיוחסו לגורמי איום המקושרים לאיראן. החוקרים ציינו כי ההתנהגות שהוצגה במהלך אותן תקריות אינה תואמת את המוטיבציה הכספית האופיינית למתקפות כופר אלא את זו של מבצעי השפעה.[21] המאמר הנוכחי מתבסס על הנחת יסוד זו, ומרחיב אותה לחקר ישימות ההשפעות דרך שכבת הרשת הפיזית, לצורך מבצעי השפעה וכתמיכה בהם.

מתקפת כופר כאמצעי השפעה

תוכנת כופר היא תת־קבוצה של נוזקות שנועדה לפגוע בזמינות הנתונים על ידי הגבלת הגישה אליהם כל עוד לא מועבר סכום הכופר המבוקש.[22] בחלוף הזמן, גורמי האיום שאימצו שיטה זו לא הסתפקו בהחדרת תוכנות זדוניות ובתקווה שהקורבן ייענה לדרישת הכופר,[23] אלא הוסיפו שני אלמנטים משמעותיים. האחד היה המעבר ל"כופרות נעילה", תוכנה שמשביתה את תפקוד המערכת ומציגה "הודעת כופר" עד לתשלום הכופר. בצורה זו משובשת זמינות המערכת המותקפת וגם מוצג מסר שקשה להתעלם ממנו. האלמנט השני הוא מעבר לטקטיקת "סחיטה כפולה", שבה גורם האיום פוגע בחיסיון הנתונים של הקורבן באמצעות גנבת

16 Cialdini, *Social Proof: Truths Are Us*.

17 לדוגמה למסרים באלה, לרבות דיסאינפורמציה ושימוש בטרולים, ראו: Hunt Allcott and Matthew Gentzkow, Social Media and Fake News in the 2016 Election, *Journal of Economic Perspectives* 31, no. 2 May 2017: 211–236, https://doi.org/10.1257/jep.31.2.211; Alexander Lanoszka, Disinformation in International Politics, *European Journal of International Security* 4, no. 2 June 2019: 227–248, https://doi.org/10.1017/eis.2019.6; Robert S. Mueller III, Report on the Investigation Into Russian Interference in the 2016 Presidential Election. Volumes I & II.(Redacted Version of 4/18/2019), 2019; J.-B. Jeangène Vilmer et al., Information Manipulation: A Challenge for Our Democracies, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

18 Pijpers and Ducheine, *Influence Operations in Cyberspace - How They Really Work*.

19 Baezner and Cordey, *Influence Operations and Other Conflict Trends*; Lin and Kerr, *On Cyber-Enabled Information Warfare and Information Operations*; Max Smeets, *The Strategic Promise of Offensive Cyber Operations*, 2018.

20 Clara Assumpção, The Problem of Cyber Attribution Between States, *E-International Relations* (blog), May 6, 2020, https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/; Florian J. Egloff, Contested Public Attributions of Cyber Incidents and the Role of Academia, *Contemporary Security Policy* 41, no. 1 January 2, 2020: 55–81, https://doi.org/10.1080/13523260.2019.1677324; Oliver Fitton, Cyber Operations and Gray Zones: Challenges for NATO, *Connections* 15, no. 2 (2016): 109–19, https://www.jstor.org/stable/26326443; Thomas Rid and Ben Buchanan, Attributing Cyber Attacks, *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37, https://doi.org/10.1080/01402390.2014.977382.

21 Boaz Dolev and David Siman-Tov, Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks, *INSS Special Publication*, January 27, 2022, https://www.inss.org.il/publication/cyber-iran/.

22 Amin Kharraz et al., Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks, in Detection of Intrusions and Malware, and Vulnerability Assessment, ed. Magnus Almgren, Vincenzo Gulisano, and Federico Maggi, vol. 9148, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2015), 3–24, https://doi.org/10.1007/978-3-319-20550-2_1

23 התקפות כופר מוקדמות בחרו רק להגביל את הגישה לנתונים, והותירו את המערכת עצמה פונקציונלית. כך הם גרמו לקורבנות להיות לא מודעים לאירוע המתרחש, כל עוד לא ניסו להשתמש בנתונים שננעלו. נוסף על כך קורבנות של אירועים כאלה עשויים להחזיק גיבוי של הנתונים ולשחזר אותם מהגיבוי במקום לשלם את הכופר.

המידע קודם להגבלת הגישה, ובכך יוצר תמריץ נוסף לקורבן לשלם את הכופר, אחרת המידע יודלף לציבור.[24]

ההתפתחות הזו הפכה את תוכנת הכופר לכלי פוטנציאלי לשימוש במבצעי השפעה, שכן "כופרות נעילה" מציעה הזדמנות לתקוף את השכבה הלוגית של מרחב הסייבר ולהחדיר מסגרת השפעה לסביבת המידע המותקפת, ובו בזמן מונעת מהיעד את היכולת להימנע מהמסגרת שהוחדרה, הודות לשיבוש שכבת הרשת הפיזית. לבסוף, באמצעות השפעות משבשות פעילות במרחב הסייבר, מתקפות כופר מתוכננות היטב יכולות לגרום לשיבוש גם בעולם הפיזי, ובאופן שעדיין יאפשר מרחב הכחשה.[25]

לאור השיבוש שנגרם בשכבת הרשת הלוגית ושכבת הרשת הפיזית בשל הפגיעה בזמינות המערכת והנתונים, ובזכות אפקט ההכחשה שמרחב הסייבר מאפשר, אפשר לראות במתקפות כופר סוג של מבצע סייבר התקפי. השילוב בין טקטיקות של "כופרת נעילה" עם "סחיטה כפולה" יכול להשיג אפילו יותר: נוצרת הזדמנות לערוץ מסרים נוסף ולכיסוי המאפשרים יכולת לניצול יעיל יותר, במקום להסתפק בפעולת 'פריצה והדלפה' קלסית. מתקפת כופר מציעה גם אפשרות מעניינת ולפיה שחקנים לא מתואמים או כמעט לא מתואמים, יהיו מסוגלים להשיג השפעות שיכולות להגיע לרמה דומה למבצע השפעה בכל הקשור לשינוי סדרי עדיפויות של מדיניות, בזכות אפקט מצטבר של השפעות מסדר שני ומעלה, כגון ערעור אמון האזרחים בשירותים ממשלתיים או הסטת משאבים.[26]

לאחר שהכרנו מתקפות כופר כצורה של מבצע סייבר התקפי, והצגנו מסגרת אנליטית להערכת מבצעי השפעה, מאמר זה ימשיך כעת ליישום המסגרת האנליטית על שני מקרי בוחן: מתקפת הכופר נגד אלבניה ביולי 2022, וקמפיין "BlackShadow" נגד ישראל בשנים 2022-2023.

מקרה בוחן 1: מתקפת הכופר על פורטל e-Albania של ממשלת אלבניה

ב־15 ביולי 2022, רגע לפני הפסגה העולמית למען אירן חופשית - אירוע המזוהה עם ארגון מוג'אהדין ח'לק[27] שתוכנן להתקיים בסוף יולי ליד העיר דורס שבאלבניה - הותקפה הסוכנות הלאומית לחברת מידע של אלבניה (AKSHI) על ידי גורם איום שכינה את עצמו "HomeLand Justice", והציג את עצמו כארגון אלבני המתנגד לתמיכת הממשלה במוג'אהדין ח'לק. התקרית כללה החדרת תוכנות כופר ששיבשו את פעילות הפורטל של ממשלת אלבניה, e-Albania , וגם פגעו באתרי אינטרנט ובשירותים רבים נוספים של ממשלת אלבניה. בהצהרה שנשא ראש ממשלת אלבניה נאמר שמטרת מתקפת הסייבר הייתה לשתק את השירותים הציבוריים, למחוק מערכות דיגיטליות, לפרוץ לרשומות מדינה, לגנוב תקשורת אלקטרונית ממשלתית פנימית, ולעורר כאוס וחוסר ביטחון במדינה. [28]

כדי לסייע לצמצום הנזק מהמתקפה, גייסה ממשלת אלבניה את תמיכת ארה"ב, בעלת בריתה בנאט"ו. אנשי ה־FBI ואנשי פיקוד הסייבר של ארה"ב הובאו כדי לסייע בחקירת האירוע, ולבצע מבצע ציד (forward hunt) ברשתות של ממשלת אלבניה. נוסף

24 Catalin Cimpanu, Reveton Ransomware Distributor Sentenced to Six Years in Prison in the UK, *ZDNet*, April 9, 2019, https://www.zdnet.com/article/reveton-ransomware-distributor-sentenced-to-six-years-in-prison-in-the-uk/; Kevin Savage, Peter Coogan, and Hon Lau, The Evolution of Ransomware, August 6, 2015, https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf.

25 Sara Morrison, The Chaotic and Cinematic MGM Casino Hack, Explained, *Vox*, September 15, 2023, https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware; Jack Beerman et al., A Review of Colonial Pipeline Ransomware Attack, in *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 2023, 8–15, https://doi.org/10.1109/CCGridW59191.2023.00017; Andy Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; Ax Sharma, BlackCat (ALPHV) Claims Swissport Ransomware Attack, Leaks Data, *BleepingComputer* (blog), February 15, 2022, https://www.bleepingcomputer.com/news/security/blackcat-alphv-claims-swissport-ransomware-attack-leaks-data/.

26 Jamie MacColl et al., The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society, *RUSI*, January 2024, https://static.rusi.org/ransomware-harms-op-january-2024.pdf.

27 People's Mujahedeen Organization of Iran is an Iranian opposition organization based in Albania, posing as a future government-in-exile.

28 Videomessage of Prime Minister Edi Rama, Albanian Government Council of Ministers, September 7, 2022, https://www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama/; Luke Jenkins et al., *ROADSWEEP Ransomware Targets the Albanian Government, Mandiant*, August 4, 2022, https://www.mandiant.com/resources/blog/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against.

על כך פנתה הממשלה למגזר הפרטי, ובמיוחד לצוותי התגובה לאירועי סייבר של Microsoft - DART ו־Mandiant.[29] במרכז האירוע עמדה נוזקת כופר חדשה, אשר, בין השאר, הציגה מסר פוליטי על מסכי המערכות שהוצפנו: "מדוע שהמיסים שלנו ישמשו כדי לממן את הטרוריסטים של דורס?". למסר הצטרף קמפיין נרחב ברשתות החברתיות על בסיס חומרים שנגנבו מפורטל AKSHI עוד קודם לשלב המשבש של המתקפה. DART Microsoft הצליח לייחס את שחקן האיום "Justice HomeLand" למשרד המודיעין והביטחון האיראני, על בסיס ממצאים פורנזיים וייחוס פומבי קודם. הייחוס צוטט על ידי ראש ממשלת אלבניה, אדי רמה, שהצהיר כי "מתקפת הסייבר ביולי בוצעה על ידי קבוצות האקרים מרובות הקשורות לרפובליקה האסלאמית. זוהו ארבע קבוצות, אחת מהן היא ארגון טרור סייבר בין־לאומי ידוע לשמצה עם היסטוריה של תקיפה במדינות כמו ישראל או סעודיה".[30].

בעקבות מתקפת הסייבר הזו, ב־7 בספטמבר 2022, פרסמה ממשלת אלבניה תגובה דיפלומטית חסרת תקדים בחריפותה שכללה ייחוס רשמי של המתקפה לאיראן. אלבניה הודיעה על ניתוק כל הקשרים הדיפלומטיים שלה עם איראן, והורתה לצוות הדיפלומטי האיראני באלבניה לעזוב את המדינה בתוך 24 שעות.[31] התגובה האלבנית זכתה להצהרות תמיכה מבריטניה, נאט"ו, האיחוד האירופי וארה"ב.[32] יתרה מזאת: הלשכה לבקרת נכסים זרים של משרד האוצר האמריקני (OFAC) הטילה סנקציות על משרד המודיעין והביטחון האיראני ועל שר המודיעין האיראני איסמעיל חטיב, והקפיאה את נכסיהם. [33]

כאשר מנתחים את רצף מתקפות הסייבר נגד אלבניה כמבצע השפעה, מתבררים הדברים האלה: אף שאי־אפשר לדעת את הכוונה האסטרטגית המלאה של מבצע ההשפעה, המסגור שנבחר למסר שהציגה תוכנת הכופר[34] וקמפיין ההמשך ברשתות החברתיות,[35] טענו שמדובר במחאה נגד "שחיתות שלטונית" ו"תמיכה בטרור". המסרים שהופיעו ברשתות החברתיות בהמשך טענו שהמתקפה כוונה נגד הממשלה ולא נגד אזרחים אלבנים. לכאורה, מתבקש להניח שהמטרה האסטרטגית מאחורי המתקפה הייתה למנוע מארגון מוג'אהדין ח'לק את התמיכה הפוליטית של ממשלת אלבניה. השערה נוספת היא שמכיוון שהמתקפה התחוללה לאחר סדרה של אירועי סייבר שהתרחשו באיראן[36] וחלקם יוחסו למוג'אהדין ח'לק, המטרה האסטרטגית הייתה נקמה וביסוס הרתעה באופן שיאלץ את ממשלת אלבניה לנקוט פעולה ולהגביל את יכולתו של הארגון לבצע מתקפות סייבר נגד איראן.[37] מתגובת הממשלה האלבנית - ובפרט הרכיב הדיפלומטי בה - אפשר להסיק כי מבחינתה נתפס מבצע ההשפעה כבלתי רצוי ואף זדוני.

תגובת ממשלת אלבניה למתקפה כללה שורה של ניסיונות ליטול יוזמה ולהרתיע מפני מתקפות נוספות. תגובתה הראשונית הייתה הגנתית, מתוך מטרה לעצור כל פעילות תקיפה נוספת ברשת AKSHI, וכדי לשחזר את זמינות השירות. השלב הבא היה ניסיון

---

29 Cyber & Infrastructure Security Agency, *Iranian State Actors Conduct Cyber Operations Against the Government of Albania*, September 23, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a; Cyber National Mission Force Public Affairs, *'Committed Partners in Cyberspace': Following Cyberattack, US Conducts First Defensive Hunt Operation in Albania*, U.S. Cyber Command, March 23, 2023, https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/; Jenkins et al., ROADSWEEP Ransomware Targets the Albanian Government; Microsoft Threat Intelligence, Microsoft Investigates Iranian Attacks against the Albanian Government, *Microsoft Security Blog*, September 8, 2022, https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/.

30 Videomessage of Prime Minister Edi Rama.

31 Florion Goga et al., Albania Cuts Iran Ties over Cyberattack, U.S. Vows Further Action, *Reuters*, September 7, 2022, https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/; Videomessage of Prime Minister Edi Rama.

32 Council of the EU, *Cyber-Attacks: Declaration by the High Representative on Behalf of the European Union Expressing Solidarity with Albania and Concern Following the July Malicious Cyber Activities* Council of the EU, September 8, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/09/08/cyber-attacks-declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-albania-and-concern-following-the-july-malicious-cyber-activities/; Foreign, Commonwealth & Development Office and The Rt Hon James Cleverly MP, UK Condemns Iran for Reckless Cyber Attack against Albania GOV.UK, September 7, 2022, https://www.gov.uk/government/news/uk-condemns-iran-for-reckless-cyber-attack-against-albania; NATO, *Statement by the North Atlantic Council Concerning the Malicious Cyber Activities against Albania* NATO, September 8, 2022, https://www.nato.int/cps/en/natohq/official_texts_207156.htm; The White House, *Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania*, September 7, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/.

33 U.S. Department of the Treasury Office of Foreign Assets Control, *Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities* (U.S. Department of the Treasury, September 9, 2022), https://home.treasury.gov/news/press-releases/jy0941; A. J. Vicens, U.S. Sanctions Iranian Ministry of Intelligence in Response to Albanian Cyberattack, *CyberScoop* (blog), September 9, 2022, https://cyberscoop.com/microsoft-albania-iran-cyberattack/.\\uc0\\u8221{} {\\i{}CyberScoop} (blog

34 *Jenkins et al., Roadsweep Ransomware Targets the Albanian Government.*

35 Microsoft Threat Intelligence, Microsoft Investigates Iranian Attacks against the Albanian Government.

36 השערה זו, כמו גם חלק מהניתוחים הבאים, מניחה שהייחוס הפוליטי של המתקפה שעליה הצהיר אדי רמה ב"סרטון הודעת ראש הממשלה אדי רמה" הוא נכון.

37 The Grugq, Albanian Cyber War, Substack newsletter, The Info Op (blog), September 7, 2022, https://grugq.substack.com/p/albanian-cyber-war; Mahmoud Hakam, Major Cyber Attack on Tehran's Islamic Culture & Relations Organization, *Iran News Update* (blog), July 4, 2022, https://irannewsupdate.com/news/iranian-opposition/major-cyber-attack-on-tehrans-islamic-culture-relations-organization/; AP News, Iran Exiles Claim Disrupting Tehran's Surveillance Cameras, *AP News*, June 2, 2022, https://apnews.com/article/politics-iran-middle-east-dubai-united-arab-emirates-f9b79784cba77adcf8c88dafde11ee84; A. J. Vicens, Deep Dive into Hack against Iranian State TV Yields Wiper Malware, Other Custom Tools, *CyberScoop* (blog), February 18, 2022, https://cyberscoop.com/iran-state-tv-hack-predatory-sparrow-indra/.

עניינה. אלבניה שקלה לזמן קצר להפעיל את סעיף 5 באמנת נאט"ו,[38] אך לבסוף חזרה בה, ככל הנראה בעקבות הייחוס הטכני המובהק לתוקפים,[39] והסכימה לתגובה דיפלומטית חזקה במיוחד בשילוב סנקציות כלכליות שיטיל משרד האוצר האמריקני נגד החשודים במתקפה. מתקפה נוספת של קבוצת "HomeLand Justice" שהתרחשה בספטמבר 2022 נגד מערכת TIMS של משמר הגבול האלבני, הראתה כי התגובה החריפה ככל הנראה לא הייתה מספיקה כדי להרתיע מפני מתקפות נוספות.

מבחינה מבצעית, מתקפת e-Albania השתמשה בתוכנה (וליתר דיוק נוזקת כופר) כדי לשבש ישויות ושירותים ברמה הפיזית, הלוגית, וברמת הפרסונה הווירטואלית של מרחב הסייבר, מה שהופך את האירוע למבצע סייבר התקפי. אם מנתחים זאת כמבצע השפעה, במהלך מתקפת e-Albania ניצלו התוקפים את השכבה הלוגית להחדרת הנרטיב והמסרים שלהם, ובד בבד ניסו לנצל גם את שכבת הפרסונה הווירטואלית, אם כי לא נמצאו ראיות שהצליחו. נוסף על החדרת המסרים, ניצלו התוקפים את הפגיעה בשכבה הלוגית לטובת גנבת מידע רגיש, שהודלף בשלב הבא של מבצע ההשפעה, אם כי שוב, לפחות ככל שהראיות הגלויות מראות, הוא אינו מונף לפגיעה נוספת.

מקרה בוחן 2: קמפיין "BlackShadow" נגד ישראל 2020–2023

במוקד המקרה השני עומדת סדרת המתקפות של קבוצת פושעי הסייבר המכנה את עצמה בשם "BlackShadow" ("צל שחור"), שהחלה בדצמבר 2020 ונמשכה עד דצמבר 2023. המתקפה הראשונה שהקבוצה ביצעה הייתה נגד חברת הביטוח הישראלית שירביט. זו לא הייתה מתקפת כופר אלא מתקפת פריצה והדלפה.[40] במהלכה לא נעשה שימוש במסרים משפיעים ספציפיים, ואפשר לראות בה מבצע השפעה רק במובן הבסיסי ביותר, של ניסיון לערער את אמון הציבור במדינה ולזרוע כאוס.[41] כאשר נחשפה המתקפה לציבור, טענו נציגי שירביט כי מדובר במתקפת טרור בסייבר נגד ישראל ולא במתקפה ממניעים כלכליים. טענה זו קיבלה חיזוק נוסף בדוח של חברת אבטחת הסייבר הישראלית ClearSky, שהודלף לעיתון כלכלי ישראלי.[42]

הדוח של ClearSky הציע קשר אפשרי לאיראן או ל־OpIsrael,[43] על סמך השימוש בהאשטאג המתאים במסרים הראשונים ש"BlackShadow" עשו בהם שימוש ברשתות החברתיות, והצליח לשים את ידיו על הנוזקה ששימשה, להערכתם - ברמת סמך בינונית, במהלך המתקפה. חברות אבטחת סייבר נוספות ייחסו מאוחר יותר את הנוזקה הזו לפעילות הקשורה לאיראן, בשל קווי דמיון טכניים ומבצעיים.[44] גורמי האיום טענו למתקפה ממניעים כלכליים, אולם הטקטיקה שלהם חרגה מהטכניקות הרגילות שמשמשות קבוצות כופר כדי ללחוץ על קורבנותיהם לשלם. כך למשל, הקבוצה פנתה ישירות לכלי תקשורת ופרסמה חלקים מתכתובת המשא ומתן.[45] התנהלות יוצאת דופן זו הובילה את שירביט לטעון שהמתקפה היא "טרור סייבר". למרות זאת, מעורבות סוכנויות הביטחון והסייבר הישראליות נותרה מינימלית, והוגבלה לדיווח על אודות האירוע ולפרסום הנחיות מעודכנות לאור לקחיו להיגיינת סייבר עבור חברות ישראליות, מטעם מערך הסייבר הלאומי של ישראל.[46]

לאחר המתקפה על שירביט המשיך גורם האיום "BlackShadow" לבצע פעולות 'פריצה והדלפה' נוספות נגד מטרות ישראליות,

---

38 Maggie Miller, Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack, *Politico* (blog), October 5, 2022, https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347.

39 אם כי היה דוח ראשוני של Mandiant שייחס את התקיפה לאיראן: *Jenkins et al., Roadsweep Ransomware Targets the Albanian Government*. בחודש לאחר המתקפה הראשונית, טענות הייחוס המשמעותיות יותר והמבוססות טכנית הוצגו על ידי CISA ומיקרוסופט בשילוב עם הגינוי הדיפלומטי. Cyber & Infrastructure Security Agency, *CISA* AA22-264A; Microsoft Threat Intelligence, *Microsoft Investigates Iranian Attacks against the Albanian Government*.

40 Tzvi Joffre, Government to Reconsider Using Shirbit Insurance After Large Cyberattack, *Jerusalem Post,* December 7, 2020, https://www.jpost.com/israel-news/government-to-reconsider-using-shirbit-insurance-after-large-cyberattack-651382.

41 Brangetto and Veenendaal, Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations; *Koval, Revolution Hacking*; Lin and Kerr, On Cyber-Enabled Information Warfare and Information Operations.

42 Amitai Ziv, Cyber Attack on Shirbit—Who Is Behind It and Why? [in Hebrew] TheMarker, December 4, 2020, https://www.themarker.com/technation/2020-12-04/ty-article/.premium/0000017f-db42-df9c-a17f-ff5a9c540000?lts=1713292167615; סקירת אירוע סייבר בחברת שירביט 1.12 Tel Aviv, Israel: ClearSky Cyber Security, December 1, 2020), https://img.haarets.co.il/bs/0000017f-db52-d856-a37f-ffd215bd0000/cd/b5/edfbba34893bebc024fc4a688593/20201204-101626.pdf.

43 OpIsrael היא מתקפת סייבר שנתית מתואמת, שבה האקטיביסטים תוקפים אתרים של ממשלת ישראל ואפילו אתרים פרטיים במתקפות DDoS ואחרות. David Shamah, As Cyber-War Begins, Israeli Hackers Hit Back, *The Times of Israel* (blog), April 7, 2013, http://www.timesofisrael.com/as-cyber-war-begins-israeli-hackers-hit-back/.

44 Amitai Ben Shushan Ehrlich, From Wiper to Ransomware: The Evolution of Agrius, *SentinelOne Labs*, May 25, 2021, https://assets.sentinelone.com/sentinellabs22/evol-agrius; An In-Depth Look at APT33, *CyberWarCon*, 2019.

45 Dolev and Siman-Tov, *Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks*.

46 INCD Spokesperson, Data Breach Event at Shirbit, *Israel National Cyber Directorate*, December 1, 2020, https://www.gov.il/en/pages/news_shirbit.

אולם הן לא הצליחו לייצר תשומת לב תקשורתית משמעותית. באוגוסט 2021 אימצה הקבוצה טקטיקה חדשה, כאשר לראשונה השתמשה בתוכנת כופר נגד יעד ישראלי בעת מתקפה נגד אוניברסיטת בר־אילן.[47] מתקפה זו לא זכתה לתשומת לב תקשורתית רבה, אך דווח כי בתגובה לאירוע הייתה מעורבות של מערך הסייבר הלאומי ושירותי הביטחון הישראליים. בדומה לקורבנות קודמים של "BlackShadow", גם אוניברסיטת בר־אילן טענה כי התקרית היא אירוע טרור סייבר, והפנתה אצבע מאשימה לאיראן. מעניין לציין כי אף ששירותי הביטחון הישראליים שמרו על שתיקה לגבי ייחוס הקבוצה, דולב וסימן-טוב[48] חיזקו טענה זו על בסיס היכרותם עם מאמצי התגובה למתקפות "BlackShadow". החוקרים ציינו כי התנהלותו של שחקן האיום אינה אופיינית למתקפת כופר, שכן היא כללה הטחת עלבונות וגידופים במנהלי המשא ומתן, ומסרים פוליטיים פשטניים באנגלית עילגת, המעידים על מניע שונה מסחיטת כסף.

לאחר המתקפה על אוניברסיטת בר־אילן, המשיכו "BlackShadow" לתקוף גופים ישראליים, כמו תעשיית היהלומים במרץ 2022,[49] ומוסדות טכנולוגיה וחינוך במהלך שנת 2023.[50] המתקפות כללו פעולות השמדת נתונים (wiper) ושימוש בתוכנות כופר, אך לא הצליחו למשוך תשומת לב ציבורית רבה. בסופו של דבר, באוקטובר 2023, נראה היה ששחקן איום נוסף (שכינה את עצמו "צוות מאלק") ביצע מתקפת 'פריצה והדלפה' מוצלחת נגד המכללה האקדמית אונו, הדליף כמות רבה של פרטים אישיים ומידע רגיש, וגרם לשיבוש מסוים בשירותי המכללה.[51]. מאוחר יותר, בדצמבר 2023, ביצע אותו שחקן מתקפת 'פריצה והדלפה' נגד המרכז הרפואי זיו, כאשר שוב הודלפו אינספור פריטי מידע פרטי ורגיש, אם כי ללא עדות לשיבוש תפקודו של המרכז הרפואי.[52] בעקבות התקרית הזו מיהר מערך הסייבר הלאומי לייחס אותה ואת שחקן האיום "צוות מאלק" לממשלת איראן, וספציפית לאותו גורם שהזדהה בעבר בתור "BlackShadow". נוסף על כך הבהירה לראשונה הצהרת הייחוס כי שיטת הפעולה הרגילה של "BlackShadow" (הכוללת את שיבוש פעילות קורבן המתקפה באמצעות תוכנות כופר או נוזקות השמדת מידע) לא יושמה במקרה של המתקפה על המרכז הרפואי זיו, הודות לפעילות של כוחות השב"כ וצה"ל, שהשתתפו אף הם בהכלת התקיפה וזיהוי מקורה. [53]

מניתוח קמפיין "BlackShadow" כמבצע השפעה עולה, כי בניגוד לקמפיין "HomeLand Justice" נגד אלבניה, קשה יותר להבחין בנרטיב או בכוונה אסטרטגית ספציפיים, שכן הנרטיבים הנבחרים משתנים לעיתים קרובות, לפעמים אפילו בתוך כדי אירוע תקיפה. התנהגות כזו עשויה להתאים למטרה אסטרטגית של "זריעת כאוס" או החלשת הלכידות החברתית דרך פגיעה באמון האזרחי במוסדות הלאומיים.[54] מבחינה טקטית, קמפיין "BlackShadow" התפתח ממבצע השפעה קלסי לסדרה של מתקפות 'פריצה והדלפה' למימוש שיטות סייבר התקפי.

---

47 Amitai Ben Shushan Ehrlich, New Version of Apostle Ransomware Reemerges in Targeted Attack on Higher Education, *SentinelOne* (blog), September 30, 2021, https://www.sentinelone.com/labs/new-version-of-apostle-ransomware-reemerges-in-targeted-attack-on-higher-education/; Mass Data Leak after Bar Ilan University Refuses to Pay Hacker $2.5m, *Times of Israel* (blog), September 9, 2021, https://www.timesofisrael.com/liveblog_entry/mass-data-leak-after-bar-ilan-university-refuses-to-pay-hacker-2-5m/; Amitai Ziv, Cyberattack Hits Israel's Bar Ilan University: 'Data Is Being Erased Right Now,' *Haaretz*, August 15, 2021, https://www.haaretz.com/israel-news/tech-news/2021-08-15/ty-article/.premium/cyberattack-on-israeli-university-data-being-erased-right-now/0000017f-e396-d75c-a7ff-ff9ff65a0000; Amitai Ziv, Does Crime Pay? A Conversation with a Hacker Targeting Israel, *Haaretz*, September 1, 2021, https://www.haaretz.com/israel-news/tech-news/2021-09-01/ty-article/.premium/does-crime-pay-a-conversation-with-a-hacker-targeting-israel/0000017f-f15d-dc28-a17f-fd7f7f3d0000.

48 Dolev and Siman-Tov, Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks.

49 Adam Burgher, Fantasy: A New Agrius Wiper Deployed through a Supply-Chain Attack, *WeLiveSecurity* (blog), September 7, 2022, https://www.welivesecurity.com/2022/12/07/fantasy-new-agrius-wiper-supply-chain-attack/

50 Or Chechik et al., Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors, *Unit 42* (blog), November 6, 2023, https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/; Marc Salinas Fernandez and Jiri Vinopal, Agrius Deploys Moneybird in Targeted Attacks Against Israeli Organizations, *Check Point Research* (blog), May 24, 2023, https://research.checkpoint.com/2023/agrius-deploys-moneybird-in-targeted-attacks-against-israeli-organizations/; Bill Toulas, Iranian Hackers Use New Moneybird Ransomware to Attack Israeli Orgs, *BleepingComputer* (blog), May 24, 2023, https://www.bleepingcomputer.com/news/security/iranian-hackers-use-new-moneybird-ransomware-to-attack-israeli-orgs/.

51 Check Point Research, The Iron Swords War, *Check Point Blog* (blog), October 18, 2023, https://blog.checkpoint.com/security/the-iron-swords-war-cyber-perspectives-from-the-first-10-days-of-the-war-in-israel/; Ryan Gallagher, War Tests Israeli Cyber Defenses as Hack Attempts Soar, *Bloomberg*, October 18, 2023, https://www.bloomberg.com/news/newsletters/2023-10-18/war-tests-israeli-cyber-defenses-as-hack-attempts-soar.

52 Daryna Antoniuk, Iran-Linked Hackers Claim to Leak Troves of Documents from Israeli Hospital, *The Record by Recorded Future* (blog), December 4, 2023, https://therecord.media/ziv-hospital-israel-hackers-claim-to-leak-data; Inon Ben Shushan, Hackers Steal IDF Patient Records from Cyberattack on Israeli Hospital, *Jerusalem Post*, December 3, 2023, https://www.jpost.com/israel-news/defense-news/article-775843; Ministry of Health Spokesperson, *Joint Announcement by Ziv Medical Center, the Ministry of Health and the Israel National Cyber Directorate*, Ministry of Health, November 28, 2023, https://www.gov.il/en/pages/27112023-01.

53 INCD Spokesperson, Iran and Hezbollah behind an Attempted Cyber Attack on an Israeli Hospital, *Israel National Cyber Directorate*, December 18, 2023, https://www.gov.il/en/pages/ziv181223.

54 Brangetto and Veenendaal, *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations*; Koval, Revolution Hacking; Lin and Kerr, *On Cyber-Enabled Information Warfare and Information Operations*.

משך הזמן של קמפיין "BlackShadow" מאפשר לבחון גם את התפתחות מאמצי התגובה של ישראל ושל מערך הסייבר הלאומי. יצוין כי במתקפות שהתרחשו בין דצמבר 2020 למרץ 2023, בחר מערך הסייבר להסתפק בעדכון על התרחשות אירועים ולתמוך במאמצי התגובה לאירועים השונים בתוך שימת דגש על תפקידו של המגזר הפרטי בחקירה ובתגובה,[55] ובפרט בחר להותיר את מאמצי הייחוס באופן בלעדי בידי המגזר הפרטי. אולם הדבר השתנה משמעותית במתקפות של אוקטובר 2023. בשלב זה נטל מערך הסייבר תפקיד מוביל בחקירה ובתגובה לאירועי הסייבר שהיו חלק מקמפיין "BlackShadow", עם ארגוני ביטחון לאומי ישראליים נוספים. יתרה מזאת: מערך הסייבר בחר לייחס את התקריות הללו באופן פומבי ורשמי לאיראן, ואף קישר את הפרסונה של "צוות מאלק" לקמפיין "BlackShadow".[56]

אפשר לשער שהסבר חלקי ואולי אף מלא לשינוי הזה הוא תהליך ה"ביטחון" שעברו המתקפות בעקבות המלחמה נגד חמאס ברצועת עזה, הן בעיני הציבור הישראלי הן לשיטתו של גורם האיום. מעניין גם לציין כי בעת הדיווח על האירוע במרכז הרפואי זיו, בחרה העיתונות הישראלית לתאר אותו כ"המתקפה הרביעית נגד בית חולים ישראלי",[57] אף שהייתה זו התקרית הראשונה שיוחסה ל"BlackShadow" (התקריות הקודמות יוחסו לשחקנים אחרים). בכך המחישה העיתונות הישראלית את אפקט ההשפעה המצטברת שיש למתקפות סייבר, אף שבפועל ביצעו אותן ארגונים שאינם בהכרח מתואמים.

כל אלה מעלים סיבה אפשרית נוספת להיגיון שמאחורי החלטת מערך הסייבר לקחת תפקיד מוביל, ולייחס רשמית את התקריות הללו לאיראן. סביר להניח שמערך הסייבר ביקש לשבור את האפקט המצטבר של המתקפות באמצעות ייחוס רשמי וגלוי של המתקפה האחרונה לירי ידוע, וכך לייצר הבחנה בין מתקפות הכופר הקודמות שהיו על רקע פלילי, לבין האירוע האחרון. נוסף על כך ייתכן שמערך הסייבר ביקש לעורר "התכנסות סביב הדגל"[58] דרך התנהגות המאותתת שהממשלה יודעת לטפל במקרים כאלה ולהגן על האזרחים כאשר התוקף הוא מדינה יריבה. אזהרת הציבור הישראלי מפני מסרים שמגיעים ממדינת אויב תרמה גם לטשטוש אפקט מבצע ההשפעה.

בחירה בולטת נוספת שעשו הרשויות הישראליות בתגובתן לקמפיין "BlackShadow" הייתה ניסיון לעשות שימוש בחוק הגנת הפרטיות והרשות להגנת הפרטיות להגבלת התפשטות החומרים שדלפו,[59] כדי להגביל את היכולת לנצל את שכבת הפרסונה הווירטואלית להעצמת ההדלפות, ולבנות חוסן למול מבצעי השפעה נוספים.

דיון ומסקנות

מאמר זה ביקש לבחון האם מבצעי סייבר התקפיים, ומתקפות כופר בפרט, יכולים למלא תפקיד במבצעי השפעה, והתשובה היא "ככל הנראה כן". מבצעי סייבר התקפיים אינם מאפשרים לקורבן לפטור את עצמו בקלות מתוצאות התקיפה כמו באירועי 'פריצה והדלפה' כדי למנוע מהתוקפים לנצל את המתקפה למשיכת תשומת לב. תשומת הלב יכולה להיות מנוצלת (וזה מה שאכן קורה) להפצת מסרים ממוסגרים שישרתו את הכוונה הנרטיבית והאסטרטגית של יוזמי מבצע הסייבר ההתקפי. הדוגמאות שהובאו במאמר ממחישות את הוורסטיליות של מבצעי סייבר התקפיים, ואת היותם מרכיב בסל רחב יותר של מבצעי השפעה, החל מקידום כוונות אסטרטגיות ספציפיות ועד למטרות רחבות יותר דוגמת "זריעת כאוס". בשני המקרים שנבחנו ראו הקורבנות בניסיון

55 Ben Zion Gad, 'Black Shadow' Hackers Leak Data from Israeli LGBT App, *Jerusalem Post,* October 31, 2021, https://www.jpost.com/israel-news/iranian-hackers-breach-israeli-company-cyberserve-683529; INCD Spokesperson, Data Breach Event at Shirbit; Tzvi Joffre and Tamar Uriel-Beeri, Black Shadow Hackers Strike Again, Leak Documents in New Cyberattack, *Jerusalem Post* (blog), March 13, 2021, https://www.jpost.com/jpost-tech/israeli-car-financing-company-hacked-private-information-held-for-ransom-661865; Ziv, Cyberattack Hits Israel's Bar Ilan University.

56 INCD Spokesperson, Iran and Hezbollah behind an Attempted Cyber Attack on an Israeli Hospital; Ministry of Health Spokesperson, Joint Announcement by Ziv Medical Center, the Ministry of Health and the Israel National Cyber Directorate; קבוצת התקיפה האיראנית Black Shadow, *Israel National Cyber Directorate*, April 9, 2024, https://www.gov.il/BlobFolder/reports/alert_1727/he/ALERT-CERT-IL-W-1727.pdf

57 Ben Shushan, Hackers Steal IDF Patient Records from Cyberattack on Israeli Hospital; Milàn Czerny, Start-up Nation? Israel's Cyber Defense Collapsed on October 7 and Iranian Hacker Groups Keep Attacking, *Ynetnews*, January 22, 2024, https://www.ynetnews.com/business/article/hjynr11jk6; Omer Kabir, Iran and Hezbollah Were behind Cyberattack on Israeli Hospital, Says National Cyber Directorate, *CTech by Calcalist*, December 18, 2023, https://www.calcalistech.com/ctechnews/article/h1owft6it.

58 Shingo Hamanaka, The Ground Operation Sent Citizens into a Frenzy: The Rally around the Flag Effect during Operation Protective Edge, *Global Security: Health, Science and Policy* 5, no. 1 (2020): 142–52; Alan J Lambert, John P. Schott, and Laura Scherer, Threat, Politics, and Attitudes: Toward a Greater Understanding of Rally-'round-the-Flag Effects, *Current Directions in Psychological Science* 20, no. 6 (2011): 343–48; Sharon Matzkin, Ryan Shandler, and Daphna Canetti, The Limits of Cyberattacks in Eroding Political Trust: A Tripartite Survey Experiment, *British Journal of Politics and International Relations*, 2023, 13691481231210383.

59 Ministry of Health Spokesperson, *Joint Announcement by Ziv Medical Center*, the Ministry of Health and the Israel National Cyber Directorate.

ההשפעה התערבות לא רצויה, ואין זה מפתיע בהתחשב באופיו הכוחני של מבצע סייבר התקפי.

על תפיסת הכוונה שעמדה מאחורי מבצעי ההשפעה במקרי הבוחן שנותחו כאן כזדונית, אפשר להסיק גם מהחשיבות ששתי המדינות שהיו יעד השפעה נתנו לייחוס הפעולה, ומהתגובה הדיפלומטית החריפה במקרה האלבני, שכללה גינוי חריף של איראן. אומנם אמצעי התגובה שיושמו בתגובה לשיבוש ולאפקט ההשפעה היו שונים בשני המקרים, אולם שתי המדינות הדגישו את החשיבות של שיתוף פעולה ציבורי-פרטי לצמצום הנזק ולהחזרת זמינות השירות. שתי המדינות גם ייחסו את המתקפות לתוקף, וכל אחת מהן נתנה משקל שונה לאחריות לאומית על בסיס ההקשר האסטרטגי והיכולות הלאומיות, בתוך כדי שהיא נעזרת בשיתוף פעולה בין־לאומי להשלמת פערים ביכולת הלאומית.

כל אלה עשויים להציע רציונל חלופי לקריאה לשיפור חוסן הלאומי למול מתקפות סייבר, במיוחד לנוכח השימוש במתקפות כופר, אם כי נדרשות בדיקות נוספות בנושא. המאפיינים הייחודיים של מרחב הסייבר (היכולת לנצל חולשות כדי לשנות את מרחב הסייבר עצמו, החולשות הרבות במרחב הסייבר והרגישות שלו לאפקטים מצטברים) פירושם שהגבלת היריב מהצלחה באירוע בודד או גביית מחיר גבוה ממנו, אינן אסטרטגיות בנות קיימא לטווח הארוך. ההנחה היא שאי־אפשר להגן באופן מלא על מדינה מפני מתקפות סייבר כל עוד היריב מתמיד במאמציו לנצל נקודות תורפה. אם יש מספיק זמן, היריב בהכרח יצליח להשיג רווחים משמעותיים שיקנו לו אפקט ברמה אסטרטגית ו"הצלחה" במבצע ההשפעה. המקרים שהוצגו מציעים גישה אחרת. המקרה האלבני מציע אסטרטגיה מקיפה, הכוללת מדיניות חזקה, פעולות הגנת סייבר וצעדים דיפלומטיים כדי ליטול את היוזמה ולהרתיע את היריב בפעילות נוספת, ואילו המקרה הישראלי מעביר את מאמצי החוסן לרמת הפרסונה הווירטואלית, במטרה לצמצם את האפשרות להעצמה ולהכפלה של האפקט האופייני לרמה זו, וכדי לפגוע באטרקטיביות השימוש במבצעי סייבר התקפיים לתמיכה במבצעי השפעה.

למחקר הנוכחי כמה תרומות. ראשית, הוא מרחיב את ההבנה שלנו על אופן השימוש במרחב הסייבר למבצעי השפעה, דרך הצגת מבצעי סייבר התקפיים, ובפרט עם תוכנות כופר, כשיטה לניצול הרשת הפיזית והשכבות הלוגיות של המרחב הסייבר למימוש מבצעי השפעה. שנית, הוא מזהה חולשה נוספת במרחב הסייבר, על בסיס הרגישות שלו להשפעות מצטברות ועל הקושי הטבוע בו לפענח ייחוס, וכך נוצרת שיטה נוספת להעצמת נרטיבים של מבצעי השפעה בעלות נמוכה יותר ממה שסברו מלכתחילה. ולבסוף, הוא בוחן מדיניות תגובה אפשרית כלפי מבצעי סייבר התקפיים המשמשים כמבצעי השפעה, ומציע שתגובות אלו יפיקו תועלת מאפקט מצטבר, בדומה לפעילויות אחרות במרחב הסייבר. יידרש מחקר נוסף כדי לקבוע כיצד לבנות תגובה שתדע למקסם את התועלת כנגד מבצעי סייבר התקפיים המשמשים כמבצעי השפעה.