כאשר פחות הוא יותר: קוגניציה ותוצאת הכפייה בסייבר

מיגל אלברשו גומס

העלייה במספר מקרי האינטראקציות ההתקפיות בסייבר בין מדינות ממשיכה לעורר עניין במה שנוגע לפוטנציאל הכפייתי של מִבצעי הסייבר. הדוגלים בגישה מהפכנית זאת מתעקשים על כך שהיא מהווה שינוי במאזן היחסים בין מדינות. עם זאת, עדויות המבוססות על מקרים שאירעו בעבר מאתגרות גישה זו, שכן הן מוכיחות שמהלכי הכפייה בסייבר מובילים לעיתים קרובות דווקא להתנגדות מתמשכת ולא לציות. אף על פי כן, וללא קשר לתוצאות, לא ניתן לבטל בקלות את פוטנציאל הכפייה שקיים במרחב הסייבר. מאמר זה טוען כי ניתן להסביר את התוצאה של מבצעי כפייה בסייבר על ידי שימוש באסטרטגיה האוריסטית של קבלת החלטות יותר מאשר בגישות הנורמטיביות, כגון האסטרטגיה של מידת "התועלת הצפויה".

מילות מפתח: האוריסטיקה קוגניטיבית, תועלת צפויה, כפייה, מרחב סייבר

מבוא

ב־23 בדצמבר 2015 השביתה התקפת סייבר יותר מחמישים תחנות חשמל משניות במערב אוקראינה והותירה יותר מ־230,000 תושבים ללא חשמל. היה זה המקרה הראשון של אירוע סייבר שהוביל לשיבוש ברשת החשמל של מדינה כלשהי.[1] שלוש

מיגל אלברשו גומס הוא חוקר בכיר במרכז ללימודי ביטחון, ETH Zurich, ודוקטורנט באוניברסיטת קרדיף, ויילס.

1 Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", *WIRED*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

שנים מאז תחילת הסכסוך האוקראיני־רוסי מתחזקת ההבנה שאירועים מסוג זה משמשים בימינו כאמצעי כפייה במצבים של סכסוך.[2]

יש מומחים הסבורים כי ככל שתלותן של הפוליטיקה, הכלכלה והחברה הגלובלית במרחב הסייבר הולכת וגוברת, כך גובר באופן פוטנציאלי האיום במרחב זה.[3] נראה כי במצב זה אכן גוברת "הרוח הגבית" לכפייה באמצעות הסייבר, וזאת בשל העלאת המחיר הפוטנציאלי של אי־ציות לאיומים על תשתיות הסייבר הבסיסיות. עם זאת, ולמרות דעותיהם של המומחים, היו גם מקרים שבהם המותקפים בחרו להתנגד לתוקף ולא לציית לדרישותיו.[4] יתר על כן, גם כאשר מבצעי הכפייה בסייבר היו מתקדמים מבחינה טכנית, הם לא הביאו לשינוים משמעותיים במדיניותו של הצד המותקף.[5]

אלה המותחים ביקורת על גישה זאת מייחסים את הביצועים החיוורים של מבצעי סייבר בכפייה למגבלות המובנות בתחום זה. עם זאת, אין למהר ולבטל במחי יד את התועלת האסטרטגית הטמונה בכפייה באמצעות סייבר. כפי שמציינים גרטצקה ולינדסי, "הפוטנציאל של מרחב הסייבר מוגבל יותר ממה שמוערך בדרך כלל, אולם הוא אינו זניח...".[6] לפיכך, מן הראוי להוסיף ולחקור את השימוש שמדינות עושות במבצעי כפייה בסייבר.

מאמר זה חורג מן הדעה הרווחת, שלפיה הצלחות של מבצעי סייבר בכפייה, או כישלונן, נגזרים מאסטרטגיות נורמטיביות של קבלת החלטות, שבאמצעותן החלטה לציית או להתנגד לכפייה בסייבר מתקבלת כפונקציה של הרווח או ההפסד הצפויים. תחת זאת עושה המאמר שימוש בהאוריסטיקה קוגניטיבית, המאפשרת תובנה ברורה יותר באשר לשאלה מדוע מדינות מתנהלות לעיתים באופן המנוגד לציפיות, לפיהן הן יישמו אסטרטגיות "יותר רציונליות". ההסבר המצומצם שאותו

---

2 "Analysis of the Cyber Attack on the Ukrainian Power Grid", *SANS*, March 18, 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

3 Myriam Dunn-Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse", *International Studies Review* 15, no. 1 (2013): 105–122; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies* 22, no. 3 (2013): 365–404; Jon R. Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited", in *Coercion: The Power to Hurt in International Politics*, eds. Kelly Greenhill and Peter Krause (New York: Oxford University Press, 2016).

4 Benjamin M. Jensen, Brandon Valeriano and Ryan Maness, "Cyber Victory: The Efficacy of Cyber Coercion" (Paper presented at the Annual Meeting of the International Studies Association, Atlanta, GA., 2016).

5 Emilio Iasiello, "Cyber Attack: A Dull Tool to Shape Foreign Policy", in *Fifth International Conference on Cyber Conflict*, eds. Karlis Podins, Jan Stinissen and Markus Maybaum (Tallinn: NATO CCD COE, 2013), pp. 451–468.

6 Lindsay and Gartzke, "Coercion through Cyberspace".

מציעות גרסאות שונות של פרדיגמת הבחירה הרציונלית מסייע לנו להבין את הסביבה המורכבת; הוספת ממד קוגניטיבי משקפת את הצורך בחיפוש אחר נרטיבים המסבירים טוב יותר את תופעת הכפייה באמצעות סייבר. בעשותו זאת, מכיר המאמר בצורך שהעלו דין ומק־דרמוט להבין כי התנהלות של מדינה במרחב הסייבר מתבססת על אינטראקציה בין גורמים הפועלים ברמות פעולה שונות.[7]

על רקע זה, המאמר בודק את מידת הסבירות של השימוש בהאוריסטיקה קוגניטיבית כאסטרטגיה לקבלת החלטות במענה לניסיונות כפייה בסייבר. לצורך זה מחולק המאמר לארבעה חלקים. החלק הראשון מביא סקירה כללית קצרה של תופעת הכפייה במרחב הסייבר. לאחר מכן באה ביקורת על התפיסה הרווחת לפיה מרחב הסייבר הוא תחום של סיכון המתבטא ביישום לקוי של אסטרטגיית "התועלת הצפויה" כדי לפרש באמצעותה תגובה של מדינות לניסיונות כפייה בסייבר. במקום אסטרטגיה זאת מציע המאמר כחלופה את ההאוריסטיקה הקוגניטיבית, מתוך הבנה שהחלטות מתקבלות על ידי ניצול של המאפיינים הסטטיסטיים הייחודיים של מרחב הסייבר. בחלק השלישי בודק המאמר את מידת ההתאמה של גישה זו על ידי בחינתה על מבצע תולעת Stuxnet. המאמר מסתיים בדיון על המגבלות של מסגרת תיאורטית זו.

כפייה ומרחב הסייבר

ההתעניינות האסטרטגית במרחב הסייבר גברה במהלך שני העשורים האחרונים בעקבות צמיחתן של תשתיות הסייבר והגידול בתפוצתן.[8] התפתחות זו הועמדה בצלם של חששות מפני מידת הפגיעות של מערכות ותת־מערכות ואפשרויות הניצול לרעה שלהן על ידי תוקפים המשתמשים באסטרטגיות של מניעה או ענישה למטרות כפייה.[9] מצב זה מדגיש את הפגיעות המובנית של מרחב הסייבר יחסית לערכו החברתי־פוליטי והכלכלי, ומציג עתיד שבו מרחב הסייבר, המתבטא במבצעי סייבר, יהפוך לכלי כפייה עיקרי בידיהם של שחקנים המסוגלים לעשות בו שימוש. מכיוון שכפייה מוגדרת כשימוש בכוח או כאיום בשימוש בכוח כדי להפיק שינוי

7 Benjamin Dean and Rose McDermott, "A Research Agenda to Improve Decision Making in Cyber Security Policy", *Penn State Journal of Law and International Affairs* no. 5, January 1, 2017.

8 Stuart Starr, "Toward a Preliminary Theory of Cyberpower", in *Cyberpower and National Security*, eds. Franklin Kramer, Stuart Starr and Larry Wentz (Washington DC: Potomac Books, 2009), pp. 43–88.

9 Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (New York: Cornell University Press, 1996); John Stone, "Cyber War Will Take Place!", *Journal of Strategic Studies* 36, no. 1 (2013): 101–108.

בהתנהגותו של יריב,[10] המצב שנוצר בפועל מאשש את התפיסה שמבצעי סייבר מתאימים לצורך השגת מטרה זו. מאחר שהתוצאה של כפייה בסייבר מתבטאת בהפסד או ברווח, עצם האיום על תשתיות התומכות באינטרס האסטרטגי של מדינה יוביל אותה להערכה מחודשת של עמדתה.

למרות שחקר הכפייה במרחב הסייבר מעורר עניין בחוגים אקדמיים, הספרות המחקרית בנושא זה הינה עדיין מועטה. מחקרים ראשוניים המצביעים על פוטנציאל הכפייה בסייבר משקפים את היתרון ההתקפי שלו. לפי זלצמן, יתרון זה מתאפשר על ידי הרב־צדדיות ו"כוח הבייט" של מבצעי הסייבר. לדבריו, הרב־צדדיות היא היכולת של הצעדים הננקטים במרחב הסייבר להשפיע באופן שלילי על האינטרסים האסטרטגיים של מדינה.[11] "כוח בייט" הוא כמות הנזק הנגרמת על ידי פעולות הננקטות במרחב הסייבר. בנוסף לכך, היעדר מגבלות חומריות מעניק גם הוא יתרון אסימטרי למבצעי הסייבר. בעוד שגישה לכלי נשק קונבנציונליים (וגרעיניים) מוגבלת לעיתים קרובות משיקולים כלכליים, הזמינות של כלים הפועלים באמצעות רשתות מחתרתיות מעניקה יתרון דווקא לתוקפים המוגבלים מבחינה חומרית. עם זאת, התוצאות של מקרים שאירעו בעבר מעמידות בסימן שאלה את פוטנציאל ההצלחה של מבצעי כפייה בסייבר.

מתוך 164 מבצעי כפייה בסייבר שזוהו בעבר, 64 אחוזים בלבד הובילו לשינויים שניתן היה להבחין בהם בהתנהלותו של היריב.[12] יתר על כן, ניסיונות להכריח יריב באמצעות מניעה עלו יפה באחוז אחד בקירוב בלבד מן המקרים. אם התנאים הבסיסיים של מרחב הסייבר, כשהם משולבים עם היתרון ההתקפי של מבצעי סייבר, אכן מגבירים את פוטנציאל הכפייה בסייבר, נשאלת השאלה מהי, אם כן, הסיבה לשיעור ההצלחה המאכזב של מבצעי כפייה אלה?

הצלחת הכפייה או כישלונה

הראיות מצביעות על הפוטנציאל המוגבל של כפייה באמצעות הסייבר, אך אינן מבטלות לחלוטין את התועלתיות הטמונה בה. למרות הצורך לטפח ציפיות, הגורמים להצלחתה של כפייה בסייבר או לכישלונה נותרו בלתי ברורים. מחקרים העוסקים במימוש הכפייה בסייבר עושים שימוש באסטרטגיית "התועלת הצפויה" כדי להעריך את התנהלות המדינה מול ניסיונות כפייה כאלה. אסטרטגיה זו מניחה כי החלטתה של מדינה להתנגד או לציית לכפייה מבוססת על מִקסום ומזעור של

10 Daniel Byman and Matthew Waxman, *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might* (New York: Cambridge University Press, 2002).

11 Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance", *Contemporary Security Policy* 34, no. 1 (2013): 40–63.

12 Jensen, Valeriano and Maness, "Cyber Victory: The Efficacy of Cyber Coercion".

רווחיה והפסדיה האפשריים. ככל שמדינות ממשיכות להשקיע במרחב הסייבר כדי לעמוד ביעדיהן האסטרטגיים, כך גוברת ההשוואה שהן עושות בין איומי הכפייה ובין יעדיהן הכלכליים, המדיניים, החברתיים או הצבאיים, וקבלת ההחלטה אם לציית או להתנגד לכפייה נעשית בהתאם לעוצמת האיום על יעדים אלה.[13]

הגורם המכריע בפוטנציאל הכפייה בסייבר הוא היכולת לנצל את הפגיעויות הטכנולוגיות.[14] איום נפוץ במרחב הסייבר הוא זה הנובע מאותן פגיעויות, מאי־ידיעה ומתרחישים בלתי נמנעים אחרים המגולמים במרחב זה, אותם מנצלים מבצעי הסייבר. קֶבֶלטי מצביע על ההמשגה של האיומים הנובעים מהפגיעויות ומן ההיקף שבו מערכות נתפסות כחשופות לאיומים אלה ומושפעות על ידם.[15] הקישוריות והתלות ההדדית בין המערכות מאפשרת ליחידים ולארגונים לרענן אותן כל העת ולהרחיב את תחומיהן, אך במקביל הן מגבירות את ההשלכות השליליות על אותן מערכות במקרה של ניצולן לרעה. המורכבות של טכנולוגיות אלו ומגבלות האנוש הבסיסיות לא מאפשרות לסלק את האיומים באמצעות פיתוח המוצר וניהול איכות בלבד.

נסיבות אלו מובילות לשרשרת של מצבים הפועלים לטובתה של הכפייה באמצעות הסייבר. הראשון שבהם הוא אובדן תחושת הביטחון. מורכבותו של תחום הסייבר מגבירה את סיכויי התקיימותם של מצבי פגיעות הניתנים לניצול. הדבר הופך את יכולתו של תוקף לזהות פגיעויות לכמעט בלתי נמנעת ומאפשר לו לנצל אותן כדי להשיג יתרון לעצמו. מכאן שכל אימת שפגיעות זו מתקיימת במערכות ובתת־מערכות הנחשבות לקריטיות, החברה האזרחית נתונה בסיכון פוטנציאלי.[16]

יישום אסטרטגיית "התועלת הצפויה" על תרחיש של איומים בכפייה מצביע בסבירות גבוהה יחסית על צפי להפסדים, וכתוצאה מכך על צפי לציות. עם זאת, תקפותה של טענה זו תלויה לא רק בהכרה בתהליך של סיבה ומסובב ובאפשרות התממשותו, אלא גם ביכולתו של היריב המותקף למתן את האיומים. האמור לעיל יוצא מהנחה כי שחקן במרחב הסייבר פועל בסביבה ממורכזת סיכונים וכי הוא בעל ידע על איומים, יכולות והשלכותיהם.

---

13 Starr, "Toward a Preliminary Theory of Cyberpower".

14 Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security", *International Political Sociology* 4, no. 1 (2010): 15–32.

15 Dunn-Cavelty, "From Cyber-Bombs to Political Fallout".

16 Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security and the Copenhagen School", *International Studies Quarterly* 53, no. 4 (2009): 1155–1175; James Lewis, "National Perceptions of Cyber Threats", *Strategic Analysis* 38, no. 4 (2014): 566–576.

סביבת מרחב הסייבר

הספרות בנושא הכפייה בסייבר נוהגת לשלב בין מושגי הסיכון ואי־הוודאות הנגרמים מיישום לא נכון של אסטרטגיית "התועלת הצפויה". המונחים "סיכון" ו"אי־ודאות" מגלמים תאימות מושגית מסוימת, אך כל אחד מהם מתאר למעשה סביבת מידע ייחודית המשפיעה על תהליכי קבלת ההחלטות ואיכותן. אם נאמץ את המינוח המשמש את סבֶג', הסיכון מתייחס ל"עולם קטן", שבו מקבל ההחלטה מודע להסתברויות של כל התוצאות והחלופות האפשריות. בניגוד לכך, אי־ודאות משקפת "עולם רחב", שבו ההסתברויות אינן ידועות או שאי אפשר לבטא אותן במידה כלשהי של ודאות מתמטית.[17]

אם נוהגים במרחב הסייבר כבתחום שבו הקישוריות והתלות ההדדית מגבילות את היכולת לחזות נקודות כישלון אפשריות ואת ההשלכות הנובעות מהן, משתמע מכך שמקבלי החלטות פועלים בהקשר של אי־ודאות יותר מאשר בהקשר של סיכון. בעניין זה הובהר זה מכבר כי אסטרטגיות נורמטיביות (כלומר, אסטרטגיית "התועלת הצפויה"), המשמשות בסביבות של אי־ודאות במקום בסביבת סיכון, נוטות להתאפיין בביצוע חסר. נושא זה מוצא ביטוי בדילמת bias-variance, המחמירה כאשר אסטרטגיות נורמטיביות מיושמות על סביבות לא מתאימות.

הדיוק ביכולת החיזוי של קבלת החלטות מאותגר על ידי שני גורמים חשובים: הטיה ושונות. המושג הראשון מתייחס למידת החריגה של מודל מן המצב האמיתי של סביבה מסוימת. מכיוון שאין לדעת מראש את מצב העניינים האמיתי, מודל שהוא נטול הטיה לחלוטין אינו יכול להתקיים. עם זאת, הטיה ממותנת על ידי שונות גוברת, הנובעת מהוספת פרמטרים המאפשרים מגוון רחב יותר של מצבים. בהתנהלות כזאת קיים סיכון של overfitting ושל הקטנת דיוק החיזוי. אסטרטגיות נורמטיביות כמו "התועלת הצפויה" מקזזות לעיתים קרובות את ההטיה על ידי הכללת פרמטרים כמו אלה שהוזכרו לעיל. זוהי גישה המתאימה לסביבות שבהן ניתן למצוא בקלות מקרים לדוגמה, או כאשר מקרים כאלה אינם דו־משמעיים. אסטרטגיות נורמטיביות עשויות להיות מסוגלות לתאר במדויק הבחנות קודמות, אך הן ייכשלו בחיזוי תוצאות עתידיות. במצבים כאלה, האוריסטיקה קוגניטיבית עשויה להתברר כמתאימה יותר להשגת המטרה.

האוריסטיקה מוגדרות כ"אסטרטגיות המתעלמות מחלק מן המידע, מתוך מטרה לקבל החלטות מהר יותר ובצורה חסכונית ו/או מדויקת יותר מאשר על

17 Kirsten G. Volz and Gerd Gigerenzer, "Cognitive Processes in Decisions Under Risk are not the Same as in Decisions Under Uncertainty", *Frontiers in Neuroscience* no. 6, July 12, 2012.

בסיס שיטות מורכבות יותר".[18] בהשוואה לאסטרטגיות הנורמטיביות, טעויות באסטרטגיית ההאוריסטיקה נובעות אך ורק מתוך הטיות. גם אם השגת דיוק באמצעות פחות מידע נראית כמנוגדת לאינטואיציה, בסביבות של אי־ודאות ההאוריסטיקה טובה יותר למעשה מן האסטרטגיות ה"רציונליות". דוגמה לכך הוא תחום ההשקעות. בורחֶס ואחרים מראים כי אפשר להשתמש בזיהוי שמה של חברה בלבד כדי לבנות תיק השקעות עם תשואות הגבוהות בעשרה אחוזים לפחות בהשוואה לשימוש באסטרטגיות אחרות.[19] במחקרם קיימת קורלציה חיובית חזקה בין החברה ובין ביצועיה בשוק, המנוצלת על ידי מקבלי ההחלטות העושים שימוש ביכולתם לזהות יחס זה מן הזיכרון (כלומר, כיסוי תקשורתי חוזר של חברה בעלת ביצועים טובים). מצב זה מאפשר לבחור חברה מסוימת על פני אחרת כאשר מרכיבים תיק השקעות.

דיון מעמיק בהאוריסטיקה נמצא מחוץ לטווח הטיפול של מאמר זה. אף על פי כן, חיוני לציין כי היתרונות של ההאוריסטיקה מבוססים על היכולת לנצל את המאפיינים הסטטיסטיים של סביבה העושה שימוש ביכולות קוגניטיביות אינהרנטיות, כגון זיכרון. במילים אחרות, ההאוריסטיקה היא מדויקת רק באותה מידה שהיא מתאימה למבנים קיימים.[20] נושא זה מוכר בהקשרים אחרים כרציונליות אקולוגית.

הרציונליות האקולוגית של מרחב הסייבר

אסטרטגיית ההאוריסטיקה מתאימה לסביבות המתאפיינות באי־ודאות, ביתירות, במחסור בנתונים ובשונות.[21] החלקים הקודמים במאמר עסקו בטבעו הבלתי ודאי של מרחב הסייבר. נושא זה דורש הסבר נוסף. שימוש מורחב בתזה של פרו (Perrow), המופיעה בספרו *Normal Accidents*, מאפשר לטעון שהקישוריות והתלות ההדדית שאותן מאפשר מרחב הסייבר גם מגבילות את היכולת לחזות את הסיבות של אירועים גורמי שיבוש ואת השלכותיהם. ללא מערכת יחסים פרדוקסלית זו לא הייתה מתקיימת האפשרות של "אסונות מתגלגלים", שהם

18 Gerd Gigerenzer and Wolfgang Gaissmaier, "Heuristic Decision Making", *Annual Review of Psychology* no. 62, January 10, 2011.

19 Bernhard Borges, Daniel G. Goldstein, Andreas Ortmann and Gerd Gigerenzer, "Can Ignorance Beat the Stock Market", in *Simple Heuristics That Make Us Smart*, eds. Gerd Gigerenzer, Peter M. Todd and the ABC Research Group (New York: Oxford University Press, 1999).

20 Laura Martignon and Ulrich Hoffrage, "Why Does One-Reason Decision Making Work?", in *Simple Heuristics That Make Us Smart*.

21 Peter M. Todd, Gerd Gigerenzer and the ABC Research Group, *Ecological Rationality: Intelligence in the World* (New York: Oxford University Press, 2011).

הבסיס לפוטנציאל הכפייה באמצעות הסייבר.[22] מעבד תמלילים, לדוגמה, הפועל בנפרד ובאופן עצמאי (stand-alone), מאפשר למומחים לאבטחת מחשבים, על בסיס ניסיונם עם תוכנות דומות, לחזות את מספר נקודות התורפה לכל אלף שורות קוד. במצב זה, הפעולה נעשית בסביבה של סיכון, תוך הכרת הפגיעויות האפשריות שנגזרות מן הגישה הישירה לקוד הבסיסי של התוכנה ו/או מן הניסיון. כדי להגביר את הפריון, משתמשים יוכלו ליצור קשר הדדי בין מעבדי התמלילים שלהם, שיאפשר להם לעבוד תוך שיתוף פעולה. אם יעשו כן, יצטמצם הידע הקודם על מאפייני הפגיעות, שכן מצבן של המערכות האחרות שאליהן הם מתחברים אינו מוכר. עקב כך, מסובך יותר ויותר לחזות היכן, מתי או כיצד עלול להתרחש כשל, מה שמציב את המשתמשים בסביבה של אי־ודאות.

כאשר מיישמים דוגמה זו על שאלת הכפייה בסייבר, מדינות התלויות במערכות סייבר אינן יכולות לחזות את ההיקף האמיתי של הנזק שתוקפים עלולים לגרום, והדבר מונע את היכולת להעריך במדויק את ההשלכות של ציות לכפייה או התנגדות לה. יש מי שטוענים כי נקודה זו מציבה אתגר בפני עצם התועלת שבכפייה במרחב הסייבר. מאמר זה טוען, לעומת זאת, כי אין בכך כדי לצמצם בהכרח את יכולת הכפייה באמצעות הסייבר, וכי המצב שתואר לעיל מצביע בעצם על כך שהיעדר מידע משפיע על בחירתה של האסטרטגיה הנכונה לקבלת החלטות באירועים מסוג אחר.

כפייה במרחב הסייבר אינה מתקיימת בחלל ריק, וחוסר הוודאות לגביה מושפע ממאפייני היתירות הקיימים. יתירות היא הקשר הקיים בין סימנים או רמזים בתחום המידע שבהם משתמשים בתהליך קבלת ההחלטות. חשוב לציין כי במבצעי כפייה בסייבר מעורבים לעיתים קרובות יריבים ותיקים עם היסטוריה של התנהלות אגרסיבית זה כלפי זה,[23] ולפיכך קיימת ציפייה להתרחשותן של פעולות מסוימות בין שני הצדדים, בין אם במרחב הפיזי ובין אם בתחום הווירטואלי. ריגול הסייבר הסיני נגד ארצות הברית, לדוגמה, אינו מפתיע במיוחד, והוא קשור בקורלציה חיובית לאינטרס הסיני להשיג יתרון במידע. בניגוד לכך, נראה כי מתקפת תוכנת הכופר WannaCry, המיוחסת לקוריאה הצפונית, אינה קשורה ליעדים האסטרטגיים או המדיניים של המשטר שם. הדבר מצביע על כך שאירועים מסוימים במרחב הסייבר מוגדרים מלכתחילה על ידי יחסים בין־מדינתיים הקיימים זה מכבר. בהתאם לכך, מקבלי החלטות עשויים לנצל מערכת יחסים זו ואת מידת ההיכרות שלהם עם הנושאים כדי להעריך את יכולתם לממש מבצעי כפייה בסייבר ואת השלכותיהם.

---

22 Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princeton: Princeton University Press, 1999).

23 Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11", *Journal of Peace Research* 51, no. 3 (2014): 347–360.

אפשר אמנם לראות את מרחב הסייבר כהארכה של המרחב הפיזי שבו מבוטאת מערכת יחסים, אך מצבים כאלה הם נדירים למדי. לכן, המידע בדבר היעילות הכוללת של מבצעי כפייה בסייבר, מבחינת הכלים המועדפים, הטקטיקה והתוצאות, כמו גם מידע רלוונטי אחר, הוא מצומצם בהיקפו. למרות שההתקדמות בטכניקות פורנזיות מאפשרת ניתוח טוב יותר של מאפיינים טכניים, מאפיינים כאלה לבדם מאפשרים להגיע לתובנה אסטרטגית מוגבלת בלבד.[24] כתוצאה מכך, חוסר הוודאות ברמה הטכנולוגית מצטרף לחוסר הוודאות ברמה האסטרטגית/מדינית ומגדיל את הספק באשר לתועלתה של כפייה באמצעות הסייבר. עם זאת, נראה כי הדבר נכון רק אם מתבוננים בו דרך העדשה של גישות נורמטיביות, כגון זו של אסטרטגיית "התועלת הצפויה". מכיוון שהחלטות מתקבלות על בסיס רווח והפסד, אין במיעוט המידע די כדי להגיע למסקנה שלא יהיו הפסדים בעתיד, או שתימשך ההצלחה באמצעות השגת פשרה, שכן מקבלי ההחלטות אינם יכולים להיות מודעים לכל התוצאות והחלופות האפשריות.

לבסוף, רמת הביצוע של אסטרטגיית ההאוריסטיקה תלויה במשקלם או בתוקפם של הרמזים הקיימים בסביבה. התוקף הוא השיעור שעל פיו סימנים או רמזים יכולים להבחין באופן נכון בין אפשרויות שונות. לדוגמה, האם היערכות קדומנית של כוחות צבא הובילה בעבר לציות של המדינה שהייתה מאוימת על ידי אותם כוחות? בתרגום דוגמה זו לעיקריה של תיאוריית הכפייה בסייבר, ניתן לומר כי התוצאה של כפייה כזאת תלויה הן ביכולתו של הכופה לגבות מחירים מן היריב על ידי איום על נכסיו, והן באופן שבו המאוים הפוטנציאלי מעריך נכסים אלה שלו. הספרות המדעית עוסקת בנקודה הראשונה של טענה זו. לעומת זאת, היא מטפלת רק לעיתים רחוקות בשונות הקיימת בין יריבים בתפיסתם את מרחב הסייבר, דבר המשפיע עליהם בבואם להעריך את נכסיהם.[25] במילים אחרות, מה שעשוי להיות רמז תקף לציות במקרה אחד, עלול לא להיות כזה במקרה אחר. דבר זה מגביר את חוסר הוודאות.

בחירת האסטרטגיה ההאוריסטית

כאמור, האסטרטגיה ההאוריסטית יכולה להיות חלופה טובה יותר מהאסטרטגיות הנורמטיביות כדי להסביר את תוצאותיה של כפייה במרחב הסייבר, וזאת בהתבסס על הרציונליות האקולוגית של מרחב זה. יתרונותיה של האסטרטגיה ההאוריסטית נובעים ממספר סיבות: ראשית, אי־ודאות מונעת ממקבלי החלטות את היכולת

24 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies* 38, no. 1 (2015): 4–37.

25 Forrest Hare, "The Cyber Threat to National Security: Why Can't We Agree", in *Conference on Cyber Conflict Proceedings*, eds. Christian Czosseck and Karlis Podins (Tallinn: CCD COE, 2010).

לקיים הערכה אמפירית של כל התוצאות והחלופות האפשריות; שנית, הקורלציה בין אירועים במרחב הסייבר ובין יריבויות קיימות מפצה על אי־הוודאות ומאפשרת שימוש בניסיון העבר במרחב הסייבר לצורך קבלת החלטות; שלישית, הנדירות של מבצעי סייבר בכפייה מגבילה עוד יותר את השימוש באסטרטגיות נורמטיביות, שכן היא מונעת ממקבלי ההחלטות נקודות ייחוס שעליהן הם יוכלו לבסס את החלטותיהסף; לבסוף, חוסר היכולת לזהות מאפייני שונות בתוקפם של רמזים מוביל לגישה ספציפית מוטעה. כאשר מודעים לנקודות אלו, השאלה הנותרת היא איזו אסטרטגיה האוריסטית היא המתאימה ביותר לטיפול במבנים ארגוניים סביבתיים (environmental structures).

המאמר מניח כי האוריסטיקה המבוססת על נימוק יחיד (one-reason) היא זו המאפשרת להבין את תוצאותיו של מבצע כפייה בסייבר. משפחה זו של האוריסטיקה פועלת היטב במקרים שבהם הרמזים משתנים במידה רבה, קיימת יתירות, וכמות המידע מצומצמת.[26] שימוש בהאוריסטיקה של נימוק יחיד כדי להחליט האם לציית או להתנגד לדרישות שנעשות בכפייה מוביל לתהליך קבלת החלטות המתנהל בהתאם לכללים של "חיפוש, עצירה וקבלת החלטה". כללים אלה קובעים את דרך החיפוש של הרמזים הנכונים, את התנאים שבהם יש להפסיק את החיפוש ואת הדרך שבה רמזים אלה ייושמו ויובילו לקבלת החלטה ספציפית.

למרות פשטותה של האסטרטגיה ההאוריסטית, ביצועיה טובים יותר מאלה של אסטרטגיות מורכבות יותר, כגון "רגרסיה רבת משתנים" (multiple regression), רשתות עצביות וכדומה. עם זאת, חשוב לקבוע כי האסטרטגיה ההאוריסטית אינה באה במקום האסטרטגיות האחרות, שכן היא נמנעת מחיפוש ראיות סותרות ומתבססת על הערכה סובייקטיבית יותר מאשר אובייקטיבית של מצב נתון. מאפיין זה עלול להתברר כבעייתי, ואפילו כמסוכן, בסביבות מסוימות. לדוגמה, מבצע הנערך על ידי צד שלישי תחת "דגל כוזב", ומחקה את התנהגות היריב, עלול להוביל, בנסיבות מסוימות, להסלמה בלתי מכוונת.

ישימות ההאוריסטיקה – המקרה של Stuxnet

כדי לתמוך בטיעונים התיאורטיים שצוינו לעיל, להלן תודגם ישימותה של אסטרטגיית ההאוריסטיקה. מספר אירועים שהתרחשו מאז שנת 2007 עשויים לשרת מטרה זו, אך המאמר ידון רק במקרה של מתקפת Stuxnet, שיוחסה הן לארצות הברית והן לישראל. ההחלטה לעשות שימוש במקרה זה לצורך הדגמה מבוססת על זמינות המידע לגביו, המאפשרת לערוך השוואה בין שתי אסטרטגיות של קבלת החלטות.

---

26 Gerd Gigerenzer, "Why Heuristics Work", *Perspectives on Psychological Science* 3, no. 1 (2008): 20–29.

את האינטראקציה בין ארצות הברית לאיראן במרחב הסייבר ניתן לאפיין כסדרה של מעשי כפייה הנעשים באינטנסיביות, בחומרה ובהיקף משתנים.[27] מבין אלה, סטאקסנט הוא המקרה המפורסם ביותר של כפייה בסייבר. על קיומו נודע לראשונה ב־17 ביוני 2010, כאשר בוצעה פנייה לחברת האנטי־וירוס VirusBlokAda בבלרוס כדי שתיתן מענה לאתחולים מחדש בלתי מוכרים של מערכות שהתרחשו באותה העת באיראן.[28] למרות "גילויה" לראשונה בשנת 2010, אנליסטים סבורים כי תוכנת סטאקסנט הייתה מבצעית כבר בחודש יוני 2009, כאשר הדביקה עשר פעמים חמישה ארגונים בתוך איראן וגרמה ל־12,000 הדבקות בסך הכל עד למועד שבו זוהתה בשנת 2010.

התכונות המתקדמות של סטאקסנט מצביעות על מעורבותן של ישויות מדינתיות, או של כאלו הממומנות על ידי מדינה, בפיתוחו ובהפצתו. תכונות אלו העניקו לסטאקסנט את ההכרה כתוכנה הזדונית "החמושה" הראשונה בהיסטוריה. מגוון התכונות של התוכנה ויעדיה (מערכות בקרה תעשייתיות) גם הצביע על שינוי ביכולות, במורכבות ובכוונות של שחקנים הפועלים במרחב הסייבר.[29] החל עידן חדש בדו־שיח על השימוש באמצעי לחימה בסייבר.

למרות מאפייניו המבצעיים ותכונותיו, סטאקסנט לא הצליח לכפות על המשטר האיראני את סיום תוכנית ההעשרה הגרעינית שלו. התחושה הרווחת היא כי כישלון זה של סטאקסנט נבע מן הנזק המוגבל שנגרם לתשתית ההעשרה האיראנית. למעשה, עד שההדבקה בווירוס נבלמה, ניזוקו יותר מאלף סרכזות ששימשו את איראן להעשרת אורניום, אך ניתוח שנעשה לאחר האירוע העלה כי מספר הסרכזות שניזוקו לא עלה על בלאי ופחת תפעוליים רגילים. הסבר זה עולה בקנה אחד עם הבנת מושג הכפייה דרך האסטרטגיה של "התועלת הצפויה". במילים אחרות, לפי אותה אסטרטגיה, הנזק שנגרם לסרכזות האיראניות לא הגיע לממדים משבשים, מחלישים או כאלה המחייבים הערכה מחדש של המדיניות האיראנית. כדי שטיעון זה יהיה תקף, יש לאמץ הנחה חיונית אחת: כי למשטר האיראני היה מידע נכון על יכולותיו ופגיעותו במרחב הסייבר, מה שנתן לו את הביטחון שהוא יכול להסתכן בהתמודדות עם ניסיונות פגיעה נוספים בתשתית הסייבר שלו. אם אכן כך הדבר, הוא מרמז על קבלת ההחלטה להתנגד לניסיונות הכפייה בסביבה של סיכון. אלא שהתגובה האיראנית מאתגרת הנחה זו, הן אמפירית והן תיאורטית.

---

27 Jason Healey, "Winning and Losing in Cyberspace", in *Eighth International Conference on Cyber Conflict*, eds. Nikolaos Pissanidis, Henry Roigas and Matthijs Veenendaal (Tallinn: CCD COE, 2010).

28 Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon", *WIRED*, March 11, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

29 Lindsay, "Stuxnet and the Limits of Cyber Warfare".

יהיה זה בלתי סביר להניח שהאחראים על ביטחון הסייבר באיראן החזיקו במידע מושלם על כל כיווני ההתקפה האפשריים על מערך הסייבר האיראני. תוכנית אבטחה מתאימה הייתה נוקטת לכל הפחות צעדים כדי למתן את האיומים שהיו מוכרים הן מניסיון עצמי והן ממידע שהיה זמין לכלל הציבור. במקרה של סטאקסנט, הדיווחים על פניית הרשויות האיראניות לגורמים שלישיים זרים כדי להיטיב להבין את ההתנהגות החריגה של המערכות שלהם, מצביעים על כך שהם לא צפו אירוע מסוג זה וגם לא העריכו את השלכותיו האפשריות. למעשה, המורכבות של סטאקסנט, שהייתה ללא תקדים, לא אפשרה לגזור ממנו חישוב כלשהו של נזקים והפסדים אפשריים.

ניתן לטעון כי מידע נוסף על יכולות הסטאקסנט ופוטנציאל הנזק שלו היה מתגלה עם התקדמות החקירה, דבר המרמז על מומחיות טכנולוגית ומערכת ארגונית מוגדרת המאפשרות קיומם של מאמצים כאלה. ארגונים זקוקים למנגנון המאפשר לבצע סינתזה של מידע בין יחידות שונות כדי להבין את מכלול ההשלכות של אירועים. עם זאת, לא ניתן לצאת מתוך הנחה שמבנה ארגוני כזה קיים בכל המדינות, וגם יעילותו אינה בבחינת דבר מובן מאליו.[30] התלות של איראן בסיוע חיצוני במהלך תקרית הסטאקסנט, יחד עם דיווחים מוקדמים יותר על יכולותיה במרחב הסייבר, מעמידים בספק את יכולתה להבין באופן מלא את השלכותיו של וירוס זה ומאתגרים עוד יותר את מידת ישימותן של אסטרטגיות נורמטיביות לצורך מתן הסבר להחלטת איראן להתנגד לכפייה באמצעותו.

אילו המשטר האיראני היה בטוח ביכולתו להתגונן מפני סטאקסנט או מפני צעדי כפייה אחרים, מדוע הוא לא הגיב תגובה חזקה יותר? הן גרטצקה והן לינדזי טוענים כי מבצעים המסתכמים בפשרה, אך למעשה נבלמים, מסתיימים לבסוף בסחרור של הסלמה.[31] לעומת זאת, מודל המשחק התיאורטי של אדוארדס ואחרים, למרות שהוא פחות קיצוני, גורס כי אלה המודעים לפגיעויות של עצמם והצליחו למתן אותן, צריכים, לפחות ברמה הציבורית, לייחס מעשי כפייה ליריביהם.[32] שום דבר מאלה לא קרה בכל מה שנוגע לסטאקסנט. אמנם, מספר חוקרים טוענים כי התגובה האיראנית התבטאה במבצעי סייבר איראניים במועד מאוחר יותר, אך לא נראה כי המאפיינים המבצעיים של התגובות היו בעלי ממדים שיכלו לשמש כמענה הולם לסטאקסנט, או שנתפרו על פי מידותיו.

---

30 Rebecca Slayton, "What is the Cyber Offense-Defense Balance?", *International Security* 41, no. 3 (2017): 72–109.

31 Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar", *Journal of Cybersecurity* 3, no. 1 (2017): 47–48.

32 Benjamin Edwards, Alexander Furnas, Stephen Forrest and Robert Axelrod, "Strategic Aspects of Cyber Attack, Attribution and Blame", in *Proceedings of the National Academy of Sciences* (forthcoming).

אם בוחנים בצורה יסודית יותר את הגרסה הרווחת באשר לכישלון מבצע סטאקסנט, המאשרת לכאורה את התועלת של השימוש באסטרטגיות הנורמטיביות, מתברר כי היא ניצבת למעשה על קרקע לא יציבה. למרות שמדובר בספקולציה, הנובעת מהיעדר מידע ממקור ראשון על הנעשה באיראן, נראה שהמשטר שם היה חסר הבנה מלאה של מיני הפגיעויות שלו בתחום הסייבר. במצב זה לא היה ראוי שמקבלי ההחלטות באיראן יסתמכו על אסטרטגיית "התועלת הצפויה" או על אסטרטגיות דומות לה כדי לגבש את תגובתם, וזאת נוכח העובדה שהמידע שהיה בידיהם על ההשלכות האפשריות של התנגדות או ציות לכפייה היה חלקי בלבד או לא זמין לחלוטין. יתר על כן, הישימות של אסטרטגיות נורמטיביות מאותגרת גם במקרים אחרים של כפייה בסייבר. כך, למשל, מבצע "BoxingRumble" נגד ריגול הסייבר הסיני לא גרם לנזק משמעותי, ולמרות זאת, תגובת סין הייתה עצירה זמנית של פעילות הריגול.[33] נראה כי סתירה לכאורה זו מעמידה בסימן שאלה את תוקף המסקנות המבוססות על שימוש באסטרטגיות הנורמטיביות.

סגירת הפער

בהנחה שאסטרטגיות נורמטיביות כמו "התועלת הצפויה" אינן מתאימות לסביבת הכפייה באמצעות הסייבר, נשאלת השאלה האם אסטרטגיית ההאוריסטיקה עשויה להיות התשובה לכך. אם מרחיבים את הטענה שכפייה באמצעות הסייבר מתרחשת בין יריבים וכי מבנים ארגוניים סביבתיים מעדיפים את אסטרטגיית ההאוריסטיקה של החלטה יחידה, ניתן להוכיח הנחה זו על ידי שימוש בהאוריסטיקה "קח את האחרון" (Take the Last – TTL).

האוריסטיקה של TTL פועלת בדרך כלל תוך שימוש באסטרטגיה המוכרת כמערך *Einstellung*. מאז שנות השלושים של המאה העשרים הבחינו פסיכולוגים כי יחידים פותרים בעיות הנראות קשורות זו בזו באמצעות אסטרטגיות שפעלו היטב בעבר.[34] מכאן נובעת ההנחה כי האוריסטיקה של TTL משמשת בסביבות שבהן ההחלטות שמתקבלות עוסקות באירועים הקשורים בדרך זו או אחרת אלה באלה. קורלציה זו מתבטאת באופן עקיף ביכולתו של מקבל ההחלטה לזהות קווי דמיון בין משימות שונות. הזיהוי במקרה זה אינו בהכרח שווה ערך לזיכרון, אלא מתייחס למאפיינים אינטואיטיביים של אירועים – מאפיינים המתחזקים על ידי חשיפה נמשכת להם.

---

33 Sean Gallagher, "NSA secretly hijacked existing malware to spy on N. Korea, others", *arsTechnica*, January 19, 2015, https://arstechnica.com/information-technology/2015/01/nsa-secretly-hijacked-existing-malware-to-spy-on-n-korea-others/.

34 Gerd Gigerenzer and Daniel G. Goldstein, "Betting on One Good Reason: Take the Best Heuristic", in *Simple Heuristics That Make Us Smart*.

מכיוון שמבצעי סייבר בכפייה מערבים יריבים משכבר הימים המקיימים אינטראקציה קבועה זה עם זה, TTL מהווה אסטרטגיה אידיאלית לטיפול בהם, לא רק בגלל המבנים הסביבתיים, אלא גם בשל יעילותה. שלא כמו אסטרטגיית "התועלת הצפויה", המחייבת חישוב אינטנסיבי (דבר המגביר את העומס הקוגניטיבי), TTL מסתמכת אך ורק על ההכרה לצורך זיהוי החלופות. יתר על כן, במצבים קריטיים מבחינת הזמן, כגון סכסוכים בין מדינות, המהירות שבה מיושמת אסטרטגיית TTL הופכת אותה לבחירה מועדפת על פני אסטרטגיות חלופיות. שיטת TTL פועלת באופן הבא: איתור הרמז שהביא לעצירת החיפוש בבעיה הרלוונטית האחרונה והשוואתו לחלופות. אם תוצאת ההשוואה שונה מבעבר, יש להשתמש באותו רמז. במקרה שהדבר אינו כך, יש לחזור לבעיה לפני האחרונה ולאתר את הרמז שהביא לעצירת החיפוש באותה בעיה.

כאשר מסבירים את תוצאות הסטאקסנט על ידי שימוש בהאוריסטיקה של TTL, התהליך מתחיל על ידי בניית מאגר של כלל האירועים הדומים שהתרחשו בעבר. מכיוון שיעדו של סטאקסנט היה מערכות הבקרה של סרכזות גרעיניות האחראיות על העשרת אורניום, מאגר האירועים כולל, במידה גבוהה של ודאות, ניסיונות קודמים לכפות על איראן את עצירת העבודה בתוכנית הגרעין שלה. אין זו בהכרח הנחה בלתי מבוססת, לנוכח המאמץ הרב שהושקע על ידי יריביה של איראן, שביקשו להשיג בדיוק מטרה זאת. בנוסף, העובדה שאירוע הסטאקסנט התרחש במרחב הסייבר, אינה אמורה לפגוע ביכולתם של מקבלי ההחלטות לאתר נקודות דמיון בין האירועים השונים, נוכח העובדה שמדובר במטרה זהה (כלומר, סיום תוכנית הגרעין של איראן).

ברגע שבו נבנה מאגר מנטלי זה, נדרש מקבל ההחלטות לזהות את המקרה האחרון שבו הרמז גרם להבחנה בין החלופות השונות. מכיוון שאין בידינו גרסאות ממקור ראשון, המאמר מתייחס לאירועי כפייה שהתרחשו לפני יוני 2010. בין השנים 2006–2010 נערכה שורה של דיונים עם איראן, ואף על פי כן מועצת הביטחון של האו"ם הטילה עליה שש סנקציות שנועדו לשבש את תוכנית ההעשרה הגרעינית שלה. בנוסף לכך, ארצות הברית החלה אז לשקול ברצינות שימוש במהלומות אוויריות נגד איראן, וישראל איימה בנקיטת פעולה צבאית נגדה. אי אפשר לקבוע איזה מן האירועים הללו שימש כנקודת התייחסות של איראן, והדבר אינו משנה למעשה, שכן התוצאה הייתה זהה מבחינתה – התנגדות.[35]

ההקשר המשותף של אירוע סטאקסנט ושל אירועים דומים בעבר מוביל למסקנה שמקבלי ההחלטות באיראן בחרו להישאר עקביים בהתנהלותם המתנגדת לכלל

35 Shreeya Sinha and Susan Campbell Beachy, "Timeline on Iran's Nuclear Program", *New York Times*, April 2, 2015, https://www.nytimes.com/interactive/2014/11/20/world/middleeast/Iran-nuclear-timeline.html?_r=0#/#time243_10809.

צעדי הכפייה שננקטו נגדם. המאפיינים של סטאקסנט מגבילים את מידת הדיוק של אסטרטגיות מורכבות יותר לקבלת החלטות, בשל היעדר מידע על יכולותיה האמיתיות של התוכנה ועל מידת הפשרה. יתר על כן, אם ההתנגדות לניסיונות הכפייה פעלה היטב כאשר האיום היה גדול יותר (כלומר, כאשר על הפרק עמדה אפשרות של התנגשות פיזית של ממש), היא הייתה אמורה לפעול גם במצב הפחות קיצוני הזה.

לקראת העתיד

מאמר זה הציג את הטענה כי האוריסטיקה קוגניטיבית יכולה לשמש ככלי אנליטי להערכת תוצאותיו של מבצע כפייה בסייבר. אסטרטגיות נורמטיביות נותרות אמנם אבן היסוד להערכת התנהלותה של מדינה, אך המאפיינים הייחודיים של מרחב הסייבר מעמידים בסימן שאלה את מידת ההלימות שלהן למרחב זה. בתחום הפיזי, הניסיון מאפשר לגבש הערכה אובייקטיבית של רווחים והפסדים. לעומת זאת, חוסר הוודאות הטבוע במרחב הסייבר מגביל את יכולת החיזוי המדויקת של אסטרטגיית "התועלת הצפויה" ושל אסטרטגיות קשורות אחרות. במקום זאת, אסטרטגיות פשוטות וממוקדות מטרה, כגון האוריסטיקת TTL, מאפשרות לגבש תמונה ברורה יותר של צעדי כפייה בתחום וירטואלי זה.

ההסתמכות על האוריסטיקה בלבד אינה מאפשרת, עם זאת, להגיע למסקנה חלוטה. מכיוון שאין בנמצא אסטרטגיה לקבלת החלטות המתאימה לכל, מידת הישימות של אסטרטגיית האוריסטיקה או של אסטרטגיות נורמטיביות היא פונקציה של מבנים סביבתיים ושל היכולות הקוגניטיביות של יחידים גם יחד. תלות הדדית זו מבוטאת באופן מיטבי באנלוגיה שמביא הרברט סיימון, לפיה רציונליות דומה ללהבי מספריים, כאשר להב אחד מייצג את מגבלותיהם הקוגניטיביות של יחידים, בעוד שהלהב השני מייצג את המבנים והתנאים הסביבתיים. כשם שמספריים אינם יכולים לפעול באמצעות להב יחיד, באותה מידה הבנתנו את מושג הרציונליות אינה יכולה להיות מוגבלת להיבט יחיד כזה או אחר.

על רקע הנאמר לעיל, יש לציין שלוש נקודות חשובות. הראשונה היא שאין להציג את השימוש בהאוריסטיקה קוגניטיבית בתחום היחסים בין מדינות ככישלון הרציונליות. למרות ממצאים מן התקופה האחרונה בפסיכולוגיה קוגניטיבית, אנשי אקדמיה בתחום היחסים הבין־לאומיים ומדע המדינה ממשיכים להגדיר האוריסטיקה קוגניטיבית כאסטרטגיה בעלת עלות נמוכה שמובילה להחלטות שאינן מיטביות. במקום זאת, המאמר הנוכחי מדגיש את חשיבות התאמתן של אסטרטגיות לסביבה ההולמת אותן, וזאת מתוך הבנה שאפילו גישות מורכבות עלולות להוביל לתוצאות עלובות אם נעשה בהן שימוש לא נכון.

שנית, על אף השימוש המוצלח באסטרטגיה של האוריסטיקה לצורך הערכת התוצאות של צעדי כפייה במרחב הסייבר, לא ניתן לעשות הכללה מתוצאות אלו על כלל צורות האינטראקציה במרחב זה. נראה כי האוריסטיקה פועלת טוב יותר כאשר מסבירים באמצעותה כפייה בסייבר. אז היא עושה זאת בזכות הניצול היעיל והנכון של מבנים ארגוניים באמצעות תהליכים קוגניטיביים בסיסיים. תנאים אלה עלולים לא להתקיים בפעולות של שיבוש באמצעות הסייבר, המהוות חלק ניכר מן האינטראקציות הקיימות במרחב זה. במקרים כאלה, סביבת האי־ודאות מפנה את מקומה לסביבה של סיכון, וזאת בשל ההשפעות המתועדות היטב של הכלים והטקטיקות הנמצאים בשימוש באותם מקרים. האמור לעיל מאפשר, אפוא, שימוש באסטרטגיות נורמטיביות המסוגלות לנצל טוב יותר את המידע הזמין.

שלישית, אין להניח שהחלטות המתקבלות בזמנים של משבר נובעות ממחשבותיו של אדם אחד בלבד. מה שתורם לאיכותן של ההחלטות המתקבלות הם סוגי דינמיקה הייחודיים לאותו ארגון. יתר על כן, גורמים נוספים, כגון עלויות הקהל (שבהם אין מאמר זה עוסק), עשויים להיות משמעותיים במה שנוגע לאופן התגובה הננקטת אל מול ניסיונות כפייה. מן הראוי לציין גם גורמים אלה לנוכח חשיבות הנושאים המשפיעים על אינטראקציות שונות במרחב הסייבר.

תחום ביטחון הסייבר נמצא עדיין בחיתוליו. אולם, נוכח האיומים המתפתחים, הן במורכבותם והן בהיקפם, קיימת דחיפות שאנשי אקדמיה ופוליטיקאים כאחד יבינו את התנהלותה של מדינה בתגובה לאירועים המתרחשים במרחב הסייבר. המאמר בא לתרום למאמץ זה על ידי כך שהוא מציע דרך לניתוח הדברים, אף שדרך זו נשקלה אך לעיתים רחוקות על ידי העוסקים בתחום הסייבר, אלה שהבנתם עשויה לסייע בשמירה על יציבותו של תחום וירטואלי זה.