

ניהול משברי גרעין והרתעה בצל לוחמת סייבר

סטפן ג'יי סימבלה

לוחמת סייבר, לפני משבר גרעיני או במהלכו, עלולה לערער את יציבות ההרתעה הגרעינית – מהשפעה שולית עליה ועד השפעה קטלנית – ובכלל זה לשבש את העברת המסרים בין ממשלים בעיתות משבר ולזרוע בלבול בהערכותיהם לגבי האירוע המתגלגל. מאמר זה בוחן את התנאים לניהול מוצלח של משבר גרעיני, את נקודות התורפה האפשריות במהלכו כתוצאה מלוחמת סייבר ואת התרחישים לכשלים.

מילות מפתח: לוחמת סייבר, לוחמת מידע, הרתעה, יציבות במשבר, מלחמה גרעינית, ניהול, שליטה ובקרה, רשתות, תקשורת, שליטה בהסלמה.

מבוא

עידן המידע ויישומיו הצבאיים-טכניים עתידיים, ללא ספק, לשנות את אופייה ומאפייניה של ההרתעה הגרעינית. התשובה לשאלה כיצד בדיוק יוכלו להתקיים זו לצד זו הרתעה גרעינית ולוחמת סייבר, או שהן יתחרו ביניהן כפרדיגמות מדיניות, פחות ברורה בשלב זה. אף שמבצעי סייבר שונים באופיים ממבצעים קינטיים, יש לראות את הרכיבים השונים של לוחמת המידע "יותר ויותר כחלקים של שלם גדול, יותר מאשר כהתמחויות נפרדות התומכות, כל אחת באופן פרטני, בפעולות צבאיות קינטיות".¹ כך, לדוגמה, פאבל ק' באב (Baev) קובע כי "הסימן

סטפן ג'יי סימבלה הוא פרופסור למדעי המדינה ב־Penn State Brandywine, ועוסק מזה שנים רבות בלימודי ביטחון בין-לאומי, בקרת נשק גרעיני ותחומים נוספים. המחבר מבקש להודות לפול דייוויס, אנדרו פוטר, לורנס קורב וסימון תומאס על תובנותיהם בנושא מחקר זה. הם, כמובן, אינם נושאים באחריות לתכניו.

1 Martin C. Libicki, "The Convergence of Information Warfare", *Strategic Studies Quarterly* no. 1 (Spring 2017): 50, 49-65; במאמר הנוכחי השתמשתי במונחים "לוחמת מידע" ו"לוחמת סייבר" כשווי ערך, למרות שיהיו מומחים שיתעקשו כי "לוחמת סייבר" מוגבלת למתקפות דיגיטליות על מערכות מידע ורשתות בלבד, בעוד ש"לוחמת מידע" היא

המסחרי" של מדיניות החוץ הרוסית העכשווית הוא השילוב בין פעולות שיבוש, מבצעי מודיעין, מתקפות סייבר ומתקפות תעמולה, וכי מצב זה מחייב סוג חדש של הרתעה מערבית.²

כאשר הנשק האולטימטיבי של השמדה המונית (נשק גרעיני) והנשק המיטבי של "הכוח הרך" (לוחמת המידע) מתערבבים זה בזה בעת משבר, התוצר ההיברידי המתקבל עשוי להיות בלתי צפוי ובלתי רצוי. משברים הם אירועים חריגים מעצם הגדרתם. לפי שעה לא התרחש אף משבר בסגנון של "מלחמה קרה" בין מדינות החמושות הן בנשק המידע של המאה ה-21 והן בנשק גרעיני. בנוסף לכך, הקשר בין סייבר לגרעין הוא בעל חשיבות מיוחדת הן עבור ארצות הברית והן עבור רוסיה: שתי המעצמות מחזיקות ביותר מתשעים אחוזים מהנשק הגרעיני העולמי, ושתיהן מפתחות יכולות לוחמת סייבר מתקדמות, הגנתיות והתקפיות כאחת.³ הדיון בהמשך המאמר מבקש לבחון מושגים והגדרות הקשורים בניהול משברים; להצביע על תכונות ודרישות לניהול מוצלח של משברים; לפרט את האתגרים שמבצעי מידע ולוחמת סייבר מציבים בפני יציבותו של משבר גרעיני; ולבסוף, להציג כמה תרחישים מסוכנים של הסתבכות בניהול משבר גרעיני שהמניע לו הוא מתקפת סייבר.

רחבה יותר ומתייחסת לסוגים שונים של פעולות מבצעיות, הכוללות שיטות דיגיטליות ו/או אחרות. ראו בנושא זה: P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), pp. 67-72; John Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military* (Chicago: Ivan R. Dee, 2008), ch. 6-7.

2 Pavel K. Baev, "Corruption Spoils Every Attempt to Cooperate With Russia," *Eurasia Daily Monitor*, July 17, 2017, <https://jamestown.org/analyst/pavel-k-baev>.

3 Timothy L. Thomas, *Russia: Military Strategy – Impacting 21st Century Reform and Geopolitics* (Ft. Leavenworth, Kansas: Foreign Military Studies Office, 2015), pp. 253-299; ומלחמה גרעינית ראו: Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar", *Journal of Cybersecurity* (2017): 1-12, <https://doi.org/10.1093/cybsec/tyw017>; Andrew Futter, "The Double-Edged Word: US Nuclear Command and Control Modernization", *Bulletin of the Atomic Scientists*, June 29, 2016, <http://thebulletin.org/double-edged-sword-us-nuclear-command-and-control-modernization.html>; Andrew Futter, "Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy", *RUSI Occasional Paper*, July 2016, https://rusi.org/sites/default/files/cyber_threats_and_nuclear_combined.1.pdf; Andrew Futter, "War Games Redux? Cyberthreats, U.S.-Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control", *European Security* (December 2015): 163-180.

ניהול משברים

מושגים והגדרות

ניהול משברים, ובכלל זה ניהול משברים גרעיניים, הוא מאמץ המשלב תחרות ושיתוף פעולה בין יריבים צבאיים. מעצם הגדרתו, משבר הוא תקופה של מתיחות רבה ואי־ודאות.⁴ באוויר מרחפים איומים, והלחץ על קובעי המדיניות הולך וגובר. לכל צד יש מטרות שהוא רוצה להשיג וערכים או אינטרסים שהוא מבקש להגן עליהם. במהלך מצב משברי, התנהגויות כל הצדדים מתאפיינות בתלות הדדית ובתגובתיות גבוהה. אפשר לראות את התלות ההדדית בעת משבר בין שתי מדינות כמערכת, בתנאי שהמונח "מערכת" אינו נתפס כישות נפרדת לחלוטין מהמדינה או מהתנהגויותיהם של הגורמים המרכיבים אותה. הממד של המערכת פירושו סיבתיות הדדית בהתנהגויות בעת משבר, שבה "A" נובע מ-"B" ולהיפך.

אחד ההיבטים של ניהול משברים הוא השאלה המטעה בפשטותה: מה מגדיר מצב כמשבר? מתי חל המעבר הסמוי מהיכולת של הסדר הבין־לאומי להכיל אלימות ואיומים לעבר התנהגות של משבר בפועל? התמוטטות ההרתעה הכללית במערכת מגבירה את תפיסות האיום בין השחקנים השונים, אך אינה ערובה לכך שמערכת יחסים מסוימת תידרדר לאיומים מרתיעים או משכנעים. תפיסתו של פטריק מורגן (Morgan) בדבר כישלון ההרתעה "המיידית" הינה שימושית לצורך הגדרת תחילתו של משבר: מדינה אחת מזהה תופעות ספציפיות המצביעות על כוונות עוינות מצד מדינה אחרת, שתי המדינות מחליפות איומים, ועתה עליהן להחליט מה תהיה תגובתיה של האחת לאיומי השנייה.⁵ הדרך המובילה למשבר מקבילה למעבר אצל תומס הובס ממצב של פוטנציאל לאלימות למצב של הנעה בפועל של חיילים והחלפת מחאות דיפלומטיות.

4 לדרישות הפוליטיות והמבצעיות הכרוכות בניהול משברים, ראו: Alexander L. George, "A Provisional Theory of Crisis Management", in *Avoiding War: Problems of Crisis Management*, ed. Alexander L. George (Boulder: Westview Press, 1991), pp. 22-27; Alexander L. George, "Strategies for Crisis Management", in *Avoiding War*, Ibid. pp. 377-394; Ole R. Holsti, "Crisis Decision Making", in *Behavior, Society and Nuclear War*, ed. Philip E. Tetlock et al. (New York: Oxford University Press, 1989), 1:8-84; Phil Williams, *Crisis Management* (New York: John Wiley and Sons, 1976); Alexander L. George, "The Cuban Missile Crisis: Peaceful Resolution Through Coercive Diplomacy", in *The Limits of Coercive Diplomacy*, ed. Alexander L. George and William E. Simons, 2nd ed. (Boulder: Westview Press, 1994), pp. 111-132.

5 ראו: Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills: Sage Publications, 1983); Richard Ned Lebow and Janice Gross Stein, *We All Lost the Cold War* (Princeton: Princeton University Press, 1994), pp. 351-355.

כל המשברים מתאפיינים, במידה מסוימת, ברמת איום גבוהה (מומנטום הסלמה מהיר, תוך סיכון משמעותי ומיידי להידרדרות למעשי איבה אינטנסיביים יותר, למרות שאף צד לא נוקט בינתיים מעשי איבה מלאים ושני הצדדים מייחסים עדיין עדיפות להרגעת ההסלמה), בלחץ זמן לקבלת החלטות, וב"ערפל משברי" המזכיר את "ערפל המלחמה" של קלאוזביץ ומקשה על המשתתפים להבין את המתרחש. עוד לפני שהחוקרים המודרניים הגו את הדיסציפלינה של ניהול משברים, כבר דיברו ההיסטוריונים על מרכיב "הסקת המסקנות החפוזות" (rush-to-judgment) המאפיין קבלת החלטות במצבי משבר בקרב מעצמות-העל.⁶ השפעת הנשק הגרעיני על קבלת ההחלטות בעת משבר אינה קלה למדידה או לתיעוד, משום שאת ההימנעות ממלחמה ניתן לייחס לסיבות רבות. נוכחות של כוחות גרעיניים משפיעה, ללא ספק, על מידת ההרס שיכולה להתרחש אם ניהול המשבר יכשל, ולכן נשק גרעיני הוא לא פעם גורם שדווקא מרגיע הסלמה. מעבר לחשש מקטסטרופה, חוקרים מעוניינים לבחון את אופן ההשפעה שיש לנוכחותו של נשק גרעיני על תהליך קבלת ההחלטות במהלך משבר. הבעיה חמקמקה להמשגה, שכן יש גורמים סיבתיים רבים בעלי חשיבות הרלוונטיים להחלטה על מלחמה או על שלום. כאשר מחפשים אחר הסברים, מגלים שההיסטוריה מלאה במשתנים תלויים.

ניהול משברים: דרישות ותנאים

ראשית לכל, ניהול משברים מוצלח מחייב שקיפות במסרים, אם כי מסרים מעורפלים או עמומים יעילים במקרים ספציפיים, כמו באופן שבו התנהגה איראן במשבר סביב פרויקט הגרעין שלה. שקיפות כוללת איתותים ברורים ומסרים לא מעוותים. איתות מתייחס לתנאים שלפיהם על כל צד לשלוח לצד השני את הערכתו לגבי המצב. למרות ששני הצדדים לא חייבים להיות בעלי אינטרסים זהים או אפילו משלימים, מספר מספיק של איתותים שיישלחו ויתקבלו בצורה מדויקת הוא תנאי מוקדם להעברה יעילה של מטרות ויעדים בין הצדדים. אם האיתותים נשלחים בצורה לא נכונה, או שאינם מובנים, הצעדים שינקטו השולח או המקבל עלולים לגרום לתוצאות לא מכוונות, כולל הסלמה עקב מיסקלקולציה. חומרת המצב עשויה לחייב שקיפות מלאה, אם כי יש דוגמאות רבות שבהן תקשורת חלקית הספיקה. זאת ועוד, העברת המסרים אינה בהכרח מילולית; היא יכולה להיות גם קינטית, כמו הזזת כוחות, היערכות צבאית או איתותים על נחישות.

6 ראו לדוגמה: Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1981); Michael Howard, *Studies in War and Peace* (New York: Viking Press, 1971), pp. 99-109; Gerhard Ritter, *The Schlieffen Plan: Critique of a Myth* (London: Oswald Wolff, 1958); D. C. B. Lieven, *Russia and the Origins of the First World War* (New York: St. Martin's Press, 1983).

שקיפות בהעברת המסרים כוללת גם תקשורת בדרגת איכות גבוהה ואמינות טכנית, הן בין היריבים והן בקרב מקבלי ההחלטות של כל צד. כל דבר שעלול להפריע מבחינה פיזית, מכנית או התנהגותית להעברת המסר עלול לעוות את דיוק התקשורת בעת משבר. פעימות אלקטרומגנטיות המשבשות מעגלי תקשורת, או הרס פיזי של רשתות תקשורת, הם דוגמאות ברורות למכשולים להשגת תקשורת מדויקת. הבדלים תרבותיים, המונעים הבנה נכונה בין מדינות, יכולים לפגוע בהרתעה שיושמה בהתאם למקובל על פי התיאוריה של כל צד. קית' ב' פיין (Payne), המתיחס לפוטנציאל של כישלון ההרתעה בעידן שלאחר המלחמה הקרה, קובע: "לצערנו, הציפיות שלנו לגבי התנהגות היריב אינן מתמלאות לעיתים קרובות, לא משום שהיריב הוא בהכרח לא רציונלי, אלא משום שאיננו מבינים את הערכים, היעדים, הנחישות והמחויבות הספציפיים שלו בהקשר של העימות, ולכן אנו מופתעים כאשר התנהגותו 'הבלתי רציונלית' שונה מהציפיות שלנו".⁷ שנית, ניהול משברים מוצלח גם מחייב להקל את לחץ הזמן המופעל על קובעי המדיניות והמפקדים, כך שהם לא ינקטו צעדים פרובוקטיביים לעבר הסלמה שלא במתכוון, רק משום שיסברו בטעות כי "הזמן נגמר". לחץ זמן הוא דבר אחד, אך צעדים בלתי מכוונים הם עניין אחר. קובעי המדיניות ואסטרטגים צבאיים מסוגלים לבנות עולמות דמיוניים של תפיסות והערכות, שבהם "שעת השיץ" הופכת להיות הרבה יותר מאשר סמן שימושי בתהליך קבלת ההחלטות. כחלק מהפתולוגיות האפשריות בעת קבלת החלטות במצבי משבר, יש נטייה לבלבל בין תאריך היעד ובין מטרות המדיניות עצמן: המטרה הופכת לאמצעי, והאמצעי למטרה. לדוגמה, תוכניות המלחמה של המעצמות הגדולות ביולי 1914 תרמו לנבואה שהגשימה את עצמה אצל המנהיגים בברלין, בסנט פטרסבורג ובווינה, לפיה רק באמצעות גיוס מהיר ומתקפה הם יוכלו למנוע הפסד מוחלט במלחמה. קובעי המדיניות הגיעו למסקנה כי מבנה לוחות הזמנים של הגיוס לא היה גמיש מספיק כדי להאט את המומנטום של סוף יולי ותחילת אוגוסט 1914, שהוביל להחלטה בלתי הפיכה לטובת יציאה למלחמה.

אחת התוצאות של לחץ זמן לקבלת החלטה בעת משבר, בהשוואה לדפוסים של ימי שלום, היא שהסיכוי לטעויות מסוג I (התקפה שלא זוהתה) ומסוג II (זיהוי שגוי של מתקפה) גובר. רשתות מודיעין והתרעה טקטית מורגלות להתנהגות השגרית של צבאותיהן של מדינות אחרות ועלולות לפרש בצורה שגויה כל חריגה מהתנהגות כזאת. קפיצות בלתי צפויות ברמות ההתרעה, או דפוסי פריסה לא

7 Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington: University Press of Kentucky, 1996), p. 57; David Jablonsky, *Strategic Rationality Is Not Enough: Hitler and the Concept of Crazy States* (Carlisle Barracks, PA: US Army War College, Strategic Studies Institute, August 8, 1991), pp. 5-8, 31-37.

אופייניים, עלולים להביא גורמים טקטיים לפרש את הסימנים המעידים בצורה לא נכונה, כפי שטען ברוס ג' בלייר (Blair): "למעשה, אחד המאפיינים הבולטים של משבר הוא העמימות שלו. מעצם הגדרתו, שיעור השגיאות מסוג I ו-II של מערכות המודיעין וההרתעה צונח במהירות. משבר מובל לא רק על ידי ערפל המשבר הידוע, האופייני להתרעות אסטרטגיות המועדות להיכשל, אלא גם על ידי ערפל הקרב, הנובע מהידרדרות מקבילה בהתרעה הטקטית".⁸

מאפיין שלישי של ניהול משברים מוצלח היא שכל צד צריך להיות מסוגל להציע לצד השני שסתום בטיחות או דרך יציאה מכובדת מהמצב הקשה שהסלים מעבר לציפיות. במקרים מסוימים אין לשני הצדדים דרך יציאה מכובדת מהמשבר, או כזו שאינה כרוכה בהפסד. במקרים כאלה תיווצר תחרות להקטנת הסיכון. אסור שהחיפוש אחר אופציות ידחק מי מהצדדים לפינה שממנה אין דרך לסגת בכבוד. לדוגמה, במהלך משבר הטילים בקובה ב-1962, הייתה לנשיא קנדי אפשרות להציע לראש ממשלת ברית המועצות חרושצ'וב יציאה מכובדת מפריסת הטילים המוגזמת שלו. קנדי התחייב פומבית שארצות הברית תימנע מתוקפנות צבאית בעתיד נגד קובה, ובאופן פרטי הסכים להסיר ולפרק את טילי ה"יופיטר" הבליסטיים לטווח בינוני שנפרסו קודם לכן בשטחי בעלות הברית של ארצות הברית בנאט"ו.⁹ לאחר כמה ימים של דיונים והבהרות לגבי האופן שבו הסובייטים תופסים את האירועים, קנדי ויועציו הקרובים הגיעו למסקנה שהשפלה פומבית של חרושצ'וב תגרום לארצות הברית להפסיד ולא להרוויח, ותפגע בתורה באינטרס של חרושצ'וב להשיג הסכם הדדי לפתרון המשבר.

מאפיין רביעי של ניהול משברים מוצלח הוא שכל צד מחזיק בתפיסה מדויקת על כוונות הצד השני ויכולותיו הצבאיות, לרבות על נקודות התורפה והפגיעויות של היריב. לדוגמה, מצג שלפיו צד אחד משדר שהוא מוכן להסלים למלחמה יכול לסיים לפעמים את המשבר בתנאים נוחים לשני הצדדים. אולם, הערכת הכוונות והיכולות של היריב הופכת לקשה במהלך משבר, משום שהכוונות והיכולות עשויות להשתנות בלהט התחרותיות והסביבה עתירת האיומים. רוברט ג'רוויס (Jervis) הזהיר בזמנו שדי היה באמונה שהמלחמה בתקופת המלחמה הקרה היא בלתי נמנעת, כדי ליצור נבואה המגשימה את עצמה, וכתב כי "האמונה של מעצמות העל לגבי השאלה האם המלחמה ביניהן היא בלתי נמנעת, יוצרת את המציאות באותה מידה שהיא משקפת אותה. מכיוון שמכת מנע יכולה להיות הסיבה הרציונלית היחידה לפתוח במלחמה כוללת, יש חשיבות רבה לאמונות

Bruce G. Blair, *The Logic of Accidental Nuclear War* (Washington: Brookings Institution, 1993), p. 237. 8

Lebow and Stein, *We All Lost the Cold War*, pp. 122-123. 9

לגבי כוונותיו המעשיות של הצד השני, ואמונות אלו תלויות, במידה רבה, בהערכה מה הצד השני מאמין שאני עתיד לעשות".¹⁰

הכוונות עשויות להשתנות במהלך משבר, ככל שקובעי המדיניות הופכים אופטימיים יותר לגבי רווחים צפויים, או פסימיים יותר לגבי הפסדים פוטנציאליים. ניהול התרעות צבאיות ופריסת כוחות, או כל תנועה אחרת של כוחות צבא, עשויים לשנות את יכולות הצדדים. מצבי מוכנות והיערכות צבאית גבוהה בכל אחד מהצדדים נועדו לשדר איתות דו־צדדי: נכונות לגרוע מכול היה והצד השני יתקוף; עמדה יציבה בלתי מאיימת במצב של פסיביות מצד האויב. זהו מסר מעורב, שקשה לשדרו גם בתנאים הטובים ביותר לניהול משברים, שכן ההתנהגויות והמסרים של מדינה מסוימת יכולים להיראות כבלתי עקביים בעיני היריב.

בתנאים של לחץ זמן ואיום צבאי, גופים שונים בארגונים ביטחוניים מורכבים עשויים לקבל החלטות שיתבססו על נקודת המבט הצרה והביורוקרטית שלהם. החלטות ופעולות כאלו לא תמיד ישקפו את כוונתם של קובעי המדיניות, או שלא ייעשו בתיאום עם ההחלטות והפעולות של גורמים אחרים בממשל. הסביר זאת אלכסנדר ל' ג'ורג': "חשוב להכיר בכך שהיכולת של סמכויות פוליטיות בכירות לשלוט במהלכים ובפעולות של כוחות הצבא נעשית קשה, בשל מספרן ומורכבותן של פקודות ההיערכות הנכנסות לתוקף ברגע שפורץ משבר, וככל שהוא מתעצם. לא קל לסמכות הפוליטית הבכירה לקבל מידע מלא ומדויק על כל פקודות ההיערכות הקיימות. כתוצאה מכך, היא עלולה להיכשל בתיאום בין פקודות חשובות ובין האסטרטגיה הכוללת שלה לניהול המשבר".¹¹

בשעה שקובעי המדיניות מתמודדים עם האתגר של נהלים מבצעיים רבים ומגוונים, מנהיגים פוליטיים עשויים לגלות גם חוסר רגישות לעלויות של שינויים פתאומיים בפקודות היערכות, או לא להיות מודעים לרציונל שבבסיסן של פקודות כאלו. לדוגמה, מנהיגי מדינה או ראשי ממשלה אולי לא יהיו מודעים לכך שככל שהם מאשרים רמות מוכנות גבוהות יותר, כך כללי הפתיחה באש של הכוח הצבאי הנמצא בשטח הופכים למתירנים יותר.¹² במקרים אחרים השליטה עשויה להיות הדוקה למדי. מנהלי המשבר לומדים עד מהרה ותוך כדי התנסות לקח חשוב הקשור להבחנה בין משבר ובין מלחמה בפועל: המעבר מהאחד לשנייה הוא פחות דיכוטומי ויותר רציף, והשלב הסופי של המשבר אינו ברור מספיק, למעשה עד הצעד הגורלי לעבר מלחמה, שאין ממנו דרך חזרה. כך, לדוגמה, מנהיגי המדינות

Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca: Cornell University Press, 1989), p. 183.

Alexander L. George, "The Tension Between 'Military Logic' and Requirements of Diplomacy in Crisis Management", in *Avoiding War: Problems of Crisis Management*, p. 18.

12 שם.

באירופה בשנת 1914 היו בטוחים בתחילה ביכולתם לנהל משבר שלא יתפתח למלחמה, אך ככל שהשליטה באירועים הלכה ונשמטה מידיהם, אמונה זו התחלפה באמונה פטליסטית, שהובילה לדך ללא מוצא.

גורמים משבשים פוטנציאליים

ללוחמת מידע (או לוחמת סייבר) יש פוטנציאל לתקוף או לשבש ניהול משברים מוצלח בכל אחת מהתכונות ומהמאפיינים שהוזכרו לעיל.¹³ ראשית, לוחמת סייבר יכולה לערפל את האיתותים שנשלחים מצד אחד למשנהו במהלך משבר. הדבר יכול להיעשות בכוונה או בשוגג. נניח שצד אחד שתל וירוס או תולעת ברשתות התקשורת של הצד השני.¹⁴ הווירוס או התולעת מופעלים במהלך המשבר ומשמידים או משנים מידע. המידע החסר או הלא תקין עלול להקשות על קורבן הסייבר לארגן התקפה צבאית. יחד עם זאת, מידע שנפגע או השתנה עלול להטעות את שני הצדדים לחשוב כי האיתות ששלחו פורש כהלכה, בשעה שלא כך היה. למשל, צד א' אולי התכוון לאותות ליריבו על "נחישות" במקום "כניעה" בסוגיה מסוימת, אולם צד ב' פירש את האיתות בטעות כמסר של "כניעה" והחליט להמשיך בתוקפנות. צד ב' ייתקל בהתנגדות בלתי צפויה, והתוצאה תהיה התפתחות מצב הרבה יותר מסוכן. יש גם אפשרות של מכת מנע בסייבר במטרה להשבית טילים גרעיניים של האויב לפני הגעתם לכן השיגור, או במהלך השיגור עצמו. ארצות הברית השתמשה ככל הנראה בטכניקות כאלו ("left-of-launch") נגד צפון קוריאה.¹⁵ האם מהלך כזה יתקבל בעת משבר גרעיני על ידי הצד המותקף כמהלך של הפחדה והרתעה? או להיפך: האם מתקפת סייבר נגד שיגור טילים תביא למכה גרעינית ראשונה מהצד המתגונן, מתוך חשש לאבד את יכולת התגמול שלו?

לוחמת סייבר יכולה גם להרוס או לשבש את ערוצי התקשורת הנחוצים להצלחת ניהול המשבר. היא יכולה לשבש קשר תקשורתי בין קובעי המדיניות

13 Paul K. Davis, "Deterrence, ו"לוחמת סייבר" ראו: Influence, Cyber Attack and Cyberwar", *International Law and Politics* 47 (2015): 327-355.

14 וירוס הוא תוכנית שמשכפלת את עצמה ומיועדת להרוס או לשנות את התוכן של קבצים אחרים המאוחסנים על תקליטונים או כוננים קשיחים. תולעים משחיתות את שלמות המידע במערכות תוכנה ומידע מ"בפנים החוצה", בדרכים שיוצרות נקודות תורפה שהאויב מנצל.

15 David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," *The New York Times*, March 4, 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?_r=0; Jesse T. Wasson and Christopher E. Bluesteen, "Taking the Archers for Granted: Emerging Threats to Nuclear Weapon Delivery Systems", Paper presented at the Annual Conference of International Studies Association, Baltimore, MD, 2017.

ובין המפקדים הצבאיים במצב של איום גבוה ולחץ זמנים קריטי. הפרעה כזו אינה חייבת להיות מתוכננת, ודי אם תהיה תוצאה של תוכנה זדונית שהושתלה קודם לכן והופעלה באופן בלתי צפוי, או שלא תחת שליטה מלאה של יוצריה. בתנאים כאלה מתעוררים שני סוגים של בעיות בלתי צפויות ביחסים בין המערכת הצבאית למערכת האזרחית: ראשית, ייתכן שמנהיגים פוליטיים יאצילו מראש סמכויות לשימוש בנשק גרעיני בתנאים מגבילים, הקובעים שרק כאשר יתקיימו תנאים מסוימים אלה (על פי הפרוטוקולים המלווים את ההאצלה מראש), המפקדים הצבאיים יהיו מורשים להשתמש בנשק הגרעיני שמצוי תחת פיקודם. תקשורת חסומה, משובשת או הרוסה עלולה לגרום לכך שהמנהיגים לא יוכלו לדעת כאשר מפקדים צבאיים יפרשו את המצב בצורה הרבה יותר נואשת ממה שהוא באמת, ולכן יסברו שיש להם היתר ליזום מהלך גרעיני. לדוגמה, תקשורת משובשת בין מטה הפיקוד הלאומי של ארצות הברית ובין הצוללות הנושאות טילים בליסטיים במהלך המלחמה הקרה, כתוצאה מהתקפה על אותן צוללות, יכולה הייתה להוביל את קציני הצוללות ואנשי הצוות שלהן להחלטה משותפת, בהיעדר הנחיות מנוגדות, לשגר טילים גרעיניים.

ביקורת שהופנתה לטיוטה מוקדמת יותר של מאמר זה זיהתה נכון את הפרדוקס שבהנחה, לפיה מנהיגים יאשרו מתקפת סייבר במהלך משבר, שאותו היו מעדיפים לסיים לפני שיתדרדר למלחמה. לכאורה, הגיוני להניח, לפחות באופן עקרוני, שמתקפת סייבר יש לשגר בשילוב עם מכה ראשונה ולא לפניה. אני מודה שיש בכך היגיון, אבל יש לכך גם צד אחר: ראשית, תקיפות סייבר במהלך משבר עשויות לשמש לא רק כאמצעי ליצירת תקלות טכניות במערכות המידע של האויב ובתהליך קבלת ההחלטות שלו, אלא גם להיות סוג של אמצעי מיקוח אסטרטגי לסיום הסכסוך מנקודת יתרון גבוהה יותר, ואפילו עם תוצאה חיובית יותר. לדוגמה, טכניקות "left-of-launch" לשיבוש הרשתות התומכות במערכות שיגור הטילים יכולות לתמוך ביכולות ההגנה מפני טילים של צד אחד, ולערער את הביטחון העצמי של הצד השני לגבי יכולתו לשגר התקפות טילים בליסטיים.

שנית, לוחמת מידע בעת משבר תגביר כמעט בוודאות את לחץ הזמן של מנהיגים פוליטיים. הלחץ יכול להיווצר מדוחק זמן אמיתי, או כתוצאה מתפיסת הזמן שקובעי המדיניות חשים שיש להם כדי לקבל החלטות. ברגע שאחד הצדדים רואה שחלקים של מערכת הפיקוד, השליטה והתקשורת שלו נפגעים בשל מידע מזויף או רעשי סייבר חיצוניים, תחושת התבהלה (פניקה) שלו מפני אובדן אפשרי של אופציות צבאיות הולכת וגוברת. כך, לדוגמה, שיבוש, ולו חלקי, של המערכת האסטרטגית לפיקוד, שליטה ותקשורת של ארצות הברית במהלך המלחמה הקרה, יכול היה למנוע ביצוע יעיל של התוכנית האסטרטגית שלה למלחמה גרעינית (SIOP). תוכנית זו הייתה תלויה באומדנים מתואמים ומתוזמנים היטב ובתחזיות

מדויקות של נזקים למטרות מסוגים שונים. שיבוש והטעיה, ולו חלקיים, של רשתות ומרכזי תקשורת היו גורמים למתקפות מיותרות על אותן מטרות, וסביר להניח שגם מביאים להתקפות בלתי מתוכננות על מתקנים צבאיים או אזרחיים ידידותיים. השפעה משבשת אפשרית שלישית שיש ללוחמת מידע על ניהול משבר גרעיני היא הסכנה שלוחמת המידע תצמצם את החיפושים אחר חלופות זמינות מבין המעטות שיש. קובעי מדיניות המחפשים דרכי נסיגה ממשבר סבוך זקוקים לאפשרויות גמישות ולפתרון בעיות יצירתי. קורבנות של לוחמת סייבר עלולים לחוות ירידה ביכולת לפתור בעיות באופן שגורתי, ובוודאי יצירתי, לאחר שרשתות המידע מתמלאות ב"זבל". השאלות למפעילים יוצגו בצורה גרועה, והתשובות (אם יהיו בכלל זמינות) ישאפו למכנה המשותף הנמוך ביותר של תהליכי ההפעלה הסטנדרטיים שתוכננו מראש.

מערכות תגמול, התלויות בשיגור במצב של התרעה, ולא במצב של הישרדות לאחר התקפה, חשופות במיוחד לקיצורי זמנים ולחלופות מוגבלות, כפי שמציין ברוס בלייר: "גם מערכת התרעה מתוכננת היטב אינה יכולה להציל מפקדים מפני קריאה שגויה של המצב כתוצאה מאילוצי זמנים ומידע במסגרת התפיסה של 'שיגור במצב של התרעה'. תפיסה כזאת קוטעת את תהליך קבלת ההחלטות מוקדם מכדי שתאפשר הערכה חוזרת שתעלה בקנה אחד עם המציאות. תגובה מהירה היא, מעצם טיבה, בלתי יציבה, משום שהיא מקצרת את זמן הלמידה הדרוש כדי להתאים את התפיסה למציאות".¹⁶

הנטייה לחפש את החלופה הזמינה הראשונה שעומדת בתנאי הסף המינימליים להשגת המטרה, חזקה אצל ארגונים ביורוקרטיים לא צבאיים גם בתנאים רגילים.¹⁷ במערכות שליטה ובקרה אזרחיות-צבאיות, הפועלות תחת הלחץ של קבלת החלטות בעת משבר גרעיני, החלופה הזמינה הראשונה יכולה להיות גם האחרונה, פשוטו כמשמעו, או כך לפחות קובעי המדיניות והיועצים הצבאיים עשויים לשכנע את עצמם. לפיכך, ההטיה לעבר פתרונות מהירים ומינימליים היא רבה. כך, למשל, במהלך משבר הטילים בקובה ב-1962, אנשי הקבוצה המייעצת לנשיא קנדי שבו והציעו, לאורך כל 13 ימי המשבר, תקיפה אווירית ופלישה לאי. אם היה פחות זמן לדיונים, או אם הנשיא לא היה מכוון את הדיונים כך שיועלו בהן חלופות שונות, ייתכן מאוד שהמכה האווירית והפלישה היו החלופה הנבחרת.¹⁸ פול ק' דיוויס ציין בהקשר זה: "הדיונים המקובלים בנושא יציבותם של משרבים מניחים כי המנהיגים שולטים ביכולות הגרעיניות שלהם. כמו תמיד, ההיסטוריה גורמת להתפכחות.

Blair, *The Logic of Accidental Nuclear War*, p. 252. 16

James G. March and Herbert A. Simon, *Organizations* (New York: John Wiley and Sons, 1958), pp. 140, 146. 17

Lebow and Stein, *We All Lost the Cold War*, pp. 335-336. 18

הנשיא קנדי החל להיות מודאג בשנת 1961 מפעולות חד-צדדיות אפשריות של מפקדים צבאיים, שיכינו מכה מקדימה נגד ברית המועצות. הוא השקיע מאמצים כדי להדק את שליטתו האישית כנשיא. ההנהגה הסובייטית, שדאגה לשרידות כוחותיה הצבאיים, פיתחה יכולת לשיגור במצב של התרעה ולתגובה אוטומטית על מתקפה. מערכות [סובייטיות] כאלו יכלו להיות מקור למלחמה בשוגג.¹⁹

לבסוף, מתקפת סייבר יכולה לגרום לכל צד להעביר לצד השני תמונה שגויה של הכוונות והיכולות שלו, שיש בה פוטנציאל לתוצאות הרות אסון. דוגמה נוספת ממשבר הטילים בקובה ממחישה את תופעות הלוואי האפשריות של אי-הבנה פשוטה ותקשורת לקויה בניהול משברים בארצות הברית. בשיא המתיחות של ימי המשבר, סטה מטוס ריגול אמריקאי מסוג U-2 ממסלולו ונכנס בטעות לתוך המרחב האווירי הסובייטי. מטוסי קרב אמריקאיים וסובייטיים נכנסו לפעולה, ועימות אפשרי בין חילות האוויר של שתי המדינות באזור הארקטי עמד על הפרק. חרושצ'וב סיפר אחר כך לקנדי כי ההגנה האווירית הסובייטית עלולה הייתה לפרש את טיסת ה-U-2 כמשימת סיור מוקדם לפני תקיפה, או לראות בו מפצץ, ולחייב את ברית המועצות להגיב.²⁰ למרבה המזל, מוסקבה בחרה לתת לארצות הברית ליהנות במקרה זה מהספק, והתירה למטוסי הקרב האמריקאיים ללוות את ה-U-2 הסורר בחזרה לאלסקה. שאלה שמעולם לא קיבלה תשובה מלאה היא מדוע לא בוטלה המשימה המתוכננת של ה-U-2 מיד עם פרוץ המשבר? ייתכן שהתשובה פשוטה וקשורה לתהליכי ביורוקרטיה, בשילוב עם חוסר תקשורת בשרשרת הפיקוד של קובעי המדיניות האמריקאים, שלא העריכו נכונה את הסיכון של משימת ריגול "רגילה" בתנאים רגישים אלה.

ההערכה של החוקר מרטין ליביצקי על היחסים בין לוחמת סייבר ובין ניהול משברים מדגישה את הדברים והדוגמאות שהובאו לעיל: "ניתן לומר בהכללה שמצב שבו אין לחץ רב להגיב במהירות ושבנו נחיתות או הפסד זמניים יהיו נסבלים ויש מקום לתת לצד השני ליהנות מעט מהספק, הוא מצב שבו יש זמן לנהל את המשבר. לעומת זאת, אם אי-יכולת להגיב במהירות יביא לשחיקה במעמדה של

Paul K. Davis, Peter Wilson, Jeongeun Kim and Junho Park, "Deterrence and Stability for the Korean Peninsula", *Korean Journal of Defense Analysis* no. 1 (March 2016):

14.

Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little, Brown, 1971), p. 141; Scott D. Sagan, *Moving Targets: Nuclear Strategy and National Security* (Princeton: Princeton University Press, 1989), p. 147; Lebow and Stein, *We All Lost the Cold War*, p. 342.

מדינה, לנחיתות זמנית או להפסד שהם בלתי נסבלים, ואין מחלוקת לגבי האירוע, האחראי לו וסיבותיו, אזי מדינות יכולות להגיע למסקנה כי עליהן לפעול במהירות".²¹

תרחיש וסיכונים

התוצאה של תרחיש שבו ניהול משבר גרעיני מושפע מלוחמת מידע אינה בהכרח חיובית. למרות מיטב המאמצים שהצדדים למשבר עשויים להשקיע, המחלוקת ביניהם עלולה להידרדר למכה או לתקיפה גרעינית ראשונה של אחד הצדדים ולמכת תגמול על ידי האחר. במצב כזה, פעולות סייבר של אחד הצדדים, או של שניהם, עלולות להקשות על ריסון המלחמה ועל כל ניסיון לסיים אותה לפני שתגרום הרס ואובדן חיים בקנה מידה קטסטרופלי. כפי שכבר צוין, הפרטים של כל מקרה חשובים. בלוחמה פסיכולוגית, התוקף והמותקף עשויים להציג במכוון הצלחות ככישלונות או כישלונות כהצלחות, אם הם מעוניינים בהרגעת ההסלמה, וייצוג כוזב כזה יכול לתרום לכך.

אף שאין מלחמות גרעיניות "קטנות", יש גם דעה הפוכה מכך. במהלך המלחמה הקרה התפתח הרעיון של "לחימה גרעינית מוגבלת", "לחימה גרעינית טקטית" או "חילופי שיגורים הדדיים מצומצמים", ורעיונות דומים צצו גם סביב יכולותיהן הגרעיניות של הודו ופקיסטן. בדומה למלחמות קונבנציונליות, ייתכנו גם סוגים שונים של מלחמות גרעיניות, בהתאם לסיבות ולתוצאות המיידיות שלהן.²² האפשרויות השונות כוללות התקפה גרעינית שמקורה אינו ידוע; מקרה לא חד-משמעי ולא מוכח של שימוש בנשק גרעיני כמכה ראשונה; פיצוץ גרעיני במסגרת "ניסוי" שנועד להפחיד, אך ללא גרימת הרס מידי; תקיפה קונבנציונלית, שלפחות בשלב הראשון פורשה בטעות כתקיפה גרעינית. כפי שציין ג'ורג' ה' קווסטר (Quester): "ארצות הברית ומעצמות אחרות פיתחו כמה ראשי נפץ קונבנציונליים גדולים ורבי עוצמה, שנועדו להרוס את הבונקרים המוקשחים שעשויים לאכסן עמדת פיקוד של האויב או מערכת נשק מסוכנת שלו. פצצות 'חודרות בונקר' כאלו מהדהדות אות קולי מסוים כאשר הן מופעלות וגורמות לאותות סיסמיים תת-קרקעיים, שממרחק עלולים להתפרש בטעות כראש נפץ גרעיני קטן".²³

התרחיש הדומיננטי, של מלחמה גרעינית כוללת בין ארצות הברית לברית המועצות, העסיק את קובעי המדיניות של ימי המלחמה הקרה. כתוצאה מכך, חששות בנוגע לשליטה בהסלמה וסיום המלחמה נסחפו בחזון אפוקליפטי של אחרית הימים. עידן הגרעין השני, שחופף למדי לסיום המלחמה הקרה ולהתפרקותה

Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica: RAND Corporation, 2012), p. 145.

George H. Quester, *Nuclear First Strike: Consequences* (Baltimore: Johns Hopkins University Press, 2006), pp. 24-52.

שם, עמ' 27.

של ברית המועצות, מציע תפריט מורכב יותר של אפשרויות ותגובות גרעיניות.²⁴ מדינות סוררות, מדינות השואפות להגמוניה אזורית, או טרוריסטים, שיש להם אינטרסים לאיים בנשק גרעיני או להשתמש בו, וכן התפשטות אפשרית של נשק גרעיני למדינות שכיום אינן גרעיניות, מותחים עד קצה הדמיון את כושר ההתמודדות וההמצאה של אסטרטגים צבאיים וסופרי מדע בדיוני.

בנוסף לגורמים האפלים ביותר המעורבים באיומים גרעיניים או באיומים להנחית מכה ראשונה, קיימת אפשרות נוספת, והיא סכנת הידרדרות התלויה בתנאים הפוליטיים השוררים בין ארצות הברית לרוסיה, בין רוסיה לסין או בין סין להודו (כלומר, בין המדינות הגרעיניות של ימינו). "הממסד" הגרעיני, המכונה "מדינות ה-P-5", פועל לעיתים להרגעה, התלויה בהמשך קיומן של נסיבות פוליטיות חיוביות בפוליטיקה האזורית והגלובלית. עימותים פוליטיים, שלא ניתן להעלותם על הדעת בעשור מסוים, עשויים להתפתח למלחמות בלתי נמנעות מבחינה פוליטית בעשור אחר. מלחמת העולם הראשונה היא דוגמה מאלפת לכך. המלחמה בין רוסיה לגיאורגיה באוגוסט 2008 הייתה תזכורת נוספת לכך שסכסוכים מקומיים לאורך קווי שבר אזוריים, בין גושים או מעצמות גדולות, יכולים להתרחב לכדי עימותים קשים, כפי שקרה גם במלחמות הבלקן בשנות התשעים של המאה העשרים. במקרים כמו אלה, היתרון הצבאי החד-צדדי של רוסיה על גיאורגיה ב-2008, והעוצמה הצבאית של נאט"ו מול זו של הבוסנים ב-1995 והסרבים ב-1999, תרמו לסיום המלחמות ללא הסלמה נוספת ברמה הבין-לאומית.

הסלמה של מלחמה קונבנציונלית לכדי שימוש ראשוני בנשק גרעיני עדיין אפשרית גם בימינו, כאשר נשק גרעיני, מבצעי או טקטי, נפרס על ידי כוחות צבא לאומיים או כוחות קואליציוניים. ארצות הברית פרסה כמה מאות כלי נשק

24 Colin S. Gray, *The Future of Strategy* (Cambridge: Polity Press, 2015), pp. 98-106; Paul Bracken, *The Second Nuclear Age: Strategy, Danger and the New Power Politics* (New York: Henry Holt – Times Books, 2012); Adam B. Lowther ed., *Deterrence: Rising Powers, Rogue Regimes and Terrorism in the Twenty-First Century* (New York: Palgrave Macmillan, 2012); Beatrice Heuser, *The Evolution of Strategy: Thinking War from Antiquity to the Present* (Cambridge: Cambridge University Press, 2010), pp. 351-383; Michael Krepon, *Better Safe than Sorry: The Ironies of Living with the Bomb* (Stanford, Calif.: Stanford University Press, 2009); Lawrence Freedman, *Deterrence* (Cambridge: Polity Press, 2004); Lawrence Freedman, *The Evolution of Nuclear Strategy*, 3rd ed. (New York: Palgrave Macmillan, 2003); Patrick M. Morgan, *Deterrence Now* (Cambridge: Cambridge University Press, 2003); Keith B. Payne, *The Fallacies of Cold War Deterrence and a New Direction* (Lexington: University Press of Kentucky, 2001); Colin S. Gray, *The Second Nuclear Age* (Boulder: Lynne Rienner, 1999); Payne, *Deterrence in the Second Nuclear Age*; Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*.

גרעיניים אוויריים טקטיים בבסיסים של בעלות הברית שלה בנאט"ו – בלגיה, גרמניה, איטליה, הולנד וטורקיה.²⁵ רוסיה מחזיקה, ככל הנראה, בכמה אלפי כלי נשק גרעיניים, טקטיים או מבצעיים, כולל מספרים משמעותיים שלהם הפרוסים במערב המדינה.²⁶ הסכם START החדש, לאחר שיאושר, ייצור שוויון בין ארצות הברית לרוסיה במערכות נשק גרעיניות בעלות טווח ביניים.²⁷ העליונות של ארצות הברית ושל נאט"ו, מבחינה טכנולוגית ומבחינת הכוח הצבאי הקונבנציונלי מבוסס המידע, משאירה את רוסיה תלויה במידה רבה בנשק גרעיני טקטי, כפיצוי על חולשתה היחסית בכוחות לא גרעיניים. מדינות נאט"ו נשמו לרווחה כאשר הדוקטרינה הצבאית של רוסיה, שאושרה רשמית ב־2010, לא הנמיכה את סף השימוש הראשוני בנשק גרעיני בהשוואה למהדורות קודמות שלה.²⁸ הדוקטרינה הצבאית מ־2010 מצביעה על נכונות לעשות שימוש ראשון בנשק גרעיני במצבי חירום קיצוניים, כפי שתגדיר אותם ההנהגה הפוליטית הרוסית.²⁹ למרות העליונות הברורה של הכוחות הקונבנציונליים של ארצות הברית ונאט"ו על פני אלה של רוסיה, המערב אינו משתוקק בהכרח להיפטר מהנשק הגרעיני הטקטי שנותר פרוס בשטחיהן של בעלות הברית. פאנל מומחים שכינס נאט"ו ב־2010 כדי לבחון את הדוקטרינה הצבאית של הארגון היה אמביוולנטי וזהיר בנוגע לעתיד פריסתו של הנשק הגרעיני של חברות הברית. הסוגיה של משא ומתן על פירוק נשק זה בתמורה לוותורים מקבילים של רוסיה נותרה פתוחה לדיון נוסף. במקביל, הדוח של מומחי נאט"ו הדגיש את האווירה הנוכחית השוררת

25 לרקע על הנשק הגרעיני הטקטי שארצות הברית פרסה באירופה ראו: Hans M. Kristensen, *U.S. Nuclear Weapons in Europe: A Review of Post-Cold War Policy, Force Levels and War Planning* (Washington, D.C.: Natural Resources Defense Council, February 2005).

26 Pavel Podvig, "What to do about Tactical Nuclear Weapons", *Bulletin of the Atomic Scientists*, February 25, 2010, <https://thebulletin.org/2010/02/what-to-do-about-tactical-nuclear-weapons/>; Jacob W. Kipp, "Russia's Tactical Nuclear Weapons and Eurasian Security", *Eurasia Defense Monitor*, March 5, 2010, <https://jamestown.org/program/russias-tactical-nuclear-weapons-and-eurasian-security/>.

27 "Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms", *US Department of State*, Washington, D.C., April 8, 2010, <http://www.state.gov/documents/organization/140035.pdf>.

28 "The Military Doctrine of the Russian Federation", February 5, 2010, in *Johnson's Russia List* 2010, #35, February 19, 2010; Nikolai Sokov, "The New 2010 Russian Military Doctrine: The Nuclear Angle", *Center for Nonproliferation Studies, Monterey Institute of International Studies*, February 5, 2010, http://cns.miis.edu/stories/100205_russian_nuclear_doctrine.htm.

29 Keir Giles, "The Military Doctrine of the Russian Federation 2010", *NATO Research Review* (February 2010): 1-2, 5-6.

אצל מדינות הברית, לפיה נשק גרעיני מהווה חוליה הכרחית בשרשרת אופציות ההרתעה של מדינות אלו.³⁰

קשה לתאר כיצד יתגלגלו משבר גרעיני או קבלת החלטה על שימוש ראשון בנשק גרעיני, כאשר גם נאט"ו וגם רוסיה יעשו שימוש בדיסאינפורמציה אסטרטגית ובלוחמת מידע במטרה לשבש את מערכות הפיקוד והבקרה, התקשורת וההרתעה של האויב. מבצעי סייבר משבשים נגד מערכות אויב, במצב של סף שימוש ראשון בנשק גרעיני או זמן קצר לאחר מכן, עלולים להגביר את הקושי, הרב ממילא, לעצור את הלחימה לפני התפשטות העימות על פני כל אירופה או הגעה למלחמה גרעינית אסטרטגית. הקשיים שפורטו לעיל – ניהול משברים בצל הרתעה גרעינית או בהמתנה להחלטה על שימוש ראשון בנשק גרעיני – יעמידו את לכידותן של מדינות הברית הצפון אטלנטית תחת לחץ וסכנה חסרי תקדים, שללא ספק יחמירו עוד יותר עקב מצבי איודאות וערפול בזירת הקרב.

ברית נאט"ו צפויה לעמוד בפני שלושה מצבי חיכוך חדשים: ראשית, ההחלטה אם להשתמש בנשק גרעיני מתקבלת כיום אך ורק בתוך שרשרת הפיקוד האמריקאית (או זו של בריטניה/צרפת). נאט"ו לא נתנה את הדעת לאתגר של ניהול תהליך קבלת החלטות במצב של סף מלחמה על ידי 29 מדינות החברות כיום בברית, לעומת 16 בלבד בתקופת המלחמה הקרה. לא רק שמספר המדינות החברות בברית גדל מאז, גם השוני במדיניות החוץ שלהן, בסדרי העדיפויות של הביטחון הלאומי שלהן ובתפיסותיהן הצבאיות-פוליטיות מציב מכשול אדיר בפני קבלת החלטות במצבי לחץ, במיוחד קבלת החלטה לשימוש ראשון בנשק גרעיני; שנית, יהיה חיוני להשיג מודיעין מהימן לגבי כוונות רוסיה בעקבות שימוש ראשוני שלה בנשק גרעיני, או שימוש כזה על ידי נאט"ו, אלא שמודיעין כזה יהיה קשה להשגה; שלישית, שימוש ראשוני בנשק גרעיני, לראשונה מאז הטלת פצצת האטום על נגסקי, יהיה פתח למצב פסיכולוגי, פוליטי ומוסרי חדש, שבו נושאים ונותנים שיבקשו לשים קץ להסלמה, או להביא לסיום המלחמה, יצטרכו לשמור על קור רוח, לשכנע את צבאותיהם להימנע מפעולה ולהחזיר משגרים של נשק גרעיני ואת הנשק הגרעיני עצמו לאתרים מאובטחים, אך כאלה שיהיו גלויים לצדדים היריבים. את כל המהלכים האלה יהיה צורך לבצע על רקע התבהלה שתתפשט ברשתות החברתיות ובאינטרנט, שיפעלו "סביב השעון".

NATO 2020: Assured Security; Dynamic Engagement, Analysis and Recommendations 30
of the Group of Experts on a New Strategic Concept for NATO (Brussels: North
Atlantic Treaty Organization, May 17, 2010), pp. 43-44.

מסקנות

השילוב האפשרי של לוחמת מידע עם המשך ההרתעה הגרעינית בתקופה שלאחר המלחמה הקרה יכול להפיק תוצרי לוואי לא מכוונים, ואלה עלולים להיות מסוכנים ליציבות העולמית. אחת המטרות של לוחמת סייבר בזמן מלחמה קונבנציונלית תהיה למנוע מכוחות האויב מודעות למתרחש בזירת הקרב, ומנגד להשיג שליטה על מודעות כזאת, כפי שארצות הברית הצליחה לעשות במידה רבה במלחמת המפרץ הראשונה ב-1991.³¹ בשעת משבר, שבו נשק גרעיני זמין בידי הצד הנתון למתקפת סייבר, הפגיעה במערכות המודיעין ובמערכות השליטה והבקרה של האויב יכולה לעמוד בסתירה לרצון להגיע לשליטה על העימות ולהשיג ניצחון במחיר נסבל. בתנאים מסוימים של ניהול משבר גרעיני, פגיעה בפקוד, בשליטה, בתקשורת, במחשבים, במודיעין וביכולת המעקב ואיסוף המידע של היריב יכולה להתברר כ"גול עצמי". כדי שמסר של הרתעה יפעל, גם כאשר עומד מאחוריו איום אמין בפעולת מניעה או תגמול, הוא חייב תחילה לעבור בהצלחה ובצורה משכנעת לידיו של הצד השני.³²

31 כפי שאמר דיוויד אלברטס: "שליטה במידע תישאר עניין אקדמי בלבד, אם לא נוכל להפוך אותה לשליטה בשדה הקרב". ראו: David Alberts, "The Future of Command and Control with DBK", in *Dominant Battlespace Knowledge*, ed. Stuart E. Johnson and Martin C. Libicki (Washington: National Defense University, 1996), pp. 77-102, especially p. 80.

32 כפי שאמר קולין גריי: "מכיוון שהרתעה נובעת מיחסי גומלין, היא אינה יכולה להתקיים במצב של יכולות, התנהגות או כוונות של צד אחד בלבד. כל מי שמתייחס ל'מדיניות ההרתעה' בהא הידיעה, כנראה שפשוט אינו מבין את הנושא". ראו: Collin Gray, *Explorations in Strategy* (Westport: Greenwood Press, 1996), p. 33.