פיתוח דוקטרינה ללוחמת סייבר במערכה הקונבנציונלית

רון טירה

תחום הסייבר נמצא בתהליך שיהפוך אותו לענף נוסף בלוחמה המדינתית, בדומה לענפי היבשה, הים, האוויר או החלל. ככזה, הוא עתיד להנביט דוקטרינת הפעלה מלאה ובשלה שתשאב מרכיבים מדפוסים והגיונות צבאיים כלליים ותשתלב במערכה הקונבנציונלית באופן סינרגטי עם מאמצים אחרים. כמה ממעצמות הסייבר כבר פיתחו דוקטרינות ויכולות מתאימות, אך רוב מדינות העולם ממוקדות עדיין באבטחת סייבר ולא בלוחמת סייבר, הגנתית והתקפית כאחת. אבטחת הסייבר מבוססת על פרקטיקות ומוצרים גנריים, המיועדים לאבטח בפני איומי ייחוס גנריים, שבמקרים רבים הם תת־מדינתיים. לעומת זאת, לוחמת סייבר מתמודדת עם יריב ספציפי, בהקשר ספציפי ועל בסיס מודיעין על היריב המאפשר את ההתמודדות איתו.

מילות מפתח: סייבר, ישראל, ארצות הברית

רקע: לקראת נורמליזציה של לוחמת הסייבר המדינתית

הסייבר נמצא בתהליך של התפתחות[1] לכדי ענף נוסף בלוחמה המדינתית, בדומה לענפי היבשה, הים, האוויר או החלל. ככזה, הוא עתיד להנביט דוקטרינת הפעלה מלאה ובשלה שתשאב, ולו חלקית, מתוך דפוסים והגיונות צבאיים כלליים ותשתלב במערכה הקונבנציונלית העיקרית, וזאת באופן סינרגטי עם מאמצים אחרים.

לוחמת הסייבר נמצאת בשלבי התפתחות שונים במדינות שונות,[2] בחלקן בתהליך סדור וקוהרנטי מעלה־מטה (top-down) ובחלקן בהתפתחות אינקרמנטלית, שבה

1 עמית שיניאק, "יתרון שאינו רק טכנולוגי – השינוי הארגוני בארצות הברית", **סייבר, מודיעין וביטחון**, כרך 1, גליון 3, דצמבר 2017.

2 גבי סיבוני ועופר אסף, **קווים מנחים לאסטרטגיה לאומית במרחב הסייבר**, מזכר 149, תל אביב: המכון למחקרי ביטחון לאומי, 2015.

סא"ל (מיל') רון טירה הוא איש עסקים ומשרת במילואים בחיל האוויר בתחום תכנון המערכה.

מכלול של צעדים נקודתיים, הננקטים לעיתים כמענה לצורך "בוער", מתחברים מטה־מעלה (bottom-up) לתמונה כוללת כלשהי. חלק ממעצמות הסייבר נמצאות בשלבים מתקדמים של פיתוח דוקטרינה ללוחמת סייבר,[3] העשויה להשתלב במערכה הקונבנציונלית. לפי פרסומים שונים, חמש מעצמות הסייבר המובילות בעולם הן ארצות הברית, רוסיה, סין, בריטניה וישראל.[4]

לוחמת הסייבר וההיערכות אליה מתרחשות בעיקרן בהסתר, והמקורות הגלויים בתחום זה מועטים. ארצות הברית חשפה בשנת 2010 טפח מתפיסת לוחמת הסייבר שלה,[5] אך מרבית הפרסומים הגלויים עוסקים בהקצאת המשאבים הלאומיים לסייבר, בקביעת המבנה הארגוני שלו (כמו מסמך "המיזם הקיברנטי הלאומי" בישראל),[6] ברגולציה או באבטחת מידע, ופחות מכך בעולם התוכן של דוקטרינת לוחמת הסייבר.

ניתן לקבוע בהכללה כי לוחמת הסייבר טרם הבשילה במרבית המדינות.[7] הסיבות לכך הן, בין היתר:

- התמקדות באבטחת סייבר[8] והבשלה איטית של רעיון המערכה ההתקפית וההגנתית בסייבר.
- היעדר דוקטרינה מלאה ובשלה ללוחמת סייבר התקפית והגנתית.
- הסתכלות על הסייבר כענף מבודד, שאינו משולב במערכה הקונבנציונלית.

---

3 "Cyberspace Operations", Joint Publication 3-12 (R), *US Joint Chiefs of Staff*; "Electronic Warfare", Joint Publication 3-13.1, *US Joint Chiefs of Staff*; William J. Lynn III, "Defending the New Domain, the Pentagon's Cyber Strategy", *Foreign Affairs*, September/October 2010; Cheryl Pellerin, "Cybercom Chief: Cyberspace Operations Key to Future Warfare", *US Department of Defense*, June 16, 2014; "The Department of Defense Strategy", *US Department of Defense*, April 2015.

4 Keith Breene, "Who are the Cyber Superpowers?", *World Economic Forum*, May 4, 2016.

5 "Cyber Command Fact Sheet", *US Department of Defense*, October 13, 2010.

6 לדוגמה, "קידום היכולת הלאומית במרחב הקיברנטי", *ממשלת ישראל*, החלטה 3611, 7 באוגוסט 2011, וכן "קידום ההיערכות הלאומית להגנת הסייבר", *ממשלת ישראל*, החלטה 2444, 15 בפברואר 2015. ראו גם "נייר מטה לדיון הוועדה העליונה למדע וטכנולוגיה בנושא: המיזם הקיברנטי הלאומי", יולי 2013, וכן "המרחב הקיברנטי והגנה על תשתיות חיוניות", *הכנסת*, 12 במאי 2013.

7 אסטרטגיית אבטחת סייבר דומה קיימת במספר רב של מדינות. להלן שתי דוגמאות להמחשה:
"Cyber Security Strategy for Germany", *German Federal Ministry of the Interior*, February 2011; "Cybersecurity Strategy", *The Government of Japan*, September 2015.

8 "National Cyber Security Strategies", *European Network and Information Security Agency*, December 2012.

- התמקדות בסייבר בסביבת ה־IT (מחשבים ומכשירים סלולריים הנגישים מהאינטרנט), לעומת מתן משקל חסר ללוחמת הסייבר בסביבת ה־OT[9] (שליטה במערכות תפעוליות) ונגד מערכות נשק.[10]
- התמקדות באיום הייחוס הפלילי, ההאקטיביסטי, הטרוריסטי, החתרני (כמו שיבוש ההליך הדמוקרטי או שוק ההון) או ה"פארה צבאי" (קרי, במקומות בהם המדינה התוקפת מבקשת להתכחש לפעולה), לעומת מתן משקל חסר לאיום הייחוס המדינתי/מעצמתי־צבאי.
- התמקדות יתר באנקדוטות, כמו למשל בשאלת ייחוס התקיפה (attribution),[11] כאילו היה זה מגדיר עיקרי של תחום הסייבר, והעלאת הטענה שסוגיית הייחוס קוטעת את הרצף ההגיוני הקלאוזביציאני (למעשה, סוגיית הייחוס אינה חדשה, שכן גם כוחות מיוחדים, צוללות או אפילו כלי טיס מסוגלים לתקוף ללא ייחוס, בלי שהדבר יהווה ערעור או שינוי בתבניות האסטרטגיות והמערכתיות המוכרות). לעומת זאת, מתן משקל חסר לנורמליזציה הצפויה של הסייבר ולהשתלבותו בזרם המרכזי (mainstreaming) של הלוחמה.

לוחמת הסייבר נמצאת בשלבי התפתחות טכנולוגית ומבצעית ראשוניים, שבאנלוגיה להתפתחות התעופה הצבאית אפשר להשוותם להופעת מטוס התצפית הדו־כנפי במלחמת העולם הראשונה. כבר אז הובהר הפוטנציאל הטמון באפשרות הטיסה אל מרכזי הכובד של האויב, מעל מערכי ההגנה הקרקעיים ומכשולי הקרקע, ולכן מצביאים כמו ג'וליו דואה ובילי מיצ'ל גיבשו את תפיסת ההפצצה האסטרטגית עוד בטרם פותחו מטוסים המסוגלים לממשה. גם דוקטרינת לוחמת הסייבר צריכה להמשיך ולהתפתח אל מול הפוטנציאל העתידי ולשמש כמצפן הטכנולוגי והמבצעי, אפילו אם אין כיום עדיין את כל הכלים הדרושים למימוש מלא של מרכיביה.

מאפייני לוחמת הסייבר

כפי שיובהר בהמשך, לוחמת הסייבר מאמצת בהדרגה דפוסים והגיונות צבאיים כלליים, אך, כבכל ענף בלוחמה, גם לסייבר מאפיינים ייחודיים שיש לאבחנם.

---

9 Nate Beach-Westmoreland, Jake Styczynski, Scott Stables, "When The Lights Went Out", *Booz Allen Hamilton*, November 2016.

10 LTG Larry Wyche, USA Ret. and Mr. Greg Pieratt, "Securing the Army's Weapon Systems and Supply Chain against Cyber Attack", *Institute of Land Warfare*, November 2017.

11 John S. Davis II, Benjamin Adam Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, Michael S. Chase, **"**Stateless Attribution, Toward International Accountability in Cyberspace", *RAND Corporation*, 2017; Martin C. Libicki, **"**It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture**"**, *RAND Corporation*, March 1, 2017.

הסייבר מאפשר השגת שליטה בתוכנה או לפחות שיבוש פעולתה, ובמקרה של תוכנה המאפשרת שליטה במערכת מכנית, הוא עשוי לאפשר גם גרימת נזק פיזי לציוד או לאדם. במקרה בו תוכנה מאפשרת שליטה במספר רב של מערכות מכניות, ניתן להשיג פגיעה פיזית נרחבת ואף המונית. הסייבר מאפשר לפיכך הרג ופגיעה בנכסים, השקולים לפגיעה קינטית. כמובן שהסייבר גם מאפשר פגיעה בתפקודה של התוכנה או בנתונים, לרבות כאלה של מערכות נשק או מערכות תפעוליות קריטיות.

הפעלת נשק הסייבר כרוכה בסיכון אופרטיבי ישיר נמוך. ככזאת, היא עשויה להציג בנסיבות המתאימות יחסי עלות־תועלת אטרקטיביים בהשוואה לתקיפה פיזית, בעיקר במקרים בהם אין צורך במבצע עזר מורכב לשם יצירת נגישות לרשתות מבודדות (air gapped) או למערכות שמשיקולים טכנולוגיים או מבצעיים מאתגר לתקוף אותן מרחוק. מצד שני, כאשר התקפת הסייבר לא הוכנה מראש בשגרה, עלול להתעורר קושי לבצעה בחירום כשההתרעה היא קצרה.

המרחק הגיאוגרפי מאבד ממשמעותו בממד הסייבר, ולכאורה ניתן לתקוף בסייבר לכל טווח. מאפיין זה מרחיב מצד אחד את קשת אויבי הייחוס ואיומי הייחוס, ומצד שני מהווה לעיתים תחליף או משלים נוח יותר למבצע קינטי מורכב נגד מדינות לא גובלות ומרחיב את אפשרויות הפעולה נגד קואליציות של יריבות. ניתן למדוד את יחסי הכוחות חזק־חלש בממד הסייבר בנפרד מממדים אחרים (כפי שמעצמה ימית עשויה, לדוגמה, להיות בעלת עוצמה צבאית יבשתית צנועה).

בחלק מהמקרים, האתגר הטכנולוגי והמבצעי של החדרת נשק סייבר הינו מורכב וכרוך בזמן, ויש להניח שבאותם מקרים התוקף ישאף להתגבר על אתגר זה עוד בטרם יפרוץ העימות (מבצעי יום ה־"ע" מינוס). החדרת נשק סייבר למערכות קריטיות של יריבים פוטנציאליים היא לפיכך שגרה של טרם מלחמה, החיונית במקרים מסוימים להפעלה אפקטיבית של הסייבר ההתקפי מאוחר יותר, בלחימה עצמה. כלומר, בניגוד למרבית ענפי הלחימה, הפעלת הסייבר במערכה הקונבנציונלית מצריכה במקרים רבים ניהול מבצעים מקדימים בתקופת השגרה של טרם הלחימה. יש להניח שחשיפת ניסיון להחדיר נשק סייבר בשגרה לא תהווה, לפחות בחלק מהמקרים, קאזוס בלי ולא תוביל בפני עצמה להסלמה, וזאת בניגוד לחשיפת חדירה צבאית פיזית למדינה אחרת בעת שגרה.

לתוקף הסייבר יש כיום, ובעתיד הנראה לעין, יתרון משמעותי על המגן.[12] המגן חייב להגן על מספר רב של נכסים – מפלטפורמות לחימה ומערכות נשק, דרך מערכות שליטה ובקרה צבאיות, מערכות תקשורת צבאיות, תשתיות ממשל,

12 "Information Technology and Cyber Operations, Modernization and Policy Issues to Support the Future Force", *Hearing Before the Subcommittee on Intelligence, Emerging threats and Capabilities, House of Representatives*, March 13, 2013.

תשתיות לאומיות קריטיות, תשתיות שאינן קריטיות אך כאלו ששיבושן יוצר אפקט מורלי, תאגידים מסחריים בעלי חשיבות לאומית כמו בנקים או בורסות, ועד לכלל העורף הדיגיטלי האזרחי. תהליכי הרישות והדיגיטליזציה של העולם, הצפויים לעלות מדרגה עם כניסת "האינטרנט של הדברים" (IOT) והרֶכב האוטונומי, מזניקים מעלה הן את מספר הנכסים שניתן לפגוע בהם (או לפגוע באחרים באמצעותם) והן את הנגישות וכיווני התקיפה (attack vectors) האפשריים. התוקף יכול לבחור למעשה מתוך אינספור אפשרויות תקיפה, וכדי לחדור למערכת הנתקפת, עליו להצליח רק פעם אחת ובכיוון תקיפה בודד. לעומתו, המגן צריך להצליח להגן כל הזמן על כל כיווני התקיפה הקיימים במערכותיו.

שני יתרונות נוספים נמצאים בידי התוקף. הראשון, מאחר והמגן צריך להגן על "הכל", והתוקף יכול למקד את מאמצי התקיפה שלו באשר יבחר, הרי שהיקפי כוח האדם הדרושים להגנה בסייבר גדולים הרבה יותר מהיקפי כוח האדם התוקף (בניגוד ללוחמה הקונבנציונלית). מכאן שניתן לרכז כוח אדם איכותי יותר בהתקפה בהשוואה לממוצע של איכות כוח האדם המגן. בתחום הסייבר ישנה חשיבות מכרעת לאיכות כוח האדם, כישוריו, יצירתיותו, הידע והעדכניות שלו. לכן, בהתמודדות האופיינית בין תוקף ובין מגן על כיוון תקיפה מסוים, ניתן להניח שהתוקף (המציב לצורך זה את טובי אנשיו) יהנה מיתרון איכותי על המגן (המציב, בהיעדר התרעה ממוקדת, כוח אדם ממוצע ברמתו); היתרון השני של התוקף, שהוא במידה מסוימת פועל יוצא של הנקודה הקודמת, הוא שלפחות בעת הנוכחית, התורפות של מערכות שונות רבות יותר מהמודעות של המגן להן. גם רמת המודעות של המגן למידת הנגישות אליו אינה מספקת – למשל, היכולת להגיע אליו באמצעות תקיפת מערכות שכנות או צדדים שלישיים בשרשרת האספקה שלו.

בסייבר קיים דמיון ניכר בין האיסוף ובין ההתקפה, עד כדי טשטוש הגבולות ביניהם. בשני המקרים יש לחדור לרשת היריבה ולהשתלט על תוכנה. קצה תהליך האיסוף הוא המידע שנאסף, בעוד שקצה תהליך התקיפה הוא שינוי או שיבוש המידע. גם התהליך הטכנולוגי והמבצעי של איסוף והתקפה בסייבר זהה ברובו, ויתכן שאותו כלי סייבר ישמש הן לאיסוף והן, במקרה הצורך, לתקיפה.

כמו כל ענף לוחמה אחר, הסייבר הוא גם צרכן של המודיעין הנחוץ לשם ניהול מערכה הגנתית או התקפית. המודיעין הדרוש לסייבר אינו חייב להיאסף דווקא בממד הסייבר. המודיעין הרלוונטי ביותר, המאפשר את ניהול המערכה בסייבר, ייאסף לעיתים באמצעים אחרים (יומינט, קומינט וכדומה), או יהיה תוצאה של מחקר מודיעיני הנעשה בשיטות קונבנציונליות.

המערכה ההגנתית בסייבר

מוצע לאבחן בין אבטחת סייבר ובין ניהול מערכה הגנתית בסייבר, על בסיס ההמשגה וההגדרות שלהלן: אבטחת סייבר היא פעילות אותה עשוי לנקוט כל גורם המבקש לאבטח את עצמו בממד הסייבר, לרבות גורמים מסחריים ופרטיים. אבטחת הסייבר מבוססת על פרקטיקות ומוצרים גנריים[13] המיועדים להגן בפני איומי ייחוס גנריים. עיקרה של אבטחת הסייבר הוא בהתבוננות של הצד המאבטח (או ה"כחול") על עצמו, ובכלל זה על הדרך בה הוא מגן על "הגדר" (מניעת חדירת נשקי סייבר למערכת ה"כחולה"), התנהגותו האבטחתית השגרתית (מהצבת "מלכודות דבש" ופיתויים, דרך הונאת התוקף באמצעות ארכיטקטורת רשת מזויפת ועד לשינויים עיתיים בטופולוגיית הרשת ה"כחולה"), ניטור הפעילות בתוך הרשת ה"כחולה", ניטור המידע המוזרם מתוך הרשת ה"כחולה" החוצה, הצפנת המידע ה"כחול" והיערכות להתאוששות הרשת ה"כחולה" מתקיפה, מחקר חולשות עצמיות של הרשת ה"כחולה" וכדומה.

לעומת זאת, הגנה בסייבר היא מערכה שמנהל גורם מדינתי (או מעֵין מדינתי) במטרה להתגונן נגד תקיפה. הגנת הסייבר אינה גנרית, אלא נעשית על פי ההקשר – מול מאמץ התקפי מסוים של תוקף מוכר או מזוהה. כבכל מערכה הגנתית, עיקרה של ההגנה בסייבר הוא בהתבוננות על התוקף (או ה"אדום"), תוך נקיטת מגוון פעולות אופרטיביות מול המאמצים המזוהים שלו. כאשר ה"אדום" נערך לתקיפה, עשוי ה"כחול" לבצע תקיפה מקדימה שתמנע את התקיפה ה"אדומה". כאשר התקיפה של ה"אדום" החלה, יכול ה"כחול" לבצע אמנעה שלה, לרבות ברשתות תקשורת של מדינות שלישיות (לרוב תמימות) שה"אדום" עושה בהן שימוש.

כמו באבטחת סייבר, גם במערכה הגנתית ינסה ה"כחול" להדוף את ה"אדום" מלחדור לתוך הרשת ה"כחולה", וכן ינטר את הרשת ה"כחולה" כדי לזהות תקיפות "אדומות" שחדרו בהצלחה. עם זאת, ניתן לנקוט צעדים אופרטיביים קונקרטיים מול מערכה התקפית מזוהה, שיסייעו לסכלה. צעדים כאלה אינם עומדים לרשותו של מי שרק מאבטח את הרשת ה"כחולה" נגד איומים גנריים. לאחר זיהוי התקפה "אדומה" מוצלחת בתוך הרשת ה"כחולה", יש צורך בכלים לעקירת כלי התקיפה, אך במקרים מסוימים יש גם מקום להערכת פוטנציאל הנזק והחשיפה שבהתקפה, הכלת ההתקפה והותרתה בתוך הרשת ה"כחולה", לעיתים תוך ניהול מבצע הונאה מולה. יש מקרים שבהם נכון להתנהל מול תקיפה מוכרת ומוכלת, יותר מאשר ליצור את המוטיבציה אצל ה"אדום" לבצע תקיפה נוספת, שיתכן שלא תתגלה. במקרים אחרים נכון לבצע תקיפה אוחרת נגד ה"אדום" כדי לשבש את יכולתו

13 "NCSS Good Practice Guide", *European Network and Information Security Agency*, November 2016.

להפיק מודיעין מכלי התקיפה שהחדיר, או לשבש את יכולתו להעביר פקודות לאותו כלי תקיפה.

ניהול מערכה הגנתית כזאת מחייב הישענות על מודיעין המצביע על התוקף, מזהה את היערכותו וכוונותיו ואת צעדיו האופרטיביים, יוצר תמונת מערכה התקפית מתוך מגוון צעדים אופרטיביים התקפיים ומנתח את היכולות הטכנולוגיות ואת כלי התקיפה של התוקף, לרבות זיהוי כלי תקיפה לא מוכרים (קרי, מתקפת אפס ימים – zero-day). בד בבד, יש צורך בכלים לזיהוי תקיפות שחדרו את הרשת ה"כחולה", לאומדן היקף הנזק הפוטנציאלי מהחדירה ולאפשרויות הכלה שלה.

המערכה ההתקפית בסייבר

מערכה התקפית בסייבר מורכבת ממספר התקפות ומבצעי עזר המבוצעים תחת היגיון אסטרטגי אחד. בכך היא שונה מתקיפה נקודתית גרידא, המאפיינת לא אחת את איום הייחוס הפלילי, ההאקטיביסטי או הטרוריסטי.

רשתות ומחשבים של מערכות קריטיות – צבאיות או של תשתיות לאומיות – הן לא אחת מבודדות (air gapped), ומגמה זו צפויה להתעצם. כיום, הרוב המכריע של תקיפות הסייבר מתבצע בסביבת ה־IT, הנגישה ברובה לרשתות תקשורת פתוחות (כמו האינטרנט), אך מבט לעתיד מחייב להתייחס גם להתקפה על מטרות איכותיות ומבודדות. אחד האתגרים העיקריים בהתקפה מסוג זה הוא יצירת נגישות לרשת או למחשב הנתקפים. יצירת נגישות למטרה מבודדת מצריכה, במקרים רבים, מבצע עזר שאינו בתחום הסייבר, כמו שימוש בכוחות מיוחדים, יומינט, כלי טיס או שיט וכדומה. נקודה זו מהווה מבדיל מרכזי בין איום הייחוס המדינתי או המעצמתי, שבו מדינות מסוגלות לבצע מבצע עזר ליצירת נגישות, ובין איום הייחוס התת־מדינתי, שיתקשה במקרים רבים לנהל מבצע עזר ליצירת נגישות.

מבצע עזר ליצירת נגישות מצריך התבוננות על היריב כ"מערכת של מערכות" (system of systems), ניתוח כיווני הנגישות האפשריים, וכמובן הוצאה לפועל של מבצע העזר ליצירת הנגישות. במסגרת זו ניתן לנצל, בין היתר, נקודות תורפה הנובעות מתתי־המערכות המרכיבות את היריב:

- כבכל התקפת סייבר, יש לנתח את הארכיטקטורה של רשת המחשבים של היריב, את נקודות התורפה של התוכנות שברשותו, את נקודות התורפה של ההצפנה, את האפשרויות של אסקלציית פריבילגיות, כשלים של היריב ביישום מדיניות האבטחה שלו וכיוצא באלה.
- כדי ליצור נגישות, יש לבחון את הפריסה הגיאוגרפית של רשת המחשבים של היריב ולבחון דרכי גישה פיזיות אליה. לעיתים ניתן ליצור נגישות באמצעות רשתות סמוכות גיאוגרפית או מערכות מקומיות שהרשת הנתקפת, או מרכיבים בתוכה, תלויים בהן.

- יש לבחון את רשת התקשורת עליה פועלת רשת המחשבים היריבה ולנסות לזהות נקודות תורפה הקיימות בה, כמו למשל מִקטעים שבהם היא הופכת לאלחוטית.
- יש לבחון אם ניתן לתקוף באמצעות שרשרת האספקה של היריב, כלומר את מקורות הרכש של רכיבי החומרה, הקושחה והתוכנה שלו.
- יש למפות ולנצל את האינטראקציה של היריב עם רשתות או ארגונים אחרים, הידידותיים לו, שבהם רמת האבטחה נמוכה יותר.

שילוב לוחמת הסייבר במערכה הקונבנציונלית

מטרת המלחמה היא כפיית רצוננו המדיני על היריב חרף התנגדותו, וזאת בכוח או באמצעות איום בשימוש בכוח, או שלילת ניסיונו של היריב לכפות עלינו את רצונו המדיני, גם זאת בכוח או באמצעות איום בשימוש בכוח. אסטרטגיית המלחמה עשויה להיות הכרעה – פגיעה בכושרו של היריב לפעול נגדנו ביעילות בהקשר הרלוונטי – או התשה – גביית מחיר מלחמה בלתי משתלם ביחס למטרותיה – או אסטרטגיה אחרת הרלוונטית להקשר הייחודי של המלחמה. האסטרטגיה מיושמת באמצעות מערכה או מערכות. מערכה היא סדרה של הפעלות כוח שיש ביניהן קשר רציונלי, פונקציונלי, גיאוגרפי, סינרגטי או אחר. הפעלת כוח בהקשר זה משמעותה שימוש בכלים צבאיים, לרבות הפעלות כוח שאינן קינטיות, כמו איסוף מודיעין, לוחמה אלקטרונית, מבצעי עזר (כמו תדלוק אווירי או מבצעים לתספוק כוחות קרקעיים) וכיוצא באלה. הגדרות אלו הן צבאיות כלליות, ומן הסתם יחולו גם על לוחמת הסייבר.

לוחמת הסייבר עשויה לתרום למערכה הקונבנציונלית בשני אופנים: הראשון, כמאפשרת את פעולתם של אחרים, למשל בשיבוש מערך ההגנה האווירית כך שיקל על מטוס הקרב לבצע את משימתו, או בשיבוש מערך הפיקוד והשליטה של המערך הקרקעי של היריב כך שיקל על כוחות הקרקע ה"כחולים" להילחם בכוחות הקרקע ה"אדומים". יחד עם זאת, מערך הסייבר עצמו עשוי להזדקק לפעולה של אחרים כדי לאפשר את פעולתו שלו, לפחות במקרה של תקיפת סייבר על מערכות מבודדות. האופן השני בו לוחמת הסייבר עשויה לתרום למערכה הקונבנציונלית הוא בפעולה ישירה שלו להשגת תכלית מערכתית או אסטרטגית, כמו למשל גביית מחיר מלחמה מן היריב, שיביא אותו לוותר על ניהול המלחמה ועל מטרותיה המדיניות.

נראה כי דרך ההפעלה האופטימלית של לוחמת הסייבר, לפחות במקרים מסוימים, היא בסינרגיה עם ענפי לחימה אחרים ובמסגרת מערכה משולבת. כך, לדוגמה, במקרים המתאימים ניתן להשמיד או לדכא מערך הגנה אווירית באמצעות שילוב של מטוסי קרב, מסוקי קרב, כוחות מיוחדים, לוחמה אלקטרונית וסייבר.

במקרים אחרים ניתן להתיש ולכפוף את רצונה המדיני של מדינה יריבה באמצעות שילוב של תקיפות אוויריות, סגר ימי ולוחמת סייבר.

קיימת טענה לפיה סוגיית הייחוס (attribution) קוטעת את הרצף הקלאוזביציאני בין מדיניות ובין לוחמה, שהרי אם רשתות מחשבים במדינה מסוימת "סתם" קורסות, והדבר אינו ניתן לייחוס לשחקן מסוים, אותו שחקן יתקשה לממש את מדיניותו באמצעות סייבר. זאת, מאחר והמדינה המותקפת לא תזהה את התוקף, לא תזהה את ההקשר ואת רצונו המדיני של התוקף ממנה, ולכן לא תוכל להיענות ללחץ (כפי שהייתה עשויה להיענות ללחץ המופעל באמצעות סגר ימי גלוי, כדוגמה). טענה זו אינה נכונה, שכן סוגים רבים של לוחמה – מבצעים מיוחדים, צוללות ולעיתים אפילו הפעלת כלי טיס – אפשריים ללא ייחוס טקטי ישיר. מדינה המצויה תחת סגר ימי אינה צריכה להכיר כל צוללת יריבה ולהבין את הנסיבות הטקטיות של כל הטבעת ספינת סחר שלה כדי להבין את הסיטואציה האסטרטגית בכללותה, והיריב עשוי להצליח לכפות את רצונו המדיני עליה באמצעות סגר ימי גם ללא ייחוס של כל אירוע הטבעה יחידני. כך גם בסייבר: אין צורך בפורנזיקה קיברנטית לכל אירוע סייבר כדי שהמדינה המותקפת תבין את הסיטואציה האסטרטגית שיצרה המדינה התוקפת. ברוב המקרים, לפחות אלה של עימות בין־מדינתי, הצד הנתקף אינו זקוק לפורנזיקה קיברנטית שתפוגג את ערפל הייחוס כדי לבצע הערכת מצב מודיעינית קונבנציונלית ולהבין את הסיטואציה האסטרטגית.

שאלה הנשאלת לעיתים קשורה לבידודו של ממד הסייבר משאר הממדים. למשל, האם התקפת סייבר עלולה להביא לתגובה קינטית, או שמא סייבר ייענה רק בסייבר, והאם התקפת סייבר עלולה להוות קאזוס בֶּלי. התשובה המוצעת במאמר זה היא שדין סייבר כדין כל ענף אחר בלוחמה וכי הסייבר אינו ענף מבודד וייחודי. כבכל מקרה אחר, גם כאן על מקבל ההחלטות לבצע הערכת מצב ולקבל החלטה בהתאם לנסיבות. מתקפת סייבר נגד בית חולים שתהרוג מאות אנשים, או נגד תחנת כוח שתחשיך חלקים ניכרים מהמדינה המותקפת, אינה שונה ממתקפה קינטית היוצרת אותו אפקט. הצד המותקף יבצע את הערכת המצב שלו ויגיב בהתאם לאפקט שיצר התוקף. הוא עשוי להגיב בסייבר או באמצעים אחרים, בהתאם לנסיבות וליתרונו היחסי. אם האפקט שיצר התוקף מצדיק זאת, התקפת סייבר עשויה להיות גם קאזוס בלי.

סיכום: אבטחה מול מערכה הגנתית

באנלוגיה לעולם הפיזי, אם נבקר בתחנת כוח נמצא בה, קרוב לוודאי, גדרות, מגדלי שמירה, מצלמות, זרקורים, מספר רכבי אבטחה ותריסר מאבטחים החמושים בנשק קל. השאלה היא נגד איזה איום ייחוס זהו כוח אבטחה ראוי. התשובה היא שאמצעי אבטחה אלה יעילים מול איומי פשיעה או טרור. טענת מאמר זה

היא שבאנלוגיה לכך, זהו שלב ההתפתחות הנוכחי של הסייבר במרבית המדינות, למעט אולי בכמה מעצמות סייבר.

אך מה אם איום הייחוס על אותה תחנת הכח הינו צבאי – למשל, פשיטה של גדוד קומנדו, תקיפה של מפציץ אסטרטגי, או צוללת המשגרת טיל שיוט כשהיא משייטת במרחק מאתיים מייל מתחנת הכוח? במקרה כזה, ברור שאבטחת תחנת הכוח אינה רלוונטית. יתרה מכך, ברוב המקרים מדינה יריבה לא תתקוף "סתם" תחנת כוח בודדת, אלא כחלק ממערכה שיש מאחוריה היגיון מדיני ואסטרטגיה והיא משולבת במבצעים נוספים. למשל, תקיפת תחנת הכוח האמורה עשויה להיות חלק ממערכה רחבה יותר לפגיעה במערך החשמל ובתשתיות לאומיות אחרות במטרה לממש אסטרטגיה של התשה ולכפות מדיניות מסוימת. היא גם עשויה לכלול מבצעים מאפשרים שונים, כמו תקיפת מערך ההגנה האווירית או הימית קודם לתקיפת מערך החשמל. ההתגוננות נגד מערכה התקפית כזאת היא במערכה הגנתית, המתנהלת הרחק מתחנת הכוח האמורה ובעצימות גבוהה הרבה יותר מזו של כוח האבטחה שלה. מערכה כזאת תכלול הפעלה של כל אמצעי העוצמה הלאומית וכל הכלים הצבאיים, כמו, לדוגמה, תקיפה מקדימה על צבא האויב או אמנעתו בדרכו לתקיפת מערך החשמל של המדינה המתגוננת. באנלוגיה, זוהי לוחמת סייבר מדינתית ועצימה.

מרבית הגופים המדינתיים והמסחריים בעולם עוסקים באבטחת סייבר. לוחמת הסייבר, ההגנתית וההתקפית כאחת, נמצאת עדיין בשלבי התפתחות מוקדמים, אך היא זו שתעצב את פני העתיד.