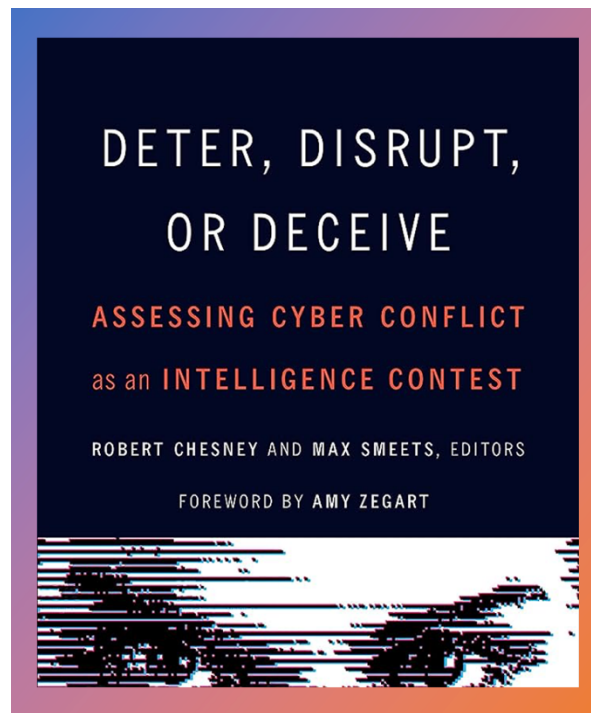


כיצד ראוי להגדיר את הפעילות הגוברת בסייבר: רכיב בתחרות המודיעינית? תחרות אסטרטגית?

סקירה בהתבסס על הספר¹



¹ הסקירה נכתבה על ידי שי יגר-גרנות, עוזר מחקר במכון לחקר המתודולוגיה של המודיעין. תודה לשובל בן יאיר ולד"ר גיל ברעם (עמיתת מחקר במרכז הסייבר של אוניברסיטת ברקלי) על הערותיהן המחכימות.

סקירה זו מתייחסת לשני פרקים² הלקוחים מספר שיצא לאחרונה בכותרת "Deter, Disrupt, Or Deceive: Assessing Cyber Conflict As an Intelligence Contest"³. הספר מחולק לשלושה חלקים:

- דיון תיאורטי - כולל את הפרקים הבאים: רכיבי התחרות המודיעינית / דמותה של תחרות הסייבר האסטרטגית ומקומה של האידאולוגיה / סיכונים נסתרים במענה הצבאי האמריקני להתמודדות עם בעיית סייבר נרחבת / חשאיות באסטרטגיה / חיכוך בסייבר, תחרות מודיעינית, תחרות אסטרטגית ומה שביניהם / ארה"ב והכשרתם של "חוקים" למשחק זה.
- מקרי מבחן מדינתיים – כולל את הפרקים הבאים: סין וגניבת הקניין הרוחני / תפיסתה ההוליסטית של רוסיה ביחס לפעילות בסייבר / ה"יציבה" הבריטית בסייבר.
- שחקנים לא-מדינתיים – כולל את הפרקים הבאים: שחקנים פרטיים והתחרות המודיעינית בהקשר הסייבר / האם יש לקחת ברצינות של שחקנים לא-מדינתיים בתחום הסייבר.

מטרת הסקירה שלפניכם היא להציג את שתי התזות המתחרות ביחס לשאלה האם יש לראות בסייבר כתחרות המודיעינית או כתחרות אסטרטגית.

הפרק הראשון בספר: "The Elements of an Intelligence Contest" שנכתב על ידי Joshua Rovner⁴ נותן רקע היסטורי למה שמכונה ה"תחרות המודיעינית". במסגרת זאת הוא מציג חמישה מרכיבים שמאפיינים את התחרות המודיעינית, הוא דן בשלושה מקרי מבחן⁵ ומנסה לאפיין בקצרה מגמות עכשוויות בכל הקשור ל"תחרות המודיעינית במרחב הסייבר".

² "The Elements of an Intelligence Contest" שנכתב על ידי Joshua Rovner ו-"Cyber Persistence, Intelligence

Contest and Strategic Competition" שנכתב על ידי Michael Fischerkeller ו-Richard Harknett.

³ בעריכת Robert Chesney (דיקאן אוניברסיטת טקסס למשפטים) ו-Max Smeets (עמית מחקר בכיר במרכז ללימודי ביטחון שבמכון הטכנולוגי של ציריך) יוצא בשנת 2023 בהוצאת אוניברסיטת ג'ורג'טאון. [לרשימת הכותבים המלאה](#)

⁴ פרוספור באמריקן יוניברסיטי שבושינגטון – חוקר מודיעין, אסטרטגיה ומדיניות חוץ – [להרחבה](#)

⁵ שלושת מקרי המבחן הנדונים –

(1) אנגליה – ספרד (סוף מאה 16 ותחילת ה-17) מלחמת מודיעין (עם שתי תקריות קינטיות חריגות) שנמשכה כ-20 שנים. הפעילות הייתה של סוכנים (בלטה דמותו של Walsingham הבריטי). אחת הבעיות שאנגליה התמודדה איתן הייתה היעדר מיסוד של המודיעין (היו תלויים באישיותו הייחודית של Walsingham).

מגמות מרכזיות בעשור האחרון (פרק 1)



פעילות נגד שחקנים
מדינתיים ולא-מדינתיים
(ניסיון להשפיע על דעת
הקהל בבחירות 2016
בארה"ב)



גניבת קניין רוחני אך
גם צבאי או מדיני אם
משרת ("ניצול
הזדמנויות")



חתימה להשגת תמונת
מודיעין משופרת
בתחום והפרעה
לשחקניות היריבות

□ הישגות אל מתחת לסף ההסלמה הקינטית

□ בדרך כלל, מתאם בין מצבה הכלכלי של המדינה ליכולותיה
בתחום הסייבר

חמשת המאפיינים העיקריים של ה"תחרות המודיעינית" כפי שרובנר מציגם בפרק:

1. מאמץ לאסוף כמות גדולה יותר ורלוונטית יותר של מידע לגבי היריבים. גופי המודיעין משיגים מידע על היכולות ועל הכוונות של יריבים מדינתיים.
2. המדינות מבקשות לנצל את המידע שהן משיגות לצרכים מעשיים. בפועל רואים שלעתים תכופות יש קושי לתרגם את המידע שמביא המודיעין להישג אסטרטגי.
3. מאמץ הדדי של מדינות לערער את ה"מורל", המוסדות והבריתות של יריביהן (את ה"ביטחון" של היריבה). זוהי דרך להעביר מסרים.

(2) אנגליה - בריה"מ (המאה ה-20, כעשרים שנים) - בריטניה ובריה"מ היו באותה תקופה שתי המעצמות היריבות הגדולות. בתקופה תחרות זו שתי המדינות הקימו את סוכנויות המודיעין שלהן שגלגוליהן קיימים עד היום. התקופה התאפיינה בשימוש בטכנולוגיות חדשות (לא רק יומינט אלא לראשונה סיגינט).

(3) ארה"ב - בריה"מ (תקופת "המלחמה הקרה") - הרחבת השימוש באמצעים אלקטרוניים (אלינט). שת"פ מודיעיני בין מדינות דוברות-אנגלית ובהמשך "בין-גושי". משבר הטילים בקובה כנקודת ציון חשובה בתחרות מודיעינית זו.

4. מאמץ של מדינות לנטרול יכולות מודיעין של יריבים באמצעות נזק (Sabotage). נזק יכול להיות כמובן גם נזק לרשתות ולמידע. האפקט הפסיכולוגי חשוב בהקשר זה לא פחות מן האפקט הפיזי.

5. מאמץ ל"בנייה מוקדמת" או "מיקום מוקדם" (Pre-position) של נכסים לאיסוף מודיעין עתידי בעת משבר.

הפרק החמישי בספר: "Cyber Persistence, Intelligence Contest, and Strategic Competition" שנכתב על ידי Michael Fischerkeller⁶ ו-Richard Harknett⁷ בוחן את שתי התיזות "Cyber Persistence" (חיכוך מתמיד בסייבר) מצד אחד ו"סייבר בחלק מה-Intelligence Contest" (תחרות מודיעינית) מן הצד השני.

Harknett ו-Fischerkeller מסבירים בפרק החמישי שתיזת "החיכוך המתמיד", התופסת את הסייבר כאמצעי שיכול להביא לתוצאות אסטרטגיות, נשענת על הנחה לפיה קישוריות (Interconnectedness) היא מצב קבוע במציאות הנוכחית. מדינות שונות בהכרח מקושרות כל הזמן. וכתוצאה מכך יש כל-הזמן פוטנציאל לניסיונות לפגוע בנכסים שלהן דרך הרשת. זאת אומרת שנכסים כלכליים, מדיניים, חברתיים, או ביטחוניים של המדינה מהווים יעד מתמיד למתקפה פוטנציאלית.

בשל כך, תומכי התיזה גורסים שמצווה (Imperative) על מדינות יריבות לפגוע⁸ באופן-תמידי זו בזו ולנצל את חולשותיו של היריב בתחום זה. התיזה הזו גורסת שמדינה שבחרת שלא לעשות כן אינה יכולה להבטיח את האינטרסים הלאומיים שלה בתחום הסייבר.

שני מונחים מפתח שהמצדדים בתזה זו משתמשים בהם:

1. "סייבר מצטבר" (Cumulative Cyber) - הכוונה במונח היא שמדינות תשאפנה לייצר באמצעות פעולות סייבר התקפיות הישג מצטבר שישרת השגת מטרות אסטרטגיות מבחינתן. כותבי הפרק נותנים את הדוגמה של צפון קוריאה שהצליחה לייצר לעצמה מקור

² חוקר ב-Institute for Defense Analyses - [להרחבה](#)

⁷ פרופסור למדע המדינה ומומחה לתחום הסייבר, אוניברסיטת סינסינטי - [להרחבה](#)

⁸ שתי הדוגמאות המובאות בפרק זה עוסקות בתקיפות סייבר. עם זאת לא נראה שמודבר בפעילות סייבר מסוג תקיפה (CNA) בלבד.

הכנסה חסין מסנקציות לאחר שהצליחה להשיג יותר מ-2 מיליארד דולר כתוצאה מפריצות למערכות פיננסיות בינלאומיות.

2. "עובדה מוגמרת" (Facts Accomplis) – הכוונה היא למעין "ניצול" הזדמנות – פעולה התקפית שהיא מתחת לסף ההסלמה ולכן היריב ישלים עם ביצועה ויימנע מתגובה קינטית. בחזרה לדוגמה הצפון קוריאנית, שאר הקהילה הבינלאומית לא באמת הצליחה לגבות מחיר מצפון קוריאיה על פעילות הסייבר שלה (גניבת הכספים).

מנגד, תזת ה"תחרות המודיעינית" גורסת, במילותיו של לינדזי⁹ ש"רוב מבצעי הסייבר נשענים על הונאה במטרה לאסוף מודיעין או לגנוב קניין רוחני, לייצר השפעה באמצעות תעמולה או חבלה או להגן מפני פעילויות כאלה". תומכי תזה זו סבורים שלא ניתן לדבר על עצמאותן של פעולות הסייבר מבחינה אסטרטגית¹⁰ אלא שהתועלת שלהן נובעת מ"יכולתן לייצר הונאה ולשלב ביוזמות אסטרטגיות רחבות יותר".¹¹

המצדדים בתזת ה"תחרות המודיעינית" סבורים שמבצעי סייבר הם פעמים רבות פועל יוצא של "ניצול הזדמנות" שהמדינה התוקפת מזהה, כאשר ההישגים שלהם אינם יכולים להביא לתוצאות אסטרטגיות. הם מנמקים קביעה זו בשני טעמים (ציר אופקי – ציר אנכי):

1. יש מתאם שלילי בין חשיבות יעד ההונאה לבין סיכויי ההצלחה שלה. כך למשל, סביר שיהיה קשה יותר לפרוץ למערכת של הבנק המרכזי מאשר למערכת המחשוב של בנק קטן ולא-חשוב. הנחה לפיה ככל שהמטרה חשובה יותר כך הסיכוי שההונאה תצליח יקטן.
 2. הונאה מורכבת תדרוש, בדרך כלל, כמה מבצעים או מאמצים מורכבים במקביל – זהו הציר האופקי. למשל, בשביל לפרוץ למערכות הבנק המרכזי כנראה יידרשו מספר גדול בהרבה של מתקפות באותו זמן מאשר המספר הדרוש כדי לפרוץ למערכת המחשוב של הבנק הקטן.
- Harknett ו-Fischerkeller סבורים שתומכי תיזת הסייבר כתחרות מודיעינית אימצו תבחינים לא נכונים בבואם לבדוק את מידת ההשפעה האסטרטגית של מבצעי סייבר, בהיעדר סכסוך צבאי

⁹ Jon R. Lindsay - פרופסור ללימודי סייבר ופרטיות, המכון הטכנולוגי של ג'ורג'יה <https://www.jonrlindsay.com>

¹⁰ לשיטתו של לינדזי, כדי שאפשר יהיה לדבר עליהן במונחים של "אסטרטגיות" הן צריכות למלא אחר משימות הקשורות לעוצמה צבאית (TERRESTRIAL FORCE) – עמ' 114.

¹¹ עמוד 111

מזוין¹². בנוסף, נראה שהם שוללים את מונח ה"הונאה", שמאפיין את תומכי תזת התחרות המודיעינית ותחת זאת הם סבורים שהמונח "חיכוך בסייבר" מתאר טוב יותר את מה שהמדינות מבקשות להשיג. כמו כן, הכותבים סבורים שמדינות שיעברו לבצע קמפיינים נגד מטרות פשוטות יחסית שהינן בעלות ערך מדיני גבוה¹³ יכולות לעבור ממבצעים יחידים שמייצרים רווח מוגבל לקמפיינים משמעותיים יותר שיוכלו לייצר רווח מצטבר ובאופן פוטנציאלי גם לייצר באופן עצמאי תוצאות אסטרטגיות.

סיכום ומסקנות

נראה שהכותבים מבקשים לייצר דיוק מושגי בכל הנוגע לפעילות, שללא ספק הופכת למשמעותית יותר ויותר במרחב הסייבר ההתקפי בשנים האחרונות. להתרשמותי, המחלוקת בין תומכי שתי התיזות מתוחמת ביותר והיא מתמקדת בשאלה הבאה: האם יש לתפוס את מבצעי הסייבר כ"מבצעים אסטרטגיים" או כ"מבצעי מודיעין"¹⁴.

ביחס למשמעויות הפרקטיות הנובעות מהתשובה הניתנת על שאלה זו ניתן לחשוב על:

1. משאבים - תפיסה שהסייבר לבדו יכול לייצר תוצאות אסטרטגיות¹⁵ תגרור כנראה השקעה רבה יותר בתשתיות הסייבר (התקפי כמו גם הגנתי). עם זאת גם תומכי גישת ה"תחרות" סבורים שראוי להשקיע ביכולות סייבר – כהתפתחות "טבעית" של התחרות המודיעינית הקלאסית.

2. בחירת מטרות - נראה בהכללה גסה שתומכי גישת ה"חיכוך" יעדיפו לבחור מטרות "מורכבות" יותר (ומכאן גם חשובות יותר לביטחון הלאומי) ואילו תומכי גישת ה"תחרות" יעדיפו לבחור במטרות "פשוטות" יותר שסיכויי ההצלחה לפגוע בהן גדולים יותר.

¹² עמוד 115 – המונח המדויק, core variables and concepts

¹³ כך למשל פריצות הסייבר הצפ"קיות לתשתיות הבנקאות הבינלאומיות.

¹⁴ עמוד 109 בספר.

¹⁵ נראה שהם מגדירים פגיעה באחד מארבעת התחומים הבאים כפגיעה "אסטרטגית" (ומכאן גם תוצאה אסטרטגית עבור הפוגעת): כלכלה, פוליטיקה, חברה וצבא – עמ' 111.

3. נכונות לנטילת סיכונים – קשה להצביע על מסקנה ברורה משום שראוי לנתח את השאלה הזו בהקשר למדינה שדנים בה¹⁶. הפעלתנות הרבה יחסית של צפ"ק ואיראן במרחב הסייבר עשויה אולי ללמד שמדינות הנתונות ב"תודעת מצור" נוטות יותר ליטול סיכונים גם בתחום הסייבר.

בנוסף לכך, מעניין לראות כיצד ההתפתחות הטכנולוגית המואצת שינתה את ההגדרה הקלאסית של "התחרות המודיעינית". כך, רובנר מסביר שאחד המאפיינים של התחרות המודיעינית הוא יצירת נזק ליריב.¹⁷ גם בפרק מספר חמש נטען שהסייבר מייצר הזדמנויות לסוכנויות המודיעין למבצעי "הטעייה"¹⁸ ושיתרון נוסף שלו הוא שיחסית קל לפעול באמצעותו באופן חשאי. כמו כן, הקביעה של לינדזי (תיזת ה"תחרות") שבשביל לתפוס דבר מה כ"אסטרטגי" יש לקשר לעוצמה הצבאית מבטאת ראייה צרה למדי על מונח זה. אם ניקח למשל את הדוגמה של השפעה על דעת הקהל של אזרחי מדינה מסוימת. לכאורה זהו נושא שאינו בעל משמעות צבאית (לפחות לא באופן ישיר) אך זהו בהחלט כיוון פעולה בעל משמעויות אסטרטגיות משום שהשפעה כזו יכולה לערער את האמון של האזרחים במוסדות המדינה.

16 ראוי להכיר את אסטרטגיית הסייבר של המדינה הנדונה, אך לא להתמקד בה בלבד (לעתים יש פער כמובן בין האסטרטגיה לבין היישום). להרחבה ראו פרק 7 בספר זה ("Deter, Disrupt, Or Deceive: Assessing Cyber Conflict As an Intelligence Contest") שעוסק באסטרטגיית הסייבר של סין.

17 במציאות שבה תשתיות חיוניות (מפעלי התפלה, מערך הרכבות) תלויות לחלוטין במערכות מחשב.
18 אלה פעמים רבות אפילו לא דורשים נוכחות פיזית של מרגלים במדינה היריבה ואשר מסוגלים להשיג את האפקט הרצוי (העברת מסר? הרתעה? גניבת מידע?)