# 'דילמת דוקו':
# הנחת העמימות והשאיפה חסרת התוחלת למלחמת סייבר סטרילית

**מת'יו קרוסטון**

הוויכוח סביב החלה או אי־החלה של הדין הבינלאומי בכל הנוגע למלחמת סייבר וסביב הצורך באמנת סייבר בינלאומית עשוי להתגלות כבלתי־רלוונטי. שני המחנות, התומכים והמתנגדים, מתווכחים האם יש צורך להחיל את דיני הלחימה, גם על תחום הסייבר, במקרה של מלחמת סייבר. במנותק מהדעה האם חוקי הלחימה חלים אם לאו, או האם יש לקדם אמנת סייבר בינלאומית, או שמא אמנה כזו תהיה חסרת משמעות, יש צורך אחד שנותר על כנו: השאיפה לחוקים שיפקחו על התנהלות מלחמת סייבר. אולם כל הצדדים מחמיצים את העובדה שמבנה תחום הסייבר מונע אסטרטגיה ש"תופסת טרמפ" על נורמות קונוונציונליות של מלחמה. נורמות אלה אפקטיביות בשל היכולת להבחין בין המגזר האזרחי למגזר הצבאי. לא ניתן ליישם הבחנה כזו בתחום הסייבר, בהיותו מאופיין במיזוג המשתתפים, המתקנים והיעדים לכדי ישות אחת, המשלבת באופן חסר־תקנה בין מוסדות אזרחיים לצבאיים. הסבר חשוב זה חסר ביחס לשאלה, מדוע מאמץ כלל־עולמי לשפר ולהבהיר נורמות סייבר נותר בלתי־מאוזן ובלתי־הולם.

וכך נוצרת 'דילמת דוקו': כל עוד המוקד הוא גיבוש יעדים לגיטימיים והצבת מגבלות על פעולה מורשית, ארצות־הברית ובעלות־בריתה חושפות את עצמן לפגיעויות, ובמקביל משקיעות מאמץ עקר שאינו מוביל לבקרת סייבר משופרת. בדיוק כמו הווירוס דוקו (Duqu) שכיכב בדיון הכלל־עולמי ב־2011, מתקפות הסייבר כיום יכולות להתבצע לצורך איסוף מידע **או** כפוטנציאל למתקפה פיזית; הן יכולות להיות יוזמה ממשלתית אך להתבצע דרך נכסים מסחריים חשובים; הן יכולת לכוון ליעדים מדיניים/צבאיים **ובמקביל** להסתייע בחדירה למערכות אזרחיות. יצירת כללי סייבר בדומה לנורמות קונוונציונליות היא לפיכך חסרת תוחלת, שכן כללים אלה אינם ניתנים לאכיפה (כפי שיידון בהמשך). משום כך

ד"ר מת'יו קרוסטון (Matthew Crosston), אוניברסיטת Bellevue, ארצות־הברית

המאמצים הנוכחיים פשוט כובלים את ידי המדינות שומרות החוק. המסקנה היא שיש להקדיש מאמץ רב יותר ליצירת אסטרטגיה מונעת, שמקבלת את בעיית העמימות האזרחית/צבאית כמציאות קיימת. הנטייה של חוקרים וקובעי מדיניות לחתור ללוחמת סייבר 'סטרילית' באמצעות הגבלת הנזק שייגרם על ידי סיווג ברור של המטרה, פירושה שאסטרטגיית הסייבר סובלת מהיעדר כוח הרתעה אמיתי. בקצרה, מומחים להגנת סייבר רק מעצימים את הדילמה.

## חוסר ההשפעה של הדין הבינלאומי

כפי שציין מכון המחקר East-West ב־2011, "קיים צורך דחוף לשיתוף פעולה בינלאומי בסוגיות אסטרטגיות אלה. אם ניכשל במשימה זו, האיום על היציבות הכלל־עולמית יהיה כאיומה של פצצה גרעינית".[1] נורמות בינלאומיות שגובשו באמנות האג וז'נבה הציבו קווי הגנה ברורים לאוכלוסיות אזרחיות בזמן שהמדינות מעורבות במלחמה. כבוד לחיי אזרחים והגנה עליהם נתפסים כיום כמקודשים, ללא קשר לצורה שבה מנוהלת המלחמה, ומכאן הציפייה שמרחב הסייבר יהיה כפוף לפיקוחן של הנורמות הקונוונציונליות.

היו שכינו סוגיה זו אחד מהקרבות הגיאופוליטיים החשובים שמתנהלים כיום, והרחיקו עד כדי האמירה שזהו ה'גראונד זירו' של הדיפלומטיה העולמית, של עבודת הביטחון הלאומי ושל המודיעין.[2] אכן, האופטימיים ביותר רוצים לראות הסכמים מרצון שמטילים מגבלות על פיתוח יכולות הסייבר, ולכאורה משפרים את ההתנהגות במרחב הסייבר. עם זאת, יש מי שהכירו בכך שקיימות סכנות פוטנציאליות בניסיון להגיע להישג כזה. סטיוארט בייקר (Stewart Baker), לשעבר יועץ כללי בסוכנות הביטחון הלאומי האמריקנית (NSA) ועוזר שר לענייני מדיניות במשרד לביטחון המולדת (DHS) בממשל הנשיא ג'ורג' וו. בוש, ניסח את החשש המובן מאליו: ארצות־הברית ובעלות־בריתה יצייתו לכללים, ובו־בזמן, אף לא אחד מיריביה יעשה כן.[3]

אולם הבעיה עלולה להיות אפילו קשה יותר מאשר אי־ציות לחוק: מרבית הרשתות הצבאיות שיכולות ליזום או לבצע מתקפת סייבר עובדות עם אינספור רשתות אזרחיות ותלויות בהן. נוסף לכך, רבים מהגורמים שהם חלק מהתכנון, היוזמה והפריסה של מתקפות סייבר אינם בהכרח גורמים צבאיים רשמיים, אלא עובדים אזרחיים של סוכנויות ממשלתיות. במילים אחרות, עולם לוחמת הסייבר אינו עולם של סיווג ברור אלא של עמימות מכוונת. למעשה, מגמות עתידיות מצביעות על כך שמיזוג זה רק יעמיק ויתחזק עם הזמן.

'הנחת עמימות' זו זכתה עד כה להתעלמות יחסית במהלך הוויכוחים השונים שהתקיימו סביב נושא הסייבר. במקום זאת, ויכוחים אלה התמקדו בשאלה עד כמה משוחררים או נוקשים, רשמיים או לא־רשמיים, בינלאומיים או מקומיים אמורים

להיות אותם קודים של מגבלות. רבים מהקודים המוצעים נועדו להגביל התנהלות בסייבר כך שתושג הגנה על בנקים, אנרגיה ורשתות אחרות של תשתית קריטית, 'למעט כאשר מדינות מעורבות במלחמה'.[4] בעיית העמימות, לעומת זאת, גורמת מבוכה למדינות: כיצד ניתן למתוח קו מפריד בין אזרחים לבין הצבא? הדילמה הגדולה ביותר, אפוא, היא לא הצלחה בזיהוי האחראי למתקפה (ייחוס נכון), אלא העמימות המובנית והמכוונת שמאפיינת את התשתית הקריטית המשמשת לפיתוח יכולות הסייבר של המדינה.

רבים מדיוני הסייבר העכשוויים לוקים באופן שבו הם מבקשים להקיש במשתמע מהלוחמה הקונוונציונלית ללוחמת הסייבר, ולראות במתקפות סייבר שוות־ערך למתקפות חמושות. אך כדי לעשות זאת, הדיון צריך לפנות להגדרות ולפרמטרים המשפטיים: מתי לוחמת סייבר עונה להגדרה של שימוש בכוח חמוש או מהלך רשמי של מלחמה? אילו פעולות ייחשבו כפשעי מלחמה? מה מידת הנזק המצדיקה תגובת נקם?[5] שאלות אלה קשות הרבה יותר למענה בזירת הסייבר בשל הסיוט הלוגיסטי שיוצרת הנחת העמימות. עובדה זו אינה מודגשת במחקרים ואינה זוכה למענה באסטרטגיה.

במקום זאת, מרבית השאלות עוסקות בהשוואה של מידת סכנת החיים, הערכות הנזק ובעיית הייחוס שהוזכרה לעיל. במידה מסוימת, כל הבעיות הללו נותרות בצל בעיית העמימות הצבאית/אזרחית. חוסר היכולת ליצור הפרדה זו פירושו שיכולת ההרס יכולה להיות קטלנית יותר, משום שהיא יכולה להתרחב מעבר לנפגעים צבאיים, הנזק יכול להיות הרסני יותר אם יקיף יותר מאשר מתקנים צבאיים, והייחוס עשוי אף להיות לא־רלוונטי כלל: השאלה **מי** עומד מאחורי המתקפה אינה הפתרון לבעיה, כל עוד ה**איך** שמאחורי ה**מי** משולב באופן שלא ניתן להפרדה לכדי ישות אחת של המגזר הממשלתי, הצבאי והאזרחי. במילים אחרות, רבים מניחים שההבנה **מי ומי** במלחמת סייבר תפתור את מרבית הבעיות המשפטיות, אך הנחת העמימות מציבה אזהרה: בסייבר, **מי** אף פעם אינו מובחן בקלות מ**איך** או חשוב יותר ממנו.

## התסכול שבהצבת תנאים

חלק מהקושי להחיל את הדין הבינלאומי ביעילות על מרחב הסייבר קשור בכישלון נושן לתרגם מונחים ופרמטרים חיוניים לדבר שישפיע על התחום. ההתקדמות לפתרון בעיה זו הייתה מוגבלת ביותר, ואכן, די בהצצה חטופה בספרות של העשור האחרון על מנת להיווכח שמלחמת סייבר אינה חופפת בדיוק למסגרות המשפטיות הקיימות בנוגע למלחמה ולשימוש בכוח.[6] למרות מציאות זו, נעשו ניסיונות נמרצים להתגבר ביעילות על קשיים טרמינולוגיים ודוקטרינריים אלה,

ולהחיל אותם על זירת הסייבר. מאמר זה טוען שניתן לייחס את חוסר ההצלחה למיזוג הצבאי/אזרחי הטבוע בהנחת העמימות.

השאיפה לתנאים, לפרמטרים, להגדרות, לחוקים ולהסכמים מפורשים מבוססת בעיקר על החשש שכישלון ליצור מצבים מפורשים כאלה יותיר את מלחמת הסייבר מחוץ לגבולות המלחמה הקונוונציונלית. המסקנות נחשבות חמורות: תשתית אזרחית קריטית תהיה יעד, כמו גם צרכים בסיסיים כגון חקלאות, מזון, מים, מערכת הבריאות הציבורית, שירותי חירום, טלקומוניקציה, אנרגיה, בנקאות ופיננסים וכן הלאה. עם זאת, הנחת העמימות מבהירה את חוסר התכלית של היעד: מרבית יכולות הסייבר של מדינה, אם לא כולן, מנצלות תשתית אזרחית קריטית שמספקת גם פונקציות אזרחיות חשובות רבות, ותלויות בה. עד היום לא יצרה שום מדינה יכולות סייבר שהן נפרדות ומובחנות במלואן מרשתות ומתשתיות אזרחיות. במילים אחרות, פגיעה ביעדים "צבאיים" פירושה, למעשה, פגיעה ביעדים אזרחיים. נראה שהספרות המחקרית העכשווית עוקפת עובדה זו, וכתוצאה מכך עוסקת בחידה מדומה: ניסיון לכפות תשובה מדויקת תיאורטית על מציאות עם עמימות אמפירית. הוכחה נוספת להתעלמות זו היא הדרישה שחוקי מלחמת הסייבר **יאסרו** למעשה על פגיעה ביעדים שהם תשתית אזרחית טהורה – דרישה המציינת שגורמי סייבר חייבים לנסות לכבד את אמנות ז'נבה בדיוק כמו גורמים קונוונציונליים.[7] אולם במלחמת סייבר, תשתית אזרחית טהורה היא קטגוריה הדומה לפחיתת תשואה. לנוכח ההעצמה וההעמקה של המיזוג הצבאי והאזרחי, תשתית אזרחית טהורה תתגלה יותר כמיתוס מאשר כמציאות.

הכישלון לתת מענה למציאות מבנית זו דומה להדגשת יתר של הגורם הפועל (agency). ג'יימס לואיס (James Lewis) מהמרכז ללימודים אסטרטגיים ובינלאומיים (CSIS) מדגיש כיצד יכולה מדינה להפחית את הסיכונים לכל הצדדים באמצעות אכיפת סטנדרטים משותפים, בדומה למעבר מ'המערב הפרוע' לשלטון החוק.[8] יוג'ין ספאפורד (Eugene Spafford) מסכים עמו, כשהוא מציין כי אבטחת סייבר היא תהליך, לא טלאי, המחייב השקעה מתמדת לטווח הארוך לצד תיקון מהיר, שכן בלעדיו מדינות ימצאו עצמן מיישמות מאוחר מדי את הפתרונות לבעיות.[9] השניים נמנים עם השמות המכובדים והמבריקים ביותר בתחום חקר הסייבר. האזהרות שלהם אינן בלתי־רלוונטיות, אך הדגש על המדינה כסוכן פעולה, ובמקביל הפשל להכיר בהשפעה ובחשיבות של מבנה הסייבר הטבוע, מותירים פער רגיש בחשיבה האסטרטגית בנושא הסייבר. ההכרה בכך היא מכרעת, שכן מדינות מעמיקות במכוון את העמימות לצורכי יתרון אסטרטגי ויעילות כלכלית. לכן, האסטרטגיה אינה אמורה להתמקד בשאלה כיצד לאכוף הפרדה אזרחית/צבאית, אלא עליה לקבל את הנחת העמימות כמציאות לוגיסטית שיש להסתמך עליה.

כדי לקבל אישור אמפירי על חוסר התועלת בניסיון לתת מענה לבעיות אלה, אין צורך להרחיק מעבר לצבא ארצות־הברית במהלך שש השנים האחרונות: גנרל אלכסנדר (Alexander) ממפקדת הסייבר האמריקנית ציין שהושגה התקדמות, אך הסיכונים עדיין צומחים במהירות;[10] סגן־אדמירל מייקל רוג'רס (Michael Rogers), מפקד מפקדת הסייבר של הצי האמריקני, הודה בפני הקונגרס שלא הושג כל הסכם בין המפקדות השונות שיסדיר את דיני לוחמת הסייבר, אך הוא מקווה לראות התפתחויות חיוביות 'בשלב כלשהו בטווח הקרוב';[11] ואפילו הפנטגון הפיק דוח סייבר, שבסופו של דבר טען כי דיני הלחימה אכן חלים על מרחב הסייבר כשם שהם חלים על לוחמה מסורתית, אולם הודה שהמונחים הבסיסיים של 'פעולת מלחמה' ו'שימוש בכוח' עדיין **לוקים בהגדרתם** בתחום הסייבר.[12]

## מלחמות מרות והליכה על חבל דק: דיון צבאי על פרמטרים של סייבר

בדיוק כמו חוקרים, קובעי מדיניות ודיפלומטים, גם הצבא מחויב בקביעות לגבש כללים נוקשים של התנהלות בסייבר, בדומה לכללי מלחמה קונוונציונלית.[13] כבר שנים אחדות תלוי ועומד תיקון לכללים הקיימים להתנהלות בעולם הסייבר.[14] נראה כי בעוד הצבא קיווה שקהילות החוקרים והדיפלומטים יוכלו לסייע, קהילות אלה עצמן קיוו לראות את הצבא מתווה את הדרך. חוסר הבהירות לגבי הנשיאה באחריות הוא עדות לבלבול הנוצר כל עוד הנחת העמימות הנוגעת למיזוג הצבאי/אזרחי אינה מטופלת.

גנרל אלכסנדר הצהיר כי בעת ניהול דיונים על כללי העימות בפעולות סייבר, ניסתה ארצות־הברית לעשות את הדבר הנכון.[15] אולם דיונים אלה נעו בין עמדות שרובן ככולן התעלמו מהעמימות המבנית העיקרית של תחום הסייבר. כתוצאה מכך, הצבא בזבז שש שנים בהבטחות להתקדמות שעתידה הייתה להגיע ולא התגשמה. אפילו הדוח הרשמי של הפנטגון תואר כ'חומק' מסדרה של שאלות מהותיות ובסיסיות חשובות, לרבות הצורך להגדיר מונחים כה בסיסיים כמו 'מלחמה', 'כוחות', ו'תגובה הולמת'.[16] נקודה זו מוזכרת לא על מנת ללעוג לצבא: לנוכח חוסר האונים של כל הצדדים הנוגעים בדבר בטיפול בהנחת העמימות, לצבא לא היה סיכוי רב להתקדם באופן מהותי במשימתו, ולהגדיר במדויק את הפרמטרים של פעולת סייבר.

כיצד, למשל, ניתן לצפות מ־USCYBERCOM לחבר את כל הנקודות, ולהיות הפוסק המתאים המכריע איזה אירוע הוא ראוי לפעולה, כאשר הוא עצמו מודה בקושי שיש לו אפילו לנסח מי בדיוק מרכיב את קבוצת לוחמי הסייבר שפועלת ומגִנה על רשתות הבית?[17] אם הסוגיות הנדונות לא היו כה חמורות ולא כל כך

מרחיקות לכת בנוגע לעתיד לוחמת הסייבר, זה היה כמעט משעשע. רק לאחרונה נראה היה שגופי הצבא הרלוונטיים מתחילים להפנים את הבעיות שנדונות כאן:

> למרות שננקטו כמה צעדים ראשונים ראויים לציון בהקמת מערך בינלאומי של נורמות סייבר – כפי שניכר בגופים דוגמת Convention on Cybercrime – כל מסגרת כלל־עולמית המפקחת על פעולות תגובה צבאית במרחב הסייבר צפויה לממש זאת בקצב איטי. אחרי הכול, כיצד ניתן להסב את כללי המלחמה, המבוססים על נוכחות פיזית של לוחמים וכלי נשק וטריטוריות ריבוניות, לעולם שבו ניתן לשגר באלפיות השנייה 'חיילים' ממספר רב של מדינות?[18]

הציטוט שלעיל תוחם לפחות את הדיון סביב אי־ההתאמה המובנית בין האופן שבו צפויה להתנהל מלחמה במרחב הסייבר, לבין האופן שבו התנהלו המלחמות בעבר. אולם עדיין, ציטוט זה מדגיש גורם פעולה על פני מבנה, ועוסק בהקמת מערך בינלאומי של נורמות סייבר, בעיקר על מנת לסמן רשמית את החלוקה בין נכסים צבאיים לאזרחיים, וכדי למתן פעולה שכבר מתבצעת. גישה זו יכולה להסביר מדוע מסמכי אסטרטגיה רשמיים מסיימים את דרכם כאוסף של אמירות שטחיות על האופן שבו ארצות־הברית מתכוונת להגן על עצמה. ראו לדוגמה את אסטרטגיית משרד ההגנה האמריקני לפעולה במרחב הסייבר, שפורסמה במחצית שנת 2011 :

> יוזמה אסטרטגית 1: יש להתייחס למרחב הסייבר כאל תחום מבצעי שיש לארגן, לאמן ולצייד, כך שמשרד ההגנה האמריקני יוכל לנצל את פוטנציאל מרחב הסייבר במלואו.
>
> יוזמה אסטרטגית 2: יש להפעיל תפיסות חדשות לתפעול הגנה, במטרה להגן על רשתות ומערכות מקומיות.
>
> יוזמה אסטרטגית 3: יש לחבור לשותפים נוספים במחלקות ובסוכנויות ממשלתיות וכן במגזר הפרטי, על מנת לבנות אסטרטגיית אבטחת סייבר כלל־ממשלתית.
>
> יוזמה אסטרטגית 4: יש לכונן קשרים איתנים עם בעלות־ברית של ארצות־הברית ועם שותפים בינלאומיים, על מנת לחזק אבטחת סייבר משותפת.
>
> יוזמה אסטרטגית 5: יש למנף את כושר ההמצאה של המדינה באמצעות כוח אדם ייחודי לסייבר וחדשנות טכנולוגית מהירה.

יש לנצל בצורה מלאה; להפעיל תפיסות חדשות; לחבור לשותפים; לכונן קשרים איתנים; למנף כושר המצאה – כל אלה סיסמאות נפלאות, אולם שום סיסמה אינה מלווה בחשיבה אסטרטגית חדשה ומפורשת שתוכל לגבש את היוזמות האמורות. כל ניסיון לאמץ אסטרטגיה קונוונציונלית חלקית ולאחר מכן לדחוק אליה את תחום הסייבר היה ויישאר פרויקט הנושא פירות דלים בלבד.

## התמודדות עם העמימות: חשיבה אסטרטגית על המיזוג האזרחי/צבאי בסייבר

הצורך בגישה אסטרטגית חדשה מומחש בצורה הטובה ביותר בטיעונים של שניים מההוגים האסטרטגיים המכובדים ביותר, האחד צבאי והשני משפטי, שבמקרה גם מייצגים שתי עמדות מנוגדות בוויכוח הסייבר בנוגע לדיני לחימה (LOAC). שני הצדדים מתעלמים מהבעיה של מיזוג מבני צבאי/אזרחי בסייבר. דנלאפ (Dunlap) אמנם מסכים לצורך בשיפור, אך מאמין שעיקרי דיני הלחימה מספיקים על מנת לתת מענה לסוגיות החשובות ביותר של מלחמת סייבר.[19] נראה שבעיית ההבחנה בין מטרות צבאיות לגיטימיות לבין מטרות אזרחיות אינה מטרידה את דנלאפ כשהוא דן בהשפעה של החלת דיני הלחימה:

> דיני הלחימה מתירים 'פגיעות מקריות' באזרחים ובאובייקטים אזרחיים, כל עוד 'לא מדובר בהיקף רחב ביחס ליתרון הצבאי הישיר והממשי הצפוי'. בקביעה מהן פגיעות מקריות, נדרשים אסטרטגים של סייבר להביא בחשבון פגיעות שניתן להעריך במידה סבירה כי ייגרמו ישירות מהמתקפה. הערכה של השפעות 'מהדהדות' מדרגה שנייה או שלישית עשויה להיות שיקול מדיני נבון, אולם לא נראה שדיני הלחימה מחייבים כרגע ניתוח מתקדם מעין זה.[20]

הבחנה זו שעושה דנלאפ חשובה למדי לנוכח האקלים האינטלקטואלי הנוכחי: הוא הכניס לוויכוח את השימוש החיוני למדי בריאליזם, בכך שהוא מזכיר לאנשים שדיני הלחימה מעולם לא היו אסטרטגיה נטולת פגמים, שהגנה בצורה מושלמת על אזרחים ועל אובייקטים אזרחיים. אולם הבעיה שעולה מדבריו היא שחששותיו בנוגע להבחנה בין הצבאי לאזרחי מוטעים.

טיעונים אלה, שתומכים בדיני הלחימה, נבנו ביעילות סביב העובדה שמלחמת סייבר אינה אמורה להיות מושלמת בכל הקשור להגנה על אזרחים, כיוון שגם דיני הלחימה אינם עומדים בכך. אך טיעונים אלה מתייחסים כאל נתון לכך שמתווה כזה **אפשרי** בדרך כלל. אין זה סביר שמלחמת הסייבר תצליח בעתיד ליצור יכולת כזו, כיוון שהוכח זה כבר עד כמה הפונקציות הקריטיות, הנכסים, ספקי השירותים ושרשרות האספקה מסתמכים כולם בצורה ניכרת על רשתות ותעבורה אזרחיות.[21] בשל כך, אסטרטגיה חדשה צריכה להיות כזו שמונעת את השימוש בנשק סייבר בכללותו, משום שבעצם הפעלתו טמונה סבירות גבוהה לכך שייגרמו **בפועל** סיכון, נזק או אבדות לאזרחים. 'סטריליזציה' של השפעת נשק סייבר שכבר נעשה בו שימוש – באמצעות ניסיון לחייב בחירת מטרות – לא תצלח.

מחנה המתנגדים לדיני הלחימה שוגה באותה שגיאה כשהוא דן בשאלה, מדוע דיני הלחימה אינם יכולים להבהיר את מלחמת הסייבר:

> דיני הלחימה נועדו להבטיח שהצדדים בעימות יראו כמטרות את הלוחמים ולא את האזרחים, ואם אזרחים הופכים למטרות, עליהם להבטיח שגורמים כאלה

> יאבדו את מעמדם המוגן. כדי לקבוע האם מתקפות סייבר מבחינות כהלכה בין יעדים צבאיים לאזרחיים, נדרשת הבנה של ההבחנה.[22]

המחנה המתנגד נכשל בכך שהוא מאמין כי הבחנה כזו אפשרית בסייבר. הוא אינו רואה את ההשפעה האסטרטגית של הנחת העמימות, ובמקום זאת מתמקד בליקויים של דיני הלחימה ושאר הסכמים ונורמות עכשוויים. בקצרה, ההנחה שלו היא 'צרו חוקים טובים יותר ועולם הסייבר יציית להם'. אי לכך, מחנה זה רחוק אפילו יותר ממציאות הסייבר. בעיקרון, המחנה המתנגד נוקט גישה ליברלית יותר ביחס לעימות, משום שהיעד הסופי שלו הוא יצירת אווירה של אמון שיכולה למזער רמות גבוהות של אלימות ובגידה.[23] גישה זו מנוגדת למבנה הנוכחי והעתידי של מלחמת הסייבר אפילו יותר מזו של המחנה השני. שני המחנות מאמינים ביכולת לנטר, לפקח ולהגביל את מלחמת הסייבר לאחר תחילתה, כפי שנעשה לרוב במלחמה קונוונציונלית. זוהי תקוות שווא. הדרך הטובה ביותר להשיג יכולת לנטר, לפקח ולהגביל פעולת סייבר היא באמצעות אסטרטגיה שתחדיר פחד מראש, ולפיכך תגרום זהירות והיסוס. אסטרטגיות סייבר נוכחיות שמכוונות לאמון, להבחנה בין מטרות ולמזעור השפעה על מי שאינם לוחמים פשוט מתעלמות ללא הסבר מהאופן שבו מלחמת הסייבר מאורגנת, נבנית ומבוצעת.

הגישה הליברלית שולטת גם בקהילה המשפטית, ונשענת עליה רבות לצורך חשיבה אסטרטגית שנועדה לשלב פרויקטים משפטיים בתחום הסייבר:

> [פתרון אפקטיבי לאתגר הכלל־עולמי של מתקפות סייבר] לא יושג בידי מדינות יחידות הפועלות לבדן. הוא מחייב שיתוף פעולה כלל־עולמי. לפיכך פירטנו את מרכיבי המפתח של אמנת סייבר, כלומר, קיבצנו חוקים להגדרות ברורות של לוחמת סייבר ומתקפת סייבר, והצגנו קווים מנחים לשיתוף פעולה בינלאומי לאיסוף הוכחות ולתביעות פליליות – אשר יספקו פתרון מקיף וארוך־טווח לאיום הגובר של מתקפות סייבר.[24]

הסקירה שלעיל מציגה צד נוסף המתמקד במיתון הסיכונים ובהגבלת הנזק בתחום הסייבר **לאחר מעשה**. ללא קשר לעמדה פילוסופית, סדר־יום פוליטי או תבונה תיאורטית, דומה שכל צד שבוחן את בעיית הפרמטרים וההגדרות בתחום הסייבר שולל שיקולים של אסטרטגיה מונעת, המבוססת על הרתעה ועל שכנוע להימנע מפעולה. גנרל אלכסנדר, ראש מפקדת הסייבר האמריקנית, ציין את הצורך לסלול את נתיבי הדרך שבה יוכלו או לא יוכלו ממשלות ללכת, וכי סלילת הנתיבים היא השלב החיוני הראשון במתן מענה לאתגר של מתקפות סייבר.[25] המשותף לכל המחנות שנבחנו כאן הוא הנטייה לשלם מס־שפתיים לאסטרטגיה, ולאחר מכן להתמקד באופן בלעדי ב**פעולות לאחר מעשה** כדי להשיג התקדמות. אם ההתמקדות תמשיך להיות על פעולת הסוכן ולא על ליקוי מבני, ההתקדמות לא רק תואט, היא לא תתקיים.

ישנם ניצני התחלה בספרות, המעידים על ניסיון ראשוני להגדיר שינוי תודעתי זה ואת חשיבותו האסטרטגית. הם מתמקדים באופן שבו יש לפעול כדי שהיעד של מעצמות גדולות לא יהיה תקוות השווא לפתח מערכת הגנה מושלמת של הרתעת סייבר, אלא היכולת להחדיר בהדרגה הרתעה המבוססת על פחד הדדי מאיום של מתקפה. מעמדה של ארצות־הברית טוב יותר הודות להתרחבותה למדיניות פתוחה ושקופה, שחותרת ליצור הרתעה המבוססת על יעילות יכולות מתקפת הסייבר שלה.[26] נעשה גם ניסיון ראשוני, אם כי בקנה־מידה קטן אף יותר, להגדיר כיצד פועל כוח סייבר מרתיע למניעה, או כיצד נראית אסטרטגיה כזו. השאיפה היא שאסטרטגיית סייבר גלויה כזו תיצור אמינות לנשק וירטואלי ככזה שמפעיל השפעה משבשת מתגלגלת כה חזקה, עד כדי שלילת השימוש בו. המפתח יהיה בביסוס חשש סביר אצל היריב.

עקב הגילויים האחרונים על תולעת 'סטקסנט' ועל יעילות הווירוסים 'דוקו' **(Duqu)** ו'פליים' **(Flame)** – שסביר מאוד להניח כי התקדמו מעבר ליכולות סטקסנט – נשק סייבר צובר במהירות מוניטין של הפחדה, ולפיכך הרתעה באמצעות אסטרטגיית סייבר גלויה כבר אינה פנטזיה בלבד. זהו טיעון מאזן חשוב לפיתוח אסטרטגיה מקיפה ומלאה, שתאפשר עוצמת סייבר אמריקנית גלויה וסמויה גם יחד.[27] העיקרון הוא לגרום ליריב להאמין מתוך אינטרס עצמי רציונלי שהתנהגות טובה תימנע פגיעה מסיבית, והתנהגות רעה תגרור השלכות חמורות. באופן מעט אירוני, אפשר לומר שהמפתח לפיתוח אסטרטגיית סייבר גלויה של הרתעה מונעת כרוך בהסתמכות על אסטרטגיות ריאליסטיות של האסכולה הישנה, תוך התרחקות מהנורמות הריאליסטיות של אותה אסכולה ישנה ביחס ללוחמה קונוונציונלית. ספרות חדשה זו משפיעה על הנחת העמימות, משום שניתן לטעון כי שינוי תודעתי ואסטרטגי זה הוא ההתמודדות המפורשת ביותר עם 'דילמת דוקו': הדרך היחידה 'להתגבר' על העמימות היא להימנע מכניסה למצב עימות שמחייב להתמודד איתה. במילים אחרות, מציאות הסייבר הנוכחית, כמו גם העתיד הנראה לעין, הופכים אסטרטגיות שמסתמכות על פעולה **לאחר מעשה** לנחותות מטבען, בהשוואה לאסטרטגיות מונעות.

## חשיבותה של 'דילמת דוקו'

הניתוח המוצג מצביע על ליקויים במאמצים הנוכחיים לגבש הגדרות ופרמטרים ברורים לפיקוח על כללי מלחמת הסייבר. הדגש שהושם כאן על קשיים מבניים מובְנים – כלומר, המיזוג הטבוע בין המגזר הצבאי לאזרחי בסייבר – מציג את ההשלכות החמורות הצפויות כתוצאה מאסטרטגיות שאינן מתמקדות במאמץ לעצור מראש פעולת סייבר. רק לאחרונה מתחילים להופיע ניתוחים משפטיים בודדים, שמציפים בעיות אלה:

> אין זה סביר שמדינה כמו ארצות־הברית תוכל לנקוט אמצעי הגנה נגד השפעתן של מתקפות על מטרות צבאיות באמצעות הפרדה בין יעדים צבאיים לבין אזרחים ואובייקטים אזרחיים במרחב הסייבר. זאת בשל התלות ההדדית הקיימת בין מערכות אמריקניות ממשלתיות ואזרחיות, כחלק מההסתמכות הממשלית המלאה־כמעט על חברות אזרחיות לצורכי אספקה, תמיכה ותחזוקה של יכולות הסייבר שלה... אומדנים של החלוקה היחסית עתידים להוכיח שקיים סיכון במיוחד במרחב הסייבר, בעוד התוצאות קשות יותר לחיזוי מאשר בעולם האמיתי: למתקפות פיזיות יש לפחות יתרון של התבססות על כללי הפיזיקה והכימיה. לדוגמה, כיוון שרדיוס הפיצוץ של פצצת חצי־טון הוא נתון ידוע, ניתן לדעת מראש ובוודאות מה יימצא מחוץ לרדיוס הפיצוץ ומה ייכלל בו. גבולות השגיאה ומתקפות הסייבר הרבה יותר רחבים ופחות מוכרים...[מרבית הדוחות אינם מסבירים באיזה אופן] ניתן לכונן שותפויות ציבוריות־פרטיות אלה כך שיוכלו ליישם בצורה סבירה סוגיות של דיני לחימה, [והם] אינם נותנים מענה לשימוש הצפוי בהגנות אקטיביות מצד המגזר הפרטי.[28]

כפי שהודגם לעיל, סוגיה מבנית זו היא יותר מאשר סמנטיקה בלבד, היא כוללת הכול: מי מעורב במלחמת סייבר, מה ניתן להרוס במלחמה כזו, מי יכול להיחשב קורבן בעת מלחמת סייבר, ואפילו את השאלות הפילוסופיות והאתיות שיש לשאול על מלחמת הסייבר עצמה. 'דילמת דוקו' היא הפצרה להתרחק מיעדים בלתי־ניתנים להשגה ומחלומות אידאליסטיים, שמקורם בתקווה חסרת־שחר ליצור מלחמת סייבר סטרילית, בדומה להגבלות שנכפו על מלחמה קונוונציונלית. מלחמת סייבר לעולם לא תוכל להפוך לסטרילית באופן זה. משום כך, החשיבה האסטרטגית העכשווית ביחס לתחום הסייבר צריכה להכיר בכך שיש להפנות משקל רב יותר ל"הנחת העמימות", מאשר לבעיית הייחוס המוכרת.

## הערות

1 Tom Leithauser, "Rules of War Should Apply to Cyber Conflict", *Cybersecurity Policy Report,* February 14, 2011.

2 Tom Gjelten,"Shadow Wars: Debating Cyber Disarmament", *World Affairs, 173;4,* November/December, 2010.

3 .Ibid

4 Aliya Sternstein, "Experts Recommend an International Code of Conduct for Cyberwar", *National Journal,* June 10, 2011.

5 Andrew Liaropoulos, "War and Ethics in Cyberspace: Cyber-conflict and Just War Theory", *European Conference on Information Warfare and Security, 177-XI,* (Reading, UK), July 2010.

6 Anatolin-Jenkins, Vida CDR, "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?", *Naval Law Review*, *51:132,* 2005.

7 Don Tennant, "The Fog of (CYBER) War", *Computerworld, 43;16,* April 27, 2009.

8 James Fallows, "Cyber Warriors", *The Atlantic Monthly, 305;2,* March 2010.

9 Ibid.

10 John Curran, "Updated Rules for Cyber Conflict Coming Soon, Defense Officials

Say", *Cybersecurity Policy Report,* March 26, 2012.
11 Lolita Baldor, "Cyber Warriors", *Army Times,* August 6, 2012.
12 Gorman, Siobhan and Julian Barnes, "Rules for Laws of War: US Decides Cyber Strike Can Trigger Attack", *The Australian,* January 1, 2011.
13 Anonymous, "Military Ponders Cyber War Rules", *Los Angeles Times,* April 7, 2008.
14 Ellen Nakashima, "Pentagon Seeks to Engage Rules of Engagement in Cyber War", *The Herald,* August 10, 2012.
15 Ibid.
16 Ellen Nakashima, "Pentagon: Cyber Offense Part of Strategy", *The Washington Post,* November 16 2011.
17 Wesley Andrues, "What US Cyber Command Must Do", *Joint Forces Quarterly, Issue 59, 4th quarter,* 2010.
18 Ibid.
19 Charles Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar", *Strategic Studies Quarterly,* Spring 2011.
20 Ibid.
21 Erik Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem", *Air Force Law Review, 68,* 2012.
22 Michael Gervais, "Cyber Attacks and the Laws of War", *Journal of Law and Cyber Warfare, 30;2*, 2012.
23 Ibid.
24 Hathaway, Oona, et al, "The Law of Cyber-Attack", *California Law Review,* 2012.
25 Ibid.
26 Matthew Crosston, "World Gone Cyber M.A.D: How Mutually Assured Debilitation is the Best Hope for Cyber-deterrence", *Strategic Studies Quarterly,* Vol. 5, No. 1, Spring 2011.
27 Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy: Breaking the Zero-sum Game", *Strategic Studies Quarterly*, Vol. 6, No. 4, Winter 2012.
28 Hannah Lobel, "Cyber War Inc: The Law of War Implications of the Private Sector's Role in Cyber Conflict", *Texas International Journal of Law, 47;3,* Summer 2012.