תוכנית להרתעת סייבר:
בניית יציבות באמצעות כוח

פרנק ג'. צ'ילופו, שרון ל. קרדאש וג'ורג' ס. סלמואירגי

במובנים רבים, אין ספק שהרתעה בעולם הסייבר היא נושא מורכב הרבה יותר מאשר ההרתעה במלחמה הקרה. טבעו של מרחב הסייבר הוא הגורם לכך. גם התיאוריות המתוחכמות ביותר של ההרתעה הגרעינית יתגלו כבלתי־מספקות בהתמודדות עם מורכבותו של תחום זה, שהוא מעשה ידי אדם, ואשר מקיף מספר אינסופי כמעט של יכולות, גורמים ומניעים המשתנים בהתמדה.[1]

איומי סייבר מציבים בעיה אמיתית וגוברת, ועד היום, מאמציה של ארצות־הברית לתת להם מענה הולם משתרכים מאחור. אמנם, היכולת להתגונן מפני התקפה או פלישה חייבת להישמר, אך ארצות־הברית, ככל מדינה אחרת, תפיק תועלת רבה אם תצליח מלכתחילה להרתיע את אויביה מפעולה – לפחות ככל שהדבר נוגע לפעולות מהסוג החמור ביותר, דוגמת לוחמת סייבר. ברור לחלוטין שלא ניתן להרתיע את כל סוגי ההתנהגות העוינת, אך חשוב לזהות סדרי עדיפויות בנושא זה, ולקבוע מהי הדרך הטובה ביותר להתמודד עם האיומים המובילים. חרף דיונים נמרצים, גיבוש פתרון מקיף ואחיד נותר חמקני. אחת הסיבות לכך הוא טיבה המורכב והמקיף של הרתעת סייבר, המחייב פתרון מקיף ומגובש הכולל בעלי עניין במגזר הציבורי והפרטי גם יחד.

על מנת לסייע בהבניית הדיון ובקידום המטרה, אנו מציעים מסגרת עבודה שבוחנת את הסוגיה בצורה ביקורתית, ומבקשת להניא, להרתיע ולהכניע גורמים עוינים מדינתיים ולא־מדינתיים גם יחד. הצבת האיומים הפוטנציאליים בתבנית רעיונית זו מסייעת להבהיר מהם מקורות הסכנה, ומשמשת נקודת פתיחה לזיהוי האחראים ולשיוכם לפעולות עוינות שמתבצעות נגד מדינה כלשהי או נגד בעלות־בריתה. הדבר יאפשר לשחקנים הרלוונטיים, שהפכו מטרה לגורמים עוינים, להמשיך

פרנק ג'. צ'ילופו הוא ראש המכון למדיניות להגנת המולדת (HSPI) ומנהל משותף של מרכז הסייבר לביטחון לאומי וכלכלי (CCNES) באוניברסיטת ג'ורג' וושינגטון. שרון ל. קרדאש היא מנהלת משותפת של ה־HSPI וחברה ב־CCNES, ג'ורג' ס. סלמואירגי הוא עורך דין ויועץ ל־HSPI בוושינגטון.

בפעולות ובדיונים הנחוצים על מנת להתוות ולהוציא לפועל אמצעי תגובה יעילים וראויים. יתרון נוסף של תבנית זו הוא סיוע בזיהוי תחומים ששיתוף פעולה בין הישויות המושפעות/המהוות יעד לפגיעה עשוי להועיל להם, או אפילו נדרש עבורם. לסיכום, מסגרת עבודה זו מספקת נקודת פתיחה לחקר הדרכים להרתעת גורמים עוינים, ובאופן זה מציעה נקודת מבט רעיונית בעלת ערך לארצות־הברית ולבעלות־בריתה גם יחד. פירוט מגוון הגורמים ופעילותם הפוטנציאלית שיובאו להלן אינו מתיימר להיות ממצה. נכון יותר יהיה לראות בו תמונת מצב או מעין טיוטה, שנועדה לתת מושג כללי במונחים של מי, מה, כיצד, מדוע וכדומה, וזאת כהקדמה לדיון מעמיק יותר על האסטרטגיה והמדיניות בתחום הרתעת סייבר.

גורמים מדינתיים

צבאות זרים עשויים להיות מעורבים ב"מתקפה על רשתות מחשב" או ב"ניצול רשתות מחשב" (CNA/CNE) כדי להגביל, לפגוע או להרוס יכולות של מדינה אחרת על מנת לקדם סדר־יום פוליטי. צבאות זרים משלבים יותר ויותר יכולות CNA/CNE במאמץ המלחמתי, בתכנון הצבאי ובדוקטרינה שלהם.[2] למאמצים כאלה יש יישומים קונבנציונליים בשדה הקרב (כלומר, שיפור במערכות נשק ופלטפורמות ו/או שיבוש מערכות אלה אצל אחרים) לצד יישומים בלתי־קונבנציונליים, ככל שמרחב הסייבר מותח את שדה הקרב וכולל בתוכו רכיבים חברתיים ואזרחיים. הפעילות במרחב הסייבר עשויה לכלול הכנות מודיעיניות של שדה הקרב, במטרה למפות תשתיות חיוניות של מי שנתפס כאויב.[3]

שירותי ביון ושירותי ביטחון: ניצול לרעה (Exploit) עשוי לכלול ריגול תעשייתי, כלכלי, צבאי ופוליטי, גניבת מידע ממשלה אחרת או על אודותיה, וכן גניבת קניין רוחני, טכנולוגיה, סודות מסחריים ועוד, שנמצאים בידי תאגידים פרטיים או אוניברסיטאות. שירותי ביון של מדינות רבות מעורבים בריגול תעשייתי בתמיכת חברות פרטיות.[4] מטרת־העל של פעילויות המתבצעות במסגרת זו היא השאיפה להשפיע על החלטות ועל מאזן הכוחות (האזורי והבינלאומי). כאן בולט שילוב של מודיעין טכני ואנושי, וכן איום מצד גורמים מבית ("insider").[5]

היבטים משולבים: ניתן לשלב רכיבים שונים ביכולתה של מדינה על מנת להשיג שלם הגדול מסכום חלקיו. בריתות (בין מדינות) יכולות להתגבש למטרה דומה. פעילות משותפת בהקשר זה עשויה לכלול איסוף מידע, שיתוף ממצאים שהשיג אחד הצדדים וביצוע משותף של מבצעים בשטח (מתקפות). מדינות יכולות גם לחפש ולגייס עזרה של גורמים לא־מדינתיים, כגון פצחנים (האקרים) להשכרה, שאינם חשים מחויבים או מוגבלים לנאמנות כלשהי.

גורמים לא־מדינתיים

ארגוני טרור לא־מדינתיים עלולים לבצע פעולות CNA/CNE כדי לקדם סדר־יום פוליטי מסוים. הם מייחסים חשיבות מרובה לאינטרנט (לצורכי גיוס, הדרכה, גיוס כספים, תכנון מבצעים וכדומה).[6] הצלחת מאמציהן של ארצות־הברית ובעלות־בריתה במלחמה בטרור בעולם הממשי עלולה להוביל ארגונים כמו אל־קאעדה ודומיו לחדור לעולם הסייבר באופן מעמיק יותר. אל־קאעדה אף עשוי לנסות להפיק לקחים מתוך פעילותם של ארגון "אנונימוס" ו"האקטיביסטים" (האקרים־אקטיביסטים) אחרים (או אפילו לחקות אותם), שעושים שימוש במרחב הסייבר על מנת למשוך תשומת לב למטרה שבה הם תומכים.

ארגוני פשע לא־מדינתיים מבצעים גניבת קניין רוחני, גניבת זהות וכן הונאות שונות, ומוּנָעים לרוב מתאוות בצע. הטכניקות והכלים הייחודיים לסייבר יכולים להניב תגמולים כספיים נכבדים. שוק עבריינות הסייבר העולמי הוערך ביותר מ־12.5 מיליארד דולר ב־2011,[7] אף על פי שהאומדנים משתנים (תוקף מתודולוגיות החישוב והאמינות של חלק מהמקורות נתון לוויכוח, וקשה להשיג הוכחה אמפירית).

היבטים משולבים: ניתן לצפות לבריתות מטעמי נוחות בין גורמים לא־מדינתיים (ארגוני טרור וארגוני פשע, ואפילו בין יחידים), במטרה לגשר על פערי יכולת כדי להשיג השפעה גדולה יותר. הסדרים דומים של נוחות הדדית אפשריים גם בין מדינה לבין ישויות שאינן מדינה (טרוריסטים, פושעים, האקרים יחידים). גורמים לא־מדינתיים יכולים להרחיב את היכולות והמיומנויות של המדינה, או לפעול כשלוחה שלה למטרות שונות. הסדרים כאלה הופכים את אתגר ייחוס האחריות (מי אחראי) למורכב עוד יותר, ומאפשרים למדינה ליהנות מיכולת הכחשה אמינה (plausible deniability).

השוואה בין הרתעת הסייבר להרתעה בתחום הגרעין[8] מעלה נקודות דמיון ושוני גם יחד.[9] מרחב הסייבר תובע במיוחד התמקדות בשחקנים ולא רק ביכולות/בנשק. לכן חיוני לסווג שחקנים אלה בהתאם להיקף, לעוצמה ולאופי האיום שהם נושאים. רק לאחר בחינה מדוקדקת שלהם נוכל לזהות את החשובים ביותר, ולהתמקד בהם באופן שמתעמת ומנטרל את הכוונות והיכולות הספציפיות שלהם.

הגנה והתקפה הן שני מרכיבים מכריעים בעמדה ובאסטרטגיה הרב־שכבתית האיתנה של ארצות־הברית, שנועדה להבטיח ביטחון לאומי. הרתעה יכולה לספק שכבת הגנה נוספת, באמצעות מניעת מהלכי פתיחה מצד בעלי אינטרסים עוינים כלפי ארצות־הברית. לכן, כדי לשמר ואף לקדם את הביטחון הלאומי/ביטחון המולדת, חשוב לשקול היטב, לפתח ולשמר לאורך זמן בתוך מערכת (טכנולוגית והגנתית/ביטחונית) מהירת צמיחה את היכולות האמריקאיות הנחוצות לתמיכה במדינה באופן אמין ויעיל, שיקנו לה מוכנות ויכולת להניא, להרתיע ולהכניע את

יריבה. אולם למרות מאמצים מרוכזים המכוונים למטרות אלה ולמערכות הגנה, אין לראות בגישה זו תחליף לבנייה ולאחזקת אמצעי שיקום משמעותיים נוספים, שמטרתם לאפשר התאוששות מהירה. אכן, יכולת התאוששות ושיקום כשלעצמה עשויה להיות הרתעה רבת־עוצמה. ברוח חוכמתו של סון צו (Sun Tzu), עצם היכולת להשתקם לאחר מכה, לצד מוכנות ברורה להגיב למתקפת סייבר, יפעלו לחיזוק מאמצי ההרתעה האמריקאית, ולכן ימנעו קרבות ושפיכות־דמים: "זכייה במאה ניצחונות במאה קרבות אינה שיא המיומנות. הכנעת האויב ללא קרב היא המיומנות בשיאה".[10]

קווי מתאר לאיום הסייבר

ארצות־הברית והאינטרסים שלה מצויים תחת איום סייבר יומיומי מגורמים מדינתיים ולא־מדינתיים גם יחד. המטרות האמריקאיות הפוטנציאליות רבות ומגוונות, ומתרחבות למגזרים חיוניים כמו מים, אנרגיה, כספים וטלקומוניקציה.[11] על פי דיווחי העיתונות המצטטים דובר של המִנהל הלאומי לביטחון גרעיני בארצות־הברית (NNSA) – "הארגון לביטחון גרעיני [של ארצות־הברית] חווה עד עשרה מיליון 'אירועי...ביטחון משמעותיים' בכל יום".[12] על פי חישובים של המשרד לביטחון המולדת של ארצות־הברית, מתגלות עשרות אלפי חדירות סייבר (ניסיונות ובפועל) בכל שנה, ועשרות מתקפות על מערכות תשתית חיוניות – כאשר מאז 2010 ועד 2012 חלה בהן עלייה בסדרי גודל.[13] טווח נושאי תפקידים בכירים בעבר ובהווה שהתריעו על כך הוא מרשים, וכולל את עוזר הנשיא לענייני ביטחון המולדת ומלחמה בטרור, ג'ון א. ברנן (John O. Brennan);[14] מנהל הסוכנות לביטחון לאומי וראש מטה הסייבר האמריקאי, גנרל קית' אלכסנדר (Keith Alexander); השר לשעבר לביטחון המולדת, מייקל צ'רטוף (Michael Chertoff); המתאם הלאומי לשעבר לענייני ביטחון ומלחמה בטרור ויועץ מיוחד לנשיא בנושא אבטחת סייבר, ריצ'רד קלארק (Richard Clarke); יו"ר ועדת הסנאט לביטחון המולדת, הסנטור ג'וזף ליברמן (Joseph Lieberman);[15] הנציג הבכיר בוועדת הסנאט לשירותים מזוינים, הסנטור ג'ון מקיין (John McCain), וראש ה־FBI רוברט מולר (Robert Mueller), שלאחרונה אף צפה שאיום הסייבר יחליף בעתיד את הטרור כאיום הראשי על המדינה.[16]

אחד הפרשנים תיאר זאת בבהירות רבה, כשאמר "מרגלים זרים ופשע מאורגן נמצאים כמעט בתוך כל רשת של חברה אמריקאית. בקרב היועצים הבכירים ביותר של הממשל בנושא אבטחת סייבר שוררת הסכמה רחבה, כי עברייני סייבר או טרוריסטים הפועלים בתחום הסייבר מסוגלים להשבית את התשתית החיונית במדינה בתחום הפיננסי ובתחום האנרגיה והתקשורת".[17] יחד עם זאת, נוסף לספיגת הפסדים כספיים שמוערכים על ידי הרשות הלאומית לריגול נגדי ופקידים

אמריקאיים נוספים במיליארדים, כתוצאה מניצול רשתות מחשב לגניבת קניין רוחני רב־ערך דרך פרצת אבטחה,[18] המדינה ניצבת נוכח מכה מאיימת יותר, עקב היותה מטרה למאמצי היריב לעסוק במה שמהווה המקבילה הסייברית להשגת מודיעין של שדה הקרב, דוגמת ניסיון מצד סין למפות תשתיות אמריקאיות חיוניות לאספקת מים ואנרגיה – שאותו הם עלולים למנף בהמשך כדי להניא, להתריע ולהכניע פעולה מצד ארצות־הברית.[19]

תעשיות חיוניות במדינות אחרות כבר חוו מתקפות סייבר. החברה הסעודית 'ארמקו' (Aramco) (חברה בבעלות המדינה ו"מפיקת הנפט הגדולה בעולם") סבלה מווירוס ממקור חיצוני שהדביק כ־30,000 מהמחשבים שלה באוגוסט 2012.[20] זמן קצר לאחר מכן, חברת RasGas מקטר ("המפיקה השנייה בגודלה בעולם של גז טבעי נוזלי") נפגעה אף היא.[21] דיווחי העיתונות מציינים כי "החברה הצרפתית Areva לתחנות כוח גרעיניות הייתה היעד למתקפת הסייבר בספטמבר [2011]".[22] והמגמה נמשכת.

מדינות מחזיקות ביכולות משתנות ברמה ובתחכום, ועשרות מהן מרחיבות את יכולת הסייבר שלהן, לרבות ארצות־הברית ובעלות־בריתה (ישראל היא שחקנית ראשית במרחב זה). אל מול ארצות־הברית, סין היא מקור מרכזי של "איום מתמיד ומתקדם", למרות שטביעות אצבע של המדינה הנותנת חסות אינן ניכרות תמיד על העכבר או על מסך המחשב. ייחוס האחריות קשה אף יותר כאשר נוצר שיהוי משמעותי בין האירוע לבין הדיווח או הבקשה לסיוע מצד הקורבן.[23] אולם עדות לכוונותיה של סין קיימת מזה כעשור: בשנת 1999 פרסמו שני קולונלים בצבא הסיני ספר תחת הכותרת "*Unrestricted Warfar*" ("לוחמה בלתי־מרוסנת"), שהדגיש אמצעים חלופיים להבסת יריב, שאינם פעולה צבאית ישירה ובעלת אופי מסורתי.[24]

גם רוסיה היא יריבה נחושה ומתוחכמת במרחב הסייבר. בעימות של 2008 בין רוסיה לגיאורגיה, תקפה רוסיה את רשת התקשורת הגיאורגית והרסה אותה. כפי שציין השגריר, דיויד סמית': "רוסיה שילבה פעולות סייבר בדוקטרינה הצבאית שלה", אם כי "בלא הצלחה מלאה... המתקפה המשולבת של רוסיה על גיאורגיה ב־2008 – מתקפה צבאית ומתקפת סייבר – הייתה המבחן המעשי הראשון של דוקטרינה זו... [ו]עלינו להניח שהצבא הרוסי למד מהלקחים שהופקו".[25] ב־2007, בנקים וממשל באסטוניה וכן גופים נוספים היו גם הם יעד ל"התקפות מניעת שירות (DDOS) נרחבות, מפוזרות וממושכות... רבות מהן – מקורן ברוסיה".[26] ממקום מושבם ברוסיה הצליחו האקרים ועבריינים להטביע את חותמם. מרחב הסייבר התגלה כמכרה זהב לעבריינים, שחדרו לעומקו ככל שההזדמנויות להרוויח בו המשיכו להכפיל את עצמן. ערך שוק עבריינות הסייבר העולמי הוערך ב־2011 בלמעלה מ־12.5 מיליארד דולר, כאשר הנתח של רוסיה בעוגה הוא כ־2.3 מיליארד

דולר (קרוב לכפול מערכו המוחלט בהשוואה לשנה הקודמת). כמו כן, ישנם סימנים לכך שגורמי פשע מאורגן במדינה החלו להצטרף "באמצעות שיתוף נתונים וכלים" כדי להגדיל את רווחיהם.[27]

הפוטנציאל לשיתוף פעולה בין ובקרב גורמים בעלי מניעים שונים לחלוטין מעורר חשש רציני. לדוגמה, מדינות שאין להן יכולות משלהן אך מבקשות להזיק לארצות־הברית או לבעלות־בריתה עשויות להצטרף, או פשוט לקנות/לשכור את השירותים והמיומנויות של עבריינים והאקרים, שיסייעו להן לתכנן ולבצע מתקפות סייבר. קל לאתר ערכות קוד בסגנון 'עשה זאת בעצמך' לניצול נקודות תורפה ידועות, ואפילו תולעת Conficker (שגרסאות שלה עדיין אורבות ומסוגלות ליצור בוטנט [botnet] מכ־1.7 מיליון מחשבים) נשכרה לשימוש.[28] לפיכך, היעדר גישה לתשתית או היעדר גיבוי ממעצמה אינם מכשול. גורמים שלוחים (פרוקסי) בעלי יכולות סייבר זמינים גם הם. קיים יריד חימוש לנשק סייבר. יריבים אינם זקוקים ליכולות, אלא רק לכוונה ולמזומנים.[29] זוהי תחזית מצמררת, אם זוכרים שארגון אל־קאעדה קרא למוג'אהידין ברשת לתקוף את ממשלת ארצות־הברית ותשתיות אמריקאיות חיוניות. סגן־אדמירל סמואל קוקס ממטה הסייבר ציין שפעילי ארגון אל־קאעדה מחפשים באופן פעיל אחר אמצעים לתקיפת רשתות אמריקאיות – יכולת שבאפשרותם לרכוש מהאקרים עבריינים.[30] כמו כן, בלי קשר לאופן השגתן, ליכולות סייבר יש פוטנציאל לשמש כמכפיל כוח במתקפה קונבנציונלית.

מוקדי דאגה אחרים הבולטים בהקשר זה כוללים את צפון־קוריאה ואיראן. את חוסר היכולת הקיימת, לפי שעה, משלימות שתי מדינות אלה בריבוי כוונות. איראן משקיעה משאבים נכבדים בהרחבה ובהעמקה של יכולות לוחמת הסייבר שלה.[31] היא גם מסתמכת זה מכבר על שלוחים כגון חזבאללה, שמתרברב עתה בארגון עמית בשם "סייבר חזבאללה" המיועד לפגוע במי שנתפס כאויב. גורמי אכיפת חוק מציינים כי היעדים והמטרות של "סייבר חזבאללה" כוללים הדרכה וגיוס אקטיביסטים בסייבר שהם תומכי משטר (כלומר, תומכי הממשל באיראן). אלה מצְדם מלמדים אחרים את הטקטיקות של לוחמת הסייבר. חזבאללה ממהר לנצל לרעה כלי מדיה חברתית דוגמת פייסבוק, כדי להשיג מודיעין ומידע, דבר שמייצר הזדמנויות נוספות לאיסוף עוד נתונים, במקביל לזיהוי יעדים פוטנציאליים חדשים ולפיתוח שיטות מותאמות ואמצעי גישה.[32]

נוסף לאלה, גורמים מתוך 'משמרות המהפכה' האיראניים עשו ניסיונות גלויים למשוך אליהם האקרים.[33] יש עדות לכך שבמוקד מאמצי הסייבר של 'משמרות המהפכה' פועלת קבוצת ההאקרים הפוליטית/עבריינית האיראנית "אשיאן" (Ashiyane).[34] משטרת הבאסיג', שמקבלת תשלום על ביצוע פעולות סייבר בשם המשטר, מספקת את מרבית כוח האדם לפעולת הסייבר של איראן.[35] במקרה של עימות במפרץ הפרסי, תוכל איראן לשלב שיטות ממוחשבות ואלקטרוניות

למתקפת רשת כדי לפגוע במערכות מכ"ם של ארצות־הברית ובעלות־בריתה, ולהקשות עליהן לבצע פעולות הגנה והתקפה גם יחד.[36] כחלק ממשימתו של ארגון חזבאללה עצמו להשיג הרתעה, הצהיר בגלוי מנהיגו, חסן נסראללה, שלא תהיה כל הבחנה בין ישראל לבין ארצות־הברית מבחינת פעולות נקם, אם תתקוף ישראל את איראן כדי לעכב את התקדמותה לעבר יכולת גרעינית: "אם ישראל תתקיף את איראן, אמריקה תישא באחריות".[37]

לסיכום, מדינות מנצלות לרעה את מרחב הסייבר כדי להשיג יתרון ולקדם את האינטרסים שלהן באמצעות איסוף מידע והשגת כושר פגיעה ביכולותיו של מי שנתפס כאויב. גם גורמים לא־מדינתיים, ארגוני טרור ועבריינים ממנפים את מרחב הסייבר למטרותיהם, ומפיקים תועלת מתחום שבו כולם ניצבים באותה נקודת זינוק, המתיר גם לשחקנים יחידים קטנים יותר להשפיע באופן שאינו יחסי לגודלם. אסימטריה זו מייצרת סביבה זרועת סכנות שונות, שבעבר לא משכו את תשומת הלב והאנרגיות של המעצמות. לפיכך, המעצמות חוששות מתרחישים מסוימים דוגמת אלה שצוינו לעיל, בשל יכולתם לערער באופן משמעותי ואף לחסל לחלוטין את האמון והביטחון במערכת (אמריקאית או אחרת).

איום זה אינו ייחודי לארצות־הברית. לוחמה אסימטרית היא כמובן אחת מהתכונות המאפיינות את ניסיונה של ישראל בשדה הקרב הממשי והווירטואלי גם יחד.[38] יש להביא בחשבון גם נפגעים ידועים פחות (לכאורה) של המאבק הסייברי. בהמשך לכך, הנה תיאור של הרשות הלאומית לריגול נגדי (Office of the National Counterintelligence Executive) – הגוף האמריקאי שמרכז את המלחמה בטרור – בדוח לשנת 2011 שהגיש לקונגרס:

> המשרד הפדרלי הגרמני להגנה על החוקה (BfV – Federal Office for the Protection of the Constitution) מעריך שחברות גרמניות הפסידו בין 28 ל־71 מיליארד דולר ובין 30 ל־70 אלף מקומות עבודה בכל שנה בעקבות ריגול כלכלי של גורמים זרים. כמעט 70 אחוזים מכל המקרים מערבים גורמי פנים (insiders).
>
> דרום־קוריאה מדווחת שהעלויות כתוצאה מריגול כלכלי של גורמים זרים ב־2008 עמדו על 82 מיליארד דולר, לאחר שכבר הגיעו ל־26 מיליארד דולר ב־2004. הדרום־קוריאנים מדווחים ש־60 אחוזים מהקורבנות הם עסקים קטנים ובינוניים, וכי מקורו של מחצית מהריגול הכלכלי הוא בסין.
>
> משרד הכלכלה, המסחר והתעשייה היפני ערך סקר בקרב 625 חברות יצרניות בשלהי 2007, ומצא כי יותר מ־35 אחוזים מהחברות המשתתפות דיווחו על אופן כלשהו של הפסד טכנולוגי. יותר מ־60 אחוזים מדליפות אלה היו קשורות לסין.[39]

הדברים שאמר הסנטור הצרפתי, ז'אן־מארי בוקל (Jean-Marie Bockel) – שתועדו ב'דוח מידע' של ועדת הסנאט הצרפתית לענייני חוץ, הגנה והכוחות המזוינים – מטרידים במידה דומה:

> בצרפת, רשויות מנהליות, חברות ומפעילי שירותים חיוניים (אנרגיה, תחבורה, בריאות וכד') נופלים קורבן מדי יום למיליוני מתקפות סייבר... המקור למתקפות סייבר אלה יכול להיות האקרים של מחשבים, קבוצות אקטיביסטיות, ארגוני פשע וכן חברות מתחרות, או אפילו מדינות אחרות. האצבע המאשימה מופנית לרוב כלפי סין או רוסיה, אם כי קשה מאוד לזהות במדויק את היוצרים שמאחורי כל מתקפה.[40]

וכך גם ההערכה שמספק ג'ונתן אוונס (Jonathan Evans), העומד בראש שירותי הביטחון בבריטניה:

> אסטרטגיית הביטחון הלאומי של בריטניה ממקמת בצורה ברורה את אבטחת הסייבר לצד הטרור, כאחד מארבעת אתגרי המפתח שניצבים בפני בריטניה. נקודות תורפה באינטרנט מנוצלות לרעה בצורה אגרסיבית לא רק על ידי עבריינים אלא גם על ידי מדינות, וההיקף הוא מדהים: מדובר בתהליכים בקנה־מידה תעשייתי המערבים אלפי אנשים, שעומדים מאחורי ריגול סייבר במימון מדינות ופשע סייבר מאורגן... חברה שעמה עבדנו, מהגדולות בלונדון, מעריכה שסבלה הפסדי הכנסות בסך 800 מיליון ליש"ט כתוצאה ממתקפת סייבר מצד מדינה, ולא רק כתוצאה מאובדן קניין רוחני, אלא גם בשל פגיעה ביתרון המסחרי שלה בעת ניהול משא־ומתן על כריתת הסכמים. אלה לא יישארו הקורבן התאגידי היחידי שסובל מבעיה זו.[41]

אוונס הוסיף ואמר את הדברים הבאים:

> עד כה, ארגוני טרור קיימים לא הציבו איום משמעותי בערוץ זה, אולם הם מודעים לפוטנציאל הקיים בניצול נקודות תורפה בסייבר כדי לתקוף תשתית חיונית, ואני צופה שהם ירכשו יכולות נוספות כדי לעשות זאת בעתיד.[42]

השאלה הנדרשת היא, לפיכך, מה צריך לעשות.

הרתעת סייבר ותגובה רב־ממדית

על רקע העדויות הרבות והמטרידות על יכולות הסייבר ועל כוונות עוינות מצד גורמים מדינתיים ולא־מדינתיים כאחד, חייבת ארצות־הברית להתוות ולגבש בקפידה מסלול התקדמות להתמודדות עוצמתית עם העובדות ועם המציאות המדאיגה המאפיינות את מרחב הסייבר כיום (ואשר לא סביר שייעלמו בקרוב). תהא זו נחמת שווא לחשוב שארצות־הברית או בעלות־בריתה יוכלו לפתור את הבעיה בעזרת 'חומות אש' (firewalls) בלבד. במקום זאת, על ארצות־הברית לנסח, להבהיר וליישם אסטרטגיה להרתעת סייבר, שתסייע בתמיכה ובחיזוק אבטחת הסייבר וההגנה על תשתיות חיוניות.

בתחומים מסוימים כבר מתקיים דיון נמרץ אך ראשוני בנושא זה, אולם בשל טבעו המורכב, חוצה המגזרים והרב־תחומי של האתגר, לא גובשה עד כה תגובה אסטרטגית משולבת. האיומים מתפתחים מדי יום ומוסיפים עוד נדבך של מורכבות, ולמרות הקצב והעוצמה של זרם האיומים, המגזרים השונים אינם משתפים ביניהם

בדרך כלל את המידע על האמצעים והכלים המשמשים את גורמי האיום, ואינם מפרסמים אותו. בעיקרון, שתיקה זו אינה חסרת הגיון, שכן הממשלה מבקשת להגן על חומר מסווג והתעשייה מעוניינת להגן על מידע קנייני. אולם בפועל, שתיקה כזו "תוקעת מקלות בגלגלים" שאמורים להניע תגובה ומאמצי מניעה.

על רקע דברים אלה, אין ספק שהיקף המשימה מעורר אימה, אולם ארצות־הברית צפויה להפיק תועלת מרובה מפיתוח ומיישום אסטרטגיה להרתעת סייבר, וממדיניות השואפת להניא, להרתיע ולהכניע – הן כגישה כללית והן באופן שמותאם במיוחד לגורם/יריב מסוים. עמדה כללית יציבה, כלומר, צעדי אבטחה בסיסיים (הגנה, היגיינה, טכנולוגיה), יכולה להוות 80 אחוזים מהפתרון ולנטרל את מרבית האיומים לפני שהם מתממשים במלואם. בכך ניתן יהיה לשחרר משאבים (אנושיים, כספיים וטכנולוגיים), שיוכלו להתמקד באופן תלוי־הקשר בשאר התחומים שמרכיבים את הבעיות והאיומים הקשים ביותר מבחינת רמת התחכום והנחישות. כדי להפוך המלצות אלה למעשיות, יש להתוות קווים ברורים. ראוי לשמור על הגמישות של תגובת ארצות־הברית באמצעות שמירה על מידת עמימות מסוימת באשר לאמצעים שברשותה, כל עוד הפרמטרים מובהרים היטב באמצעות הצבת סימני דרך ייעודיים או קווים אדומים נבחרים, שחצייתם לא תעבור בשתיקה.[43]

על מנת לייצר הרתעה אפקטיבית מול יחיד או ישות, ובכך למנוע מהם מלהשיג את מטרתם – ומוטב למנוע מהם לפעול מלכתחילה – הכרחי להבין באופן מוחלט מה בדיוק מנסה הצד היוזם להשיג. (הרעיון מבוסס על הנושא/העיקרון של האסטרטג הנודע, מיאמוטו מוסאשי (Miyamoto Musashi): "דע את אויבך, דע את חרבו"[44]). הבנה בסיסית זו מהווה את הצעד הראשון בדרך להניא את היריב מפעולה או להכניעו, ויישומה כרוך בבחינה יסודית של המצב מנקודת מבטו של הצד האחר. אמנם, כל מקורות האיום שצוינו לעיל עוסקים בריגול ובניצול של מידע ומערכות דרך אמצעי סייבר, אולם יש לזכור שלגורמים שונים יש יעדים שונים ומובחנים. למרות שהם עושים שימוש באמצעים וירטואליים ובמדיום וירטואלי, כל אחד מגורמים אלה שואף להשיג תוצאות מסוימות בעולם האמיתי, ובהתאם לכך יכוון את מעשיו.

מה חייבת ארצות־הברית לעשות כדי לשכנע גורמים מדינתיים להימנע מהפעלת שירותי המודיעין והצבא שלהם לצורך ניצול רשתות מחשב או לשם מתקפה על רשתות מחשב, בשם מטרות־על כלשהן? תגובת הסייבר של ארצות־הברית צריכה להיות תוצאה של אסטרטגיית הרתעה רחבה יותר ביחס לגורם נתון. במילים אחרות, הרתעת הסייבר תהיה תואמת ומשלימה לאסטרטגיית הרתעה אמריקאית מקיפה יותר. מדינות אחרות צריכות להבין ולהעריך את העובדה שארצות־הברית מסוגלת להטיל עונש מידתי אם תותקף במרחב הסייבר, וכי

התגובה האמריקאית עשויה בסופו של דבר להיות 'סייברית' או צבאית, כאשר כל האפשרויות מונחות על השולחן. לגבי תגובת סייבר, יש להפגין את יכולת ההתקפה באופן שלא יותיר ספק באשר להשלכות שיהיו לחציית קו אדום של ארצות־הברית. עם זאת, הפגנת היכולת חייבת להתבצע תוך הכרה מלאה בעובדה שניתן יהיה ללמוד ולשנות כל כלי, טכניקה, טקטיקה או הליך שייושמו, ולהשתמש בהם כדי לנקום בארצות־הברית ובבעלות־בריתה. התגובה בהקשר זה תלויה ביכולת לייחס את המתקפה לגורם ספציפי אחד או יותר (כוחות זרים).

מבחינת המודיעין, יש לזכור שמאז ומתמיד עסקו מדינות בגניבת סודות. אמנם הריגול הפך דיגיטלי, אך ממשלות זרות משתמשות באמצעי סייבר למטרה המקורית: להשיג מידע שיכול לשמש לעיצוב ולחידוד קבלת החלטות, ולשם כך הן מנסות להתאים את 'המקצוע העתיק בעולם' השני למאה ה־21. במילים אחרות, מדינות משתמשות באמצעי סייבר (דוגמת האקרים רוסיים וסיניים העובדים בשירות ממשלותיהם) כדי להגביר את יכולתן לאסוף מידע בעל ערך עבור קובעי המדיניות שלהן. השאלה היא, איזה מידע מעוניינים גורמים אלה להשיג, ומדוע? המידה שבה הממשלה שעל הכוונת (ארצות־הברית או בעלת־בריתה) תהיה מסוגלת להגן טוב יותר על המערכות שלה ולהתאים להן פעולות הרתעה תלויה ביכולתם של המומחים להרתעת סייבר להציג תובנות, ולנסח תשובות ברורות לשאלה זו.

ריגול תעשייתי הוא תת־קבוצה בסוג זה של פעילות המתקיימת בחסות מדינה. הכוונה היא להגביר את השגשוג הכלכלי או את יישומם של שיקולים עסקיים במדינה מסוימת. למרות שפעולת הריגול מוכוונת על ידי המדינה, הנהנים ממנה עשויים להיות גורמים פרטיים או פרטיים־למחצה. מצד אחר, מנקודת מבטו של יעד הריגול, ההשלכות של גניבת סודות מסחריים עלולות להיות מעמיקות ולהתרחב מעבר לאובדן הכלכלי, עד כדי פגיעה במעמדה של המדינה בעולם. על פי הערכתו של רוברט בראיינט (Robert "Bear" Bryant) מהרשות הלאומית האמריקאית לריגול נגדי, ריגול סייבר הוא "איום שקט על הכלכלה שלנו עם תוצאות ניכרות ביותר... סודות מסחריים שפותחו במשך אלפי שעות עבודה על ידי המוחות המבריקים ביותר שלנו נגנבים בשבריר שנייה, ומועברים למתחרים שלנו".[45] החדשנות והפריון של ארצות־הברית עלולים גם הם לסבול כתוצאה מכך, עם השלכות פוטנציאליות משניות נוספות על צמיחה ופיתוח עתידיים. אם מידע צבאי נחשף ונגנב, עלולות להיות לכך גם השלכות על הביטחון הלאומי. אין צורך בדמיון רב כדי לשער מה יכול לעשות גורם עוין עם טכנולוגיה אמריקאית גנובה בעלת פוטנציאל ליישום צבאי.[46]

בדומה למדינות, גם ארגוני טרור על־לאומיים מבקשים להשיג יתרון אסימטרי שאותו יוכלו למנף, בניסיון להנחיל את סדר־היום הפוליטי שלהם. עם זאת, בדרך

כלל מחזיקים ארגונים כאלה משאבים פחותים מאלה של מדינה, ומשתדלים להימנע ממעורבות בתהליך הפוליטי ולהעדיף שימוש באלימות להשגת מטרותיהם. מנקודת מבט זו, לא יהיה זה מאמץ גדול מדי עבורם להשיג תמורה נוספת להשקעתם, באמצעות שימוש באמצעים דיגיטליים כמכפיל כוח של פעולה צבאית. ככל שניתן יהיה ללמוד פרטים נוספים על הסייבר הטקטי ועל המטרות והשאיפות הפוליטיות והאסטרטגיות של ארגונים אלה, כך יתקבל חומר גלם מועיל יותר לעיצוב הרתעת סייבר שתמנע מהם לפעול.

ארגוני הטרור והפשע עשויים גם להתאחד וליצור איום משולב המתבסס על ברית מטעמי נוחות, שבה כל צד נשען על המיומנויות והנכסים של הצד השני כדי לקדם את מטרותיו בהתאם. בניגוד לארגוני הפשע שמקור הכנסתם העיקרי הוא הפשע בלבד, רווח כשלעצמו אינו המניע של ארגוני טרור. הבדל מהותי זה מהווה למעשה פתח שניתן לנצלו באמצעות תצוגה וביצוע מקצועיים של אסטרטגיית הרתעת סייבר מותאמת.

יש לזכור שהרתעה היא תת־קבוצה של הכנעה, שמטרתה לגרום ליריב להימנע מפעולה על ידי כך שהיא גורמת לו להאמין שהסבירות להצלחתו קלושה, או שהנזק מהתגובה יהיה גדול ממה שיהיה מוכן לשאת.[47] בעבר נדרש שהרתעה תכלול "שלושה רכיבים גלויים: ייחוס, איתות ואמינות".[48] בהקשר הנוכחי, הרתעה מגלמת הנחה מוקדמת על כך שהקווים האדומים הכלליים של ארצות־הברית הובהרו ליריביה וכן לבעלות־בריתה, שהיא אותתה כי חציית גבולות אלה לא תעבור בשתיקה, וכי היא יכולה ומוכנה להטיל את ההשלכות של כל הפרה כזו על מי שחוצה אותם. התגובה האמריקאית הצפויה צריכה להיות מאיימת דיה על מנת להניא את הגורם המאיים הפוטנציאלי מביצוע הפעולה מלכתחילה.

כאשר ארצות־הברית מגדירה קווים אדומים במרחב הסייבר, עליה לפעול במחשבה תחילה ובזהירות ניכרת, ולזכור שפעילויות שמתקרבות לקווים אלה אך אינן חוצות אותם יגררו עונש מופחת, כפועל יוצא של הגדרת הגבולות. יש להעריך בהתאם פעילויות שאינן מבוצעות למטרה חיובית, כגון מאמצים למפות את התשתית החיונית בארצות־הברית. שום טובה לא תצמח מכך שלמדינה אחרת או לגורם לא־מדינתי זר יהיה ידע מפורט על מערכות אלה.

הייחוס הוא מכריע בביסוס ההרתעה. חשוב שניתן יהיה לדעת מי פעל, על מנת להטיל עליו את ההשלכות. עם זאת, קשה לאתר את "המקלדת המעשנת" במרחב הסייבר, שכן מרחב זה נוצר כך שיאפשר הכחשה אמינה. סדרי הגודל והמשמעות של אתגר הייחוס בהקשר של תגובה למתקפת סייבר זכו להדגשה מצד אנליסטים בכירים,[49] אם כי יש גם דעות מנוגדות.[50] אם נתעלם לרגע מהקושי לעשות זאת, היכולת לקשר בין הפעולה לבין הגורם לה תאפשר לצד המותקף להגיב. היכולת להגיב באותה מטבע מעלה את מספר האפשרויות שהצד המותקף יוכל להסתמך

עליהן בדיעבד, לרבות האפשרות להגיב בעוצמה רבה יותר מזו שהצד המותקף ספג. ראוי אפוא להשקיע זמן ומשאבים במאמץ מרוכז שתכליתו לפתח יכולת ייחוס משופרת, באמצעות טכנולוגיות ואמצעים אחרים.

היריבים חייבים גם הם להבין ולהעריך שארצות־הברית ערוכה ומוכנה להשתמש במלוא הכוח שברשותה – במגוון, בהיקף ובעומק – על מנת לאכוף כללים אלה. כדי לשדר מסר זה בצורה משכנעת ולהביא לכך שהוא יגיע ליעדו ולאוזניהם של בעלי הכוונות העוינות, חייב להתקיים מצג פומבי של היכולות באופן שיבהיר את המסר לאשורו, מבלי לחשוף יותר מדי ולאבד את היתרון בשל כך. למשל, עליו למנוע אפשרות שהאויב יוכל לבצע "הנדסה הפוכה" (או לחקות בדרך אחרת), ולהשתמש באותם אמצעים ושיטות של ארצות־הברית שהוצגו בפומבי, שמא יהיה זה "גול עצמי". היבט ה"מצג" של התרגיל הופך מתעתע אף יותר כאשר זוכרים שהחוקים השולטים בלוחמת הסייבר עדיין בשלבי התפתחות, ולכן אינם חד־משמעיים במידה מסוימת. נקיטת זהירות ותשומת לב נדרשים, אם כך, גם ברמה המשנית.

אף על פי שארצות־הברית נדרשת להפגין את ארגז הכלים שלה, המצויד בכל הנדרש כדי להילחם בגורמים עוינים בעת הצורך, עד היום לא הייתה הפגנה פומבית חד־משמעית כזו של עליונות סייבר, שארצות־הברית טענה באופן יזום והחלטי לבעלות עליה. על רקע זה, האם עליה לשקול ביצוע מקביל דיגיטלי של ניסוי גרעיני חי? יש להפנות שאלה זו לקובעי המדיניות, למומחים ולאנשי הטכנולוגיה האמריקאיים, המבקשים להגדיר את מסלול ההתקדמות ולפתח דוקטרינה ואסטרטגיה עבור מרחב הסייבר. האירוניה היא שאם תרגיל כזה יתבצע בזהירות (ההולמת את גודלו), הוא יוכל לפעול ביעילות להרתעת גורמים עוינים, כך שאין להוציא מכלל אפשרות שהוא יתרום למניעת מלחמה.

בניית יציבות באמצעות עוצמה

נהוג לומר שההגנה הטובה ביותר היא ההתקפה. על פי דיווחים ממקורות גלויים, ארצות־הברית מפתחת כללים למעורבות בכל הקשור למתקפות סייבר, ומשרד ההגנה חותר לחיזוק ארסנל נשק הסייבר שברשותו [51](אם כי מתקפת סייבר עשויה להביא לתגובה צבאית או לתגובת סייבר). כפי שציין סגן יו"ר המטות המשולבים לשעבר, הגנרל ג'יימס אי. קרטרייט (James E. Cartwright), מאמצים והשקעה מהסוג שתואר כאן יסייעו להתאים מחדש את יחס ההגנה מול ההתקפה – שעד לאחרונה עמד על 90% מול 10% לערך לטובת ההגנה[52] – ויחזקו ויבנו אמון ביכולתה של ארצות־הברית להרתיע ביעילות פעולה עוינת במרחב הסייבר.

עם זאת, קהילת ביטחון הסייבר בארצות־הברית, כמו המקבילות לה אצל בעלות־בריתה, טרם השלימה את התהליך. עוד ארוכה הדרך עבור קהילה זו, בייחוד

בארצות־הברית, עד שתגיע לרמת המיומנות והבשלות שמציגות כיום הקהילות העוסקות במלחמה בטרור בארצות־הברית.[53] סנכרון סעיפים 10 ו־50 בחוק האמריקאי ששילב יחדיו פונקציות מודיעין וצבא מהווה פריצת דרך משמעותית בעידן שלאחר פיגועי ה־11 בספטמבר, שהביאה לשיפור ניכר במצבה הכולל של ארצות־הברית במלחמה בטרור. היא יכולה למנף הישג זה באמצעות התאמה והחלה של תפיסה דומה גם על הסייבר. עליה לחתור לכך תוך התייחסות לשני אתגרים (שעדיין יש לעמוד בהם): הסדרת החוקים העוסקים במעורבות וחתירה לעמדה יוזמת יותר.[54]

כדי להתקדם בחוכמה במרחב הסייבר, חייבות ארצות־הברית ובעלות־בריתה להפגין מנהיגות ולהציג חזון, לצד תוכנית פעולה מבוססת. זמן רב מדי הניעו התקריות את האסטרטגיה, למעשה, זוהי טקטיקה במסווה של אסטרטגיה. ארצות־הברית מחזיקה במספר יכולות ייחודיות, אך אלה לא ינוצלו במלואן עד שתגובש מסגרת אסטרטגית רחבה יותר שבתוכה ניתן יהיה לשבצן. בהמשך למסגרת הרעיונית שהוצגה כאן, עולים עקרונות מפתח מסוימים שיכולים לשמש בסיס לפיתוח וליישום אסטרטגיה, יכולת ועמדה להרתעת סייבר יעילה. עקרונות אלה מהווים את ראשיתה של תוכנית להרתעת סייבר, כדלקמן:

כיול במטרה לממש את החזון. בהקשר זה, יכולת תומכת באמינות. יש לשקול בזהירות את הכיול הקיים ולכוונו כנדרש, בהתאם להשקעות ולמאמצים המשקפים את היחס בין הגנה להתקפה – שחוסר איזון בו עלול להשפיע לרעה על הביטחון הלאומי. בהיותו דרישה מקדימה לאכיפת ההשלכות, כיול (או כיול מחדש) מתקיים בד בבד עם הרצון הפוליטי לפעול לאכיפת סנקציות בבוא העת.

התחלה ובנייה מעמדת כוח. כדי להרתיע ולהניא יריבים בהצלחה, נדרשת יכולת לשכנע אויבים פוטנציאליים שהמחיר של פעולה עוינת מצדם יעלה על התועלת שהם מייחסים לה. פיתוח של יכולת מכת פתיחה ואיתות נכון על קיומה הם, לפיכך, בסיסיים.

שימת הדגש על מהירות, הפתעה ויכולת תמרון. במרחב הסייבר, כל ננו־שנייה קובעת. לכן, היעד הוא להגיב בזמן אמת ככל האפשר. בעוד אין לפקפק בעיקרון שלכל חציית קו אדום יהיו השלכות, יש ערך לשמירה על מידה של עמימות באשר לטיבן המדויק של השלכות אלה, ועל ידי כך יישאר אותו גורם במצב של אי־ודאות תמידי. גמישות ובהירות נראות סותרות לכאורה, אך למעשה הן מייצרות אסטרטגיה שקולה.

אין להותיר אף אחד מאחור. יכולת של מכת פתיחה בלבד תותיר את המדינה פגיעה ובלתי־מוכנה לתגובה באותה מטבע, אם היריב מסוגל לכך. כמו בשלב המלחמה הקרה של עידן הגרעין, יידרשו תכנון מראש וזהירות בהפעלת יכולת מכה שנייה באופן שיבטיח הגנה על הכוח. שימור העליונות המדעית והטכנולוגית

הוא גורם מכריע, שכן ניתן להגיע לפתרונות טכניים לנוכח האתגרים המטרידים במרחב הסייבר.

דע את האויב. הביטוי אולי ישן ושחוק, אך הוא עדיין תקף. כדי להביס אויב פוטנציאלי נדרשת הבנה מעמיקה של מטרותיו ושאיפותיו הספציפיות. תובנה מעין זו תאפשר לבנות את האסטרטגיה והטקטיקה לאותו מקרה תוך התאמת הרכיבים ליריב הספציפי, ובכך למקסם את פוטנציאל הסיכול. הכלל שתקף כאן הוא מה שמכונה "לולאת OODA": התבונן, התכוונן, החלט ופעל (observe, orient, decide, and act).

הובלה שמהווה דוגמה. ברעיון של הרתעת סייבר איתנה טמונה הנחת המוצא, שהישות המנסה להרתיע מחוסנת מפני מה שהיא מנסה לעולל לאחרים (שכן תמיד קיימת האפשרות לאפקט בומרנג). כל דרך אחרת כמוה כקפיצה מהמטוס ללא מצנח. לכן, המסקנה המכרעת היא שעל ממשלת ארצות־הברית לשאוף תחילה לפתרון בעיותיה שלה, כדי להתמודד עם האיום. יתרה מכך, על הממשלה ליזום את הצעדים הדרושים להקלת שיתוף המידע, כך שעובדות חיוניות יגיעו לידי כל גורמי המפתח האחראיים להגנה על נכסים ומשאבים לאומיים, לרבות אלה שבבעלות המגזר הפרטי ובתפעולו (תשתית חיונית).

שותפים להצלחה. אין מרכיב יחיד בממשלה, גם לא הממשלה כגוף אחד, שיוכל להתמודד לבדו במרחב הסייבר. חיוני לכונן שותפויות אמת בתוך המגזרים השונים וביניהם. בתוך הממשל לדוגמה, סנכרון זהיר ושילוב של פונקציות מודיעין וצבא (סעיפי החוק 10 ו־50) למטרות הרתעת סייבר עשוי להתגלות כבעל ערך רב, כפי שהיה בהקשר של מלחמה בטרור. החשיבות של התגוננות מראש מתרחבת מעבר למגזר הציבורי, לעבר רשתות ומערכות חיוניות שמצויות בידיים פרטיות. בהתאם לכך, על המגזר הפרטי להתחייב לנקוט את הצעדים הדרושים לחיזוק הביטחון הלאומי. כדי להבטיח עמידה בסף זה, הרשויות הפדרליות צריכות להושיט יד למגזר הפרטי, בגישה שתשלב תמריצים חיוביים ושליליים להשגת התוצאה המבוקשת, בשיטת "המקל והגזר".

חשיבה ופעולה במושגים בינלאומיים. אתגרים חוצי־גבולות מחייבים פתרונות חוצי־גבולות, ומרחב הסייבר הוא חסר גבולות מטבעו. שותפים נאמנים ברמה הבינלאומית יכולים וצריכים לספק ערך רב בהקשר זה. יש להודות שאינטרסים לאומיים עלולים לפגוע ביכולת לשתף נתונים ומידע רגיש. יחד עם זאת, ההימנעות ממינוף יחסים בילטרליים ובריתות מרכזיות תהיה "גול עצמי", החל מהסכם שיתוף המודיעין "Five Eyes" (בין אוסטרליה, קנדה, ניו־זילנד, ארצות־הברית ובריטניה), דרך ברית נאט"ו ועד האיחוד האירופי, וכן שותפות אסטרטגיות נוספות כמו באזור המזרח התיכון ואסיה, הכוללות את ישראל, סינגפור, הודו ויפן.

עם מנהיגות מעוררת השראה בלוחמת הסייבר ברמה של דמויות המופת הצבאיות, בילי מיטשל (Billy Mitchell), ביל דונובן (Bill Donovan) או ג'ורג' פטון (George Patton) – שהיטיבו להבין את השימושים האסטרטגיים והטקטיים של חידושי טכנולוגיה ונשק – ארצות־הברית יכולה לעצב ולהוציא לפועל אסטרטגיית הרתעת סייבר רבת־עוצמה שמישירה מבט אל אויביה כשהיא מוכנה כיאות, בשאיפה שהאירועים שנכונו לה יישארו כרוכים בבייטים וביטים בלבד, במקום בכדורים, בפצצות ובשפיכות־דמים.

הערות

1 Eric Sterner, "Deterrence in Cyberspace: Yes, No, Maybe," in *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century* (Washington, DC: George C. Marshall Institute, 2011), p. 27.

2 Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corporation, March 7, 2012, p. 54, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf.

3 Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html; and Mark Clayton, "Exclusive: Potential China Link to Cyberattacks on Gas Pipeline Companies," *Christian Science Monitor*, May 10, 2012, http://www.csmonitor.com/USA/2012/0510/Exclusive-potential-China-link-to-cyberattacks-on-gas-pipeline-companies.

4 Office of the National Counterintelligence Executive (NCIX), *Foreign Spies Stealing US Economic Secrets in Cyber Space: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011* (October 2011), p. 4, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf;

5 שם.

6 Eben Kaplan, *Terrorists and the Internet*, Council on Foreign Relations, January 8, 2009, http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005; and Special Report by the Homeland Security Policy Institute (HSPI) and the University of Virginia's Critical Incident Analysis Group (CIAG), *NETworked Radicalization: A Counter-Strategy* (Washington, DC: May 2007).

7 Group IB, *State and Trends of the Russian Digital Crime Market 2011*, p. 6, http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf.

8 ראו:
Thomas C. Schelling's classic text, *Arms and Influence* (New Haven: Yale University Press, 1966).

9 ראו לדוגמה:
Martin C. Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation, 2009).

10 Sun Tzu, *The Art of War*, translated by Samuel B. Griffith (New York: Oxford University Press, 1963).

11 Ellen Messmer, "DHS: America's Water and Power Utilities under Daily Cyber-Attack," *Network World*, April 4, 2012, http://www.networkworld.com/news/2012/040412-dhs-cyberattack-257946.html?t51hb&hpg1=mp.

12 Jason Koebler, "U.S. Nukes Face up to 10 Million Cyber Attacks Daily," *US News & World Report*, March 20, 2012, http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily.

13 Joe Lieberman, "Cyber Networks Sitting Ducks for Attacks" *Hartford* Courant, April 8, 2012, http://articles.courant.com/2012-04-08/news/hc-op-lieberman-cyber-security-biggest-national-th-20120408_1_cyber-attack-cyber-networks-cyber-threats

14 John O. Brennan, "Time to Protect against Dangers of Cyberattack," *Washington Post*, April 15, 2012, http://www.washingtonpost.com/opinions/time-to-protect-against- dangers-of-cyberattack/2012/04/15/gIQAdJP8JT_story.html.

15 Lieberman, "Cyber Networks Sitting Ducks for Attacks."

16 Jason Ryan, "FBI Director Says Cyberthreat will Surpass Threat from Terrorists," January 31, 2012, http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists/.

17 "המציאות היא שהתשתיות שלנו עוברות קולוניזציה", אמר טום קלרמן, לשעבר הממונה מטעם הנשיא אובמה על המועצה לאבטחת הסייבר. ראו: David Goldman, "Cybersecurity Bills Aim to Prevent 'Digital Pearl Harbor,'" April 23, 2012, http://money.cnn.com/2012/04/23/technology/cybersecurity-bills/?source=cnn_bin.

18 "בכיר במודיעין שתידרך עיתונאים בנושא האנונימיות ציין כמה מקרים שבהם ניתנו אומדנים כחלק מתביעות נגד ריגול כלכלי במהלך שש השנים האחרונות: מחקר של Dow Chemical על הדברת חרקים בשווי של 100 מיליון דולר, נוסחאות כימיות של DuPont בשווי של 400 מיליון דולר, נתונים קניניים של מוטורולה בשווי 600 מיליון דולר, נוסחאות צבע של Valspar בשווי של 20 מיליון דולר". ראו :
Ellen Nakashima, "In a World of Cybertheft, U.S. names China, Russia as Main Culprits," *Washington Post*, November 3, 2011, http://www.washingtonpost.com/world/national-security/us-cyber-espionage-report-names-china-and-russia-as-main-culprits/2011/11/02/gIQAF5fRiM_story.html.

19 Nick Hopkins, "Militarisation of Cyberspace: How the Global Power Struggle Moved Online," *The Guardian*, April 16, 2012, http://m.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle?cat=technology&type=article; and Nick Hopkins, "US and China Engage in Cyber War Games," *The Guardian*, April 16, 2012, http://m.guardian.co.uk/technology/2012/apr/16/us-china-cyber-war-games?cat=technology&type=article.

20 Reuters, "Saudi Oil Producer's Computers Restored After Virus Attack" *New York Times*, August 26, 2012, http://www.nytimes.com/2012/08/27/technology/saudi-oil-producers-computers-restored-after-cyber-attack.html?_r=1.

21 Elinor Mills, "Virus Knocks out Computers at Qatari Gas Firm RasGas," *CNET News*, August 30, 2012, http://news.cnet.com/8301-1009_3-57503641-83/virus-knocks-out-computers-at-qatari-gas-firm-rasgas/.

22 Christopher Brook, "Report: French Nuclear Company Areva Hit by Virus" *ThreatPost*, October 31, 2011, http://threatpost.com/en_us/blogs/report-french-nuclear-company-areva-hit-virus-103111.

23 מייקל מק'קול (McCaul), יו"ר ועדת המשנה לנושאי ביקורת, חקירה וניהול של ועדת בית הנבחרים לביטחון המולדת, אמר: "איסוף המידע האגרסיבי ביותר על הכלכלה והטכנולוגיה של ארצות־הברית נעשה מצד סין...יכולות לוחמת הסייבר של סין ומבצעי הריגול שהיא מפעילה הם הנפוצים ביותר מבין הגורמים המדינתיים. סין יצרה קבוצות האקרים אזרחיות המעורבות בריגול סייבר, והקימה יחידות צבאיות ללוחמת סייבר". ראו:
NCIX, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, p. 5;.
ראו גם:
Cindy Saine, "Experts Warn of Increased US Cyber Security Threat" *VOA News*, April 24, 2012, http://www.voanews.com/english/news/usa/Experts-Warn-of-Increased-US-Cyber-Security-Threat-148786975.html.

24 Qiao Liang and Wang Xiangsui, published by China's People's Liberation Army, Beijing.

25 David J. Smith, "How Russia Harnesses Cyberwarfare," *American Foreign Policy Council Defense Dossier* (August 2012), http://www.afpc.org/files/august2012.pdf.

26 Jason Healey and Leendert van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow" *Atlantic Council Issue Brief* (2011) p. 2, http://www.acus.org/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf.

27 Group IB, *State and Trends of the Russian Digital Crime Market 2011*, p. 6, http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf;
ראו גם:
http://group-ib.com/images/media/Group-IB_Cybercrime_Inforgraph_ENG.jpg (איור).

28 Frank J. Cilluffo, "The Iranian Cyber Threat to the United States," Testimony Before the House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, and Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, April 26, 2012, p. 4, http://www.gwumc.edu/hspi/policy/Iran%20Cyber%20Testimony%204.26.12%20Frank%20Cilluffo.pdf; and Conficker Working Group, *Conficker Working Group: Lessons Learned*, http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.

29 Cilluffo, Testimony Before the House of Representatives, p. 4.

30 Jack Clohurty, "Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad'" *ABC News*, May 22, 2012, http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875#.UEieyEQrOlg.

31 Yaakov Katz, "Iran Embarks on $1b. Cyber-Warfare Program," *Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864.

32 Cilluffo, Testimony Before the House of Representatives, p. 6.

33 Golnaz Esfandiari, "Iran Says it Welcomes Hackers Who Work for Islamic Republic," Radio Free Europe, March 7, 2011, http://www.rferl.org/content/iran_says_it_welcomes_hackers_who_work_for_islamic_republic/2330495.html

34 Iftach Ian Amit, "Cyber [Crime/War]," paper presented at DEFCON 18 conference, July 31, 2010.

35 "The Role of the Basij in Iranian Cyber Operations," *Internet Haganah*, March 24, 2011, http://internet-haganah.com/harchives/007223.html.

36 Michael Puttre, "Iran Bolsters Naval, EW Power," *Journal of Electronic Defense* 25, no. 4 (2002): p. 24; Robert Karniol, "Ukraine Sells Kolchuga to Iran," *Jane's Defense Weekly* 43, no. 39 (September 27, 2006), p. 6; Stephen Trimble, "Avtobaza: Iran's Weapon in Alleged RQ-170 Affair?" *The DEW Line*, December 5, 2011, http://www.flightglobal.com/blogs/the-dewline/2011/12/avtobaza-irans-weapon-in-rq-17.html.

37 Reuters, "Nasrallah: Iran could Strike US Bases if Attacked," *Jerusalem Post*, September 3, 2012, http://www.jpost.com/IranianThreat/News/Article.aspx?id=283706.

38 Ilan Evyatar, "Falling into the Trap, Over and Over Again," *Jerusalem Post*, November 17, 2010, http://www.jpost.com/Features/InThespotlight/Article.aspx?id=195767; Dan Harel, "Asymmetrical Warfare in the Gaza Strip: A Test Case," *Military and Strategic Affairs* 4, no. 1 (2012): pp. 17-24, http://www.inss.org.il/upload/(FILE)1339053338.pdf; Yolande Knell, "New Cyber Attack Hits Israeli Stock Exchange and Airline," *BBC* News, January 16, 2012, http://www.bbc.co.uk/news/world-16577184; and Joshua Mitnick, "Israel's Businesses Losing the Cyber War," *Wall Street Journal*, July 25, 2012, http://online.wsj.com/article/SB10000872396390443477104577549262451192148.html.

39 NCIX, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, p. 19.

40 Jean-Marie Bockel, Senator for Haut-Rhin, "Cyber Defence an International Issue, a National Priority," *Information report no. 681 – Committee on Foreign Affairs, Defence and Armed* Forces, July 18, 2012, http://www.senat.fr/rap/r11-681/r11-681-syn-en.pdf.

41 נאום בהרצאה השנתית על ביטחון והגנה ע"ש לורד מאיור, שנערכת בעיר לונדון, https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html.

42 ראו:
Tom Whitehead, "Cyber Crime a Global Threat, MI5 Head Warns," *The Telegraph*, June 26, 2012, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9354373/Cyber-crime-a-global-threat-MI5-head-warns.html.

43 Cilluffo, *Testimony Before the House of Representatives*, pp. 7-8.
ראו גם:
Frank J. Cilluffo, "The U.S. Response to Cybersecurity Threats," *American Foreign Policy Council (AFPC) Defense Dossier* (August 2012), http://www.afpc.org/files/august2012.pdf; and Martin C. Libicki, "The Strategic Uses of Ambiguity in Cyberspace" *Military and Strategic Affairs* 3, no. 3 (2011): pp. 3-10, http://www.inss.org.il/upload/(FILE)1333532281.pdf.

44 *The Book of Five Rings.*

45 Nakashima, "In a world of cybertheft, U.S. names China, Russia as main culprits" [citing NCIX Bryant].

46 שם.

47 W. W. Kaufmann, "The Requirements of Deterrence," in W. W. Kaufman, ed., *Military Policy and National Security* (Princeton: Princeton University Press, 1956); Peter Marquez, "Space Deterrence: The Pret-a-Porter Suit for the Naked Emperor," אילוץ מבקש להשפיע על היריב לפעול in *Returning to Fundamentals*, pp. 9-10.

או להימנע מפעולה באמצעות איום, או בפועל, לגבות מחיר מהיריב כדי להגביל את אפשרויותיו ו/או את חישובי העלות־תועלת שלו כך שהיריב מחליט כי העלות של פעולתו המשוערת אינה מצדיקה את התועלת שתופק ממנה.

Marquez, "Space Deterrence" at p. 10, citing G. Schaub, Jr., "Deterrence, Compellence and Prospect Theory" *Political Psychology* 25, no. 3 (2004), pp. 389-411.

48 Marquez, "Space Deterrence," p. 10.

49 לדוגמה, ראו:

Yasmin Tadjdeh, "U.S. Military Overestimates Value of Offensive Weapons Cyberweapons, Expert Says," *National Defense*, September 13, 2012, citing Martin Libicki, senior management scientist at RAND Corp, http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=887.

50 F. Hare, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective." Paper presented at the *Cyber Conflict (CYCON), 2012 4th International Conference* on June 5-8, 2012.

51 Federal News Radio, "DoD Hammering out Rules of Cyberspace," October 21, 2011, http://www.federalnewsradio.com/?nid=398&sid=2602063; and Ellen Nakashima, "Pentagon to Fast-track Cyber Weapons Acquisition," *Washington Post*, April 9, 2012, http://www.washingtonpost.com/world/national-security/pentagon-to-fast-track-cyberweapons-acquisition/2012/04/09/gIQAuwb76S_print.html.

52 Lolita C. Baldor, "Pentagon to Publish Strategy for Cyberspace War," *Navy Times,* July 14, 2011, http://www.navytimes.com/news/2011/07/ap-pentagon-publish-strategy-cyberspace-war-071411/;

ראו גם:

"A Conversation on Cyber Strategy with General James E. Cartwright," *Homeland Security Policy Institute (HSPI) Capstone Series on Cyber Strategy*, May 14, 2012, http://www.gwumc.edu/hspi/events/cartwrightCS501.cfm.

53 Frank Cilluffo and Andrew Robinson, "Analysis: While Congress Dithers, Cyber Threats Grow Greater," *Nextgov*, July 24, 2012, http://www.nextgov.com/cybersecurity/2012/07/while-congress-dithers-cyber-threats-grow-greater/56968/.

54 Cilluffo, *AFPC Defense Dossier*.